Axel Schemberg

PC-Netzwerke

Galileo Computing

Liebe Leserin, lieber Leser,

Dieses Buch antwortet auf das Bedürfnis vieler PC-Nutzer: Den Aufbau eines eigenen Netzwerkes. Ich will ehrlich sein, es ist zunächst aus meinem eigenen Bedürfnis heraus entstanden, mehrere Rechner gleichzeitig ins Internet zu bringen. Schnell stieß ich auf eine Open-Source-Software-Lösung: Fli4L, eine Linux-basierte Routerlösung, die auf eine Diskette passt und so einen alten Pc – ein 486er reicht – zum Router Ihres Netzwerkes umfunktionieren kann. Axel Schemberg hatte auf der Webseite von Fli4L (www.fli4l.de) eine leicht verständliche Anleitung und anschauliche Schritt-für-Schritt-Lösung veröffentlicht. So kamen wir ins Gespräch und planten dieses Buch, das Sie jetzt in den Händen halten.

PC-Netzwerke spielen in unserem Alltag eine immer größere Rolle. Nicht nur im Büro, auch zu Hause und beim Spielen übers Netz braucht man umfassende Kenntnisse und Praxiswissen von Profis. Ich war froh, als Axel Schemberg bereit war, sein Wissen mit unseren Lesern zu teilen und ein umfangreiches Werk vorzulegen, in dem Sie alles finden, was Sie zur Planung, zum Aufbau und zum Betrieb Ihres eigenen Netzwerkes benötigen.

Antwort auf Fragen und Hilfe wird Ihnen Axel Schemberg zusätzlich zum Buch auch in unserem Forum geben. Schauen Sie doch einfach mal auf unsere Webseite unter www.galileocomputing.de. Auch Ihre Rückmeldung ist hier immer herzlich willkommen.

Stephan Mattescheck
Lektorat Galileo Computing
stephan.mattescheck@galileo-press.de

Galileo Press
Gartenstraße 24
53229 Bonn

Auf einen Blick

Inhalt

1 Einleitung

1 Einleitung

Wie sollten Sie mit diesem Buch arbeiten? Ich möchte Ihnen hier das Konzept dieses Buches vorstellen und die verwendeten Auszeichnungen von Text erklären, sodass Sie sich besser zurechtfinden.

1.1 Aufbau des Buches

Dieses Buch besteht aus drei Teilen:

- Grundwissen Netzwerke
- Praxiswissen
- Workshop

Der Teil **Grundwissen Netzwerke** vermittelt Ihnen die theoretischen Grundlagen, die Sie immer wieder benötigen werden. Meiner Meinung nach ist es unabdingbar, über eine solide Wissensbasis zu verfügen, bevor man sich weiter mit Netzwerken in der Praxis beschäftigt; daher ist dies der erste Teil des Buches.

Im Teil **Praxiswissen** vermittle ich Ihnen die notwendigen Grundlagen, um ein Netzwerk aufzubauen. Grundlage für den Aufbau dieses Teils ist das ISO-/OSI-Modell (vgl. Abschnitt 2.4.2, ISO-/OSI-Modell), daher beginne ich beim Kabel und schließe mit den Anwendungen. Anhand von praktischen Beispielen werden in diesem Teil alle einzelnen Schritte erklärt und vorgeführt. Sie finden hier die Beschreibungen, wie Sie die Netzwerkeinstellungen bei den Betriebssystemen vornehmen können oder welche Programme sich zur Administration eines Netzwerks eignen.

Der letzte Teil, **Workshop**, befasst sich intensiver mit speziellen Themen. Ein Workshop beschreibt Schritt für Schritt den Aufbau eines kleinen LANs; ein anderer das Einrichten eines Linux-NSs oder das Überprüfen der Sicherheitseinstellungen von WLANs.

Sie müssen nicht das ganze Buch von vorne bis hinten lesen! Ich habe darauf geachtet, dass jeder Bereich, den Sie lesen möglichst auch dann verständlich ist, wenn Sie nur diesen lesen.

Meine Empfehlung lautet, dass Sie den Teil **Grundwissen Netzwerke** zuerst lesen. Damit haben Sie die wichtigste Grundlage für das Verständnis von Netzwerken gelegt. Nebenbei bemerkt, gehören Sie dann zu den wenigen Menschen auf diesem Planeten, die wissen, wovon sie reden, wenn über TCP/IP gesprochen wird.

1.2 Verwendete Formatierungen und Auszeichnungen

Ein umfangreicher Text kommt um Formatierungen nicht herum. Zunächst möchte ich Ihnen die Symbole vorstellen, die Sie in der Randspalte finden können:

Symbol	Bedeutung
	**Beispiel:** Zur Verdeutlichung nenne ich ein Beispiel. Es kann sein, dass ich im weiteren Text Bezug auf dieses Beispiel nehme, allerdings habe ich umfangreichere Beispiele vermieden, sonst müssten Sie doch das ganze Buch von vorn bis hinten lesen.
	**Hinweis:** Wenn Stellen mit diesem Zeichen versehen sind, möchte ich Sie auf eine Sache besonders hinweisen.
	**Vorsicht, Falle:** Wenn Sie diese Sache ausprobieren/machen, laufen Sie Gefahr, in eine Falle zu tappen. Daher weise ich Sie gesondert darauf hin.
	**Warnung:** Die beschriebene Funktion/Aktion hat nicht nur Vorteile. Wenn Sie sie umsetzen, dann können erhebliche Nachteile, z. B. Sicherheitslücken auftreten.
	**Auf der CD-ROM:** Dieses Buch enthält eine CD-ROM. Viele der von mir angesprochenen Tools sind dort enthalten. Dieses Symbol macht Sie darauf aufmerksam.
	**Bug:** Manchmal enthält Software einen Bug. Diesen Bug, (dt. Fehler), habe ich mit dem Käfer (engl. Bug) gekennzeichnet.

Tabelle 1.1 Symbole in der Randspalte

Nachdem Sie sich jetzt über die Symbolik völlig im Klaren sind, möchte ich Ihnen noch kurz die Textformatierungen erläutern:

- **Befehle** oder Angaben, die Sie eingeben müssen, habe ich in nichtproportinaler Schrift ausgezeichnet, z.B.: `ping www.web.de`.
- Wenn der Eintrag variabel ist, habe ich ihn in spitze Klammern gesetzt (`ping <IP-Adresse>`). Sie müssen dort ohne Klammern den variablen Wert eintragen. Sollten Teile des Eintrags in eckigen Klammern stehen, so handelt es sich um optionale Bestandteile (`ping [-t] <IP-Adresse>`).
- **Menüpunkte** oder Programm-**Namen** habe ich **fett** formatiert, so z.B. **Start · Programme · Einstellungen · Systemsteuerung**. Sie müssen die genannten Menüpunkte nacheinander anklicken, um an die gewünschte Stelle zu kommen.
- **Wichtige Begriffe** sind über die Formatierung **fett** gekennzeichnet. Ebenso sind alle Hyperlinks **fett** markiert.

Tasten, die Sie auf Ihrer Tastatur drücken müssen oder Tastenkombinationen sind auch als Tasten dargestellt, z.B. [↵]. Entsprechend bedeutet [Strg]+[Alt]+[Entf], dass Sie diese Tasten gleichzeitig drücken müssen.

Es ist nicht ganz einfach die Bedienung eines Programms zu beschreiben. Ich erwähne die Menüleiste:

Mit dem Begriff Schaltfläche meine ich einen Button:

Mit Reiter bezeichne ich diese programmiertechnische Errungenschaft:

Ich hoffe, mit dieser umfangreichen Erklärung lassen sich Missverständnisse vermeiden, sodass Sie sich voll und ganz auf den Inhalt dieses Buches konzentrieren können. Darüber hinaus finden Sie Erläuterungen zu vielen Begriffen im Glossar am Ende des Buches.

1.3 Buch-CD

Zu diesem Buch gibt es eine CD-ROM mit Programmen und Dokumenten, die ich im Text erwähnt habe und nützlich finde.

Es gibt auf der CD-ROM nur wenige Linux-Programme (RPMs), weil fast alle erwähnten Programme Teil der SuSE-Distribution 8.1 sind.

Bei Windows werden sehr wenige Programme mit dem Betriebssystem mitgeliefert, entsprechend ist der Bedarf an ergänzenden Programmen größer.

Die Software finden Sie in verschiedenen Ordnern, sodass sie thematisch leichter gefunden werden kann und Sie die Möglichkeit haben, auch einfach ein bisschen auf der CD-ROM zu stöbern.

Bei den Dokumenten, die auf der CD-ROM enthalten sind, handelt es sich einerseits um Konfigurationsdateien, z.B. für DNS und DHCP unter Linux, andererseits um Anleitungen oder Normierungsunterlagen.

Ich hoffe, die CD-ROM ist Ihnen eine Hilfe bei der Arbeit mit diesem Buch.

Teil 1
Grundwissen Netzwerke

2 Grundlagen der Kommunikation

2 Grundlagen der Kommunikation

Dieser Teil des Buches soll Ihnen einen vertieften Überblick über das theoretische Gerüst von aktuellen Netzwerken geben und damit eine Wissensbasis für die weiteren Kapitel des Buches schaffen. Das Verständnis der Theorie wird Ihnen bei der praktischen Arbeit, insbesondere bei der Fehleranalyse, helfen.

Aktuelle Netzwerke werden strukturiert aufgebaut. Diese Strukturen basieren auf verschiedenen technologischen Ansätzen.

Wenn Sie ein Netzwerk aufbauen wollen, dessen Technologie und Struktur Sie verstehen möchten, dann werden Sie ohne Theorie sehr schnell an Grenzen stoßen, die Sie der Möglichkeit berauben, ein optimal konfiguriertes Netzwerk zu administrieren.

In Fehlersituationen werden Ihnen die theoretischen Erkenntnisse helfen, einen Fehler im Netzwerk möglichst schnell zu finden und geeignete Maßnahmen zu seiner Beseitigung einzuleiten.

Ich bin mir sicher, dass die theoretischen Ausführungen nicht zu umfangreich sind. Dieses Buch legt den Schwerpunkt auf die praxisorientierte Umsetzung von Netzwerken und konzentriert sich auf die Darstellung von kompaktem Netzwerkwissen.

Ein Computernetzwerk kann man allgemein als Kommunikationsnetzwerk bezeichnen. Ausgehend von der menschlichen Kommunikation, möchte ich versuchen, die Kommunikation von PCs im Netzwerk zu erklären.

2.1 Kommunikation allgemein

Als Kommunikation bezeichnet man im Alltag alles Mögliche. So wird Telekommunikation oft als Kommunikation bezeichnet. Wenn Menschen miteinander reden, nennen wir das Kommunikation, aber wenn sie nicht reden, sondern lediglich durch ihre Körpersprache etwas ausdrücken, kann man das Kommunikation nennen. Wichtig ist nicht, über welches Medium Informationen übertragen werden, sondern der Informationsaustausch an sich ist das Entscheidende.

Jede Art von Kommunikation ist durch folgende Merkmale gekennzeichnet:

1. Sender
2. Empfänger
3. Übertragungsmedium
4. Regeln
5. Kodierung des Inhalts

Die Punkte 1 und 2 sind wohl nicht erläuterungsbedürftig, doch was ist ein Übertragungsmedium (Punkt 3)? Beim Sprechen wird Schall über die Luft, bei einem Bild die Farbe über Lichtreflexion und bei der Telekommunikation wird elektrische Spannung durch Kabelleitungen übertragen; die Medien sind Luft, Licht und das Kabel.

Entweder benutzen beide Gesprächspartner das gleiche Medium oder es gibt einen Wandler, der die Informationen umwandelt, beispielsweise wandelt das Telefon die akustischen Signale der menschlichen Sprache in elektrische Spannung. Diese werden dann über Kupferleitungen transportiert, bis sie schließlich beim empfangenden Telefon von elektrischen in akustische Signale zurückgewandelt werden.

Regeln (Punkt 4) in der menschlichen Kommunikation sind – soweit sie erfolgreich verlaufen soll – z. B.: »Mit vollem Mund spricht man nicht«, »Lass mich ausreden«, »Jetzt spreche ich!« und Ähnliches. Im Allgemeinen unterbricht man einen anderen beim Sprechen nicht, sodass er ausreden kann. Macht Ihr Gesprächspartner eine Sprechpause, so können Sie sich äußern, das besagt die Regel.

Kodierung (Punkt 5) des Inhalts meint z. B. eine Sprache (Deutsch). Eine Sprache selbst hat schon viele eigene Details. Wenn man sie verstehen will, muss man wissen, welche Wörter welche Bedeutung haben und wie grammatische Beziehungen hergestellt werden.

Erfüllen beide Kommunikationspartner die Punkte eins bis fünf, kommt es zu einer erfolgreichen Kommunikation. Sie können sich unterhalten.

2.2 Kommunikation zwischen Rechnern

Auch bei der Kommunikation zwischen Rechnern sind die oben genannten Voraussetzungen wichtig:

1. Sender
2. Empfänger

3. Übertragungsmedium
4. Regeln
5. Kodierung(en)

Es gibt also hinsichtlich der betrachteten Anforderungen keinen Unterschied zwischen der menschlichen und der PC-Kommunikation. Selbstverständlich handelt es sich beim PC um dumme Kommunikationsteilnehmer, entsprechend müssen die Regeln zu eindeutigen Informationen führen, damit sie für PCs verwertbar sind.

Wichtig ist ebenfalls, dass es Medienwechsel geben kann. Ein Handygespräch zu einem Festnetzanschluss erfolgt bis zum Sendemast des Mobilfunkbetreibers über Funk. Dort wird dann eine Transformation in elektrische oder optische Signale auf Kabelbasis vorgenommen.

Es ist sinnvoll, für alle Anwendungen, die über ein Netzwerk kommunizieren wollen, bestimmte Aufgaben einheitlich zu lösen. Es werden für jede Anwendung Netzwerkschnittstellen bereitgestellt, auf denen diese Anwendung aufsetzen kann. Bestimmte Aufgaben, wie die eindeutige Adressierung in einem Netzwerk, müssen daher nicht von jeder Anwendung gelöst werden, sondern werden einheitlich (z.B. vom Betriebssystem) übernommen.

2.3 Was ist ein Netzwerk?

Als Netzwerk bezeichne ich die Verbindung von mindestens zwei PCs. Selbstverständlich können auch andere Computer als PCs in ein Netzwerk eingebunden werden. Dieses Buch wird die Einbindung z.B. von UNIX-Workstations und Ähnlichem nicht weiter beschreiben, sondern sich auf die Verbindung von PCs mit den Betriebssystemen Windows oder Linux konzentrieren. Ich werde daher im weiteren Verlauf dieses Buches den Begriff »PC« verwenden; allgemeiner formuliert steht der PC stellvertretend für »Netzwerkteilnehmer«.

Wenn ich von einem Netzwerk oder LAN spreche, dann meine ich ein-Netzwerk, das auf dem Ethernet-Standard basiert. Ethernet (vgl. Kapitel 3.1, Ethernet) ist ein Standard, um Datenpakete zu kodieren und Daten zu versenden oder zu empfangen. Man kann sagen, Ethernet regelt die grundsätzlichen Dinge der Netzwerkkommunikation, den Zugang zum Netzwerk. Um die Ausführungen zu diesem und zu den nächsten zwei Themen besser verstehen zu können, ist es notwendig, einen kurzen Exkurs zu den Kommunikationsmodellen zu machen.

Exkurs

Ein Netzwerk kann nicht nur als LAN (vgl.Kapitel 3, Lokales Netz (LAN)) aufgebaut werden, sondern z.B. auch mit seriellen Leitungen oder mittels Verbindungen über das Telefonnetz (vgl. Kapitel 4, Weitverkehrsverbindung (WAN)).

2.3.1 Netzwerktopologien

Topologie = Anordnung, Aufbau

Man kann Netzwerke in verschiedenen Topologien aufbauen. Grundsätzlich unterscheidet man zwischen der Bus-, der Ring- und der Sterntopologie.

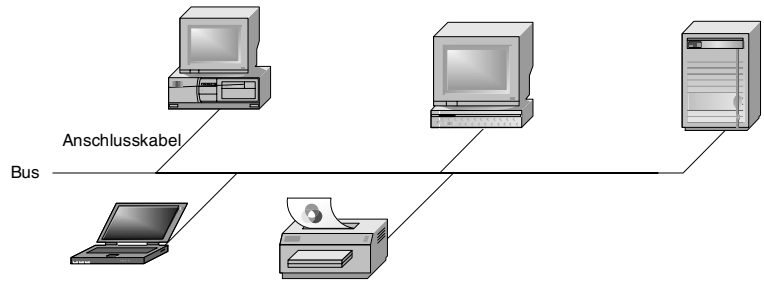

Abbildung 2.1 Bustopologie

Die Urform von Ethernet war die **Bustopologie** (vgl. Abbildung 2.1). Ähnlich wie eine Hauptwasserleitung gibt es ein zentrales Kabel, an das alle teilnehmenden Stationen mit Stichleitungen angeschlossen werden. Ein eindeutiges Merkmal ist, dass eine dezentrale Struktur entsteht: Jedes Gerät ist gleichrangig an den Bus angeschlossen. Kommt es zu einer Störung der »Hauptwasserleitung«, sind alle angeschlossenen Stationen von dieser Störung betroffen. Diejenigen von Ihnen, die die BNC-Verkabelung (vgl. Kapitel 3.1, Ethernet) kennen, wissen, dass es sich bei dieser Art von Netzwerken um Museumsstücke handelt.

Token-Ring und ATM sind Beispiele für eine **Ringtopologie** (vgl. Abbildung 2.2). Vereinfacht erklärt, wandert ein Token (dt. *Zeichen, Symbol*; stellen Sie sich einen Stab beim Staffellauf vor) im Kreis – daher der Name Token-Ring. Wenn das Token frei ist, kann jeder Netzteilnehmer das Token nehmen, ein Netzwerkpaket daran hängen und es innerhalb des Kreises an einen anderen Netzwerkteilnehmer schicken. Bei ATM (vgl. Kapitel 3.1, ATM), der schnelleren Variante der Ringtopologie, wandert nicht ein einziges Token im Kreis, sondern es fährt – bildlich gesprochen – ein Güterzug im Kreis; erwischt Ihr PC einen leeren Wagon – eine ATM Zelle –, kann er seine Daten dort ablegen und weiterreisen lassen.

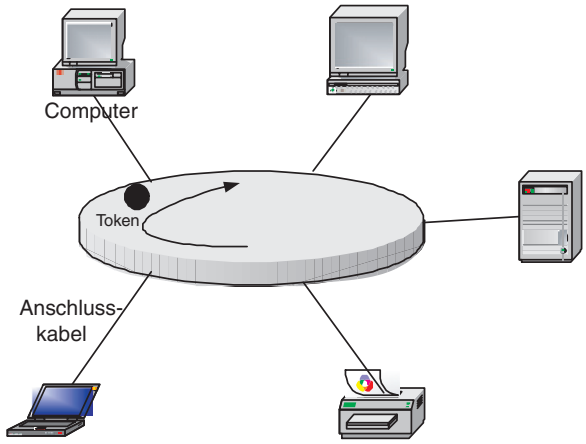

Abbildung 2.2 Ringtopologie

Exkurs

Token-Ring wird auch als »Toter Ring« bezeichnet, weil diese Technologie innerhalb der nächsten Jahre verschwinden wird. Sollten Sie noch ein solches Netzwerk einsetzen, ist das Thema Migration (vgl. Kapitel 5.11, Migrationsmöglichkeiten) für Sie wichtig. ATM konnte sich im LAN nicht durchsetzen, weil es zu kostenintensiv betrieben werden muss, im WAN (vgl. Kapitel 4, Weitverkehrsverbindung (WAN)) hat sich die Technologie etabliert, wird aber inzwischen dort durch andere Technologien verdrängt.

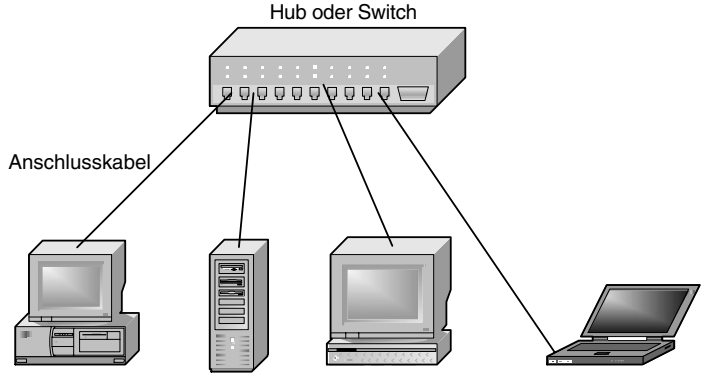

Abbildung 2.3 Sterntopologie

Die **Sterntopologie** ist die Struktur, die sich bei Twisted-Pair-Verkabelungen ergibt (vgl. Abbildung 2.3). Fast-Ethernet, die 100 Mbit/s schnelle Variante von Ethernet, wird ausschließlich in Sterntopologie realisiert. Wenn Ethernet – mit 10 Mbit/s – über eine Twisted-Pair-Ver-

kabelung betrieben wird, handelt es sich ebenfalls um eine Sternstruktur. Es gibt ein zentrales Element, ursprünglich den Hub (dt.: *Radnabe*), von dem sternförmig die Zuleitungen zu den einzelnen Netzteilnehmern wie Speichen eines Rades führen. Jeder Netzteilnehmer hat eine eigene Zuleitung; ist eine Zuleitung gestört, bleiben die anderen Teilnehmer davon ungestört.

2.4 Kommunikationsmodell

Das Wort »Kommunikationsmodell« wird Sie vielleicht ein wenig verschrecken. Es klingt komplizierter, als es ist. Mit einer Einschätzung haben Sie aber recht: Es ist Theorie.

Damit die Kommunikation in einem Netzwerk allgemein beschrieben werden kann, wurden kluge Leute damit beauftragt, ein Kommunikationsmodell zu entwickeln. Diese Leute fanden heraus, dass es möglich ist, die wesentlichen Leistungen in einem Netzwerk in verschiedene Aufgaben zu gliedern. Diese Aufgaben werden im Kommunikationsmodell als **Schichten** bezeichnet. Jede Schicht erfüllt eine Hauptaufgabe, damit die Kommunikation im Netzwerk stattfinden kann. Sie erinnern sich sicherlich noch an den Beginn dieses Abschnitts der das Thema menschliche Kommunikation behandelt (vgl. Kapitel 2.1, Kommunikation allgemein). Analog zu den dort genannten Voraussetzungen für die menschliche Kommunikation, werden im Kommunikationsmodell die Schichten definiert.

Eine Schicht muss für eine eindeutige Adressierung im Netzwerk sorgen, eine weitere muss regeln, wann Daten gesendet werden, eine Art Vorfahrtsregelung für das Netzwerk.

Als alle Aufgaben festgelegt waren, mussten diese nur noch praktisch umgesetzt werden. Die Schichten arbeiten unabhängig voneinander. Wenn es also mehrere Implementierungen (Umsetzungen) einer Schicht gibt, sind diese beliebig austauschbar. Es gibt definierte Schnittstellen zu den benachbarten Schichten.

Es existieren zwei bekannte, konkurrierende Kommunikationsmodelle, auf denen sämtliche Netzwerke basieren: **DoD** und **ISO/OSI**. Diese beiden Modelle widersprechen sich nicht, allerdings sind sie unterschiedlich umfangreich, und dadurch entspricht die Schicht 1 des DoD-Modells nicht der Schicht 1 des ISO-/OSI-Modells. Leider verwenden die beiden Modelle nicht die gleichen Bezeichnungen für die einzelnen Schichten.

Schichten-Denken

Lernen Sie, in den Schichten dieser Kommunikationsmodelle zu denken und insbesondere Probleme anhand dieser Einteilungen zu lösen. Wenn Sie das Modell der Netzwerke verstanden haben, werden Sie auch Netzwerke verstehen!

Wenn Sie einige der nachfolgenden Begriffe nicht kennen, so seien Sie unbesorgt, diese werden alle in den folgenden Kapiteln erklärt. Wenn Sie schon jetzt neugierig sind, können Sie eine kurze Erklärung der Begriffe und Abkürzungen auch im Glossar finden.

2.4.1 DoD-Modell

Das *Department of Defense*, das US-Verteidigungsministerium, hat ein theoretisches Modell entwickeln lassen, nach dem das Internet aufgebaut werden sollte.

Exkurs

Dabei bedeutet »Internet« nicht das Internet (als WWW), das Sie und ich heute täglich benutzen. Das Internet war als rein militärisches Netz konzipiert, das durch eine dezentrale Struktur vor einfachem Ausschalten einer zentralen Stelle geschützt sein sollte. In einem Krieg kann die Kommunikation über dieses Netz stattfinden, auch wenn einige Knotenpunkte ausgeschaltet sind.

Nr.	Schicht	Beispiele in der Praxis			
4	Process	HTTP	SMTP	FTP	DNS
3	Host-to-Host	TCP		UDP	
2	Internet	IP		IPX	
1	Network Access	Ethernet	ATM	FDDI	TR

Tabelle 2.1 Das DoD-Modell

Die Physik, also das Kabel und die Signalisierung, vermissen Sie sicherlich in dem abgebildeten Modell, Sie können sich diese als weitere Schichten vorstellen, die unterhalb von *Network Access* angeordnet sind.

- **Network Access** ist die Netzzugangsschicht. Eine Implementierung dieser Schicht ist das Ethernet, das ich noch ausführlich besprechen werde.
  Aufgabe: Wann darf gesendet werden? Wie wird gesendet? Adressierung?

- **Internet**: Für uns ist die Implementierung »Internet Protocol« (IP) interessant.
  Aufgabe: Wie bringe ich die Daten zum Empfänger? Wegewahl?
- **Host-to-Host**, auch »Session-Layer« genannt.
  Aufgabe: Überwachen der Kommunikation (Sind alle Pakete angekommen?) und Adressieren der Pakete an die richtige Anwendung.
- **Process**: Ihre Anwendungen.
  Aufgabe: Was auch immer die Aufgabe der Software ist.

Das DoD-Modell verfügt über vier Schichten, die Sie in der praktischen Arbeit an Ihrem Netzwerk wiederfinden werden. Sie verwenden als Netzwerkverfahren Ethernet – Sie verwenden **Ethernet**-Karten –, vergeben **IP**-Adressen, vielleicht kennen Sie **TCP**/UDP-Ports, und sicherlich haben Sie schon einmal in die Eingabezeile Ihres Browsers »http://... « eingegeben. Wie die einzelnen Schichten in Form der verschiedenen Verfahren (Ethernet, IP, TCP und HTTP) zusammenarbeiten, werde ich im weiteren Verlauf darstellen.

2.4.2 ISO-/OSI-Modell

ISO ist die *International Standardization Organization*, also das Gremium für international gültige Standards. Dort wurde das **ISO-/OSI-7-Schichtenmodell** entwickelt, um die Kommunikation innerhalb des Netzwerks zu beschreiben. Statt der vier Schichten des DoD-Modells gibt es dort sieben Schichten (engl. *layer*):

Nr.	Schicht	Beispiele			
7	Application	HTTP	SMTP	FTP	DNS
6	Presentation				
5	Session				
4	Transport	TCP		UDP	
3	Network	IP		IPX	
2	Data Link	Ethernet	ATM	FDDI	TR
1	Physical	Manchester	10B5T	Trellis	

Tabelle 2.2 ISO-/OSI-7-Schichtenmodell

Die Aufgaben der einzelnen Schichten entsprechen denen des DoD-Modells. Im Unterschied zum DoD-Modell gibt es als Schicht 1 den

Physical Layer, dieser regelt die Kodierung der Bits in Stromsignale. Daher entspricht die Schicht 2 des ISO-/OSI-Modells der Schicht 1 des DoD-Modells.

Der **Presentation**- und der **Session**-Layer haben nur wenig Bedeutung erlangt, weil die dort vorgesehenen Funktionen durch die Applikationsschicht, den **Application**-Layer, erfüllt werden.

Ein direkter Vergleich der beiden Modelle zeigt, dass die Unterschiede eigentlich so groß nicht sind:

DoD	ISO	Schicht	Beispiel			
4	7	Application	HTTP	SMTP	FTP	DNS
	6	Presentation				
	5	Session				
3	4	Transport	TCP		UDP	
2	3	Network	IP		IPX	
1	2	Data Link	Ethernet	ATM	FDDI	TR
	1	Physic	Manchester	10B5T	Trellis	

Tabelle 2.3 Vergleich zwischen dem DoD- und dem ISO-OSI-Modell

Wichtig!

Das ISO-/OSI-7-Schichtenmodell hat im Netzwerkbereich die größere Bedeutung der beiden Modelle erlangt. Es prägt die Begrifflichkeiten der Netzwerktechnologie (Layer-3-Switch), daher verwende ich in diesem Buch die Schichten nach dem ISO-/OSI-Modell, sodass Sie sich an die Benutzung der Schichten gewöhnen können.

2.4.3 Kommunikation

Ich möchte in diesem Abschnitt beschreiben, wie die einzelnen Schichten zusammenarbeiten, also wie die Kommunikation im Netzwerk funktioniert. Dazu werde ich mein Beispiel auf der Applikationsschicht beginnen.

Stellen Sie sich vor, Sie geben im Internet Explorer z.B. diese Adresse ein: **http://www.web.de**. Wenige Sekunden später sehen Sie die Webseite von web.de. Zwischen der Eingabe der Adresse in den Browser und dem Erscheinen der Webseite liegen viele übertragene Datenpakete und viel Netzwerkkommunikation. Jedes Datenpaket wird auf die gleiche Art und Weise abgearbeitet.

Schritt	Beschreibung	ISO/OSI
1	Ihre Anfrage nach der Webseite wird in ein **HTTP**-Paket verpackt und über eine Schnittstelle an TCP übergeben.	7
2	Sie möchten einen Webserver ansprechen, d.h. mit diesem HTTP-Pakete austauschen. Es ist festgelegt, dass HTTP die **TCP**-Port-Nummer 80 hat. Entsprechend wird nun ein TCP-Paket erzeugt, in dessen Datenteil das HTTP-Paket enthalten ist und in dessen Verwaltungsteil (engl. *header*) die Ziel-Nummer 80 (TCP-Server-Port) steht. Zusätzlich wird dort ein zufälliger TCP-Client-Port eingetragen, z.B. 1333.	4
3	Der Webserver von web.de hat eine **IP**-Adresse. Anhand dieser IP-Adresse kann der Weg zu ihm gefunden werden. Das IP-Paket enthält im Datenteil das TCP-Paket (mit dem HTTP-Paket aus Schritt 1) und im Verwaltungsteil (Header) die Ziel-IP-Adresse sowie die IP-Adresse Ihres PC als Quell-IP-Adresse.	3
4	Sie senden das Datenpaket in Ihrem LAN aus, daher muss dieses Datenpaket mit dem Ethernet-Verfahren übertragen werden. Es entsteht ein **Ethernet**-Paket, das neben den Paketen aus den Schritten 1 bis 3. die Ziel-/Quell-**MAC**-Adresse enthält. Das ist die MAC-Adresse Ihres DSL-Routers. Die Netzwerkkarte führt nun das Ethernet-Verfahren durch und sendet erst dann, wenn die Leitung frei ist.	2
5	An Ihre Netzwerkkarte ist ein Kupferkabel angeschlossen, daher können Informationen über dieses Medium nur als elektrische Spannungen übertragen werden. Jede binäre Null wird durch keine Spannung und jede binäre Eins durch eine Spannung von fünf Volt dargestellt.	1
	Das Paket wird über das Internet übertragen und passiert dabei viele Router. All das ist an dieser Stelle nicht wichtig, daher beschreibe ich es hier nicht. Schließlich wird das Paket vom Webserver empfangen.	
6	Der Empfänger stellt an seiner Netzwerkkarte wechselnde **Spannungen** fest, er interpretiert für 5 Volt eine binäre Eins und für keine Spannung eine binäre Null. Das Ergebnis ist eine binäre Codierung.	1
7	Von der Netzwerkkarte erhält der Netzwerkkarten-Treiber ein Datenpaket im **Ethernet**-Format. Es enthält seine MAC-Adresse als Ziel-MAC-Adresse und eine Quell-MAC-Adresse. Im Datenteil befindet sich ein IP-Paket.	2
8	Das IP-Paket enthält als Ziel-IP-Adresse die **IP**-Adresse des Webservers und die Quell-IP-Adresse Ihres PCs zu Hause. Im Datenteil befindet sich ein TCP-Paket.	3

Tabelle 2.4 Kommunikation im ISO-/OSI-Modell

Schritt	Beschreibung	ISO/OSI
9	Das TCP-Paket wendet sich an den Server-Port 80, also an den Webserver. Entsprechend wird der Datenteil an die Webserver-Applikation übergeben. Eine Antwort muss an den TCP-Client-Port 1333 gerichtet werden.	4
10	Der Webserver-Prozess bekommt ein HTTP-Paket, in dem die Hauptweb-Seite angefordert wird.	7

Tabelle 2.4 Kommunikation im ISO-/OSI-Modell (Forts.)

Ihre Anfrage an die Webseite geht von einer Applikation, einem Programm aus, das ein Applikationsdaten-Paket erzeugt (HTTP-Paket). Dieses Paket wandert – logisch gesehen – die ISO-/OSI-Schichten herunter (sieben, vier, drei, zwei, eins) und wird schließlich als elektrische Kodierung übertragen. Der Webserver von web.de empfängt eine elektrische Kodierung mit seiner Netzwerkkarte und erzeugt daraus ein Daten-Paket. Dieses beginnt seine Wanderung die ISO-/OSI-Schichten hoch (eins, zwei, drei, vier, sieben) und wird auf der Applikationsschicht von der Anwendung Webserver verarbeitet. Abbildung 2.4 verdeutlicht diesen Vorgang.

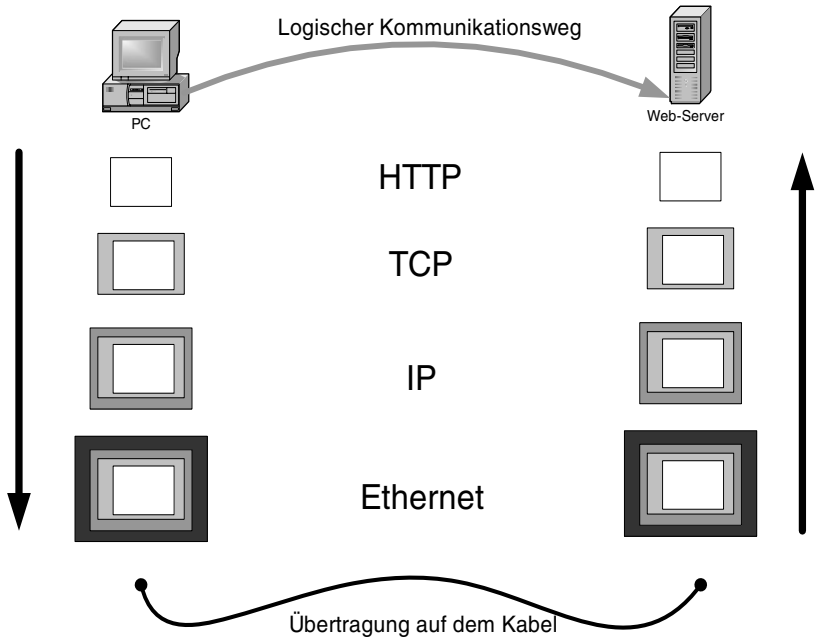

Abbildung 2.4 Datenkommunikation nach ISO-/OSI-Modell

Das Verfahren, dass ich hier beispielhaft für eine HTTP-Anfrage dargestellt habe, findet für jedes Datenpaket statt. Wenn Sie eine Webseite aufrufen, werden durchschnittlich 20 Pakete übertragen.

Geht das nicht einfacher?

Das klingt alles sehr kompliziert. Warum also macht man es nicht einfacher? Es könnte doch direkt die Anwendung mit der Anwendung sprechen, oder?

Alles ist denkbar, doch zwischen Ihnen und dem Webserver von web.de liegen noch weitere Provider-Backbones. Alle Komponenten müssten die Applikation Internet-Explorer/HTTP direkt verstehen. Die Applikation Internet Explorer müsste sich darum kümmern, wie sie den Eingang von Paketen überwacht, wie man von Ihnen zum Ziel **http://www.web.de** kommt, wie sie die Integrität der Daten überwacht, wie die Signale auf dem Kabel in elektrische Spannung umgesetzt werden. Das sind sehr viele Aufgaben, die diese Applikation erfüllen müsste. Wenn Sie nur Internet-Explorer/HTTP betrachten, ist der Aufwand genauso groß wie bei der Entwicklung selbstständiger Schichten.

Über das Internet kommunizieren noch weitere Applikationen Ihres PC (z.B. FTP, Netmeeting = H.323, ICQ, Napster ...), und jede dieser Anwendungen müsste sich um alle Teile der Netzwerkkommunikation kümmern. Das würde bedeuten, dass einerseits die Entwicklung von Anwendungen sehr komplex würde und andererseits die Übermittlung von Daten über allgemeine Netzwerke (z.B. das Internet) fast unmöglich wäre, denn schließlich müsste jedes Netzwerkgerät – insbesondere der Router – z.B. die Adressierung verstehen, IP-Adressen gäbe es nicht.

3 Lokales Netz (LAN)

3 Lokales Netz (LAN)

Sie haben nun einen Eindruck von den theoretischen Grundlagen. In diesem Kapitel werde ich Ihnen alle gängigen Techniken für LANs vorstellen.

3.1 Ethernet

Historisches

Die ersten Grundlagen von – drahtgebundenem – Ethernet wurden von der Firma Xerox in den frühen 70er Jahren gelegt. Die weitere Entwicklung von Ethernet wurde in einem Ausschuss der US amerikanischen Ingenieursvereinigung – kurz **IEEE** –, der Gruppe 802, Untergruppe 3, vorangetrieben. 1985 wurde mit dem Standard IEEE 802.3 eine internationale Normung geschaffen. 1990 folgte 10BaseT, das eine Übertragungsrate von 10 Megabit/s über Twisted-Pair-Verkabelung ermöglichte. Fast-Ethernet mit 100 Mbit/s wurde 1992 normiert. Der Ethernet-Standard wird laufend weiterentwickelt; die letzte Normung ist die des Standards IEEE 802.3ae, 10-Gibit/s-Ethernet, somit eine Vertausendfachung der ersten Datenrate von 1985.

Die Urform von Ethernet ist bereits 18 Jahre alt (1985–2003) und setzt als Übertragungsmedium Koaxialkabel ein. Alle PCs sind an dieses Kabel angeschlossen, es handelt sich um ein Bussystem. Die PCs teilen sich die Bandbreite, weil der Bus nur einen Kommunikationskanal hat und daher nur ein Rechner senden kann, ohne andere zu stören; alle anderen Rechner müssen zuhören.

Der Ethernet-Standard wendet als Zugriffsverfahren das CSMA/CD-Verfahren an. Das CSMA/CD-Verfahren wird als **nicht deterministisches Verfahren** beschrieben. Anders gesagt: Es gibt keine Kontrollinstanz, die ein Senderecht erteilt, sondern jeder Netzteilnehmer entscheidet selbst, wann er senden darf. Damit sich die Netzteilnehmer nicht gegenseitig stören, darf nur gesendet werden, wenn keine andere Station sendet. Sollten zufällig zwei Stationen gleichzeitig senden, kommt es zu einer Kollision und die Daten sind zerstört[1]. Dieser Fehlerfall muss erkannt werden, daher sendet die erkennende Station das JAM-Signal. Die beteiligten Sender müssen einen zufällig ermittelten Zeitraum warten und dürfen erst danach wieder senden.

1 Es ist nicht die Aufgabe von Ethernet, die Datenpakete erneut zu senden, das macht TCP.

Mit diesem Wissen fällt es leicht die Abkürzung CSMA/CD zu verstehen:

- **C**arrier **S**ense = Das Kabel wird abgehört.
- **M**ultiple **A**ccess = Alle Stationen haben gleichzeitig Sendemöglichkeit.
- **C**ollision **D**etect = Kollisionen müssen erkannt werden.

Wie Sie wissen, ist die Technologie vorangeschritten, und Koaxialkabel werden heute nicht mehr eingesetzt. Aktuell sind Twisted-Pair-Verkabelungen (vgl. Kapitel 5.6.1, Kupferkabel), die über vier oder acht getrennte Adern verfügen. Üblicherweise wird ein Adernpaar für das Senden und ein Adernpaar für das Empfangen benutzt. Das Senden und Empfangen wird so auf getrennten Kommunikationskanälen übertragen, folglich stört es nicht, wenn eine Station gleichzeitig sendet und empfängt. Anders als beim Koaxialkabel-Ethernet, das nur Senden **oder** Empfangen erlaubte (= Halfduplex), ist beim Twisted-Pair Fullduplex (vgl. Kapitel 5.7.5, Sonderfunktionen) gleichzeitiges Senden und Empfangen möglich. Der Geschwindigkeitsvorteil liegt bei ca. 15% und nicht bei 100%, wie manche Hersteller von 200-Mbit/s-Netzwerkkomponenten gerne suggerieren.

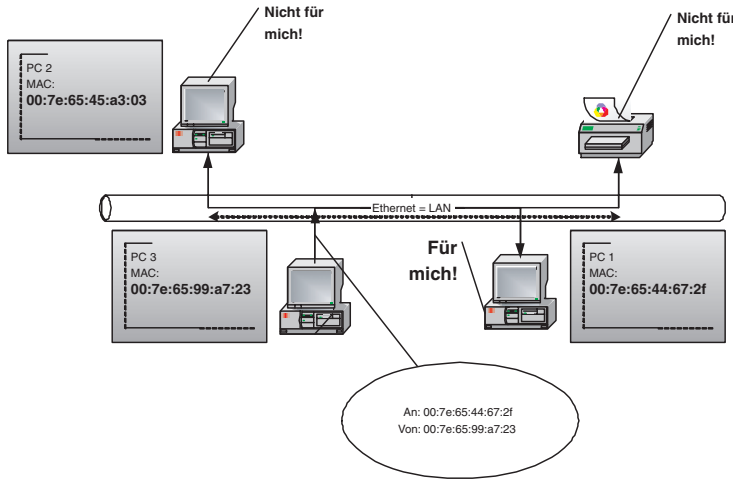

Abbildung 3.1 Kommunikation im Ethernet

In der Abbildung 3.1 erkennt PC3, dass das Netzwerk frei ist, und sendet an PC1. Er schickt einen Ethernet-Frame an die MAC-Adresse von PC1. Er flutet damit das ganze Kabel, d.h., jede am Kabel angeschlos-

sene Station kann diese Daten empfangen. Anhand der MAC-Adresse wird von der Netzwerkkarte für jede angeschlossenen Station entschieden, ob die Daten angenommen werden müssen oder die Daten ignoriert werden können.

Eine Ausnahme bildet der so genannte **Promiscuous Mode**, in den sich viele Netzwerkkarten versetzen lassen. Es wird nicht überprüft, ob die Daten für die eigene MAC-Adresse sind, sondern es werden alle Datenpakete angenommen. Diese Funktion wird typischerweise bei Netzwerküberwachungen eingesetzt, so kann der gesamte Datenverkehr erfasst werden und nicht nur der, der an einen speziellen PC adressiert ist. Exkurs

Die Entwicklung des Ethernet-Standards können Sie der Abbildung 3.2 entnehmen.

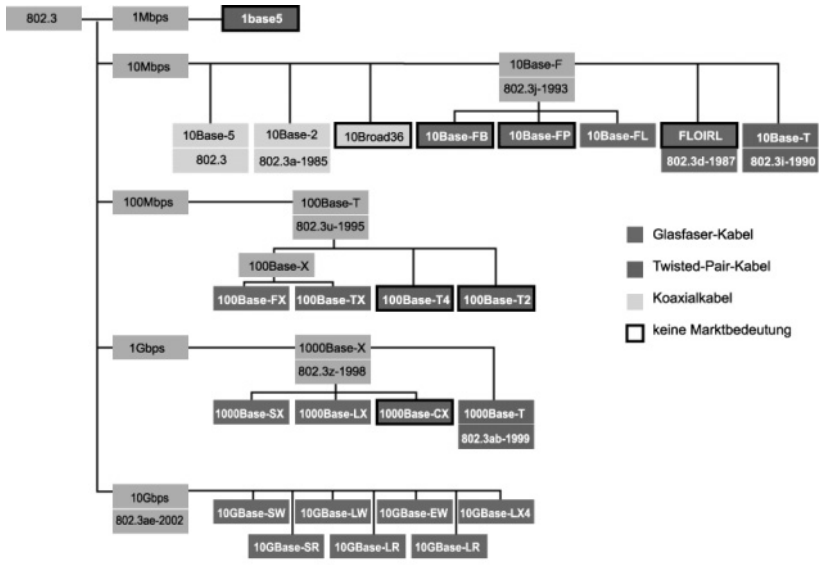

Abbildung 3.2 Ethernet (IEEE 802.3): Ausprägungen, Quelle: tecchannel

Das schon antiquierte Verfahren 10Base-2-10 Mbit/s Ethernet über Koaxialkabel von 1985, ist auch unter der Bezeichnung BNC-Verkabelung bekannt. Wie man ein solches Netz in eine moderne Netzstruktur integriert, erfahren Sie in Kapitel 5.11, Migrationsmöglichkeiten. Eine aktuelle Verkabelung realisieren Sie mit Twisted Pair. Exkurs

3.1.1 Fast-Ethernet

Das schnelle Ethernet bietet eine Geschwindigkeit von 100 Mbit/s und ist als IEEE 802.3u 1995 normiert worden. Der Erfolg des Verfahrens liegt darin begründet, dass sich das Paket-Format von Ethernet mit 10 Mbit/s zu Fast-Ethernet mit 100 Mbit/s nicht geändert hat. Somit kann vorhandenes Know-how weiter eingesetzt werden, und auch der Datenaustausch zwischen den beiden Ethernet-Varianten ist nur eine Frage der Geschwindigkeit. Dadurch sinken die Kosten für den Aufbau eines Fast-Ethernet-Netzes und ein Mischbetrieb ist möglich. Viele Komponenten (wie Netzwerkkarten), die Fast-Ethernet beherrschen, sind abwärtskompatibel und können auch mit 10-Mbit/s-Ethernet betrieben werden.

Die physikalische Ausbreitungsgeschwindigkeit von etwa 200.000 km/s konnte nicht verändert werden. Wie hat man dagegen die effektive Übertragungsgeschwindigkeit verzehnfachen können? Die Daten werden dichter übertragen, sodass die Laufzeit von Daten nicht mehr 51,2 µs, sondern 5,12 µs beträgt.

Exkurs

Da bei beiden unten genannten Varianten (100Base-FX und 100Base-TX) zwei Kanäle (Senden und Empfangen) zur Verfügung stehen, ist es möglich, – anders als noch im BNC-Netzwerk – Daten gleichzeitig zu senden und zu empfangen. Das Verfahren wird **Fullduplex** genannt und bietet theoretisch 100%, praktisch 15% mehr Leistung gegenüber der noch vorhandenen Halfduplex-Variante.

Welche Geschwindigkeit (10 oder 100 Mbit/s) zu benutzen ist, wird meist mit dem **Autosensing-Mechanismus** erkannt. Auch für Half- oder Fullduplex gibt es eine Erkennung, **Autonegotiation**. Beide Technologien sind nicht genormt, daher funktionieren sie nicht zuverlässig zwischen Komponenten verschiedener Hersteller (z.B. Cisco und 3Com). Es handelt sich um eine echte Fehlerquelle! Weitere Informationen finden Sie in Kapitel 5.7.5, Sonderfunktionen.

Es gibt zwei Ausprägungen von Fast-Ethernet:

- 100Base-FX:Fast-Ethernet auf Glasfaser
- 100Base-TX:Fast-Ethernet über Twisted-Pair-Kupferkabel

100Base-FX erlaubt die Übertragung von 100 Mbit/s auf Glasfaser (engl. *fiber*), auch LWL (**L**icht**W**ellen**L**eiter) genannt. Dabei kommen zwei LWL-Fasern zum Einsatz, eine für das Senden, eine für das Empfangen. Die LWL-Fasern müssen 62,5/125 µm dünn sein. Sie können

damit eine Entfernung von 450 Metern überbrücken. 100Base-FX ist eine unattraktive Variante, weil man bei ähnlichen Kosten und Entfernungen auch eine 1000Base-SX-Variante (vgl. Kapitel 3.1.2, Gigabit-Ethernet) realisieren kann.

100Base-TX ist die weit verbreitete Kupfervariante von Fast-Ethernet. Die Übertragung findet auf vier Kupferadern (also zwei Adernpaaren, und zwar auf den Adern: eins, zwei, drei und sechs) mit 100 Mbit/s statt. Üblicherweise sind Twisted-Pair-(TP-)Kabel achtadrig; von den acht Adern werden lediglich vier genutzt. Mit 100Base-TX kann man wie schon bei 10Base-T einhundert Meter überwinden. Dabei gilt die Regelung, dass 90 Meter verlegt werden und 10 Meter PC-Anschlusskabel sind.

3.1.2 Gigabit-Ethernet

Gigabit-Ethernet ist der zurzeit bezahlbarste schnelle Standard. Die Kapazität von 1000 Mbit/s nutzt kaum ein einzelner Server aus – High-End-Server schaffen ca. 600 Mbit/s –, doch eine Serverfarm mit zehn Servern kann eine Verbindung mit 1000 Mbit/s leicht auslasten.

Gigabit-Ethernet wird hauptsächlich für Verbindungen im so genannten Backbone, also auf den Hauptnetzwerkverbindungen, eingesetzt. Zunehmend werden auch einzelne PCs mit Gigabit-Ethernet versorgt, und das meist weniger aus Gründen mangelnder Kapazität, sondern wegen der sehr guten Paket-Laufzeiten von 0,512 µs. Durch die zehnfach schnelleren Laufzeiten von Daten ist es möglich, sehr zeitkritische Systeme wie z. B. Clustersysteme[2] aufzubauen.

Das Paketformat von Ethernet bleibt wie schon beim Umstieg von 10 auf 100 Mbit/s auch bei Gigabit-Ethernet gleich. Zusätzlich zu dem bestehenden Paketformat wurde ein Burst-Modus eingefügt. Dieser bietet die Möglichkeit, viele kleine Pakete zu einem größeren Paket zusammenzufassen und gemeinsam zu übertragen. Dadurch soll die Effektivität des Netzwerks bei Belastung mit vielen kleinen Paketen gesteigert werden. Man erkauft den Vorteil mit dem Nachteil des leicht verzögerten Versandes, sodass mit dem Einsatz dieser Funktion die Eignung eines Netzes für Multimedia, insbesondere Echtzeit-Video, sinkt.

2 Ein Cluster (dt. *Gruppe*) sind mehrere Rechner, die für Anwender wie ein Rechner wirken. Dabei findet zumeist Lastverteilung zwischen diesen Rechnern statt. Übrigens müsste man korrekterweise von Parallel-Servern statt von Clustern sprechen.

1000Base-SX, -LX sind die oft eingesetzten LWL-Varianten von Gigabit-Ethernet. Meist werden über diese Verfahren Netzwerkkomponenten miteinander verbunden oder ein Backbone aufgebaut.

1000Base-SX ist die günstigere der beiden Varianten. Sie kommt mit einer Laserdiode als Lichtquelle aus, die wesentlich günstiger als ein echter Laser ist. SX nutzt 850 nm als Lichtwellenlänge auf Multi-Mode-Fasern (62,5/125 µm oder 50/125 µm Durchmesser). Damit können Entfernungen von 220 m oder 550 m überwunden werden (siehe auch Kapitel 6.2.1, Glasfaserkabel, Grundlagen).

1000Base-LX nutzt 1300 nm als Lichtwellenlänge, kommt ebenfalls mit einer Laserdiode aus und schafft auf Multi-Mode-Fasern 550 m. Setzt man die hochwertigeren Mono-Mode-Fasern (9/125 µm) ein, können bis zu 5000 m Entfernung überwunden werden.

1000Base-T, ein Kupferkabelstandard wurde erst 1999 als IEEE 802.3ab (SX und LX schon 1998 als IEEE 802.3z) standardisiert. Um diese Variante wurde sehr gerungen. Ziel war es, Gigabit-Ethernet auf bestehenden Kategorie-5-Kupferkabeln zu realisieren. Dieses Ziel wurde erreicht, indem man acht Adern, also vier Adernpaare, nutzt. Der Datenstrom wird in vier Übertragungskanäle aufgeteilt und auf fünf Spannungslevel verteilt. Durch die neue Art der Übertragung werden die in Kategorie 5 (Cat 5) festgelegten Minimalanforderungen überschritten. Es wurde daher die Cat-5e-Normierung vorgenommen, die die Gigabit-Ethernet-Tauglichkeit für Kabel bescheinigt. In der aktuellen Ausgabe der DIN/EN 50173 (von 2000) sind die Anforderungen ebenfalls angepasst. Die DIN/EN-Norm ist für Europa und Deutschland maßgeblich. Weitere Informationen zu den Kabelstandards finden Sie in Kapitel 6.1.1, Kupferkabel.

1000Base-TX gibt es offiziell nicht, d.h. es existiert keine Norm von IEEE. Einige Hersteller geben 1000Base-T als 1000Base-TX aus, doch es steckt mehr hinter dieser Sache. Der 1000Base-T-Standard erfordert, alle vier Adernpaare zu nutzen, weil das Kabel (Cat 5) an sich qualitativ eine höhere Belastung nicht zulässt. Dabei wird mit Hilfe von komplexen Techniken versucht, Fehler zu beseitigen, die das Übersprechen (engl. *Next*) auftreten lassen. Angaben in der Fachliteratur zufolge kann mit 1000Base-T nicht die volle Kapazität von 1000 Mbit/s ausgenutzt werden, in der Praxis werden lediglich 400 Mbit/s erreicht.

Mit einer Cat-6-Verkabelung hat sich dieses Problem eigentlich erledigt, denn die Qualität dieser Kabel liegt deutlich höher und lässt Frequenzen bis 250 MHz (statt 100 MHz) zu. 1000Base-TX ist daher die Entwicklung eines Gigabit-Ethernet auf Kupferkabeln, das auf allen vier Adernpaaren 250 MHz nutzt und so ohne technische Tricks 1000 Mbit/s Fullduplex (250 * 8 = 2.000) erreicht. Ein Normungsvorschlag stammt von der TIA (Telecommunications Industry Association), TIA854, den Sie auch auf der CD-ROM im Verzeichnis **Dokumente** finden.

3.1.3 Ausblick

Ethernet wird Sie auch zukünftig begleiten. Im Jahre 2002 ist der 10GBase-Standard als IEEE 802.3ae normiert worden. Dieser Standard bietet 10 Gigabit/s als Kapazität und wird auch mit XGE abgekürzt. Hinzu kommen zahlreiche Änderungen, die den Standard auch für längere Entfernungen von bis zu 40 km verwendbar machen.

Noch 2002 wurde verneint, dass ein 10-Gbit/s-Standard für Kupferkabel entwickelt wird. Anfang 2003 konnte ich aber in der Fachpresse lesen, dass sehr wohl an einer Normierung gearbeitet wird und dass diese vermutlich Ende 2004 abgeschlossen sein wird. Ziel ist es, 10 Gbit/s über Cat-5e- und Cat-6-Kupferkabel zu übertragen. Die Gründung einer Untergruppe wurde im November 2002 beschlossen, und diese wird den Standard erarbeiten, der vermutlich IEEE 802.3ak heißen wird.

Sie sehen, dass die Entwicklung im Bereich der Kupferkabel noch kein technisches Ende gefunden hat und sicherlich noch einige Jahre fortgesetzt wird. Es ist keine Fehlinvestition, wenn Sie in gute Kupferkabel investieren und Ihr Netzwerk mit Kabeln ausstatten, die der Linkklasse E genügen.

Multimedialer Internetzugang

Ein Trend, der von einigen Firmen propagiert wird, ist ETTH oder ETTX, ausformuliert *Ethernet To The Home* oder *Ethernet To The X*[3]. Gemeint ist der Ausbau von Stadt- bzw. Regionalnetzwerken, über die Ihnen ein Provider TV, Internet und Telefon über z. B. ein Fernsehkabel auf der Basis von Ethernet anbietet. Ein Kabelmodem de-/kodiert die Ethernet-Pakete. Damit lassen sich Geschwindigkeiten von 10 Mbit/s erzielen, die ausreichen, um Multimedia, also TV, in digitaler Qualität zu realisieren.

3 »X« soll für »überall« stehen.

Diese Projekte werden von der Organisation IEEE unterstützt. Dort gibt es ein eigenes Gremium, welches sich um *EFM* (Ethernet in the First Mile) unter dem Kürzel IEEE 802.3ah kümmert. Basistechnologien werden über Telefonleitungen VDSL und S-HDSL (vgl. 4.2, xDSL) sein.

... und es geht weiter!

So, wie Sie und ich heute über Modemgeschwindigkeiten von 19,2 kBit/s in Zeiten von T-DSL mit 768 kBit/s lächeln, so werden wir auch in fünf bis zehn Jahren über 1000Base-T lächeln. Ich vermute, dass es weitere Entwicklungen im Bereich der Kupferkabel geben wird. Schließen Sie sich meiner Argumentation an, so lassen sich höhere Investitionen in Kupferkabel rechtfertigen.

3.1.4 Hub

Ein Hub (dt. *Radnabe*) ist eine aktive Netzwerkkomponente, die im Zentrum der Sterntopologie (vgl. Kapitel 2.3.1, Netzwerktopologien) steht. Alle Anschlusskabel zu den Stationen beginnen im Hub. Der Hub selbst verbindet die einzelnen Anschlüsse intern über einen Bus.

Wenn Sie das Schema von Bus- und Sterntopologie vergleichen, stellen Sie sich bitte vor, dass der Bus nun im Hub steckt und lediglich die Anschlusskabel nach außen geführt werden.

Technisch ist der Hub ein elektrischer Verstärker. Er arbeitet auf Schicht 1 des ISO-/OSI-Modells. Das Gerät trifft keinerlei logische Entscheidungen, sondern gibt alle eingehenden Signale ungeprüft und elektrisch verstärkt an allen übrigen Anschlüssen aus.

Auch fehlerhafte Pakete (zu groß, zu klein, fehlerhafte Prüfsumme) werden weitergeleitet und nicht schon am Hub verworfen.

Typischerweise wurden Hubs bei Twisted-Pair-Verkabelungen eingesetzt. Sie bieten zwischen fünf und 100 Anschlussmöglichkeiten für RJ45-Stecker.

Ein Hub wird zur Netzwerkanalyse benötigt. Wie im Ethernet üblich, kann an jedem Anschluss der gesamte Datenverkehr empfangen werden. Dadurch ist es möglich, durch Zwischenschalten eines Hubs den gesamten Datenverkehr zu einem PC zu überprüfen. Diese Möglichkeit besteht bei Switches nicht grundsätzlich, sondern lediglich über Zusatzfunktionen.

3.1.5 Switch

Der Switch ist aus den Bridges (dt. *Brücken*) hervorgegangen. Eine Bridge – und somit auch ein Switch – trennt ein Ethernet in mehrere Segmente auf. Die Bridge besitzt dabei einen Anschluss pro Segment (vgl. Abbildung 3.3) und leitet Pakete aus dem Segment A nur dann in das Segment B, wenn die adressierte MAC-Adresse dort angeschlossen ist. Die Bridge/Der Switch trifft die Entscheidungen anhand der ISO-/OSI-Schicht 2. Wenn also PC1 an PC2 sendet, bleiben die Datenpakete im Segment A, parallel kann innerhalb des Segments B gesendet werden, ohne dass es zu Kollisionen kommt.

Das in Abbildung 3.3 dargestellte Netzwerk hat eine Bandbreite von 10 Mbit/s. Ohne Bridge würden sich die fünf PCs die Bandbreite teilen: (10 Mbit/s) : 5 = 2 Mbit/s pro PC. Die Bridge hat die effektive Netzwerkkapazität pro PC nahezu verdoppelt: Im Segment A teilen sich zwei PCs die Bandbreite von 10 Mbit/s, somit 5 Mbit/s pro PC, im Segment B sind es drei PCs, daher stehen jedem PC 3,33 Mbit/s zur Verfügung. Das gilt unter der Voraussetzung, dass die Kommunikation selten segmentübergreifend (also zwischen A und B) stattfindet.

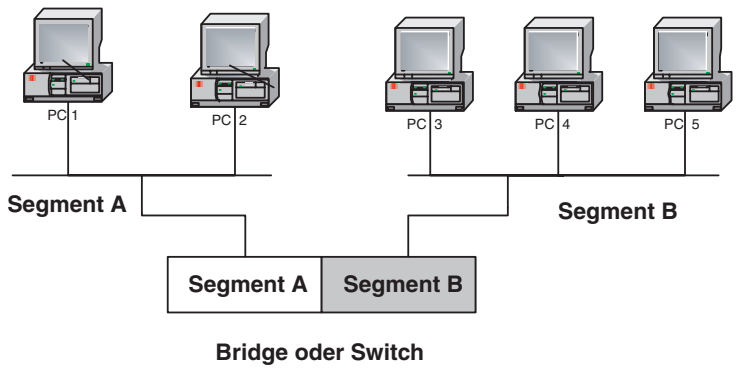

Abbildung 3.3 Eine Bridge erzeugt Segmente auf Ethernet-Ebene.

Ein Switch unterscheidet sich nur durch wenige Eigenschaften von der Bridge. Der Switch hat mehr als zwei Anschlüsse, und seine Intelligenz ist nicht ein Programm, das von einer CPU abgearbeitet wird, sondern ist in Hardware gegossen, in ASICs. In den unteren Preissegmenten werden Switching Hubs angeboten. Damit ist gemeint, dass das Gerät die Funktion eines Switchs besitzt, jedoch ohne – teure und schnelle – ASICs, sondern mit einer CPU als Hardware.

Üblicherweise wird pro Switch-Anschluss ein PC (vgl. Abbildung 3.4) angeschlossen. Damit entsteht pro PC ein Ethernet-Segment. Jedem PC steht damit die volle Bandbreite von 100 Mbit/s pro Kommunikation zur Verfügung, denn es werden nur noch Datenpakete an ihn weitergeleitet, wenn sie für seine MAC-Adresse bestimmt sind.

Ein Switch-Anschluss, also eine RJ45-Buchse eines Switchs wird als **Port** oder **Switch-Port** bezeichnet.

Ausnahme(n)

Es gibt zwei Arten von Ethernet-Paketen, die grundsätzlich auf allen Ports ausgegeben werden: Broadcasts und Multicasts. Sie belasten alle Switch-Ports gleichzeitig.

Broadcast

Ein Broadcast ist ein Paket, das an alle Netzwerkteilnehmer adressiert ist. Es wird also jede Ethernet-Karte unabhängig von der MAC-Adresse angesprochen. Die Ziel-MAC-Adresse lautet ff:ff:ff:ff:ff:ff. Diese Möglichkeit wird z.B. bei ARP (vgl. Kapitel 3.4, Address Resolution Protocol) benutzt.

Leider verwenden viele Anwendungen diese simple, aber unschöne Möglichkeit, alle Rechner eines Netzwerks zu erreichen.

Multicast

Ein Multicast wendet sich an eine Gruppe von Stationen. Es wird vom Sender nur einmal gesendet und das Netzwerk verteilt die Pakete. So wäre es möglich, **einen** Videodatenstrom zu 100 Empfangsstationen gleichzeitig zu senden. Nur professionelle Switches unterstützen intelligente Mechanismen, bei denen sich Empfänger beim Switch für bestimmte Multicasts anmelden, sodass der Switch gezielt die Datenpakete an diesen Port weiterleiten kann (Stichwort: IGMP). Meist werden Multicasts wie Broadcasts an allen Ports ausgegeben, unabhängig davon, ob es einen wartenden Empfänger gibt oder nicht.

Broadcasts und Multicasts belasten das Netzwerk, weil sie auf allen Ports ausgegeben werden. Während eines Broadcasts kann keine weitere Kommunikation stattfinden, weil alle Ports belegt sind. Es sollte Ziel der Netzwerkadministration sein, möglichst wenig Broadcasts und Multicasts im Netzwerk zu haben.

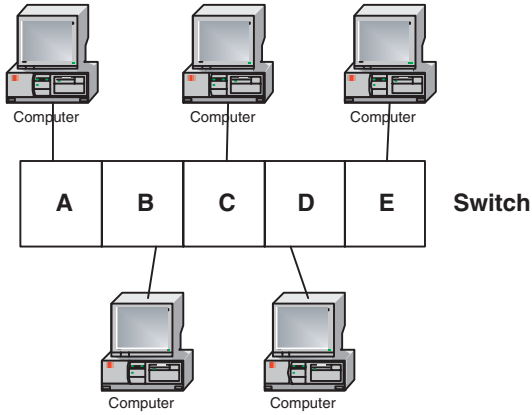

Abbildung 3.4 Ein Switch erzeugt pro PC ein Segment.

Die Multicast-MAC-Adresse für die Umsetzung von IP-Multicasts in Ethernet-Multicasts ist in RFC 1112 definiert und lautet 01:00:5e:00:00:00. Exkurs

ATM

ATM, Asynchronous Transfer Mode, ist eine ISO-/OSI-2-Technologie. ATM ist als Basistechnologie für Breitband-ISDN entwickelt worden und stellt in seiner aktuellen Entwicklung bis zu 622 Mbit/s bereit. Exkurs

Die besonderen Fähigkeiten von ATM liegen in der Möglichkeit, Datenströme sehr zuverlässig zu priorisieren: Man spricht hier von **Q**uality **o**f **S**ervice. Mit seinen Dienstgütemerkmalen eignet sich ATM für die Daten- und mehr noch für die Sprachübertragung. ATM ist also eine Technologie, die es ermöglicht, Sprache, Daten und Video in der jeweils erforderlichen Güte zu übertragen.

Bevor eine Kommunikation beginnt, reserviert der Sender eine bestimmte Bandbreite zu seinem Ziel. Steht nicht genügend Bandbreite zur Verfügung, so wird der Verbindungsaufbau abgelehnt.

Die Kommunikation läuft innerhalb von virtuellen Verbindungen (VPI, Virtual Path Identifier, und VCI, Virtual Channel Identifier) ab. Die Möglichkeit von Punkt-zu-Mehrpunkt-Verbindungen gibt es – eigentlich – nicht. Daher bereitet die Umsetzung von IP-Broadcast auf ATM-Broadcasts einige Probleme. Man benötigt dazu einen gesonderten Server: LANE, LANEmulation. Durch ihn wird zu jedem Teilnehmer eine gesonderte Verbindung eröffnet und somit Broadcast simuliert.

ATM hat sich u.a. deshalb nicht im LAN gegen Ethernet durchgesetzt, weil es zu teuer ist. Das Verfahren ist relativ komplex und erfordert entsprechend aufwändige Komponenten und ausgefeiltes Know-how. Der Bedarf im LAN an QoS (Quality of Service) war bisher nicht groß genug, um ATM zu erzwingen. Der ursprüngliche Geschwindigkeitsvorteil von 155-Mbit/s-ATM gegenüber 10-Mit/s-Ethernet hat sich umgekehrt. Nun konkurriert 1.000-Mbits/s-Ethernet gegen 622-Mbit/s-ATM.

Die Netzwerktechnologie hat sich für das schnellere Verfahren, nämlich Ethernet, entschieden. Es ist günstiger, ein Gigabit-Ethernet aufzubauen als ein 155-Mbit/s-ATM.

3.2 Das Internetprotokoll (IP)

3.2.1 Allgemeines

Das Internet-Protokoll wird nicht nur im Internet, sondern auch sehr erfolgreich im LAN eingesetzt. Es wird von allen aktuellen Betriebssystemen unterstützt. IP ist ein Protokoll der dritten Schicht des ISO-/OSI-Modells und hat die Aufgabe der Wegewahl: Wie kommt ein Datenpaket von IP-Netz A in das IP-Netz B (vgl. Abbildung 3.5)? Die Wahl des richtigen und möglichst auch des geeignetesten Weges, das ist die Aufgabe dieser Netzwerkschicht und damit von IP.

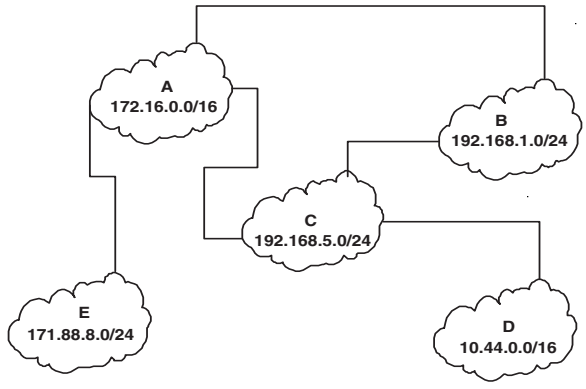

Abbildung 3.5 Verbundene IP-Netze

Eine IP-Adresse, das bekannteste Element von IP, beinhaltet **zwei** Informationen:

- die Zugehörigkeit zu einer Gruppe (IP-Netz) und
- eine eindeutige Nummer innerhalb dieser Gruppe (Host-ID).

Beide Informationen müssen trennbar sein. Die **Subnetzmaske** gibt an, welche Bits der IP-Adresse die Gruppenzugehörigkeit beschreiben. Die restlichen Bits, die nicht von der Subnetzmaske erfasst werden, beschreiben die eindeutige Nummer eines Rechners innerhalb der Gruppe und werden Hostanteil oder Host-ID genannt.

Wichtig!

Sie benötigen das hier dargestellte Wissen für die Themen Routing und Firewall (vgl. Kapitel 3.2.2, Routing, und Kapitel 11.2.1, Firewalls).

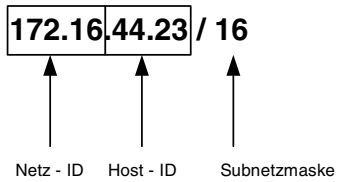

Abbildung 3.6 Aufbau einer IP-Adresse

Die IP-Adresse ist vier Byte, also 32 Bit, lang, und normalerweise wird jedes Byte von den anderen durch einen Punkt getrennt. In einem Byte können $2^8 = 256$ Werte dargestellt werden. Diese entsprechen dezimalen Werten von 0 bis 255.

Von den 256 möglichen Werten haben die 0 und die 255 eine besondere Bedeutung, wenn die Host-ID ausschließlich aus den Bereichen 0 oder 255 besteht.

Die Schreibweise: 172.16.0.0/16 meint das IP-Netz 172.16. Der Weg in ein Netz wird im Rechner etwa so beschrieben:

```
172.16.0.0 über 192.168.1.12 mit Anschluss Ethernet1
```

Der Eintrag, ein Routing-Eintrag, bedeutet, dass das IP-Netz 172.16 über den Router 192.168.1.12 erreicht werden kann. Die Nullen in den beiden letzten Bytes geben in Verbindung mit der Subnetzmaske an, dass das gesamte IP-Netz gemeint ist.

Die zweite Sonderbedeutung – neben der 0 – hat die 255, wenn sie den Bereich der Host-ID ausfüllt. Ein IP-Paket, das als Zieladresse

172.16.255.255 eingetragen hat, spricht jede Station im IP-Netz 172.16.0.0 an. Näheres zum Thema Ethernet-Broadcast finden Sie in Kapitel 3.1.5, Switch. IP-Broadcasts werden in einen Ethernet-Broadcast umgesetzt werden. Die Ziel-IP-Adresse 172.16.255.255 ist die IP-Broadcast-Adresse des IP-Netzes 172.16.0.0. Wird die Broadcast-Adresse 172.16.255.255 verwendet, werden alle PCs in dem IP-Netz angesprochen. Derselbe Effekt wird erreicht, wenn als IP-Adresse 255.255.255.255 angesprochen wird.

Wichtig! Broadcasts und Multicasts werden durch Router nicht von einem IP-Netz in ein anderes IP-Netz geleitet.

Exkurs Alternativ zur dezimalen Schreibweise könnte man IP-Adressen auch binär schreiben. Man hat pro Byte acht Stellen, die entweder auf 0 oder 1 gesetzt sind. Dabei wird deutlicher, dass eine dezimale 0 in einem Byte acht binären Nullen entspricht und 255 acht Einsen und dass daher deren Sonderbedeutung resultiert. Sehr selten kann es schon mal vorkommen, dass die IP-Adresse hexadezimal geschrieben wird. Ausnahme: Bei der neuen IP-Version 6 (vgl. Kapitel 3.2.6, IP Version 6) werden IP-Adressen immer hexadezimal geschrieben.

Beispiele:

- 192.168.4.1 mit einer Subnetzmaske von 255.255.255.0:
  Die 255 bei der Subnetzmakse bedeutet jeweils, dass das Byte auf die Netz-ID entfällt, entsprechend sind bei der Subnetzmaske drei Bytes gesetzt (= 24 Bit). Die ersten drei Bytes beschreiben den Netzteil (Netz-ID) der IP-Adresse: 192.168.4. Das letzte Byte mit dem Wert 1 ist der Hostteil (Host-ID), die Nummer der Station innerhalb des IP-Netzes.
- 172.16.5.77 mit einer Subnetzmaske von 255.255.0.0:
  Die ersten zwei Bytes sind das Netz 172.16.0.0, die zweiten beiden Bytes 5.77 bestimmen den Rechner in dem IP-Netz. Möchte man alle Rechner in dem IP-Netz ansprechen, lautet die IP-Adresse 172.16.255.255. Das ist die Broadcastadresse dieses Netzes.
- 10.6.8.9 mit einer Subnetzmaske 255.0.0.0:
  Der Netzteil der IP-Adresse umfasst lediglich das erste Byte, das IP-Netz lautet daher: 10.0.0.0, der Rechner hat die Nummer 6.8.9.

Wie Sie bemerkt haben, ist die Subnetzmaske bei den Beispielen immer kleiner geworden, der Bereich, mit dem man die Rechner (= Hosts) anspricht, wurde immer größer. Wozu?

Stellen Sie sich vor, Sie haben eine Rechtsanwaltskanzlei und möchten ein IP-Netz für Ihre Kanzlei einrichten. Es wird vermutlich ausreichen, ein IP-Netz mit einer 24-Bit Subnetzmaske – also 255.255.255.0 – zu nehmen. Zur Adressierung von Hosts innerhalb dieses Netzes haben Sie 254 Möglichkeiten[4]. Wenn Sie jetzt Vorstandschef von DaimlerChrysler wären und ein IP-Netz einrichten wollten, in dem jeder PC Ihres Unternehmens eine IP-Adresse bekommen soll – würden 254 Möglichkeiten reichen? Nein, Sie brauchen ein IP-Netz, das mehr Adressraum für Host-IDs bereitstellt. Im Fall von DaimlerChrysler benötigen Sie ein Netz, das eine 8-Bit-Subnetzmaske – also 255.0.0.0 – hat. Dann haben Sie 24 Bit oder 2^{24} = 16,7 Millionen Möglichkeiten, eine Host-ID zu vergeben. Von diesen IP-Netzen mit 8-Bit-Subnetzmaske gibt es weltweit rechnerisch 254 Stück, tatsächlich sind es weniger.

IP-Netze wurden früher in Klassen eingeteilt:

- 24-Bit-Subnetzmaske (255.255.255.0) = Class C
- 16-Bit-Subnetzmaske (255.255.0.0) = Class B
- 8-Bit-Subnetzmaske (255.0.0.0) = Class A

Die Einteilung in Klassen ist weitestgehend überholt (Stichwort: CIDR), häufig trifft man aber auf die Begrifflichkeit Klasse-C-Netz, sodass es sinnvoll ist, die Sache hier kurz zu erwähnen.

Über welche Art von IP-Netz reden wir? Es geht um ein offizielles aus dem Internet erreichbares IP-Netz. Jeder dort angeschlossene PC hat eine weltweit eindeutige IP-Adresse innerhalb des Internets und ist direkt von dort erreichbar.

Nur wenige Privatleute benötigen eine feste IP-Adresse. Als normaler Anwender »leihen« Sie sich eine offizielle IP-Adresse von Ihrem Internetprovider für die Dauer der Internetverbindung. Bei jeder Einwahl bekommen Sie eine andere IP-Adresse zugewiesen. Die wechselnde IP-Adresse führt dazu, dass Sie trotz Flatrate keine Dienste von zu Hause im Internet anbieten können. Die Namensauflösung Ihrer URL würde zu wechselnden IP-Adressen führen.

Exkurs

Das Problem der dynamischen Adressen lösen Dienste wie **http://www.dyndns.org**. Sie lassen automatisch von Ihrem PC aus Ihre öffentliche IP-Adresse nach der Einwahl auf ihre Seiten aktualisieren, sodass Ihre URL stets zur richtigen IP-Adresse aufgelöst wird.

4 Es sind deshalb 254 Möglichkeiten, weil von 256 Möglichkeiten die 0 und die 255 wegfallen.

Hat ein Unternehmen einen festen Internetzugang ohne Einwahl, ist es also 24 Stunden online, stellt der Internetprovider eine feste IP-Adresse zur Verfügung. Wie man mit nur einer offiziellen IP-Adresse mit mehreren Rechnern im Internet erreichbar ist, lesen Sie in Kapitel, 3.2.4, NAT, Network Address Translation. Private, also nicht offizielle IP-Adressen werden in Kapitel 3.2.3, Private IP-Adressen, behandelt.

Offizielle IP-Netze werden an Unternehmen, Behörden und Universitäten vergeben. Diese haben dann einen zugeteilten Adressbereich. Hat man als Unternehmen ein Klasse-C-Netz zugeteilt bekommen (z. B. 192.140.252.0/24), so hat man 254 offizielle IP-Adressen, die im Internet erreichbar sind.

Vergeben werden die IP-Adressen von der Organisation RIPE, die diese Aufgabe an die Provider delegiert hat. Wenn Sie sich also einen Adressbereich reservieren wollen, wenden Sie sich an Ihren Provider. Doch eines vorweg: Sie werden nur mit einer sehr guten Begründung noch einen Adressbereich bekommen, eine einzelne IP-Adresse bekommen Sie leichter.

Praxis Wenn Sie wissen möchten, wem eine bestimmte IP-Adresse zuzuordnen ist, sehen Sie dies im Internet unter **http://ailab.de/modules/ip-telligence/index.php4** nach. Innerhalb von Deutschland hilft Ihnen **http://jan.kneschke.de/projects/localizer** sogar dabei, die Stadt herauszufinden – zumindest, wenn es sich um eine IP-Adresse von einem Provider handelt.

3.2.2 Routing

Möchte ein PC aus dem IP-Netz A mit dem Rechner aus dem IP-Netz B kommunizieren, so benötigt er dafür mindestens **einen Router**. Der Router arbeitet eine ISO-/OSI-Schicht höher als ein Switch, nämlich auf der ISO-/OSI-Schicht 3.

Der Router verbindet – im einfachsten Fall – zwei IP-Netze miteinander. Dabei funktioniert er ähnlich wie eine Bridge (vgl. Kapitel 3.1.5, Switch). Er leitet alle Datenpakete aus dem IP-Netz A in das IP-Netz B, wenn sie an einen Rechner in diesem Netz addressiert sind. Eine Bridge oder ein Switch teilt ein Ethernet in einzelne Segmente, sodass es zu einer Bandbreitenerhöhung kommt. Im IP ist das Einteilen in Segmente schon vorgesehen: Segmente heißen IP-Netz oder Subnetze. Diese IP-Netze verbindet ein Router. Er hat dazu zwei Anschlüsse, in jedem IP-Netz (A und B) jeweils einen. Man nennt diesen Anschluss Interface,

manche sprechen von »Beinchen«. Empfängt der Router auf seinem IP-Netz-A-Interface ein Datenpaket, schaut er in die IP-Adressierung, dort steht u.a. die IP-Ziel-Adresse. Lautete die Zieladresse IP-Netz B, so sendet der Router das Datenpaket auf dem Interface B in das IP-Netz B.

Router ist Technik

Es wird deutlich, dass mit dem Begriff Router weniger ein konkretes Gerät gemeint ist als vielmehr eine Funktionalität, die von verschiedenen Geräten, z.B. PCs, ausgeübt werden kann.

Ein Router, so kann man es vereinfacht ausdrücken, entscheidet anhand der IP-Adresse, wohin er das Paket schicken muss, damit es seinem Ziel näher kommt. Dazu hat ein Router mindestens zwei Netzwerkanschlüsse.

In Abbildung 3.7 sendet der PC 1.2 (Netz 1, PC 2) an den PC 2.1 (Netz 2, PC 1) Daten. Unterstellen Sie in diesem Beispiel eine Subnetzmaske von 24 Bit (255.255.255.0), können Sie zunächst feststellen, dass sich der PC 1.2 und der PC 2.1 nicht im selben IP-Netz befinden, daher kann man sagen: Der PC 2 aus dem Netz 1 möchte mit dem PC 1 aus dem Netz 2 kommunizieren.

Aus Gründen der Übersichtlichkeit habe ich die IP-Adresse auf zwei Bytes verkürzt. Eine korrekte IP-Adresse würde z.B. 192.168.1.2 oder 192.168.2.1 sein.

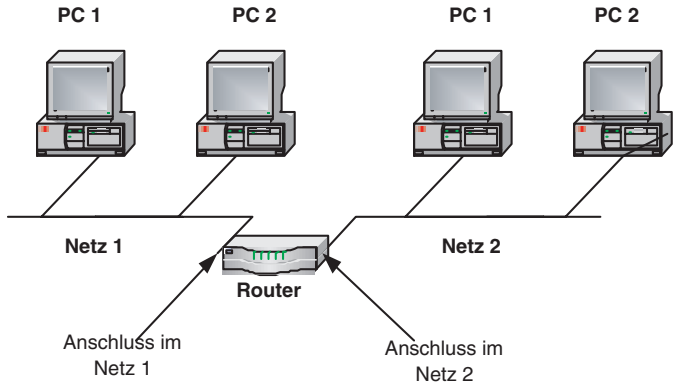

Abbildung 3.7 Routing von 1.2 zu 2.1

Weil beide Rechner unterschiedlichen IP-Netzen angehören, können sie nicht direkt miteinander kommunizieren. Das gilt auch dann, wenn Sie sie mit einem gedrehten Kabel (vgl. Kapitel 6.1.4, Cross-Kabel) direkt verbinden würden. Ein PC rechnet aus, ob die Zieladresse im eigenen Subnetz liegt. Wenn das nicht der Fall ist, dann braucht er

einen so genannten Routing-Eintrag. Hat er keinen Routing-Eintrag, ist das Ziel für den PC nicht erreichbar.

PC 1.2 schickt die Daten also zu seinen Standardgateway, diese Adresse muss in seinem IP-Netz liegen, z.B. die IP-Adresse 1.10. Der Router hat eine Verbindung zum Netz 2 über sein Interface 2.10 und sendet also die Datenpakete an den Rechner 2.1 über sein Interface 2.10.

Stellen Sie sich einen DSL/ISDN-Router vor. Dieser hat zwei Interfaces, eines in Ihrem LAN (= Netzwerk), eines zum Provider (DSL/ISDN). Der Router hat nur zwei Einträge:

- Das Netz 192.168.1.0/24 leite über die Netzwerkkarte 1.
- Alle anderen Netze (0.0.0.0) leite über DSL/ISDN zum Provider.

Der letzte Eintrag heißt Default-Routing. Ist kein anderer Routing-Eintrag genauer, dann wird das Default-Routing ausgeführt.

Exkurs

Sie können sich den Weg eines Datenpaketes zum Ziel ansehen. Der Befehl dazu heißt Traceroute. Unter Windows wählen Sie **Start · Ausführen**... `cmd` und geben dann in der DOS-Box beispielsweise: `tracert www.web.de`: Sie erhalten eine Auflistung der Knotenpunkte (= Router) vom eigenen Rechner bis zum Ziel im Internet. Abbildung 3.8 zeigt, wie ein solches Ergebnis aussehen kann. Weitere Informationen zu Traceroute finden Sie in Kapitel 10.1.2, Bordmittel der Betriebssysteme.

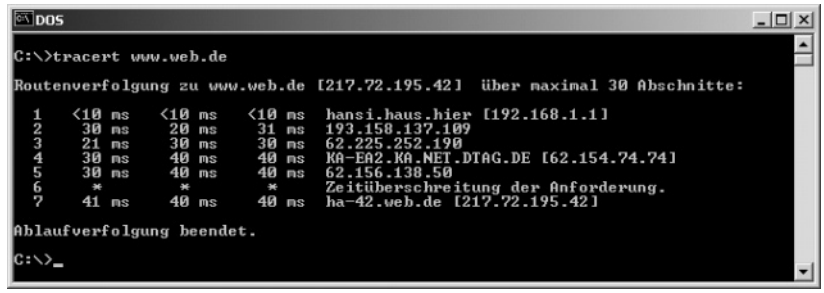

Abbildung 3.8 Traceroute vom eigenen PC zu web.de

Routing-Einträge, also die Information, welches Ziel über welchen Router erreichbar ist, können auf zwei verschiedene Arten in den Router gelangen:

- **Statisch:** manuell eingetragen
- **Dynamisch:** durch Informationsaustausch zwischen Routern

Die **statischen Routen** werden oftmals von Hand gepflegt und genauso konfiguriert wie eine IP-Adresse. Moderne Betriebssysteme helfen ein wenig und fügen Routen automatisch für die Netze ein, für die ein Anschluss existiert.

Dynamische Routen werden durch so genannte Routing-Protokolle gelernt. Router tauschen Informationen über die von ihnen erreichbaren IP-Netze, aus, einschließlich der IP-Netze von denen sie durch andere Router gehört haben. Zusätzlich zu der Information IP-Netz und Router wird angegeben, wie günstig (d.h. nah, schnell) die Route zu dem IP-Netz ist.

Bekommt ein Router (X) die Information von einem Nachbarrouter (Y), dass jener das IP-Netz A mit 5 Schritten erreichen kann, so verbreitet Router X, dass **er** das IP-Netz A mit 5 + 1 = 6 Schritten erreichen kann.

Bekannte Beispiele für Routing-Protokolle sind: RIP, OSPF und (E)IGRP. Ich werde nicht weiter auf Routing-Protokolle eingehen, da sie für die meisten von Ihnen keine Rolle spielen werden, weil sie erst in größeren Netzwerken zum Einsatz kommen.

3.2.3 Private IP-Adressen

Als ich schrieb, dass IP-Adressen durch die Organisation RIPE vergeben werden, haben Sie sich vielleicht gefragt, ob Sie eine IP-Adresse für Ihr Netzwerk beantragen müssen. Die Antwort lautet: »Das kommt darauf an!«

Offizielle IP-Adresse(n)

IP-Adressen, die aus dem Internet erreichbar sein sollen, müssen eindeutig sein. Dafür sorgt die RIPE, normalerweise über die Internetprovider. Diese haben ihrerseits einen Pool von offiziellen IP-Adressen zur Verfügung und leihen jedem Kunden für die Dauer der Einwahl eine IP-Adresse.

Wenn Sie IP-Adressen für Ihr lokales LAN benötigen, kommt es selten zu Problemen: Benutzen Sie und jemand anderes gleichzeitig dieselbe Adresse, dann ist diese zwar nicht eindeutig, aber sie stören sich nicht gegenseitig, weil ihre beiden Netze nicht verbunden sind. Verbinden Sie Ihr Netz dagegen mit dem Internet, verbinden Sie es ja gleichzeitig mit vielen anderen Netzen, und es käme zu einem Adresskonflikt, wenn eine IP-Adresse zweifach genutzt würde.

Für Ihr internes Netzwerk gibt es Adressbereiche, die im Internet nicht verwendet werden und deren IP-Adressen nicht aus dem oder in das Internet transportiert werden:

- Class C: 192.168.0.0 bis 192.168.254.0
- Class B: 172.16.0.0 bis 172.31.255.0
- Class A: 10.0.0.0

Für ein kleines Netz mit weniger als 255 Rechnern benutzt man ein IP-Netz aus dem Klasse-C-Bereich, z.B. 192.168.1.0/24. Entsprechend reichen die IP-Adressen dieses IP-Netzes von 192.168.1.1 bis 192.168.1.254.

Vergeben Sie IP-Adressen nicht mit der Gießkanne, planen Sie ein wenig. Die Administration eines Netzwerks wird umso einfacher, je systematischer Sie IP-Adressen vergeben. Sie erhalten im Idealfall so genannte sprechende IP-Adressen. Das folgende Schema bietet eine Orientierung für ein Klasse-C-Netz:

- 192.168.1.200 – 192.168.1.249 = Drucker
- 192.168.1.100 – 192.168.1.199 = PC-Clients
- 192.168.1.20 – 192.168.1.29 = Linux-Server
- 192.168.1.10 – 192.168.1.19 = Windows-Server
- 192.168.1.1 = Routerinterface

Sobald Sie eine IP-Adresse genannt bekommen, wissen Sie sofort, um welche Art von Netzwerkteilnehmer es sich handelt, und können gezielt Hilfe leisten.

3.2.4 NAT, Network Address Translation

Die meisten Netzwerke sollen mit dem Internet verbunden werden. Damit ein PC aus einem lokalen Netz direkt mit dem Internet kommunizieren kann, benötigt er eine offizielle IP-Adresse. Sollen also zehn PCs gleichzeitig auf das Internet zugreifen, so benötigen Sie zehn offizielle IP-Adressen. Weil sich das Problem vergrößert, je mehr Rechner gleichzeitig auf das Internet zugreifen sollen, und weil IP-Adressen knapp, sind, wurden zwei Lösungen erfunden: NAT und Proxy.

Das Grundprinzip von NAT ist einfach: Beispielsweise ersetzt ein Router die privaten Adressen des internen LAN in den Datenpaketen (z.B. 192.168.4.2) durch die ihm vom Internetprovider zugewiesene offizielle

IP-Adresse (z.B. 62.182.96.204). Wenn die Antworten aus dem Internet kommen, erreichen diese zunächst den Router, der sich gemerkt hat, welche Daten zu welchem Ziel gesandt wurden, und er kann die Antwortpakete dem ursprünglichen internen PC zuordnen. Der Router tauscht im Antwortpaket die Ziel-IP-Adresse 62.182.96.204 gegen die private IP-Adresse 192.168.4.2 aus und schickt dem PC das Paket.

Exkurs

Der Router bedient sich dabei der UDP-/TCP-Port-Nummern. Ein IP-Paket enthält ein UDP- oder TCP-Paket. Das UDP-/TCP-Paket enthält zwei Ports, den Ziel-Port und den Ursprungs-Port. Der Router baut sich eine Tabelle auf, in der er sich notiert, an welchen PC Antworten geschickt werden müssen:

Ursprungs-IP	Ursprungs-Port	offizielle IP-Adresse	Neuer Port	Ziel IP-Adress	Ziel-Port
192.168.1.23	1333	80.44.53.222	5555	62.34.5.6	80
192.168.1.77	23675	80.44.53.222	5556	10.77.33.2	25

Tabelle 3.1 NAT-Tabelle

Wenn im obigen Beispiel der Router ein IP-Paket für seine offizielle IP-Adresse und den TCP-Port 5555 empfängt, weiß er, dass er das Paket an die IP-Adresse 192.168.1.23 auf dem TCP-Port 1333 weiterleiten muss.

Betrachtet man den Router vom Internet aus, so scheint er ein »Super-Surfer« zu sein, weil er sehr viele gleichzeitige Anfragen ins Internet schickt.

Der Vorteil von NAT ist, dass man für ein ganzes Netzwerk mit PCs, die auf das Internet zugreifen, nur eine offizielle IP-Adresse benötigt. Anders ausgedrückt: Sie benötigen NAT, wenn Sie mit nur einer offiziellen IP-Adresse mehreren PCs den Zugriff auf das Internet ermöglichen wollen. NAT wird übrigens unter Linux Masquerading genannt.

Das LAN ist unsichtbar.

Ein weiterer Vorteil von NAT ist, dass ein potenzieller Angreifer nur den Router im Internet erkennen kann, weil nur der Router bei der Kommunikation ins Internet in Erscheinung tritt. Der Hacker bzw. Cracker weiß nicht, dass sich hinter dem Router ein ganzes Netzwerk verbirgt. Man versteckt also durch NAT die eigene Netzwerkstruktur und macht es so einem Hacker/Cracker schwieriger, die für ihn eigentlich interessanten PCs im LAN anzugreifen. NAT und eine Firewall ergänzen sich. Genaueres dazu erfahren Sie in Kapitel 11.1.2, Sicherheitsprobleme im Überblick, mehr.

Leider gibt es einige Anwendungen, die nicht mit NAT zusammenarbeiten. Die meisten von diesen Anwendungen verarbeiten die IP-Adresse in der Applikation, dadurch kommt es zu Problemen, wenn die tatsächliche Absender-IP-Adresse nicht mit der Absender-IP-Adresse der Applikationsdaten identisch ist.

Ein weiterer Nachteil von NAT ist, dass Sie keine Dienste aus dem LAN im Internet anbieten können. Wenn ein Client aus dem Internet auf einen Webserver in Ihrem LAN zugreifen möchte, kann der NAT-Router die Anfrage keinem PC zuordnen, sodass die Anfrage abgewiesen wird.

Exkurs

Das Problem lösen die meisten DSL-Router so, dass über eine Funktion, z. B. **Virtual Server** genannt, Verbindungen auf einem bestimmten TCP/UDP-Port immer zu einem PC im LAN weitergeleitet werden. Das ist z. B. auch der Fall für die Einstellungen im eDonkey-Netzwerk.

3.2.5 Proxy

Während NAT auf Schicht 3 des ISO-/OSI-Modells arbeitet und lediglich IP-Adressen austauscht, arbeitet ein Proxy auf Schicht 7. Das ermöglicht dem Proxy, Benutzer auf der Applikationsebene zu authentifizieren, sodass sich steuern lässt, wer auf das Internet zugreifen darf und wer nicht.

Proxy bedeutet auf deutsch Stellvertreter. Der PC, auf dem der Proxy-Dienst läuft, wird Proxy-Server genannt. Ihm kommen zumindest zwei Aufgaben zu:

- Anfordern und Weiterleiten der Internetseiten
- Zwischenspeichern von Internetseiten

Ein PC im lokalen Netz fordert eine Internetseite (HTTP, FTP u. a.) beim Proxy-Server an, behandelt den Proxy also wie einen Webserver. Der Proxy-Server fordert die Seite, falls erforderlich, bei dem entsprechenden Webserver im Internet an, und der Webserver antwortet dem Proxy, behandelt ihn also wie einen Client.

Proxy-Cache

Die Seiten, die der Proxy angefordert und bekommen hat, speichert er in seinem Proxy-Cache zwischen. Wird die Seite vom Client erneut angefordert, so fordert der Proxy die Seite vom Webserver mit der Bedingung an, dass sie nur dann übertragen werden soll, wenn sie sich seit der letzten Anforderung verändert hat. Damit wird verhindert, dass die immer gleichen Seiten aus dem Internet – mit entsprechender Zeitverzögerung – übertragen werden.

Da der Proxy alle Anfragen ins Internet stellt, wird ähnlich wie bei NAT nur eine offizielle IP-Adresse benötigt. Das gesamte Netzwerk versteckt sich hinter dem Proxy-Server, sodass es für Hacker/Cracker unsichtbar ist.

Der Proxy-Dienst muss alle Protokolle beherrschen, für die er Proxy ist, beherrschen. Das führt insbesondere bei Audio- und Videosoftware, die über das Netzwerk arbeitet, zu Problemen, weil diese Software teilweise nicht Proxy-fähig ist.

3.2.6 IP Version 6

Die Zukunft hat begonnen.

Die bekannte und weltweit im Einsatz befindliche IP-Version ist die Version 4. IPv6 oder auch IPnG (IP next Generation) wird der Nachfolger von IPv4[5] sein. Bei dieser Aussage sind sich alle Experten einig. Die Frage, auf die man von zehn Experten zwölf Antworten bekommt, ist: Wann wird IPv6 IPv4 ersetzen?

IPv6 ist schon älter, als Sie annehmen werden. Die ersten Schritte zur Normung sind bereits 1994 unternommen worden. Die Normungen werden von der IETF vorgenommen. Nach den damaligen Berechnungen sollten die vorhandenen IP-Adressen im Internet nur noch bis 2005 reichen und man sah sich daher gezwungen, auf eine IP-Version mit mehr Adressraum umzusteigen. Man erwartet heute, dass durch den Boom der mobilen Datenkommunikation über das Internet (UMTS, iMode) ein sehr großer Bedarf an IP-Adressen entstehen wird, sodass in den nächsten Jahren IPv6 eingesetzt werden wird.

Exkurs

Die meisten mobilen Technologien setzen auf eine Always-on-Funktion. Das mobile Gerät ist immer im Internet erreichbar, lediglich die Datenübertragung muss bezahlt werden. Es handelt sich dann um ein volumenbasiertes Abrechnungsmodell, wie es häufig bei DSL-Providern anzutreffen ist. Der Boom ist bisher ausgeblieben. Bei der Umsetzung vom UMTS treten immer weitere Verzögerungen ein, für den Sommer/Herbst 2003 sind aber die ersten Starts in Deutschland angekündigt.

Eigentlich hat IPv6 gegenüber IPv4 nur Vorteile:

- Der Adressraum beträgt 2^{128} statt 2^{32} Adressen.
- Mehr Sicherheit (IPSec ist Bestandteil von IPv6)
- Die Autokonfiguration (ähnlich DHCP) ist Bestandteil von IPv6.

5 IPv5 ist übrigens nicht existent, nur falls es jemand von Ihnen vermisst.

- Schnellere Routing-Algorithmen sind durch die bessere IP-Struktur möglich.
- Quality of Service wird möglich (feste Bandbreiten z. B. für Video).
- Die neue Möglichkeit Anycast ist ideal für redundante Server-Systeme.

Leider sind mit der technischen Umrüstung auch finanzielle Investitionen verbunden. Davon sind weniger die Endgeräte (PCs, Server) betroffen, die lediglich einen neuen IP-Treiber bekommen, als vielmehr die Infrastruktur des Internets, wo alle Router das neue IPv6 beherrschen müssen. Das bedingt oft den Austausch der Hardware. Es wird daher einen sanften Umstieg auf IPv6 geben, der einige Jahre dauern wird. Auf diese Situation ist IPv6 eingerichtet. Es gibt explizite Migrationstechnologien.

Für Windows ist der IPv6-Treiber (Protokollstack) bei Microsoft in einer Beta-Version erhältlich. Linux bringt in aktuellen Distributionen die IPv6 Unterstützung für den Kernel mit.

Wenn Sie IPv6 ausprobieren möchten, dann finden Sie nähere Informationen unter **http://www.6bone.net**. Dort können Sie sich bei einem so genannten Tunnelbroker anmelden und dann über Ihre (IPv4) Internetverbindung das IPv6-Protokoll – verpackt in IPv4-Datenpaketen – übertragen. Viele sinnvolle Anwendungen gibt es allerdings noch nicht.

3.3 Transmission Control Protocol (TCP)

Das Transmission Control Protocol dient u. a. zur Überwachung der Kommunikation über IP. Weder Ethernet noch IP bieten Möglichkeiten, zu überprüfen, ob alle Datenpakete ankommen. Defekte Datenpakete werden einfach weggeworfen. TCP arbeitet auf der ISO-/OSI-Schicht 4.

TCP regelt zunächst den Verbindungsaufbau (Three-way-handshake). Der Sender wendet sich also an den Empfänger: »Ich möchte Daten schicken!« Der Empfänger antwortet: »OK«, worauf der Sender sein Vorhaben mit »Gut, dann fang' ich jetzt an!« beginnt und die eigentlichen Datenpakete sendet.

Der Verbindungsabbau ist ähnlich umständlich: »Ich bin fertig mit Senden.« »Ich habe auch nichts mehr!« »Ich baue dann die Verbindung ab!« »Ist gut!«. Das Ganze dient dem Ziel, dass zwei Rechner miteinander kommunizieren, als ob sie allein auf der Welt wären und eine direkte Verbindung zueinander hätten.

TCP handelt aus, nach wie vielen gesendeten Bytes eine Bestätigung über empfangene Pakete gesendet werden muss. Kommt die Empfangsbestätigung nicht, weil z.B. ein einzelnes Paket verloren gegangen ist, werden die nicht bestätigten Pakete alle noch einmal gesendet. Man könnte den Vorgang als empfängerseitige Flusskontrolle bezeichnen.

Woher weiß Ihr Betriebssystem, welche Anwendung welche Datenpakete bekommt, wenn Sie gleichzeitig im Internet surfen und E-Mails abrufen?

Die TCP-Ports (gilt analog für UDP-Ports) haben eine eindeutige Nummer für eine Anwendung. Man unterscheidet Server- und Client-Ports. Erstere sind einheitlich festgelegt, letztere sind zufällig. Jeder Rechner besitzt die Textdatei *services*, die die Zuordnung der Server-Ports zu den Anwendungen enthält. So ist der TCP-Server-Port 80 für HTTP reserviert. Die Client-Ports sind immer größer als 1024 (bis maximal 65536) und werden dynamisch für die Client-Anwendung vergeben.

Erhält Ihr PC ein Datenpaket, so steht im TCP-Paket, von welchem Quell-TCP-Port die Daten verschickt wurden und an welchen Ziel-TCP-Port (Client-Port) sich das Datenpaket wendet. Das Betriebssystem kann das Datenpaket eindeutig einem Anwendungsprozess zuordnen, wie man in Abbildung 3.9 sehen kann.

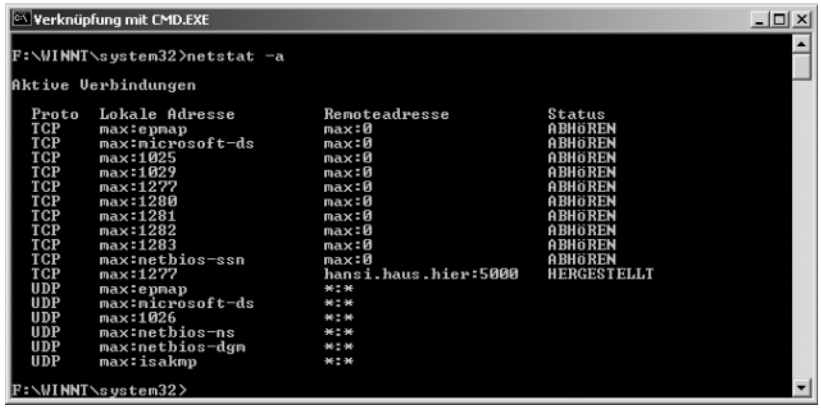

Abbildung 3.9 netstat –a listet alle TCP/UDP-Verbindungen auf.

Es gibt eine normierende Behörde, die IANA (**http://www.iana.com**), die weltweit diese Nummern – Ports – vergibt. Dort erhält man auch eine stets aktuelle Datei mit den Zuordnungen, die Sie als *services* einsetzen können.

UDP, User Datagram Service, ist auf der gleichen Schicht (ISO-/OSI-Schicht 4) wie TCP angesiedelt. UDP ist ein so genanntes verbindungsloses Protokoll. Im Gegensatz zu TCP wird bei UDP die Kommunikation nicht kontrolliert: Daten werden einfach gesendet, egal, ob der Empfänger damit etwas anfangen kann und ob die Daten ankommen oder nicht. Man erreicht natürlich deutlich höhere Netto-Datendurchsatzraten, weil viel Overhead wegfällt. Einige Anwendungen verwenden UDP und kontrollieren den Erfolg der Kommunikation auf Applikationsebene (ISO-/OSI-Schicht 7).

3.4 Address-Resolution Protocol (ARP)

Das ARP hat die Aufgabe, IP- in MAC-Adressen aufzulösen. Es handelt sich um eine sehr wichtige Funktion, die auf ISO-/OSI-Schicht 3 arbeitet. Wenn Ihr PC ein IP-Paket in einem Netzwerk versenden möchte, muss dieses Paket in ein Ethernet-Paket verpackt werden. Der Ethernet-Frame wird mit der MAC-Adresse versehen, doch welche MAC-Adresse gehört zur Ziel-IP-Adresse?

Diese Frage wird durch ARP beantwortet. Dabei ist ARP wenig geschickt, es versendet eine Broadcast-Nachricht an alle Stationen mit der Frage »Welche MAC hat 192.168.1.4?« Die Station, die diese IP-Adresse hat, meldet sich mit »192.168.1.4 hat 00:08:90:4b:33:2e«. Damit kann das Ethernet-Paktet erzeugt und versendet werden. Für eine festgelegte Dauer (zwei bis 20 Minuten) merkt sich der PC nun die Zuordnung der IP- zur MAC-Adresse im so genannten **ARP-Cache**. Die Informationen dieses Caches kann man bei Windows und Linux mit dem Kommando: `arp -a` auslesen. Das Ergebnis mit einem Eintrag können Sie sich in Abbildung 3.10 ansehen.

Abbildung 3.10 ARP-Cache mit einem Eintrag

Exkurs

Das oben beschriebene Verfahren kann man als dynamisches Lernen bezeichnen. Man kann auch statisch Einträge in den ARP-Cache einfügen, diese haben Vorrang vor den dynamischen Einträgen. Statische Einträge kann man ebenfalls mit dem Kommando `arp` hinzufügen. (dazu mehr in Kapitel 10.1.2, Bordmittel der Betriebssysteme)

3.5 Internet Control Message Protocol (ICMP)

ICMP ist Bestandteil aller TCP/IP-Implementierungen und damit auf jedem Rechnersystem verfügbar. Die TCP/IP-Implementierungen werden übrigens auch als IP-/TCP-Stack bezeichnet. Die Aufgabe von ICMP ist es, Fehler- und Diagnoseinformationen an die Kommunikationspartner zu übermitteln. Es ist ein Hilfsprotokoll zu IP und parallel zu IP auf der ISO-/OSI-Schicht 3 angesiedelt.

Der bekannteste Teil des ICMP ist der `ping`-Befehl. Technisch gesehen handelt es sich beim `ping` um ein *ECHO request* und ein *ECHO response* des ICMP. Dabei werden von ICMP zusätzlich Zeitinformationen erfasst, die Auskunft über die Paketlaufzeit geben. Diese Laufzeiten sind neben der Frage, ob ein Ziel überhaupt erreichbar ist, eine wichtige Information für Sie. An ausgefallenen Paketen (*Packet loss*) und/oder schwankenden Laufzeiten kann man Probleme im Netzwerk erkennen und diese dann eingrenzen.

Über ICMP werden weitere Informationen transportiert: z.B. *Source Squench*, wenn der für Datenpakete reservierte Puffer vollgelaufen ist, *Destination unreachable* wenn ein Zielrechner nicht erreichbar ist, *Time out* wenn die maximale Laufzeit eines Datenpaketes erreicht wurde, oder *Redirecting* wenn der Sender in Zukunft einen anderen, günstigeren Weg zum Ziel nehmen soll. Insgesamt gibt es zurzeit 24 ICMP-Pakettypen.

Insbesondere das *Redirecting* ist eine ernst zu nehmende Sicherheitslücke, weil Hacker mit seiner Hilfe Datenströme beliebig umleiten können. Dabei befiehlt der Hacker einem Rechner im Internet, dass dieser den gesamten Datenverkehr über den eigenen Rechner des Hackers laufen lassen soll. So erlangt der Hacker die Möglichkeit, Ihre Daten komplett mitzulesen.

Das war selbstverständlich nicht der ursprüngliche Sinn des *Redirecting*. Es dient dazu, einem Rechner oder Router im Netzwerk bzw. Internet mitzuteilen, dass es einen kürzeren Weg gibt und welcher das ist.

3.6 Simple Network Management Protocol (SNMP)

SNMP wurde, so wird es auf Seminaren gern erzählt, in der Kneipe erfunden. Stellen Sie sich vor, Sie haben 200 Netzwerkkomponenten. Wie hoch ist die Wahrscheinlichkeit, dass eine dieser Komponenten ausfällt oder überlastet ist, und wie hoch ist die Wahrscheinlichkeit, dass Sie automatisiert darüber informiert werden?

Aus diesen und ähnlichen Überlegungen ist SNMP erfunden worden. Es besteht aus zwei Komponenten: aus dem SNMP-Agenten, der Hardware- und Softwareinformationen in Variablen ablegt, und aus der Managementkonsole, die die Intelligenz besitzt, um diese Variablen zyklisch bei allen Geräten abzufragen und in eine Datenbank zu schreiben, möglicherweise Alarme zu generieren und Statistiken zu erstellen.

Der dumme Agent schreibt beispielsweise jede Sekunde die aktuelle CPU-Last in eine Variable, die Mangementkonsole holt jede Sekunde den Wert ab und kann daraus einen Graphen entwickeln. Sobald die CPU-Last für die Dauer von fünf Minuten über 97% steigt, wird ein Alarm am Bildschirm des Administrators ausgelöst.

Die Summe der Variablen heißt MIB, Management Information Base. Die Werte werden per SNMP ausgelesen. Die Mangementkonsole ist ein PC mit einer Software, die die notwendigen zyklischen Abfragen durchführt.

Damit nicht jeder beliebige Teilnehmer beispielsweise das Telnet-Zugangspasswort per SNMP auslesen kann, gibt es ein SNMP-Passwort, die so genannte *Community*. Meist gibt es zwei Communities: *read*, um auszulesen, und *write*, um zu schreiben – schließlich können Sie mittels SNMP auch Werte setzen, z. B. die IP-Adresse oder den Namen des Verwalters. Standardmäßig heißt die *read-Community* `public` und die *write-Community* `private`. Da die Passwörter bei jeder Anfrage im Klartext übertragen werden – also möglicherweise mehrfach pro Sekunde –, stellen diese Passwörter für einen Angreifer keine echte Hürde dar. Es scheint aber so zu sein, dass nur wenige Menschen SNMP beherrschen, sodass noch kein riesiger Schaden über SNMP verursacht wurde.

Neben dem Auslesen und Setzen von Werten gibt es noch die Möglichkeit, Alarme zu generieren. Diese so genannten *Traps* werden direkt durch die betroffene Station an die festgelegte Management-Station

versendet. Üblicherweise ist das Starten eines Systems ein solcher Fall, es wird ein *Coldstart-Trap* oder Ähnliches von dem PC, Switch oder Router ausgesendet.

Weil zusätzlich zu den Traps der Stationen die Netzwerk-Managementstation (oder Managementkonsole) in regelmäßigen Abständen abfragt, werden Sie alarmiert, wenn eine Ihrer 200 Netzwerkkomponenten, z.B. ein Server, ausfällt. Sie bekommen einen Alarm (am Bildschirm, Handy o.Ä.) und können agieren, bevor der erste Benutzer den Ausfall bemerkt hat. Allerdings müssen Sie viel Geld für dieses proaktive Management investieren. Die Software für die Netzwerk-Managementstation kostet ab 25.000 € aufwärts. Es gibt auch freie Softwarelösungen, die aber nicht den Komfort der kommerziellen Lösungen bieten. Weitere Informationen finden Sie im Kapitel 10.2, Netzwerkmanagement.

3.7 Wireless LAN

Drahtlose Netzwerke haben – zumindest in der Theorie – viele Vorteile und sind zurzeit en vogue. Auch außerhalb der Netzwerke wird alles drahtlos: Tastaturen, Mäuse und Headsets sollen bald mit Bluetooth versorgt werden. Handys haben sich längst durchgesetzt. Dieser Trend setzt sich nun auch innerhalb des Netzwerks durch. Es sind jedoch zahlreiche Sicherheitslücken und andere Probleme zu beachten.

Das **ISM-Band** ist der Bereich von 2,4 GHz, auf dem jedermann innerhalb seines Grundstücks[6] mit der maximalen Sendeleistung von 100 mW – Handys senden mit bis zu zwei Watt – funken darf. Dem Benutzer entstehen keine Lizenzkosten o.Ä., und dieses Frequenzband ist – fast – international reserviert. Leider arbeiten auch Mikrowellen und andere Geräte auf diesem Frequenzband, sodass es vielfältige Störquellen gibt. Es bestehen einige Einschränkungen, sodass Sie sich bei einem Einsatz außerhalb von Deutschland zunächst über die rechtlichen Vorschriften des Landes informieren sollten (z.B. in Frankreich, Spanien und Japan).

Bluetooth: Bluetooth ist ein Standard nach IEEE 802.15 für Personal Area Networks (PANs). Weitere Informationen dazu finden Sie unter **http://www.bluetooth.org**. Bluetooth (dt. *Blauzahn*[7]) ist zur Versor-

6 Grundstücksübergreifend ist ein Netzwerk bei der Regulierungsbehörde TP anzeigepflichtig, aber genehmigungsfrei.

7 Der Name geht auf den dänischen Herrscher zurück, der die Einheit Dänemarks im Mittelalter herbeigeführt hat.

gung von Tastaturen, Mäusen und ähnlichem Zubehör gedacht. Man spricht in diesem Zusammenhang von Personal Area Networks (PANs). Bluetooth bietet eine Bandbreite von 1 Mbit/s, funkt im allgemein benutzbaren ISM-Band und hat eine Reichweite von bis zu 10 Metern. Zur Vernetzung von PCs wird Bluetooth keine Rolle spielen, weil die Bandbreite und die Reichweite zu gering sind. Zunehmend werden Internetzugangslösungen auf Basis von USB und Bluetooth angeboten. Von der *Bluetooth Special Interest Group* wurde sogar im August 2002 ein Standard für ISDN über Bluetooth verabschiedet. Dabei wurde die Entfernung hoch- und die Datenrate heruntergesetzt.

Sie können Daten per **Infrarot** übertragen. Viele Notebooks verfügen über einen so genannten IrDA-Port, der Infrarot ermöglicht. Die Übertragung erfordert Sichtkontakt zum Übertragungspartner und wird durch starke Sonnenstrahlung sehr gestört. Die Übertragungsraten liegen im Bereich von 1 Mbit/s. Auch diese Variante scheidet als flächendeckende Vernetzungsmethode aus.

Überall ins Internet

Weltweit nimmt die Anzahl der so genannten **Hot Spots** stark zu. Bei einem Hot Spot handelt es sich um einen öffentlichen Wireless-LAN-Zugang (WLAN), der meist einen Internetzugang ermöglicht. In Cafés der Kette *Starbucks* wurden in den USA 1200 Hot Spots installiert, in Flughäfen (z. B. München und Hannover) sollen Geschäftsreisende die Wartezeiten besser nutzen können, und auch Hotels haben erkannt, dass heutige Notebooks üblicherweise ab einem gewissen Preis über eine integrierte WLAN-Karte verfügen. Die Anzahl der Hot Spots steigt ständig, einen Überblick bezüglich Hot Spots in Ihrer Nähe können Sie sich unter **http://mobileaccess.de/wlan** verschaffen.

Vor nicht allzu langer Zeit träumten einige davon, dass WLAN **UMTS** die Butter vom Brot nehmen könnte. WLAN ist ohne Lizenzkosten verwendbar, während für UMTS-Lizenzen Milliardenbeträge gezahlt wurden. Von einigen Fachleuten, unter anderem von der RegTP, der Regulierungsbehörde für Telekommunikation und Post, wird WLAN jetzt als Hilfe für UMTS angesehen. Dabei geht man davon aus, dass sich die Reichweite von UMTS und die Datenrate von WLAN ergänzen und zu einer höheren Kundenakzeptanz führen. In der Nähe von Hot Spots sollen die Handys WLAN nutzen und dem Anwender für Datenanwendungen bis zu 54 Mbit/s zur Verfügung stellen, an allen anderen Orten kann der Benutzer über die Bandbreite von maximal 2 Mbit/s über UMTS verfügen.

Für alle WLAN-Varianten und UMTS gilt gleichermaßen, dass es sich bei den angegebenen **Datenraten** um Bruttodatenraten handelt, deren Bandbreite sich alle Teilnehmer teilen und von denen noch Steuerungsdaten abgezogen werden müssen, um die Nettodatenrate zu erhalten.

3.7.1 IEEE 802.11b

Der zurzeit in Deutschland erhältliche und inzwischen bezahlbar gewordene WLAN-Standard ist IEEE 802.11b. Datenraten von – theoretisch – 11 Mbit/s sind bereits sehr attraktiv für den Anwender. Die Nutzdatenrate liegt – ebenfalls theoretisch – bei maximal 7, durchschnittlich bei 5 bis 6 Mbit/s und alle Stationen teilen sich diese Bandbreite.

Geteilte Bandbreite

Gibt es also sieben Stationen, die einen WLAN-Zugang (Accesspoint) benutzen, dann steht im Idealfall jeder Station 1 Mbit/s zur Verfügung. Ein multimediales Erlebnis wird sich über den Zugang wohl nicht transportieren lassen, insbesondere, wenn man bedenkt, dass die tatsächlichen Datenraten unter den oben genannten liegen.

WLAN nach IEEE 802.11 definiert dabei die Schichten 1 und 2 des ISO-/OSI-Modells. Dank der Unabhängigkeit der Schichten ergeben sich z.B. für IP, TCP und andere höhere Protokollschichten keine Auswirkungen.

Es gibt zwei Möglichkeiten für den Betrieb eines WLANs:

- Im **Ad-hoc-Modus** funkt eine WLAN-Karte zu einer anderen WLAN-Karte. Dabei können mehrere WLAN-Verbindungen gleichzeitig bestehen. Der einzige Nachteil im Vergleich zum Infrastruktur-Modus ist die geringere Sende- und Empfangsleistung. Andere Ausdrücke sind: Peer-to-Peer-Netz oder Independent Basic Service Sets (IBSS).
- Der **Infrastruktur-Modus** kann betrieben werden, wenn man über mindestens einen Accesspoint (AP) verfügt. Ein AP ist eine Empfangsanlage, meist mit integrierter Antenne für ein WLAN, und wird üblicherweise mit Steckernetzteilen oder über das LAN-Kabel mit Strom versorgt. Üblicherweise stellt der AP auch die Verbindung zum drahtgebundenen LAN her. Teilweise wird die Bezeichnung Basic Service Set (BSS) verwendet.

Welchen Modus sollte man einsetzen, werden Sie sich sicherlich fragen. Die Preise für einen Accesspoint liegen über den Preisen für PC-

WLAN-Adapter, allerdings haben Hersteller günstige WLAN-DSL-Router zu Kampfpreisen auf den Markt gebracht, sodass sich ein reines Ad-hoc-WLAN nur noch selten lohnt. Im Ad-hoc-Modus wird ein WLAN aufgebaut, wenn man nur eine begrenzte Zahl von Clients untereinander verbinden will. Insbesondere ist es nicht ohne weiteres möglich, den WLAN-Clients eine Verbindung ins drahtgebundene LAN zu ermöglichen.

Im Infrastruktur-Modus mit AP melden sich die WLAN-Clients bei einem AP an; die Sicherheitseinstellungen bestimmen, ob das in jedem Fall erfolgreich ist (vgl. Kapitel 3.7.3, Sicherheit von WLAN).

Ein wesentlicher Unterschied zwischen drahtgebundenen und drahtlosen Netzen aus physikalischer Sicht ist, dass man bei einem drahtlosen WLAN keine Kollisionen erkennen kann. Im Ethernet kann es aber aufgrund des nicht-deterministischen Zugangsverfahrens immer zu Kollisionen kommen, die bei IEEE 802.3 durch das CSMA/CD-Verfahren behandelt werden. Wenn man Kollisionen nicht erkennen kann, ist es auch nicht möglich, den Fall einer Kollision zu behandeln. Bei WLAN gilt daher: CSMA/**CA** steht für **Collision Advoidance**, die Kollisionsvermeidung. Bei diesem Verfahren hört die sendewillige Station das Medium – also den Funkkanal – ab und wartet, falls dieser frei ist, eine weitere definierte Zeit (IFS = Interframe Space) ab. Ist das Medium am Ende der Wartezeit immer noch frei, wird gesendet. Dabei muss man beachten, dass der Mechanismus nur dann funktioniert, wenn sich alle Stationen gegenseitig empfangen können.

Stellen Sie sich vor, dass drei Stationen im Abstand von jeweils 100 Metern voneinander aufgestellt werden, sodass die beiden äußeren Stationen 200 m entfernt sind und sich nicht gegenseitig empfangen können (vgl. Abbildung 3.11). Möchten die Stationen A und C zur Station B senden, so kann der CSMA/CA-Mechanismus keine Kollisionen verhindern, weil die Station A nicht feststellen kann, dass gleichzeitig die Station C sendet, und daher das Medium als frei erkennt.

Es kann und wird bei WLANs also zu Kollisionen kommen. Daher wurde schon auf dieser Protokollschicht – eigentlich wäre das Aufgabe von z. B. TCP – ein Sicherungsmechanismus implementiert. Gesendete Pakete werden vom Empfänger durch ein **ACKnowledge** bestätigt. Kommt das ACK nicht, beginnt die Sendestation mit der Wiederholung (Retransmission) nach einer definierten Zeit.

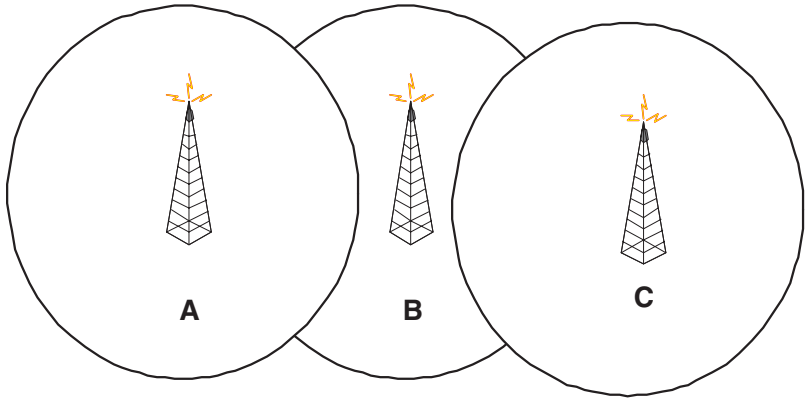

Abbildung 3.11 WLAN ohne CSMA/CA-Funktion

WEP, Roaming ...

Der IEEE 802.11b-Standard lässt einige Fragen offen. So ist die oft eingesetzte WEP-Verschlüsselung nur optionaler Bestandteil und eine Regelung für das Roaming, das Wandern zwischen verschiedenen APs, gibt es gar nicht. Andere Ungenauigkeiten führten dazu, dass bis vor kurzem die Komponenten eines Herstellers zu denen von anderen Herstellern inkompatibel waren und es heute teilweise noch sind. Abhilfe schafft die WiFi-Alliance[8]. Diese zertifiziert die Kompatibilität zwischen den beteiligten Herstellern durch das WiFi-(Wireless Fidelity-) Zertifikat. Dadurch arbeiten heute die meisten WLAN-Komponenten verschiedener Hersteller zusammen. Weil man sich nicht darauf verlassen kann, muss man es ausprobieren.

Exkurs

Sie sollten nach Möglichkeit nur Geräte eines Herstellers einsetzen, weil es Funktionen gibt, die Ihnen nur dann zur Verfügung stehen, wenn Sie die Geräte vom gleichen Hersteller haben, und weil sich bei Problemen die Hersteller gegenseitig die Schuld für die Inkompatibilität zuweisen werden und Sie am Ende der Leidtragende bleiben.

Eine standardisierte Funktion von IEEE 802.11b ist es, eine niedrigere Datenrate auszuhandeln, wenn die Empfangsbedingungen schlechter werden. Der Standard ist abwärtskompatibel zu IEEE 802.11, welcher zwei Datenraten von 1 oder 2 Mbit/s ermöglicht. IEEE 802.11b hat 4 Bandbreitenstufen von 11, 5,5, 2 und 1 Mbit/s. Dabei gilt, dass die möglichen 11 Mbit/s nur in Idealfällen zustande kommen, wenn die Stationen in unmittelbarer Nähe zueinander oder zum AP aufgebaut sind. Wenige Zentimeter entscheiden zum Schluss über den Empfang;

8 Die Alliance hieß bis September 2002 WECA, d.h. Wireless Ethernet Compatibility Alliance.

man spricht von Link. Zwischen den Herstellern gibt es massive Unterschiede, was die Sende- und Empfangsqualität angeht. Dabei ist Stahlbeton der Killer aller Funkverbindungen. Es kommt beim Aufstellen eines AP sehr auf die geschickte Standortwahl an, um den WLAN-Clients möglichst gute Datenraten bieten zu können. Dabei bietet ein AP gegenüber vielen Karten den Vorteil einer Antenne, die bei WLAN 12,5 cm misst.

Test Das Magazin *tecchannel* hat Modelle verschiedener Hersteller getestet (**http://www.tecchannel.de/hardware/620/index.html**) und herausgefunden, dass die Sendequalität der einzelnen Hersteller sich signifikant unterscheidet. Weitere Unterschiede ergeben sich bei der Handhabung oder dem Komfort bei der Installation und bei der Benutzung.

Die Produkte verschiedener Hersteller unterscheiden sich einerseits in der Qualität der Hardware, andererseits aber auch in der mitgelieferten Software, die bei WLAN-Karten eine wesentlich größere Rolle als bei normalen Netzwerkkarten spielt. Insbesondere die Software zur Administration eines AP sollte komfortabel sein und eine breite Funktionsfülle bieten. Häufig sind die Tester von *tecchannel* jedoch auf weniger komfortable Lösungen gestoßen.

Die meisten APs bieten zur Konfiguration eine Web-Konsole an, alternativ oft noch eine Telnet-Konsole für fortgeschrittene Anwender. Über das Web-Interface werden vor allem die Sicherheitseinstellungen vorgenommen. Ein weiteres Kriterium zur Auswahl eines AP kann die Managebarkeit mittels SNMP sein, wenn Sie dieses Protokoll für das Management Ihrer Komponenten einsetzen.

Die Software für die WLAN-Karten – meist im PCMCIA-Format – umfasst in der Regel die Information über aktuelle Sende- und Empfangsleistung, Paketverlust usw. Nähere Informationen finden Sie in Kapitel 9, Betriebssystem(e) einrichten.

Exkurs Mittels IEEE 802.11b lassen sich mit Richtfunkantennen auch längere Strecken überbrücken, wenn Sichtkontakt besteht. Möglich sind ein bis zwei Kilometer bei relativ geringen Datenraten. Diese Verbindung ist störanfällig, u.a. bei Regen, Schnee, Vögeln, Baukränen und ähnlichen Hindernissen. Sollten Sie eine Richtfunkverbindung benötigen, so gibt es mit dem HiperLAN-Standard oder verschiedenen anderen Laservarianten gute, aber deutlich teurere Alternativen zu WLAN.

3.7.2 IEEE 802.11a und 802.11g

Die Anforderungen an Netzwerke steigen und insbesondere die verfügbaren Datenraten sollen steigen. Diese Forderung gilt natürlich auch für drahtlose Netze. Dort herrscht im Vergleich zu drahtgebundenen Netzen erheblicher Nachholbedarf.

Die Lösung wird in Form von **IEEE 802.11a** angeboten; Bruttodatenraten von 54 Mbit/s sind – theoretisch – möglich. Bei diesem Standard wird ein anderes Frequenzband im 5-GHz-Bereich benutzt. In den USA ist das gewünschte Frequenzband unbenutzt und kann für WLANs verwendet werden. In Europa und auch in Deutschland sind gewisse Bereiche für Satelliten u.Ä. reserviert; große Teile des Frequenzbandes wurden aber schon von der RegTP für WLAN freigegeben. Die ersten Produkte werden angeboten, jedoch fehlen zurzeit noch Erfahrungen zu diesen. IEEE 802.11a ist aufgrund des anderen Frequenzbandes nicht zu den älteren 802.11-Varianten abwärtskompatibel. Doch auch dieses Problem hat z.B. der Hersteller Cisco gelöst, indem er einen AP mit beiden WLAN-Varianten ausstattet. Inzwischen wurde vom Chip-Hersteller Texas Instruments ein einziger Chip (TNETW1130) vorgestellt, der sowohl IEEE 802.11a als auch IEEE 802.11g und zusätzlich viele weitere Verfahren des WLAN beherrscht.

Der Vorteil des 5-GHz-Frequenzbandes liegt vor allem in den nicht vorhandenen Störquellen, weil es ausschließlich für die drahtlose Datenkommunikation reserviert ist. So viel ist allerdings schon jetzt klar: Die 54 Mbit/s werden in der Praxis nur selten erreicht werden, weil man Sender und Empfänger dazu in greifbarer Nähe zueinander aufstellen muss.

Auch **IEEE 802.11g** soll 54 Mbit/s erreichen, und das im ISM-Band. Damit ist es dann auch abwärtskompatibel zu z.B. IEEE 802.11b und bietet einen besseren Investitionsschutz als der Bruder IEEE 802.11a, weil an den neuen Accesspoints auch PCs mit alten IEEE 802.11b-Adaptern betrieben werden können. Der Standard wird vermutlich im Frühjahr 2003 verabschiedet. Erst danach sind standardkonforme Komponenten erhältlich.

OFDM

Beide Verfahren ermöglichen die höheren Datenraten bei gleicher Sendeleistung von 100 mW durch ein neues Kodierungsverfahren, das Orthogonal Frequency Division Multiplexing (OFDM). Durch das OFDM-Verfahren wird insbesondere eine höhere Widerstandsfähigkeit gegenüber Störquellen erreicht.

Die für IEEE 802.11b gemachten Aussagen zu Infrastrukturmodus und Ad-hoc-Modus gelten für IEEE 802.11a/g in gleicher Weise.

3.7.3 Sicherheit von WLANs

In den Fachmedien ist von enormen Sicherheitslücken berichtet worden, die entstehen, wenn man ein WLAN einsetzt.

Die Darstellungen sind insoweit richtig, als dass Lösungen von Herstellern als *Plug-and-Play* verkauft werden. In den Standardeinstellungen haben die meisten Geräte keinerlei Sicherheitsvorkehrungen, sodass jeder Hacker/Cracker, der mit einem Notebook und einer WLAN-Karte bewaffnet vor Ihrem Gebäude parkt, in Ihr Netz kann, und zwar ohne eine Straftat zu begehen.[9]

Betrachten Sie einen WLAN-Zugang ähnlich wie einen Internetzugang als öffentlich, und sichern Sie ihn entsprechend ab, dann können Sie auch weiterhin gut schlafen, ohne vor Hackern/Crackern Angst haben zu müssen. Ich möchte wie folgt auf den Punkt bringen: »Es hängt von Ihnen ab, wie sicher Ihr WLAN ist.«

Als Sicherheitsmechanismus wird oft WEP (Wired Equivalent Privacy), ein Verschlüsselungsverfahren, erwähnt. Dabei gibt es noch weitere Sicherheitsmöglichkeiten, die ich im Folgenden aufzeigen werde.

Der Administrator legt den Zugang zum Netz über die SSID/**ESSID** (Electronic System ID), einen Schlüssel, fest. Diese ID wird bei allen Clients und APs konfiguriert.

Wichtig!

Die ausgelieferte Einstellung heißt meistens *any*, was bedeutet, dass jede Station mit beliebiger ESSID sich am AP anmelden darf. Diese Einstellung sollten Sie noch vor der eigentlichen Inbetriebnahme ändern, sonst kann jeder in Ihr Netz.

Eine echte Hürde stellt die ESSID nicht dar. Sie kann erspäht werden, weil sie bei der Anmeldung von Clients am AP mitgesendet wird und die Übermittlung – wenn keine Verschlüsselung wie WEP eingesetzt wird – im Klartext erfolgt.

Die meisten APs bieten die Möglichkeit, so genannte **Accesslisten** zu führen. Dabei handelt es sich um eine Liste, in der die zulässigen MAC-Adressen aufgeführt werden. Andere als die dort aufgeführten Adressen werden ausgesperrt. Die MAC-Adressen der meisten WLAN-Karten

9 Da es keine Schutzmechanismen gibt, ist das Eindringen kein Einbruch und juristisch nicht strafbar.

sind veränderlich, sodass eine mitgelesene MAC-Adresse auch mit einer anderen Karte benutzt werden kann; auf diese Weise können Angreifer Zutritt erhalten. Eine Hürde gegen Hacker/Cracker bieten diese Accesslisten also nicht.

Exkurs

Die Veränderbarkeit von MAC-Adressen ist auch deshalb wichtig, weil in großen Installationen an jedem AP Änderungen vorgenommen werden müssten, wenn eine WLAN-Karte ausgetauscht wird. So kann einfach die MAC-Adresse von der defekten Karte übernommen werden, und die Konfiguration der APs muss nicht geändert werden.

Das oft erwähnte **WEP** ist optionaler Bestandteil des IEEE 802.11b-Standards. Dabei wird der Inhalt der Nachrichtenpakete mit einem 40-Bit-RC4-Algorithmus (WEP 64) verschlüsselt. Der Administrator legt maximal vier Passphrasen fest, die er auch bei jedem WLAN-Client hinterlegt und mit deren Hilfe die Verschlüsselung durchgeführt wird. Die 104-Bit-Variante von WEP (WEP 128) ist nicht viel sicherer als die 40-Bit-Variante und nicht Teil des IEEE-Standards, es kann daher zu Inkompatibilitäten zwischen Produkten verschiedener Hersteller kommen. WEP ist zu knacken, das ist inzwischen bewiesen worden. In einem sicherheitskritischen Umfeld sollten Sie sich nicht auf WEP verlassen. Die WEP-Verschlüsselung kann zu Leistungseinbußen im zweistelligen Prozentbereich beim AP führen, sodass Sie möglicherweise auf WEP verzichten, wenn Sie VPN-Technologie verwenden. Damit ersparen Sie sich auch die Installation der notwendigen WEP-Passphrasen auf den Clients. Wie Sie ein WLAN insbesondere hinsichtlich der WEP-Sicherheit selbst überprüfen können, erfahren Sie in Kapitel 15.1, WLAN-Sicherheit analysieren.

Der Königsweg für eine sichere WLAN-Lösung ist ein so genanntes **VPN (Virtual Private Network)**. Dabei wird der AP vor einer Firewall angeschlossen, die nur verschlüsselte VPN-Daten in das lokale Netz zum VPN-Endpunkt (Server) lässt. Von dort aus geht es dann unverschlüsselt weiter (vgl. Abbildung 3.12). Diese Lösung folgt der Anmahme, dass es sich bei einem WLAN um einen öffentlichen Zugang, vergleichbar mit dem Internetzugang, handelt, der besondere Schutzmaßnahmen erfordert. Beim Einsatz von VPN-Technologie, die als sicher gilt, können Sie auf weitere Sicherheitsmechanismen, wie sie oben beschrieben wurden, verzichten. Damit ersparen Sie sich Konfigurationsaufwand und können die WLAN-Komponenten als Plug-and-Play einsetzen. Die VPN-Lösung bietet dabei den Vorteil, dass sie auch über das Internet einen sicheren Zugang in das eigene LAN gewähren kann.

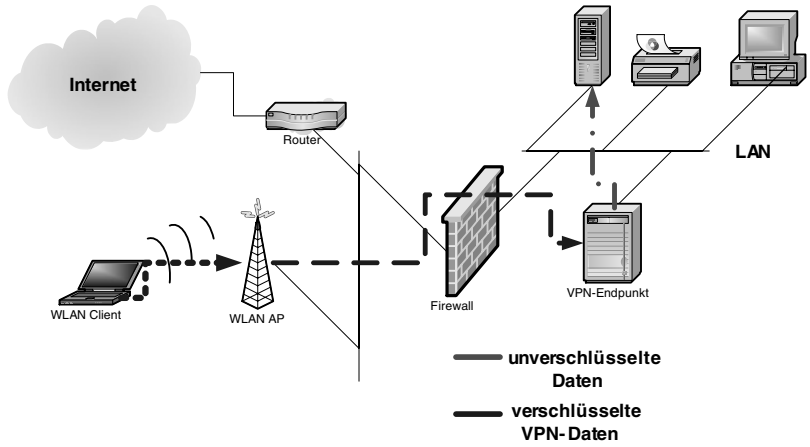

Abbildung 3.12 Sicherer Aufbau eines WLAN-Zugangs zum LAN

3.8 Virtual Private Network (VPN)

Sie möchten sicherheitskritische Daten über ein unsicheres Medium transportieren: Sie wollen über das Internet auf Ihren E-Mail-Server im Firmen-LAN zugreifen. Vielleicht beabsichtigen Sie aber auch, das Netzwerk einer Filiale mit dem Netzwerk der Hauptverwaltung zu verbinden oder ein grundstücksübergreifendes WLAN aufzubauen?

Damit diese Kommunikation sicher stattfinden kann, geht ein VPN den folgenden Weg: Es wird ein Tunnel zwischen den Kommunikationspartnern aufgebaut, so als ob der eine bei dem anderen Teilnehmer angerufen hätte. Bei diesem Tunnelaufbau findet eine Authentifizierung und Autorisierung statt. Nach dem Tunnelaufbau werden die eigentlichen Daten übertragen. Diese können z. B. mit IPSec verschlüsselt werden.

Da Internetzugänge häufig anzutreffen sind und die Bandbreiten der Internetzugänge sich in den letzten Jahren deutlich erhöht haben, besteht immer häufiger Bedarf an VPNs, die das Internet als Transportnetz verwenden. Selbst ein permanenter Internetzugang mit 2-Mbit/s-SDSL ist kostengünstiger als eine Standleitung über eine größere Entfernung mit 128 kBit/s.

Ein VPN kann zwischen (mindestens) zwei Rechnern oder zwischen (mindestens) zwei Netzen aufgebaut werden. Im Zusammenhang mit VPNs begegnen Ihnen mindestens drei Abkürzungen: PPTP, L2TP und IPSec. Hinter diesen Abkürzungen verbergen sich im VPN verwendete Verfahren. Es gibt noch weitere Möglichkeiten, die in diesem Buch nicht weiter vertieft werden:

- **PPTP** (Point to Point Tunneling Protocol) ist eine ISO-/OSI-Schicht-2-Technologie. Es verpackt Datenpakete in PPP-Rahmen. Alle Möglichkeiten des PPP wie Authentifizierung, Adressvergabe, Datenkompression und Datenverschlüsselung stehen zur Verfügung. Die Authentifizierung findet meist mittels CHAP oder MS-CHAP statt. PPTP übermittelt die PPP-Rahmen, in IP-Paketen verpackt, über das IP-Netz zum Kommunikationspartner. PPTP hat den Nachteil, dass es nur über IP-Netzwerke arbeiten kann. Der Vorteil von PPTP ist seine große Verbreitung. So ist es ab Windows 95 bereits werkseitig in Microsoft Windows enthalten.
- **L2TP** konkurriert mit PPTP, ist ebenfalls ein ISO-/OSI-Schicht zwei Protokoll und kann auch über andere als IP-Netzwerke übertragen. Dabei ist es das modernere Protokoll und bietet deutlich mehr Möglichkeiten als PPTP. Die Windows-Unterstützung besteht ab Windows 2000. Entgegen den Beschränkungen von PPTP besteht bei L2TP die Möglichkeit, eine Multi-Tunnel-Verbindung aufzubauen.
- **IPSec, IP Secure,** ist eine ISO-/OSI-Schicht-3-Technologie, also auf der Ebene von IP angesiedelt. IPSec umfasst dabei drei Funktionen:
  - **AH**, Authentication Header
  - **ESP**, Encapsulation Security Payload
  - **IKE**, Internet Key Exchange

IPSec dient zur Verschlüsselung von Daten und kann mit und ohne Tunnel eingesetzt werden. Es ist möglich, das gesamte IP-Paket inklusive IP-Header zu verschlüsseln: Dies geschieht im **Tunnelmodus**. Man nimmt Firewalls und Virenscannern bei der vollständigen Verschlüsselung die Möglichkeit, die IP-Pakete zu analysieren. Deshalb gibt es auch noch den Modus, der lediglich die Nutzdaten eines IP-Paketes verschlüsselt, den IP-Header aber unverschlüsselt lässt: Das ist der **Transportmodus**. Allerdings hilft dieser Modus nur einer Packetfiltering-Firewall (vgl. Kapitel 11.1.3, Sicherheitslösungen im Überblick), schließlich können weder die Firewall noch der Virenscanner die verschlüsselten Nutzdaten analysieren.

Bei IPSec kann man eine Schlüsselverwaltung, IKE, einsetzen. Dabei handelt es sich um eine Anwendung, die zu IPSec gehört, jedoch auf der Applikationsebene (ISO-/OSI-Schicht 7) angesiedelt ist. Alternativ zur integrierten Schlüsselverwaltung kann man auch manuell Schlüssel verwalten. Häufig werden **pre-shared** Schlüssel (engl. *keys*) verwendet. Dazu installieren Sie auf beiden Rechnern einen Schlüssel. Von diesen

Schlüsseln wird zur Authentifizierung ein Hash-Wert gebildet, den der jeweilige Partner überprüft. Bei dem Verbindungsaufbau zwischen den VPN-Teilnehmern müssen einige Parameter ausgehandelt werden (»Wie oft wird der Schlüssel neu generiert?«, »Welches Verschlüsselungsverfahren kommt zum Einsatz?« u.Ä.). Diese Parameter werden in SAs[10] abgelegt und verwaltet.

Es gibt mehrere Möglichkeiten eine VPN-Lösung aufzubauen. Die Architekturen orientieren sich dabei an den Anforderungen.

End-to-Site VPN

Wenn Sie Außendienstmitarbeiter und Heimarbeiter mit ihren **Homeoffices**[11] an Ihr Unternehmens-LAN anbinden möchten, so spricht man von einem **End-to-Site-VPN** (vgl. Abbildung 3.13). Ein Endgerät – das Notebook des Außendienstmitarbeiters, der PC des Heimarbeiters – verfügt über eine Software, den VPN-Client, und greift über das Internet auf den VPN-Punkt in Ihrem Netzwerk zu.

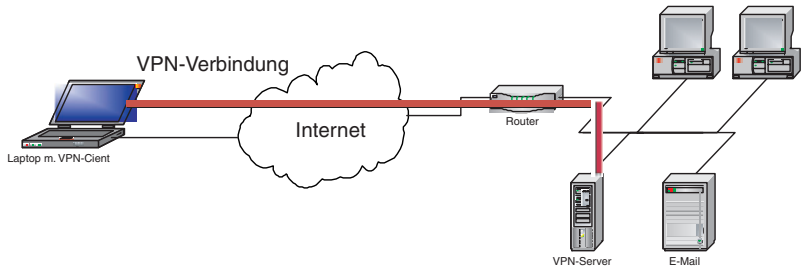

Abbildung 3.13 End-to-Site-VPN

In dem in Abbildung 3.13 dargestellten Beispiel ist der Datenverkehr vom Laptop aus bis zum VPN-Endpunkt im LAN verschlüsselt. Je nach eingesetzter Verschlüsselung könnte eine im Router implementierte Firewall die Datenpakete nicht kontrollieren. Daher wird im Idealfall zwischen dem VPN-Endpunkt und dem LAN noch eine weitere Firewall installiert, sodass eine DMZ (demilitarisierte Zone) entsteht.

Der größte Vorteil einer End-to-Site-VPN-Lösung gegenüber einer Lösung mit direkter Einwahl über ISDN oder Modem ist einerseits, dass sie sehr kostengünstig angeboten wird, andererseits, dass man sehr flexibel ist und dass ein Internetzugang reicht, um weltweit auf das Unternehmensnetz zuzugreifen.

10 Security Association
11 Die Sprache der Netzwerke ist Denglisch, teilweise auch Germisch.

Bei einer Lösung, die das Internet als Transportmedium benutzt, müssen das Notebook und der Firmen-Router eine offizielle IP-Adresse haben.

Wichtig!

Die Firma Cisco Systems, der größte Netzwerkausrüster weltweit, bietet seinen Mitarbeitern die Möglichkeit, über das Internet und einen VPN-Client auf dem Notebook auf das Firmennetzwerk zuzugreifen. Dabei ist es unerheblich, wie der Internetzugang ausgestaltet ist. Genutzt werden können Internetzugänge von Hotels, Flughäfen (z. B. Hot Spots) oder von zu Hause. Die VPN-Software stellt sicher, dass es unmöglich ist, die Daten zu entschlüsseln.

Die Kopplung von zwei LANs über ein VPN nennt man **Site-to-Site-VPN**. Dabei findet die Verschlüsselung zwischen zwei VPN-Gateways statt; innerhalb des LANs werden die Daten unverschlüsselt übertragen.

Site-to-Site-VPN

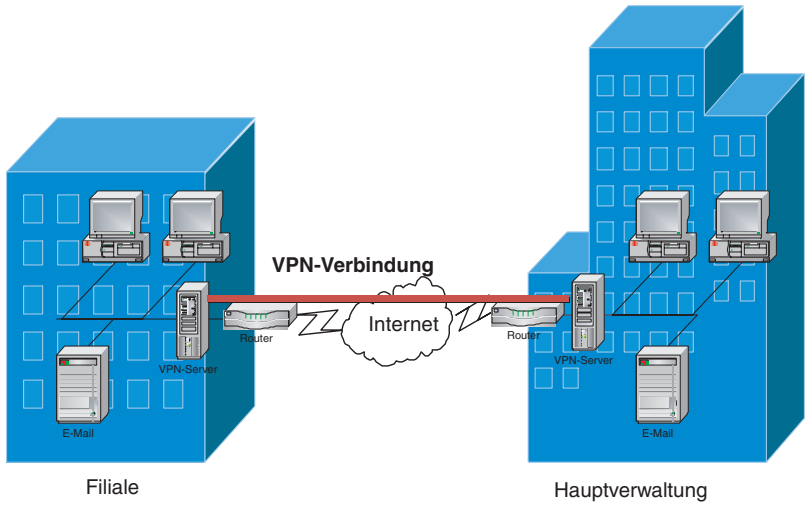

Abbildung 3.14 Site-to-Site-VPN

Das in Abbildung 3.14 dargestellte VPN hat den Vorteil, dass lediglich die VPN-Server über die notwendigen Schlüssel verfügen müssen. Die einzelnen PCs adressieren ihre Daten über das VPN-Gateway an das andere Netz. Die Verschlüsselung ist Aufgabe des VPN-Servers. Dabei sind üblicherweise der Router und das VPN-Gateway als Hardware, in Form eines Gerätes und nicht als Software, realisiert.

Wichtig!

Bei einem Site-to-Site-VPN ist es erforderlich, dass die VPN-Gateways über offizielle IP-Adressen verfügen, wenn die Kopplung über das Internet erfolgt. Sie nehmen die Adressumsetzung (siehe Kapitel 3.2.4, NAT, Network Address Translation) vor.

VPN als Netzwerk

VPNs werden nicht nur über das Internet eingesetzt, sie kommen auch zur Kopplung von Unternehmensnetzen zum Einsatz. Unterhält man viele Site-to-Site-VPNs, so kann dies in einer sternförmigen Struktur oder voll vermascht geschehen. In der sternförmigen Struktur muss es einen Mittelpunkt geben. Diese Situation ist insbesondere dann nicht gegeben, wenn kooperierende Unternehmen sich gegenseitig LAN-Zugänge einrichten. Möglich wäre der Aufbau eines voll vermaschten VPN, wie in Abbildung 3.15 dargestellt.

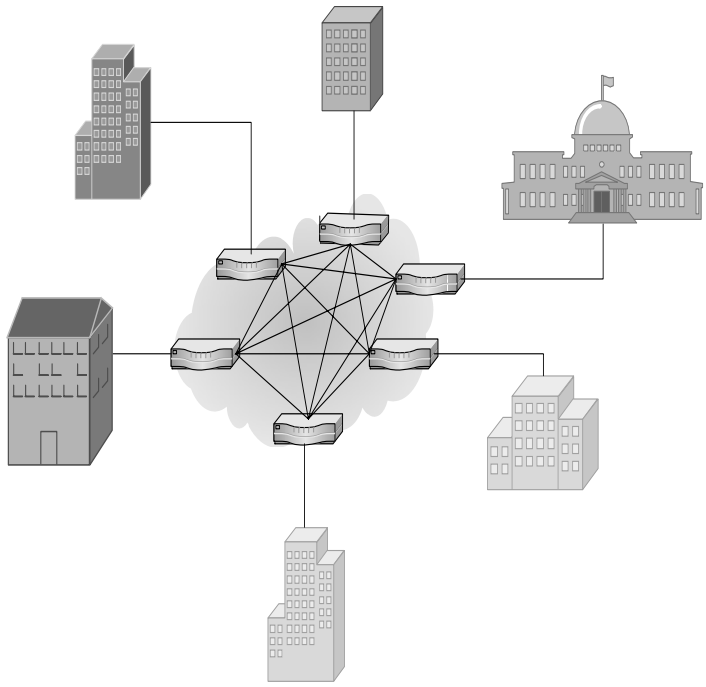

Abbildung 3.15 Voll vermaschtes VPN

Jeder Teilnehmer dieses VPN-Verbundes hat einen VPN-Tunnel zu jedem anderen Teilnehmer. Wie Sie sehen, entstehen auch bei wenigen Teilnehmern schon recht komplexe Strukturen. Es handelt sich bei n Teilnehmern um $(n^2\text{-}n)/2$ Verbindungen und um $n^2\text{-}n$ Tunnelenden, die verwaltet werden müssen.

Entsprechend gibt es im Beispiel der Abbildung 3.15 sechs Teilnehmer, 15 Verbindungen und 35 Tunnelenden. Bei nur drei weiteren Teilnehmern, in Summe also neun Teilnehmern, steigt der Administrationsaufwand auf 36 Verbindungen und 72 Tunnelenden, hat sich also mehr als verdoppelt. Stellen Sie sich einen großen Verbund von 50 Teilnehmern vor. Sie müssten sich um 1225 Verbindungen und 2450 Tunnelenden kümmern. Mit dem Wort *unübersichtlich* kann man eine solche Struktur sehr gut kennzeichnen.

Alternativ zur eigenen Verwaltung können Sie auch bei einem Provider VPNs mieten. Auf diese Weise ersparen Sie sich die aufwändige Konfiguration und Administration.