Anhang C

TCP/IP-Technologie für Internet und Intranet

Der Begriff Internet, das »Netz der Netze«, verkörpert eine einzigartige, weltumspannende Infrastruktur vernetzter Netzwerke und die Software-Technologien, auf denen diese Netzwerke aufbauen. Die TCP/IP-Technologie (Transmission Control Protocol/Internet Protocol) ist das eigentliche Herz des Internet. Erst die hohe Verbreitung der TCP/IP-Protokolle ermöglichte die weltweite Vernetzung der Rechnersysteme bis hin zum »kleinsten« PC im letzten Winkel dieser Erde /Hamp96/.

Die TCP/IP-Technologie ist kein feststehendes Gebilde, sondern besteht aus unterschiedlichen Diensten und Anwendungen, die im Laufe der Jahre ständig weiterentwickelt wurden. TCP- und IP-Protokoll sind streng genommen nur zwei Komponenten der gesamten Kommunikations-Architektur, haben sich aber als übergeordneter Begriff im Sprachgebrauch durchgesetzt.

C.1 Von den Anfängen bis heute

Ursprünglich hatte das Internet, wie viele Produkte der Hochtechnologie, militärische Zielsetzungen. Die ersten Gedanken machte man sich bereits Ende der fünfziger Jahre, als die amerikanische *»RAND Corp.«* ein Konzept für ein Kommando- und Überwachungsnetzwerk militärischer Einrichtungen entwickelte. Der Kern dieses Konzepts bestand aus einem dezentralen Aufbau, der auch nach teilweiser Zerstörung der Infrastruktur, beispielsweise nach einem Atomschlag, die Funktionsfähigkeit der amerikanischen Militäreinrichtungen gewährleisteten sollte.

Um im technologischen Wettstreit mit der Sowjetunion die amerikanische Militärtechnologie in eine führende Position zu bringen, rief die US-Regierung unter anderem die *»Advanced Research Projects Agency«* (ARPA) ins Leben. Deren Aufgabe war es, neue Technologien zu entwikkeln. Aus den ursprünglichen Konzepten der *»RAND Corp.«* entwickelten die ARPA-Ingenieure die paketorientierte Datenübertragung, die die Datenkommunikation in den folgenden Jahren revolutionieren sollte. Ende 1969 wurde zwischen der *»University of California at Los Angeles«*, der *»University of California at Santa Barbara«*, der *»University of Utah«* und dem *»Stanford Research Institute«* (SRI) in Menlo-Park in Kalifornien das erste experimentelle Netz (ARPANET) in Betrieb genommen. Für den Erfolg des ARPA-

NET sorgten vor allem die auf allen angeschlossenen Rechnern zur Verfügung gestellten Dienstleistungen wie Terminalsitzung (Remote Login), Dateiübertragung (File Transfer) und Elektronische Post (Electronic Mail).

Im Jahr 1973 begann die inzwischen in *»Defense Advanced Research Projects Agency«* (DARPA) umbenannte Organisation ein weiteres Projekt, um die zwischenzeitlich neben dem ARPANET entstandenen, unterschiedlichen Übertragungsmechanismen zu verbinden. So entstand auf der Basis des TCP/IP-Konzepts das Internet. Die Grundzüge dieser Technologie wurden 1974 von *Victor Cerf* (Stanford University) und *Bob Kahn* (DARPA) erstmals in einem veröffentlichten Artikel festgelegt. Ein erstes Testnetz wurde 1977 in Betrieb genommen und in den kommenden Jahren ständig erweitert. 1983 hatte das immer noch experimentelle ARPANET eine derartige Ausdehnung erreicht, dass man beschloss, die Kontrolle über dieses Netz an die *»Defense Communication Agency«* (DCA) abzugeben. Gleichzeitig wurden sämtliche Netzknoten auf das TCP/IP-Protokoll umgestellt und das bisherige Netz in einen militärischen Bereich (MILNET) und einen forschungsorientierten Bereich (ARPANET) aufgeteilt.

In den letzten Jahren hat sich das Internet sehr stark gewandelt. Die Fortschritte der Kommunikationstechnologie und das stetig wachsende Informationsbedürfnis haben das Internet explosionsartig anwachsen lassen. Waren früher fast ausschließlich Universitäten, Forschungsinstitute und deren Wissenschaftler ans Internet angeschlossen, so ist es heute zu einem Informationsforum für die breite Öffentlichkeit geworden. Ende 2001 waren schätzungsweise 500 Millionen Benutzer in über 240 Ländern an das Internet angeschlossen.

Als Anfang der neunziger Jahre das World Wide Web (WWW) eingeführt wurde, bot sich erstmals die Möglichkeit, unter einer einheitlichen Darstellung unterschiedliche Dienste mit multimedialen Inhalten, beispielsweise Bildern, Tönen, Animationen und Videos, zu transportieren. Einige Strategen erkannten das Potential dieses Mediums, und innerhalb weniger Jahre wurde das World Wide Web zu einem globalen Marktplatz, auf dem fast alle großen, aber auch immer mehr mittlere und kleine Organisationen vertreten sind. Die meisten Internet-Provider stellen für ihre Kunden heute, bis zu einem gewissen Umfang kostenlos, Platz auf ihren Servern zur Verfügung. Damit bietet sich für jeden privaten Anwender die Möglichkeit, auf einer eigenen Homepage sich selbst, seine Hobbies, Interessen und Neigungen weltweit zu präsentieren und Kontakt mit Gleichgesinnten aufzunehmen.

Die elektronische Post (E-Mail) ist heute im geschäftlichen und privaten Umgang ein fester Bestandteil unserer täglichen Kommunikation geworden. Die meisten Mitarbeiter in Firmen und Behörden sind heute per E-Mail zu erreichen und auf Visitenkarten ist die Angabe einer E-Mail-Adresse mittlerweile obligatorisch.

Die rasante Entwicklung des Internet hat aber auch Schattenseiten: Die TCP/IP-Technologie war nicht für ein solches globales Netz vorgesehen. Durch die in den Anfangsjahren auf wenige Teilnehmer begrenzte Ausdehnung des Internet waren Sicherheitskonzepte wie Zugriffsberechtigung, Vertraulichkeit der Daten während der Übertragung und Schutz von Netzsegmenten vor unberechtigten Zugriffen nicht in solchem Maße erforderlich wie heute. Da sich inzwischen jeder von fast jedem Ort auf der Welt in das Internet einschalten kann, sind damit natürlich auch Sicherheitsmaßnahmen unumgänglich geworden.

C.2 Vorteile der TCP/IP-Technologie

Die TCP/IP-Technologie bietet entscheidende Vorteile:

- Für jeden Benutzer besteht die Möglichkeit, auf jede für ihn freigegebene Information innerhalb des gesamten Netzwerks zugreifen zu können. Zusätzlich kann jeder angeschlossene Benutzer mit jedem anderen angeschlossenen Rechnersystem kommunizieren. Es gibt bereits Anwendungen, die weltweites Telefonieren oder Videokonferenzen von einem Rechnersystem zum nächsten ermöglichen. Dadurch wird der Informationsaustausch zwischen den Benutzern gewährleistet, der das Internet in Zukunft zum globalen Informationsmedium schlechthin machen wird.
- Bereits bei der Konzeption Anfang der siebziger Jahre legte man fest, dass die Protokolle unabhängig von der verwendeten Netzwerktechnologie sein sollten. Durch diese Forderung ist die Kommunikation zwischen unterschiedlichen Rechner- und Netzwerktypen, wie z. B. im Internet, möglich geworden. Gleichzeitig bietet dies die Möglichkeit, neue technologische Entwicklungen mit bereits vorhandenen Strukturen zu verknüpfen. Durch die permanente Weiterentwicklung der Technik im Computer- und Kommunikationsbereich lässt sich die bewährte Technologie ohne weiteres auf neue Entwicklungen übertragen, ist dann aber immer noch in der Lage, mit älteren Systemen zu kommunizieren.
- Durch die ständige Weiterentwicklung ist das Internet zu einer ausgereiften Technologie geworden, die sich im alltäglichen Einsatz bewährt hat.
- Die Internet-Technologie ist heute weit verbreitet, daher gibt es auch ein breites Angebot kompatibler Netzkomponenten. Da die meisten Softwarevarianten auch durch Implementierungen anderer Hersteller ersetzbar sind, bedeutet das eine geringe Herstellerabhängigkeit. Durch die starke Verbreitung innerhalb des Internet werden die Produkte auch zunehmend billiger.
- Die einzelnen Protokollspezifikationen sind standardisiert und für jedermann frei zugänglich. Dadurch sind Implementierungen für neue oder spezielle Systeme jederzeit leicht zu entwickeln oder anzupassen.

C.3 Das OSI-Referenzmodell

Um eine einheitliche Struktur für gegenwärtige und zukünftige Entwicklungen von Netzwerktechnologien festzulegen, einigte man sich auf das so genannte OSI-Referenzmodell (Open System Interconnection), das 1983 von der »International Organisation for Standardization« (ISO) als Standard festgelegt wurde. Es hat eine klare Architektur und eignet sich daher besonders gut für die Darstellung einer Kommunikationsarchitektur und der Prinzipien des Schichtenmodells. In diesem Modell wird davon ausgegangen, dass ein Kommunikationsprotokoll aus mehreren Modulen besteht, von denen jedes einzelne Modul während einer Kommunikation unterschiedliche Aufgaben zu erfüllen hat /Tann 98/.

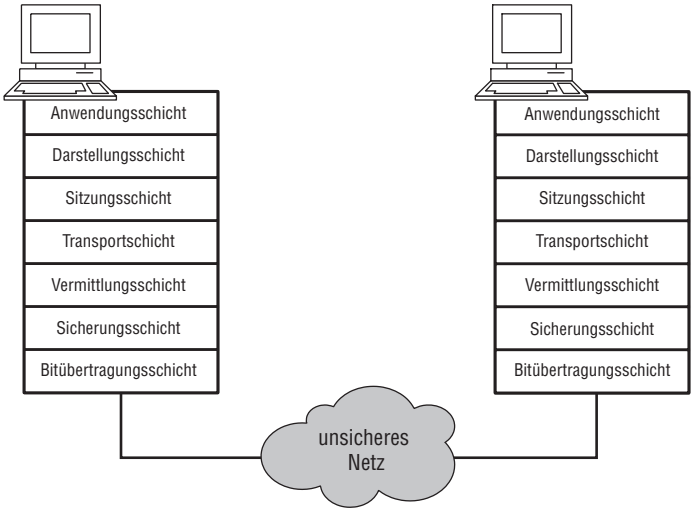

Abb. C.1: Das OSI-Referenzmodell

Das OSI-Referenzmodell besagt, dass bei einer Verbindung beispielsweise zwischen zwei Rechnersystemen jede Schicht des Rechnersystems A mit der gleichen Schicht des Rechnersystems B kommunizieren kann. Dazu werden den Daten in jeder Schicht bestimmte Bitmuster in einem Header vorangestellt oder in einem Trailer am Ende angefügt. Diese Bitmuster enthalten so genannte Protokollinformationen, die zum Beispiel darüber Auskunft geben,

- wer die Daten abgesandt hat,
- wer die Daten empfangen soll,
- welchen Weg die Daten während der Übertragung nehmen sollen,
- wie die Daten weiterverarbeitet werden dürfen oder
- wie sie vom Empfänger behandelt werden sollen.

Jede weitere Schicht übernimmt die Datenpakete der übergeordneten Schicht und fügt, falls dies für den Ablauf der Kommunikation notwendig sein sollte, ihre eigenen Protokollinformationen in einem weiteren Header oder Trailer hinzu. Die Auswertung der Protokolldaten erfolgt beim Empfänger nur auf der jeweils gleichen Schicht, das heißt die Daten einer übergeordneten Schicht werden von einer niedrigeren Schicht nicht ausgewertet.

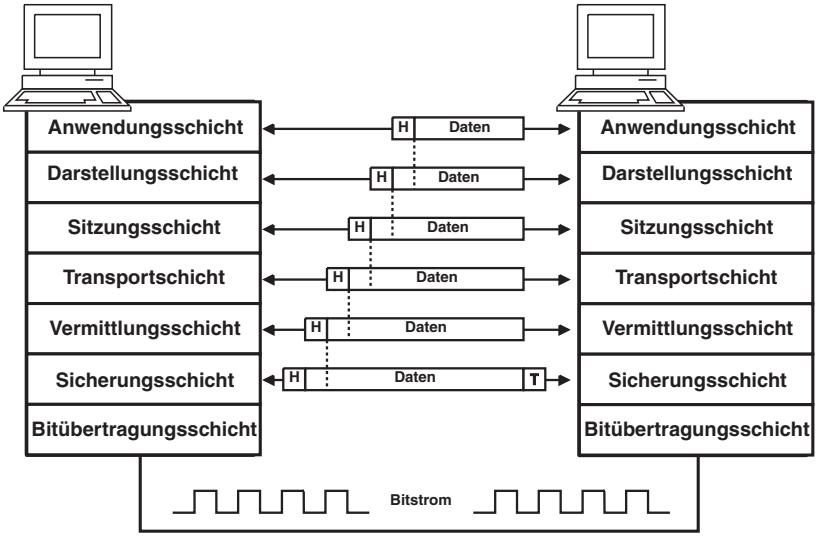

Abb. C.2: Kommunikation zwischen zwei Rechnern

Im folgenden Abschnitt soll kurz erläutert werden, welche Aufgaben die jeweiligen Schichten übernehmen:

1. Die Bitübertragungsschicht (Physical Layer) legt fest, wie die Daten physikalisch übertragen werden. Zu den Parametern dieser ersten Schicht gehören Informationen über die verwendeten Übertragungsmedien wie Kupferkabel, Glasfaser, Infrarot- oder Funkübertragung, und die Spezifikation von Schnittstellen mit Spannungspegeln, Steckverbindern und Datenübertragungsraten.
2. Die Aufgabe der Sicherungsschicht (Data Link Layer) ist die sichere Datenübertragung zwischen zwei benachbarten Stationen, zum Beispiel zwei Routern, innerhalb eines Netzwerks. Dazu werden die zu übertragenden Bits in Rahmen (Frames) zusammengefasst und mit einer Prüfsumme versehen. Wird ein solcher Rahmen unvollständig übertragen oder zerstört, so fordert der Empfänger nach einem Vergleich der Prüfsumme den entsprechenden Rahmen erneut beim Absender an.

3. Die Vermittlungsschicht (Network Layer) legt die Übertragungswege (Routen) für die Daten zwischen zwei Rechnersystemen fest. Dazu werden Informationen, wie die Übertragungszeit, die Auslastung des Übertragungsweges usw. benutzt, um nach den in Routing-Protokoll festgelegten Regeln eine Verbindung herzustellen. Die innerhalb dieser Schicht transportierten Daten werden in Datenblöcken übertragen, die man als Pakete bezeichnet.
4. Die Transportschicht (Transport Layer) stellt eine Art virtueller Verbindung zwischen den beiden Rechnersystemen bereit. Sie sorgt vor allem für eine Korrektur von Übertragungsfehlern und ist sehr stark von den untergeordneten Schichten abhängig.
5. Die Sitzungsschicht (Session Layer) dient der Verwaltung von Kommunikationsprozessen. Dabei wird die Verbindung mit einem oder mehreren Kommunikationspartnern kontrolliert und gleichzeitig dafür gesorgt, dass die jeweilige Kommunikation synchron abläuft, das heißt, dass bei einem aufgetretenen Fehler die Daten wieder in der richtigen Reihenfolge zusammengefügt werden.
6. In der Darstellungsschicht (Presentation Layer) werden die zu übertragenden Daten in ein einheitliches Format gebracht. Dies ist vor allem bei der Verwendung von unterschiedlichen Zeichensätzen, zum Beispiel ASCII und EBCDIC, notwendig. Zusätzlich können in dieser Schicht weitere Funktionen zur Umwandlung, Verschlüsselung oder Komprimierung der zu übertragenden Daten enthalten sein.
7. Die Anwendungsschicht (Application Layer) beinhaltet schließlich die eigentlichen Anwendungs- und Dienstprogramme für die unterschiedlichen Funktionen, die über die Netzwerkverbindung ausgeführt werden sollen.

C.4 TCP/IP-Protokollarchitektur

Obwohl es keine generelle Vereinbarung über ein spezielles TCP/IP-Schichtenmodell gibt, kann man sagen, dass es aus weniger Schichten aufgebaut ist als das OSI-Referenzmodell. In den folgenden Kapiteln wollen wir uns deshalb auf ein Vier-Ebenen-Modell beziehen.

In diesem Modell gibt es analog zum OSI-Referenzmodell unterschiedliche Kommunikationsebenen, wobei die Daten von der übergeordneten zur nächsttieferen Ebene weitergereicht werden. Jede Kommunikationsebene fügt den Daten eigene Kontrollinformationen hinzu, bis sie über das Netz gesendet werden. Beim Empfänger werden diese Daten dann Ebene für Ebene nach oben weitergeleitet, wobei jede Ebene nur die für sie relevanten Daten auswertet und aus dem Datenpaket entfernt, bevor es an die nächsthöhere Ebene weitergegeben wird.

Abb. C.3: Ebenen der TCP/IP-Protokollarchitektur

- Die Netzzugangsebene ermöglicht einem Rechnersystem, Daten zu einem anderen Rechnersystem innerhalb des direkt angeschlossenen Netzes (zum Beispiel Ethernet) zu übertragen. Dazu sind genaue Kenntnisse des zugrunde liegenden Netzaufbaus nötig. Die Netzzugangsebene umfasst die zwei unteren Ebenen des OSI-Modells und beinhaltet die Kapselung von IP-Paketen in Netzrahmen (Frames) sowie die Zuordnung von IP-Adressen zu physikalischen Netzadressen, beispielsweise MAC-Adressen.
- Die Netzwerkebene definiert den Aufbau von IP-Paketen und bestimmt, auf welchem Weg die Daten durch das Internet übertragen werden (Routing).
- Die Transportebene stellt eine Verbindung zwischen zwei Endpunkten (Rechnersystemen) her. Die wichtigsten Protokolle sind hier TCP und UDP.
- Die Anwendungsebene beinhaltet sämtliche Programme und Dienste, die über die Netzwerkverbindung durchgeführt werden sollen. Dazu gehören Dienste wie Telnet (Login auf einem anderen Rechnersystem), FTP (Datentransfer zwischen zwei Rechnersystemen), SMTP (E-Mail-Funktionen), HTTP (World Wide Web) usw.

C.5 Internet-Adressen

Wie finden die Daten im Internet ihr Ziel? Ganz klar, jedes Rechnersystem im Internet hat eine bestimmte IP-Adresse und einen Namen.

Bei der Entwicklung der Internet-Adressierung legte man nicht nur hohen Wert auf die Identifizierung jedes angeschlossenen Rechnersystems, sondern auch darauf, an welcher Stelle innerhalb eines Netzwerkes es sich befindet und über welche Übertragungswege die Daten ihr Ziel erreichen können. Dazu bekommt jeder Benutzer im weltweiten Netzwerk eine einmalige 32 Bit oder 4 Byte lange Internet-Adresse (IPv4-Adressierung), bestehend aus einer Netzwerk- und einer Rechnersystem-Identifikation, die als 4 Dezimalzahlen dargestellt werden und jeweils durch einen Punkt getrennt sind.

Beispiel: 11000011 . 10010011 . 00111000 . 11101101 entspricht 195 . 147 . 56 . 237

Diese Adressierung wird in 5 Klassen (Klasse A bis E) aufgeteilt. Jede dieser Klassen unterscheidet sich in der Länge der Netzwerk- und der Rechnersystem-Identifikation (Abb. c.4). Diese Aufteilung wurde getroffen, da man in den Anfangstagen des ARPANET davon ausging, dass es in Zukunft nur wenige große (Klasse-A-) Netzwerke (z. B. für Militär und Forschung) geben würde. Doch nach einigen Jahren zeigte sich mit der Einführung von lokalen Netzwerken in vielen Organisationen, dass diese Annahme nicht mehr zutraf. Durch die Vergabe von Klasse-A-Adressen wurden die Möglichkeiten schnell begrenzt. Aus diesem Grund führte man zwei weitere Klassen für mittelgroße (Klasse B) und kleine Netze (Klasse C) ein. Den Klasse-D-Adressen fällt eine besondere Bedeutung zu. Sie werden als so genannte Multicast-Adressen bezeichnet. Das bedeutet, dass bestimmte Datenpakete nicht mehr an jedes Rechnersystem einzeln verschickt werden müssen, sondern gleichzeitig an eine ganze Gruppe von Rechnersystemen gesendet werden können, denen eine Multicast-IP-Adresse zugeordnet wurde. Die IP-Adressen der Klasse E sind für zukünftige Anwendungen reserviert und werden derzeit zu Forschungszwecken verwendet. Sie sollen genutzt werden, um IPv6-Pakete über IPv4-Netze zu routen.

Das starke Wachstum des Internet hat zu einem Mangel an IP-Adressen geführt. Außerdem sind dadurch die Routing-Tabellen der Backbone-Router, die die einzelnen Netze verbinden, zu groß geworden. Aus diesem Grund hat man die starre Aufteilung in nur 5 Netzklassen aufgehoben (vgl. RFC 1517). Die 32 Bit der IP-Adresse können nun beliebig auf Netz-ID und Rechnersystem-ID verteilt werden. Somit ergeben sich 33 mögliche Netzwerk-Klassen. Für die ursprünglichen fünf Klassen, die immer noch am häufigsten vorkommen, werden die alten Bezeichnungen (Klasse A bis E) weiterverwendet.

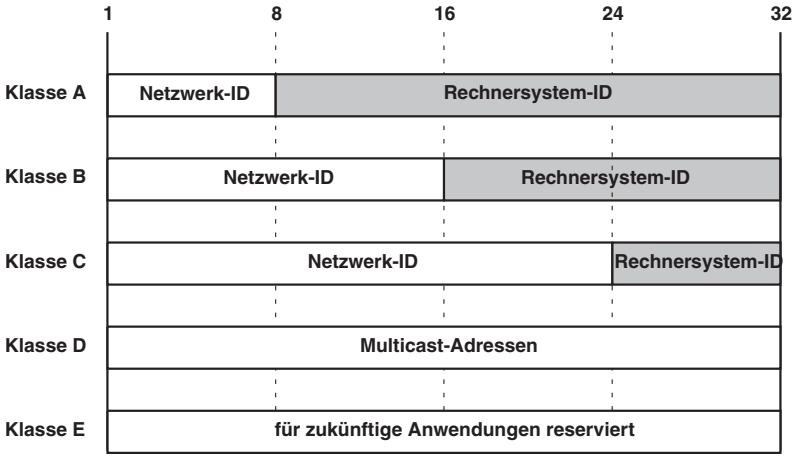

Abb. C.4: Aufbau von Internetadressen und Einteilung in Klassen

Viele Anwender sind nur gelegentlich über einen Provider mit dem Internet verbunden. Für diese Rechnersysteme ist es nicht notwendig, eine permanente IP-Adresse zu vergeben. Hier benutzt man die Möglichkeit, IP-Adressen automatisch zu vergeben. Wenn ein Kunde Zugang zum Internet haben möchte, wählt er zunächst einen Einwahlknoten eines Providers in seiner Nähe an. Das Rechnersystem des Providers hat zu diesem Zweck eine Reihe von IP-Adressen reserviert, die dem jeweiligen Anrufer dann automatisch zugeordnet werden und nur für die aktuelle Sitzung gültig sind. Dieses Verfahren nennt man »dynamische IP-Adressierung«.

Da aufgrund des starken Wachstums des Internet abzusehen war, dass die Anzahl der freien IP-Adressen eines Tages erschöpft sein wird, wird seit 1995 daran gearbeitet, die Adresslänge zukünftig auf 128 Bit oder 16 Byte (IPv6 oder IPnG next generation) zu verlängern. Natürlich sind die alten IP-Adressen weiterhin gültig und können auch nach dem neuen Standard weiterhin verarbeitet werden. Es muss damit gerechnet werden, dass der fließende Übergang zwischen IPv4 und IPv6 noch sehr lange dauern wird.

Unternehmen verwenden heute meistens nur noch wenige offizielle IP-Adressen, sondern arbeiten mit verborgenen, intern reservierten IP-Adressen, was die Adressenproblematik stark reduziert.

Die IP-Adressierung ist für technische Systeme hervorragend geeignet. Im praktischen Umgang hat sich aber gezeigt, dass dieses Verfahren für viele Anwender zu kompliziert und undurchsichtig ist. Wer schon einmal durch das World Wide Web gesurft ist, dem ist sicherlich aufgefallen, dass viele Rechnersysteme nicht über ihre IP-Adressen aufgerufen werden, sondern über einen oder mehrere symbolische Namen.

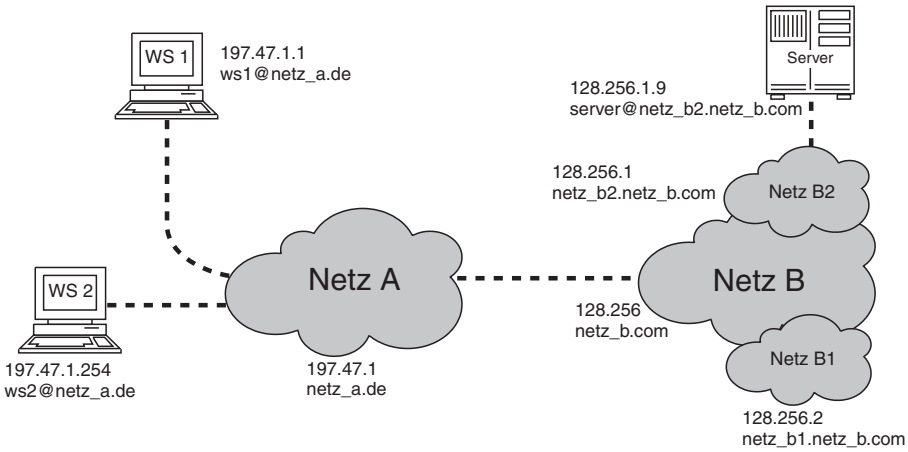

Abb. C.5: IP- und Domainnamenadressierung

Jedes ans Internet angeschlossene Netz kann zu diesem Zweck neben einem IP-Adressbereich zusätzlich einen Domainnamen erhalten. IP-Netze und DNS-Domains müssen nicht deckungsgleich sein, auch wenn dies meistens der Fall ist. Innerhalb der Domain kann der jeweilige Netzbetreiber für untergeordnete Netze weitere Subdomains erstellen, um sein Netz noch tiefer zu strukturieren. Die Domainnamen werden zentral vom Network Information Center (NIC) und seinen Unterorganisationen (zum Beispiel DENIC in Deutschland) vergeben und verwaltet. Wenn eine Organisation einen eigenen Domainnamen verwenden möchte, so muss sie oder ihr Provider bei der verantwortlichen Unterorganisation des NIC die Zuordnung dieses Namens beantragen. Die Top Level Domains sind vom Network Information Center fest vorgegeben und in unterschiedliche Nutzerprofile oder lokale Gruppen eingeteilt:

- .arpa für Einrichtungen des ARPANET
- .com für kommerzielle Organisationen aus Industrie und Handel
- .edu für Universitäten und Schulen
- .gov für Regierungsstellen und staatliche Einrichtungen
- .mil für militärische Einrichtungen der US-Streitkräfte
- .org für nicht kommerzielle Einrichtungen
- .de für Einrichtungen in Deutschland
- .uk für Einrichtungen in Großbritannien

Neue, so genannte generic Top Level Domains (gTLD), sind in Vorbereitung:

- .aero für Unternehmen der Luftfahrtindustrie
- .biz für Unternehmen
- .coop für genossenschaftliche Organisationen
- .info für allgemeine WWW-Angebote

- .museum für Museen
- .name für Privatpersonen
- .profür Ärzte, Anwälte, Steuerberater etc.

Die Vorschläge ».firm«, ».shop« und ».web« wurden verworfen.

Ausführlichere Informationen dazu und eine Sammlung von Links, mit deren Hilfe Sie die Entwicklung verfolgen können, finden Sie unter `http://www.denic.de/doc/gtld/index.html`.

C.6 Die Kommunikationsprotokolle

Die folgenden Beschreibungen der am häufigsten im Internet verwendeten Kommunikationsprotokolle und Dienste sollen als Hinweis dienen, welche Informationen jeweils übertragen werden. Diese Informationen sind äußerst wichtig für den Transport der Daten innerhalb und zwischen den Netzen. Gleichzeitig können die übertragenen Daten aber auch manipuliert werden und bei falschem Umgang enormen Schaden beim Empfänger verursachen.

Grundsätzlich unterscheidet man zwei verschiedene Arten von Kommunikationsprotokollen. Die verbindungslosen Protokolle kann man mit Telegrammen vergleichen. Die Daten werden vom Absender ins Netz geschickt und können während der Übertragung verloren gehen, dupliziert werden oder verspätet eintreffen, ohne den Absender darüber zu informieren. Man nennt derartige Informationseinheiten auch Datagramme. Diese Art der Kommunikation ist wie der Paketdienst einer Post-Gesellschaft. Man gibt das Paket an einer Stelle ab; wie es dann weitergeleitet wird, darauf hat man keinen Einfluss.

Im Gegensatz dazu bauen die verbindungsorientierten Protokolle eine Kommunikation nach einem bestimmten Schema auf. Zuerst wird eine virtuelle Verbindung zwischen Absender und Empfänger aufgebaut. Nach dem gegenseitigen Austausch von festgelegten Informationen erfolgt dann der eigentliche Datentransfer, und erst wenn beide Seiten den ordnungsgemäßen Empfang der Daten bestätigt haben, wird die Verbindung wieder abgebaut. Eine Analogie hierzu ist eine Telefonverbindung: Ein Teilnehmer baut die Verbindung auf, und wenn der andere abgenommen hat, kann das Telefonat beginnen.

C.6.1 IP-Protokoll

Das Internet Protocol (IP) ist ein verbindungsloses Protokoll auf der Netzwerkebene. Ein IP-Header besteht aus mehreren Feldern, die folgende Bedeutungen oder Funktionen haben:

- Version: Versionsnummer des verwendeten IP-Protokolls, mit dem das IP-Paket (Datagramm) erstellt wurde.

- Headerlänge: Dieses Feld bestimmt die Länge des IP-Headers in 32-Bit-Einheiten.
- Servicetyp: Man kann die Wichtigkeit eines IP-Paketes mit diesem Feld festlegen und bestimmen, auf welche Art oder welchem Weg dieses IP-Paket übertragen werden soll, zum Beispiel mit geringer Verzögerung, mit hohem Datendurchsatz oder auf einer sicheren Route.
- Gesamtlänge: Die Länge des gesamten IP-Pakets in Bytes.
- Identifikation: Während der Übertragung kann ein IP-Paket in mehrere Fragmente aufgeteilt werden. Dabei wird jedes IP-Paket mit einer Identifikation versehen. Anhand dieser Identifikation und der Quell-Adresse kann ein fragmentiertes IP-Paket beim Ziel-Rechnersystem wieder zusammengefügt werden.
- Flags: Das erste Bit legt fest, ob ein IP-Paket während der Übertragung fragmentiert werden darf. Das zweite Bit ist bei der Zusammensetzung einer fragmentierten Nachricht von Bedeutung. Es bestimmt, ob die enthaltenen Daten aus der Mitte oder vom Ende der ursprünglichen Nachricht stammen.
- Fragment-Offset: Wenn eine Nachricht in mehrere Fragmente zerlegt wird, werden diese Fragmente der Reihe nach durchnummeriert und dann abgeschickt. Da die einzelnen IP-Pakete innerhalb des Netzwerks unterschiedliche Wege nehmen können, treffen die IP-Pakete beim Ziel-Rechnersystem nicht immer in der richtigen Reihenfolge ein. Dieser kann die Teile einer Nachricht erst dann wieder zu einer vollständigen Nachricht zusammensetzen, wenn er sämtliche Teile erhalten hat.
- Time to Live (TTL): Wenn ein IP-Paket vom Quell-Rechnersystem ins Netz geschickt wird, muss das Ziel-Rechnersystem nicht unbedingt erreichbar sein. In einem derartigen Fall würde das IP-Paket solange im Netz kursieren, bis das Ziel-Rechnersystem irgendwann bereit ist, das IP-Paket zu empfangen. Damit dies nicht passiert, wird vom Quell-Rechnersystem für jedes IP-Paket eine Lebensdauer in Sekunden festgelegt. Jedesmal, wenn das IP-Paket von einer Zwischenstation, zum Beispiel einem Router oder einem Netzknoten, weitergeleitet wird, wird der Wert dieses Feldes herabgesetzt. Hat das Feld den Wert Null erreicht, wird das IP-Paket gelöscht beziehungsweise nicht mehr weitergeleitet.
- Protokoll: In diesem Feld wird protokolliert, welche weiteren Protokolle in das IP-Paket eingebettet sind, beispielsweise TCP, UDP, ICMP, usw.
- Header-Prüfsumme: Um die Unversehrtheit eines Headers zu gewährleisten, wird aus den vorhandenen Feldern eine Prüfsumme errechnet und vom Quell-Rechnersystem in dieses Feld eingetragen. Wenn das IP-Paket weitergeleitet wird oder beim Ziel-Rechnersystem angekommen ist, wird die Prüfsumme neu berechnet und mit dem eingetragenen Wert verglichen.
- Quell-Adresse: Dieses Feld enthält die IP-Adresse des Quell-Rechnersystems (Absender).
- Ziel-Adresse: Dieses Feld enthält die IP-Adresse des Ziel-Rechnersystems (Empfänger).

- IP-Optionen: Dieses Feld dient hauptsächlich dem Testen von Netzwerken und der Fehlersuche. Hier können bestimmte Optionen festgelegt werden, die unter anderem Einschränkungen oder Informationen zur Weiterleitung der Daten enthalten. So können hier etwa Informationen für das Source Routing eingefügt werden, das heißt jede Zwischenstation einer Verbindung wird vor der Übertragung genau festgelegt.

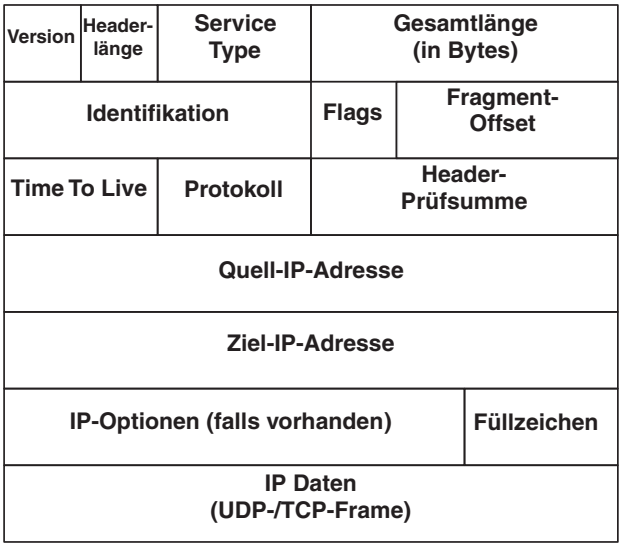

Abb. C.6: Header eines IP-Datenpaketes

C.6.2 Routing Protokolle

In einem komplexen Netzwerk wie dem Internet gibt es viele verschiedene Möglichkeiten, wie Daten von der Quelle an ihr Ziel gelangen. Den Prozess, bei dem die Verbindungswege innerhalb der Netze festgelegt werden, nennt man Routing.

Zu diesem Zweck gibt es an der Verbindungsstelle von zwei oder mehreren Netzen spezielle Rechnersysteme (Router oder Gateways), die nach festgelegten Regeln bestimmen können, welchen Weg die Daten nehmen sollen. Jeder Router benutzt zur Festlegung der Wege eigene Routingtabellen.

Darin sind alle direkt angeschlossenen Rechnersysteme und die Verbindungsstellen zu benachbarten Netzen enthalten. Diese Tabellen können sich in Abhängigkeit von verschiedenen Faktoren wie zum Beispiel der Netzauslastung oder der Verfügbarkeit bestimmter Rechnersysteme oder Netze jederzeit ändern. Dieses Verfahren nennt man dynamisches Routen.

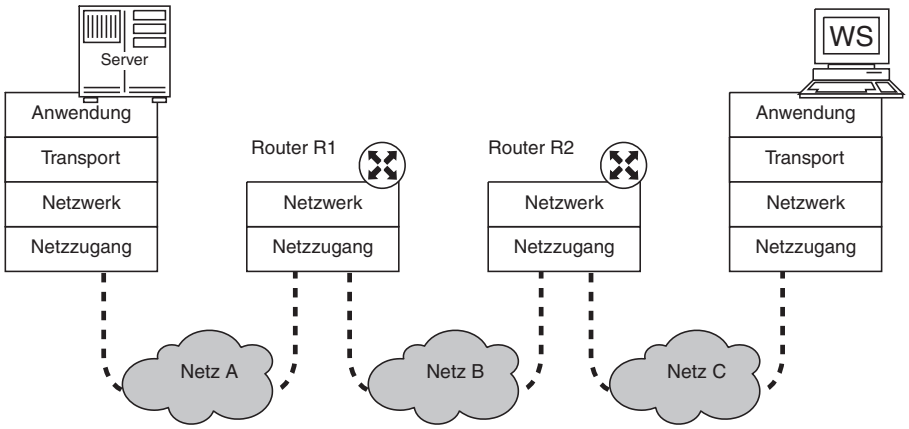

Abb. C.7: Routing über verschiedene Netze

Routing Protokolle wie RIP (Routing Information Protocol) oder OSPF (Open Shortest Path First) dienen dazu, diese Veränderungen der Routen an die beteiligten Systeme weiterzuleiten. Ein Angreifer hat die Möglichkeit, falsche RIP-Informationen zu erzeugen und dadurch unerwünschte Routen beziehungsweise Zwischenstationen einzufügen. Eine dieser Zwischenstationen kann es ihm dann ermöglichen, die Informationen abzuhören oder zu manipulieren. /Boro92/

Als wesentlich sicherer hat sich dagegen die Methode des statischen Routings erwiesen. Bei diesem Verfahren wird nicht jedem einzelnen Router die Entscheidung überlassen, welchen Weg die Daten zu nehmen haben, sondern der Übertragungsweg wird vorher detailliert festgelegt und in die Datenpakete mit eingefügt. Das statische Routing ist wegen der Dynamik im Internet nicht möglich. Im Intranet kann es eine höhere Sicherheit gewährleisten.

Im Gegensatz zu Rechnersystemen, in denen die Daten alle Protokollebenen durchlaufen, werden die Daten bei Routern nur bis zur Netzwerkebene weitergereicht.

C.6.3 ICMP

In einem verbindungslosen Protokoll besteht keine Möglichkeit, den Absender zu informieren, ob das Datenpaket die vorgesehene Lebensdauer (Time To Live) überschritten hat, der Empfänger nicht erreichbar ist oder die Daten unterwegs verloren oder zerstört wurden. Dennoch braucht man eine Möglichkeit, derartige Informationen zwischen Rechnersystemen auszutauschen. Aus diesem Grund wurde das Internet Control Message Protocol (ICMP) in das IP-Protokoll integriert, das ein unverzichtbarer Bestandteil der Internet-Protokolle ist und in keiner Internet-Anwendung fehlen darf.

Router oder Rechnersysteme werten diese Nachrichten meist automatisch aus und veranlassen bestimmte Aktionen oder Umkonfigurationen. Ein Angreifer wird so in die Lage versetzt, durch Absenden falscher ICMP-Informationen Einfluss auf das System zu nehmen und bestimmte Reaktionen zu erzeugen, die es ihm später ermöglichen, die Funktionsfähigkeit zu beeinträchtigen oder ins System einzubrechen.

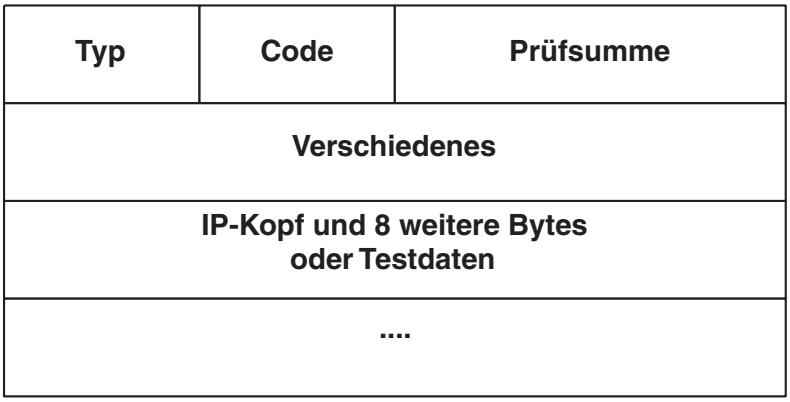

Abb. C.8: Header eines ICMP-Datenpaketes

Das ICMP-Datenpaket enthält Fehler- und Diagnoseinformationen. Es wird intern vom IP angestoßen und verarbeitet. Obwohl die ICMP-Nachrichten in ein IP-Datenpaket gekapselt werden, bilden sie kein höheres Protokoll, wie zum Beispiel TCP oder UDP, sondern sind ein direkter Bestandteil des IP-Protokolls. Das IP-Protokoll kann in der Praxis nicht ohne das ICMP-Protokoll verwendet werden.

ICMP-Nachrichten werden nur von dem Rechnersystem abgesendet, das den Fehler versendet oder ausgelöst hat, und direkt an den ursprünglichen Absender der Daten zurückgeschickt.

Man unterscheidet verschiedene Typen von ICMP-Nachrichten. Diese werden durch eine Ziffer im Header eines ICMP-Paketes (Typ) gekennzeichnet und können je nach ICMP-Datentyp unterschiedliche Daten enthalten. Die wichtigsten sind:

- Echo Reply (0): Diese Nachricht wird ausgelöst, sobald eine EchoRequest-Nachricht von einem anderen Rechnersystem empfangen wurde. Im Datenfeld dieses Paketes werden Testdaten versendet, die unter anderem Aufschluss über Betriebsbereitschaft, Laufzeit usw. geben.
- Destination Unreachable (3): Wenn eine Nachricht nicht an ihr beabsichtigtes Ziel gelangt, wird diese Nachricht an den Absender zurückgesandt. Ein Grund dafür kann sein, dass ein Netzwerk, ein Host, ein Protokoll oder ein Port nicht

erreichbar waren. Möglicherweise wäre auch während der Übertragung eine Fragmentierung des gesendeten Datenpakets nötig gewesen, dies wurde aber durch das Setzen des Fragmentierungsbits im Header des IP-Pakets verboten. Ein weiterer möglicher Grund ist, dass ein bestimmtes Rechnersystem, das vom Absender in der Source-Routing-Option eingetragen wurde, nicht erreichbar war. Die Meldung »Destination Unreachable« kann beispielsweise von einem Angreifer dazu missbraucht werden, alle Verbindungen zwischen den beteiligten Rechnersystemen zu unterbrechen.

- Source Quench (4): Wenn ein Router nicht über die entsprechende Kapazität verfügt, um die empfangenen Daten direkt weiterzuleiten, sendet er an den Absender diese Nachricht. Dieser muss dann die Aussenderate von weiteren Nachrichten verringern.
- Redirect (5): Wenn ein Router erkennt, dass der Absender, anstatt direkt an den nächsten Router zu senden, einen unnötigen Umweg nimmt, sendet er diese Nachricht an den Absender. Das Datenfeld enthält die IP-Adresse des direkt erreichbaren Routers und wird in die Routingtabelle des Absenders eingetragen. Dieses Vorgehen kann von einem Angreifer missbraucht werden, um unerwünschte Routen zu konfigurieren und die Daten unterwegs abzuhören oder zu manipulieren.
- Echo Request (8): Diese Nachricht wird ausgesendet, um zu überprüfen, ob der beabsichtigte Empfänger erreichbar ist. Zusammen mit der Echo-Reply-Antwort auf diese Nachricht lassen sich Rückschlüsse über Betriebsbereitschaft, Laufzeit usw. ziehen.
- Time exceeded (11): Wenn ein IP-Datenpaket seine Lebensdauer (Time to Live) überschreitet, bevor es sein Ziel erreicht hat, wird es verworfen. Der Absender erhält dann von dem Rechnersystem, das diesen Vorgang ausgeführt hat, diese Meldung.
- Parameter Problem (12): Wenn ein IP-Datenpaket aufgrund fehlerhafter Angaben im Header verworfen wurde, erhält der Absender des Paketes diese Nachricht.

Ein Beispiel für die Benutzung von ICMP-Nachrichten ist der Befehl »Ping«, der auf den meisten Rechnersystemen verwendet wird. Dieser Befehl wird auf der Benutzerebene erzeugt und sendet eine oder mehrere ICMP-Nachrichten an den Empfänger. Dabei werden die Befehle »EchoRequest« und »EchoReply« verwendet, und der Absender erhält Informationen über:

- die IP-Adresse des Empfängers und die Erreichbarkeit des Rechnersystems,
- die MAC-Adresse des nächsten Routers beziehungsweise Rechnersystems,
- Routing-Einträge,
- Laufzeit der Daten,
- Datenverluste.

C.6.4 Portnummern

Ein wichtiger Begriff, der im Zusammenhang mit den Kommunikationsprotokollen auf der Transportebene immer wieder auftaucht, sind die so genannten Ports. Ein Rechnersystem, zum Beispiel ein Server, muss in der Lage sein, mit mehr als einem anderen Rechnersystem gleichzeitig zu kommunizieren. Anderenfalls wäre der Server während einer aufgebauten Verbindung für alle anderen Rechnersysteme nicht erreichbar. Bestimmte Anwendungen erfordern auch den gleichzeitigen Aufbau von zwei oder mehr Verbindungen, zum Beispiel jeweils eine für die Übertragung von Kommandos und für die Datenübertragung. Zu diesem Zweck verfügt jedes Rechnersystem über so genannte Portnummern, die zusammen mit der Netzwerk-Identifikation und der Rechnersystem-Identifikation einen Kommunikationsendpunkt (Port) bilden. Dieser Aufbau ist in etwa vergleichbar mit einer Telefonnummer. Die Netzwerk-Identifikation ließe sich mit der Vorwahl vergleichen, die Rechnersystem-Identifikation mit der Rufnummer und die Portnummer mit der Nebenstelle.

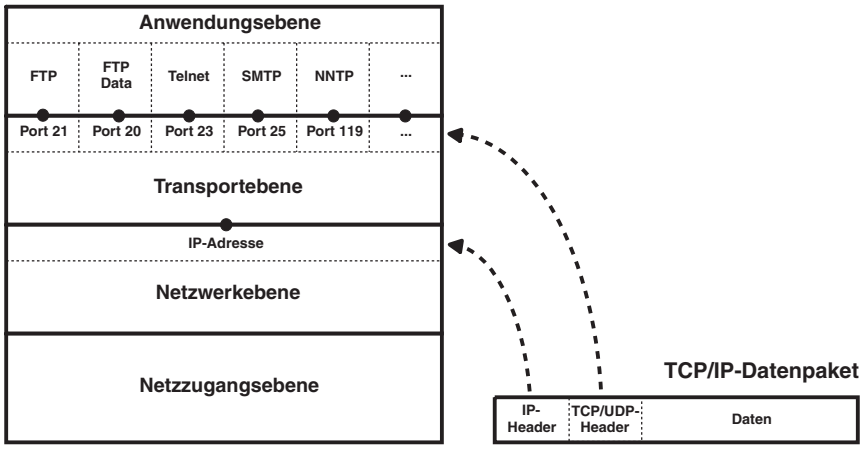

Abb. C.9: Eindeutige Identifizierung des Kommunikationsendpunkts durch IP-Adresse und Portnummer

Da eine Portnummer aus 16 Bit aufgebaut wird, wäre ein Rechnersystem mit einer IP-Adresse rein theoretisch in der Lage, gleichzeitig 65 535 Verbindungen zu anderen Kommunikations-Endpunkten herzustellen. Dies ist in der Praxis jedoch nicht der Fall, da die unterschiedlichen Kommunikationsprotokolle wie TCP oder UDP unterschiedliche Adressräume verwenden, die zwar identische Portnummern haben können, aber physikalisch nicht übereinstimmen.

Die Dienste der Anwendungsschicht (beispielsweise Telnet oder FTP) erfordern, wie weiter unten erläutert wird, eine bestehende virtuelle Verbindung zwischen

zwei Rechnersystemen. Um diese Verbindung überhaupt aufbauen zu können, muss dem aktiven, Kontakt aufnehmenden Rechnersystem (Client) aber zumindest ein Port bekannt sein, auf dem der entsprechende Dienst des passiven Rechnersystems (Server) erreichbar ist.

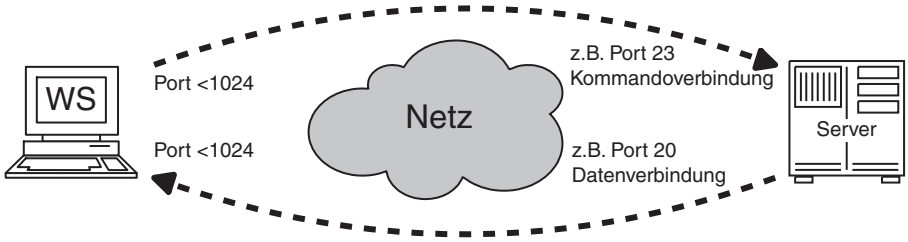

Abb. C.10: Verbindung zwischen zwei Rechnern (z. B. FTP-Verbindung)

Zu diesem Zweck wurden bestimmte Portnummern (well-known ports) definiert, die standardmäßig für die entsprechenden Dienste zur Verfügung stehen. Der Client kann dem Server dann über diesen Port seine eigene verwendete Portnummer mitteilen, und einem Verbindungsaufbau steht damit nichts mehr im Wege.

Dienst	Portnummer	Protokoll
echo	7	UDP oder TCP
ftp-data	20	TCP
ftp	21	TCP
telnet	23	TCP
smtp	25	TCP
dns	53	UDP
tftp	69	UDP
finger	79	TCP
http	80	TCP
nntp	119	TCP

Tabelle 3.1: Auszug aus der Liste mit well-known-ports

C.6.5 UDP

Das User Datagram Protocol (UDP) ist ein verbindungsloses Kommunikationsprotokoll der Transportebene. Es benutzt das untergeordnete IP-Protokoll, um Nachrichten von einem Rechnersystem zum anderen zu transportieren. In Ergänzung zum IP-Protokoll kann es aber zwischen mehreren Anwendungsdiensten (Ports) des Empfängers unterscheiden.

Der entscheidende Vorteil von UDP ist der geringe Overhead. Dadurch eignet es sich beispielsweise zur Übertragung von kleinen Datenmengen. Hier ist es einfacher, die Daten bei einem aufgetretenen Fehler einfach noch einmal zu übertragen, als eine garantiert fehlerfreie Verbindung aufzubauen. Dazu braucht man einen Frage-Antwort-Dialog zwischen zwei Rechnersystemen. Wenn nach einer bestimmten Zeit keine Antwort vom Ziel-Rechnersystem kommt, wird das Datenpaket noch einmal auf den Weg geschickt. Eine weitere Möglichkeit ist, einer übergeordneten Anwendung die Sicherungsfunktionen zu überlassen. In diesem Fall ist es unnötig, die Datenübertragung doppelt zu überwachen.

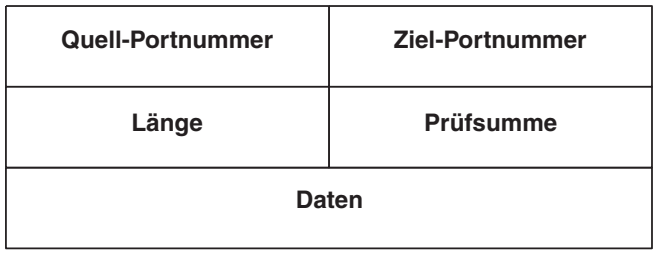

Abb. C.11: Header eines UDP-Datenpaketes

- Das UDP-Protokoll erzeugt keinerlei Transportquittungen oder andere Sicherheitsmaßnahmen, um die Korrektheit der Übertragung zu bestätigen. Es werden keine Informationen an das Quell-Rechnersystem zurückgegeben.
- Wenn die Daten auf dem Weg zum Ziel-Rechnersystem in mehrere Fragmente aufgeteilt wurden, können die Daten unterschiedliche Wege nehmen. So können Daten im Ziel-Rechnersystem in vertauschter Reihenfolge ankommen. Das UDP-Protokoll gibt die Daten unsortiert an die übergeordnete Anwendung weiter.
- Wenn die Daten schneller eintreffen, als das Ziel oder ein Rechnersystem im Netz sie verarbeiten kann, beispielsweise weil es überlastet ist, können die Daten verloren gehen. Es gibt keinerlei Informationen, die den Datenfluss zwischen den Rechnersystemen steuern oder kontrollieren.
- Der Header enthält zwei 16-Bit-Portnummern, die unabhängig von den beim TCP-Protokoll benutzten Portnummern sind.
- Grundsätzlich ist diese Form der Datenübertragung nicht vertrauenswürdig und sehr leicht zu manipulieren. Auf exponierten Rechnersystemen, die öffentlich zugänglich sind, sollte das UDP-Protokoll vermieden werden, es sei denn, eine übergeordnete Ebene (Anwendungsebene) übernimmt die Sicherungsfunktionen.

C.6.6 TCP

Das Transmission Control Protocol (TCP) ist nach dem IP-Protokoll das wichtigste Transportprotokoll. Das TCP-Protokoll ist ein verbindungsorientiertes Kommuni-

kationsprotokoll der Transportebene, das heißt, bevor die Daten von der Quelle zum Ziel geschickt werden, wird eine virtuelle Verbindung hergestellt, die in beide Richtungen (duplex) funktioniert. Die Daten werden in Form von festgelegten Paketen übertragen und die korrekte Übertragung durch unterschiedliche Verfahren sichergestellt.

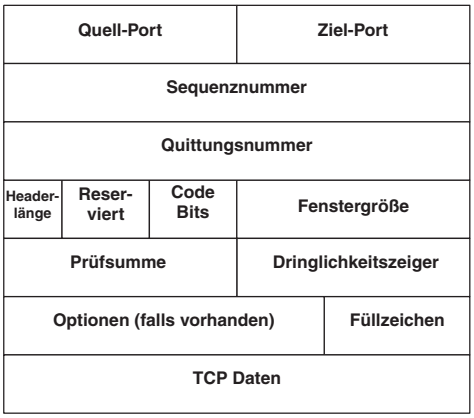

Abb. C.12: Header eines TCP-Datenpaketes

- Der Header eines TCP-Datenpaketes enthält unter anderem zwei 16-Bit-Portnummern, die zur Identifikation der Kommunikationsendpunkte von Quelle und Ziel dienen. Über die standardisierte Zuordnung (well-known ports) können die unterschiedlichen Dienste der Anwendungsschicht Verbindung miteinander aufnehmen.
- Beim Aufbau einer Verbindung generiert jede TCP-Einheit eine Anfangs-Sequenznummer. Diese Nummern werden ausgetauscht und gegenseitig bestätigt. Jedes gesendete Datensegment enthält eine fortlaufende Sequenznummer, wobei Duplikate ausgeschlossen werden. Anhand dieser Sequenznummern können die Daten beim Ziel, unabhängig vom Zeitpunkt des Eintreffens der Segmente, in der korrekten Reihenfolge zusammengesetzt werden.
- Die Quittungsnummer wird vom Ziel-Rechnersystem an das Quell-Rechnersystem übermittelt. Die Quittungsnummer ist immer um eins höher als die letzte Sequenznummer, die korrekt empfangen wurde. Anhand dieser Nummer kann das Quell-Rechnersystem die Pakete, die noch für eine eventuell erforderliche Wiederholung vorhanden sind, aus seinem Datenpuffer löschen.
- Das Feld Headerlänge bestimmt die Länge des Protokollkopfes in 32-Bit-Worten und damit den Anfang der Nutzdaten.
- Die Codebits oder Flags lösen bestimmte Reaktionen im TCP-Protokoll aus. Auf die genaue Bedeutung soll hier aber nicht weiter eingegangen werden.

- Ein Quell-Rechnersystem darf nicht mehr Daten abschicken, als ein Ziel-Rechnersystem verarbeiten oder weiterleiten kann. Dazu gibt das Ziel-Rechnersystem im Feld »Fenstergröße« an, wieviel Daten es zur sofortigen Verarbeitung in seinem Puffer zwischenspeichern kann.
- Jedes Datensegment enthält eine Prüfsumme, die aus dem Header und den Nutzdaten gebildet wird. Das Ziel-Rechnersystem errechnet aus den erhaltenen Daten ebenfalls eine Prüfsumme und vergleicht diese mit dem Datenfeld im Header des Datensegmentes. Stimmen die Werte überein, so schickt das Ziel-Rechnersystem eine positive Bestätigung an das Quell-Rechnersystem. Ein beschädigtes Datensegment wird zunächst ignoriert und nach einer angemessenen Wartezeit erneut angefordert.
- Für einige Dienste wurde ein Mechanismus konzipiert, mit dem der Server dazu veranlasst werden kann, dringende Anweisungen auszuführen, obwohl noch nicht alle Eingabedaten verarbeitet wurden. Diesem Zweck dient der Dringlichkeitszeiger (Urgent Data), der auf das Datenbyte vor der dringenden Meldung verweist (zum Beispiel die Übertragung eines Ctrl-C-Zeichens bei einer Telnet-Session).
- Normalerweise wird in einem TCP-Paket als Option nur die maximale Segmentgröße (Maximum Segment Size) verwendet. Damit teilt das Quell-Rechnersystem dem Ziel-Rechnersystem die maximale Größe der zu sendenden Datensegmente mit. Die weiteren Optionen sind No Operation und End of Option List.
- Das Feld »Füllzeichen« wird dazu benutzt, die Länge des Optionsfelds auszugleichen, damit die Gesamtgöße des Headers immer ein Vielfaches eines 32-Bit-Wortes ergibt.

Jedes Segment enthält eine Zeitüberwachung, das heißt, dass ein Ziel-Rechnersystem nach einer bestimmten Zeit eine Quittung über die enthaltenen Pakete an das Quell-Rechnersystem zurückschicken muß. Wenn ein Quell-Rechnersystem nach Ablauf der Quittungszeit keine Antwort erhalten hat, wird das entsprechende Datensegment erneut gesendet.

Damit haben wir die Protokolle der Transportschicht abgehandelt. In den folgenden Kapiteln werden die Protokolle und Dienste der Anwendungsschicht genauer betrachtet.

C.6.7 DNS

Um Rechnersystem-Namen entsprechende IP-Adressen zuordnen zu können, musste man in den Anfängen des Internet eine Liste der Rechnersystem-Namen von einem zentralen Server regelmäßig per Datenübertragung auf jedem Rechnersystem aktualisieren. Durch die rasante Ausbreitung des Internet ist diese Methode nicht mehr praktikabel. Aus diesem Grund wurde der Domain Name Service (DNS) entwickelt. Damit werden die Rechnersystem-Namen nicht mehr auf

jedem einzelnen Rechnersystem registriert, sondern auf speziell für diesen Dienst bereitgestellten Servern innerhalb jedes Teilnetzwerks. Die einzelnen Rechnersysteme senden bei Bedarf Abfragen (Queries) an diese Namen-Server, die als Antwort die entsprechende IP-Adresse oder den dazugehörigen Rechnersystem-Namen liefern.

Um dieses System benutzen zu können, ist jedes Internet-Teilnetzwerk dazu verpflichtet, einen Domain-Namens-Server zu betreiben oder betreiben zu lassen, auf dem sich so genannte Zonen-Datenbanken befinden. In diesen Datenbanken befinden sich unter anderem zwei Tabellen, mit der einem bestimmten Rechnersystem-Namen die dazugehörige IP-Adresse zugeordnet werden kann und umgekehrt.

Prinzipiell muss beachtet werden, dass alle vom DNS zur Verfügung gestellten Informationen missbraucht werden können, da diese Informationen nicht durch kryptographische Verfahren geschützt werden. Um Zugriff auf ein Rechnersystem eines Netzes zu erhalten, benötigt ein Eindringling zunächst dessen IP-Adresse, die er entweder durch blindes Probieren oder einfacher durch Auswertung der DNS-Informationen erhalten kann. Mittels dieser Informationen kann der Eindringling dann beispielsweise eine Adressfälschung (IP-Spoofing) vornehmen und damit Zugriff auf Rechnersysteme innerhalb des zu schützenden Netzes erhalten.

C.6.8 Telnet

Das Telnet-Protokoll erlaubt einem Benutzer (Client), eine Terminalsitzung auf einem entfernten Rechnersystem (Server) durchzuführen. Dazu wird zuerst eine TCP-Verbindung zwischen Client und dem Port 23 des Servers aufgebaut. Anschließend wird eine Login-Prozedur durchgeführt, in der sich der Benutzer durch die Angabe des Benutzernamens und des Passwortes identifizieren und authentisieren muss.

Abb. C.13: Beispiel einer Telnet-Sitzung

Bei dieser Authentikation über den Telnet-Dienst wird das Passwort im Klartext übertragen. Dabei besteht die Gefahr, dass sich ein Angreifer auf dem Übertragungsweg in eine autorisierte Telnet-Verbindung eingeschaltet hat, um sicherheitsrelevante Informationen (zum Beispiel Passwörter) abzuhören, oder um eigene Befehle in die Telnet-Verbindung einzugeben.

Anschließend kann der Angreifer sich unter Angabe der vorher abgehörten Identität auf dem Server anmelden (Maskerade-Angriff), um für ihn relevante Daten auszuspionieren, zu manipulieren oder zu löschen.

C.6.9 FTP

Das File Transfer Protocol (FTP) ermöglicht den Austausch und die Übertragung von beliebigen Dateien, ähnlich einem Datei-Manager, zwischen entfernten Rechnersystemen ähnlich einem Datei-Manager. Bei der Nutzung von FTP werden zwei unterschiedliche Verbindungen genutzt. Der Client baut als erstes von einem beliebigen Port eine Verbindung zum Port 21 des Servers auf. Über diese Verbindung sendet der Client dem Server die Kommandos. Mit dem Kommando »port« teilt der Client dem Server mit, über welchen Port er die Daten übertragen soll. Der Server baut nun anhand dieser Angaben eine TCP-Verbindung vom Port 20 zum angegebenen Port des Client auf und überträgt die angeforderten Daten.

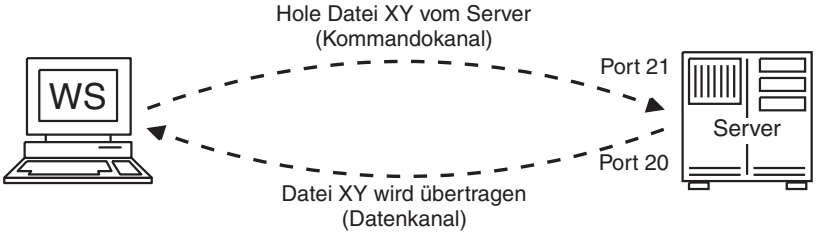

Abb. C.14: Beispiel einer FTP-Verbindung

Während der Client die Kommandoverbindung zum Port 21 des Servers aufbaut, ist der Server für den Aufbau des Datenkanals von seinem Port 20 zu einem beliebigen Port des Clients verantwortlich. Dies stellt eine Sicherheitslücke dar, da sich ein Angreifer selbst als Server ausgeben oder eigene Daten in die Kommunikation mit dem Server einfügen kann. Damit bekommt er die Möglichkeit, gefährliche Programme wie Viren oder Trojanische Pferde in das Rechnersystem einzuschleusen, die anschließend Daten ausspionieren oder zerstören können. Eine Abhilfe bietet die passive Methode des Verbindungsaufbaus.

C.6.10 SMTP

Das Simple Mail Transport Protocol (SMTP) ist ein einfaches Protokoll für die Übertragung von elektronischen Nachrichten (E-Mails) durch das Internet/Intranet. Das E-Mail-System besteht aus zwei Komponenten: dem Message Transfer Agent (MTA) und dem Mail User Agent (UA). Der Message Transfer Agent wird vom jeweiligen Internetprovider oder Intranetbetreiber installiert und hat die Aufgabe, die elektronische Post über die Teilnetzwerke an ihren Bestimmungsort wei-

terzuleiten. Der Mail User Agent ist nichts anderes als die E-Mail-Software, mit der der Benutzer je nach Programm seine elektronische Post verfassen, versenden und empfangen kann. Die elektronische Post wird auf dem Message Transfer Agent so lange gespeichert, bis der Benutzer sie mit Hilfe seiner Software auf das lokale Rechnersystem lädt.

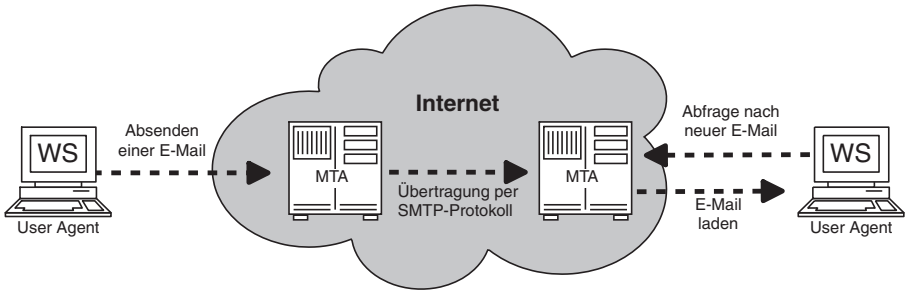

Abb. C.15: Funktionsweise des E-Mail-Dienstes

Der Übertragungsmodus der Nachrichten durch das Internet mit Hilfe des SMTP-Protokolls ist sehr einfach aufgebaut und wird im Klartext durchgeführt. Es ist bisher nicht möglich, die Identität des Absenders zu überprüfen. Dadurch ist es möglich, Nachrichten mit beliebigem oder gefälschtem Absender (Mail-Spoofing) über das Internet zu verbreiten. Einziger Schutz für den Anwender ist die Verwendung von kryptographischen Verfahren wie zum Beispiel der digitalen Signatur mit Verschlüsselung.

Ein weiterer Schwachpunkt des E-Mail-Systems ist das Programm Sendmail als die am weitesten verbreitete Umsetzung eines Message Transfer Agent unter Verwendung des SMTP-Protokolls. Die Komplexität und umfassende Leistungsfähigkeit macht Sendmail gleichzeitig sehr fehleranfällig und schwer zu konfigurieren. Dadurch wurden in den letzten Jahren immer wieder Sicherheitslücken entdeckt, mit denen Daten von Angreifern kopiert, manipuliert oder zerstört werden konnten.

C.6.11 HTTP

Wenn ein Anwender von seinem Rechnersystem aus eine »Reise« ins Internet unternimmt, benötigt er dafür ein spezielles Programm (Browser), das unter anderem die Darstellung von so genannten HTML-Dokumenten ermöglicht. HTML (Hyper Text Markup Language) ist ein Standard, der den Aufbau und das Format der für das World Wide Web charakteristischen Seiten definiert. Dabei muss es sich nicht nur um Textinformationen handeln. Es können gleichzeitig auch Grafiken, Töne oder Animationen und Videos übertragen werden. Um diese Informationen

im Internet übertragen zu können, wurde ein spezielles Kommunikationsprotokoll entwickelt, das Hypertext Transfer Protokoll (HTTP).

Das HTTP-Protokoll arbeitet nicht Session-orientiert, das heißt, die Übertragung eines HTML-Dokuments erfolgt unabhängig von einem zuvor übertragenen HTML-Dokument. Dazu wird, wie bei anderen Kommunikationsprotokollen der Anwendungsschicht (z. B. FTP oder Telnet), zunächst eine virtuelle Verbindung (TCP) zwischen Client und Server aufgebaut. Diese bleibt aber nicht über mehrere Anforderungen des Clients hinweg bestehen, sondern wird sofort nach dem Versenden der Antwort vom Server wieder abgebaut.

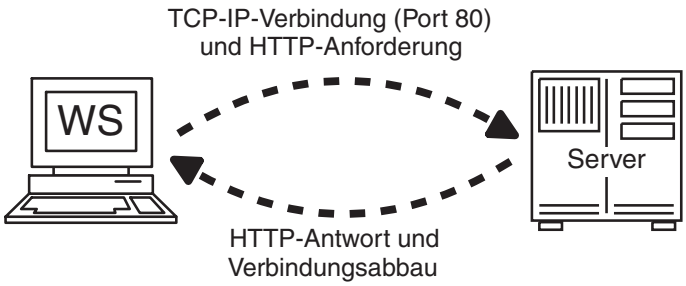

Abb. C.16: Prinzip einer HTTP-Verbindung

Wenn ein Benutzer eine beliebige Seite auf einem Server aufruft, so liest der Browser zunächst das HTML-Dokument und baut den Text entsprechend der angegeben Formatierungen (Größe, Farbe, Schriftart usw.) auf. Wenn eine WWW-Seite zusätzliche Informationen enthält, beispielsweise Grafiken, Töne oder Videos, so ist im HTML-Dokument der genaue Speicherort dieser Datei verzeichnet. Der Browser baut dann über das HTTP-Protokoll eine erneute Verbindung auf und holt sich die Grafik, Klangdatei, Videodatei oder sonstige Information vom Server. Nach dem Abschluss der Übertragung wird diese Information vom Browser auf dem Rechnersystem des Anwenders direkt dargestellt beziehungsweise wiedergegeben. Die meisten Browser kann man so konfigurieren, dass sie nur die gewünschten Informationen darstellen. Wenn zum Beispiel nur eine sehr langsame Verbindung ins Internet vorhanden ist, so kann man auf die Darstellung von großen Dateien wie Grafiken verzichten und nur die Textinformationen darstellen.

C.6.12 NNTP

Das Internet bietet durch seine enorme Größe eine Fülle von unterschiedlichen Informationen. Da die Entwicklung auf fast allen Wissensgebieten schnell fortschreitet, ist man darauf angewiesen, ständig auf dem neuesten Wissensstand zu sein. Eine Möglichkeit dazu bieten die so genannten Newsserver.

Manche Newsserver haben sich wegen der Vielzahl an Informationen auf spezielle Themengebiet spezialisiert.

Um die Newsserver ständig auf dem aktuellen Stand zu halten, tauschen diese untereinander in regelmäßigen Abständen neu eingegangene Beiträge aus. Innerhalb des Internet erfolgt dieser Datenaustausch mittels eines eigenständigen Protokolls. Das Network News Transfer Protocol (NNTP) wird benutzt, um neue Beiträge an den nächsten Newsserver zu versenden. Dieser überträgt die aktuellen Informationen dann weiter zum nächsten usw. Diesen Vorgang bezeichnet man als »News Feed«. Da einige dieser Server die Informationen nicht nur an einen, sondern gleich an mehrere Server weiterleiten, kann sich eine neue Information innerhalb weniger Tage innerhalb des gesamten Internet ausbreiten.

Das heute benutzte NNTP-Protokoll verfügt über einen Mechanismus, mit dem es möglich ist, nur jene Artikel zu übertragen, die auf dem Rechnersystem des Empfängers noch nicht vorhanden sind.