



Ziele des Kapitels

- Aufbau eines Internetworks
- Grundlagen des OSI-Modells
- Unterschied zwischen verbindungsorientierten und verbindungslosen Diensten
- Die unterschiedlichen Adresstypen in einem Internetwork
- Grundlagen von Flusskontrolle und Fehlerprüfung

Grundlagen des Internetworking

Dieses Kapitel stellt die grundlegenden Konzepte und Begriffe aus dem Bereich des Internetworking vor. So wie das Buch als Ganzes dem Verständnis der modernen Netzwerk-Technik dient, werden in diesem Kapitel Themen, die im Allgemeinen bekannt sind, nur kurz behandelt. Dazu gehören die Flusststeuerung, die Fehlerprüfung und das Multiplexing, jedoch wird der Schwerpunkt auf die Darstellung des OSI-Modells (*Open System Interconnect*) im Zusammenhang mit Netzwerk-/Internetworking-Funktionen gelegt. Es wird ein Überblick zu Adressierungsverfahren in Hinblick auf das OSI-Modell gegeben. Das OSI-Modell stellt den Grundbaustein für Internetworks dar, weshalb das Verstehen des Modellkonzepts beim Verstehen der komplexen Teile hilft, die ein Internetwork ausmachen.

1.1 Was ist ein Internetwork?

Ein Internetwork besteht aus mehreren einzelnen Netzwerken, die über dazwischengeschaltete Netzwerk-Geräte miteinander verbunden sind, sodass ein großes Netzwerk entsteht. Internetworking bezieht sich auf die Industrie, Produkte und Verfahren, die es ermöglichen, ein Internetwork aufzubauen und zu administrieren. Bild 1.1 zeigt verschiedene Netzwerk-Technologien, die über Router oder andere Netzwerk-Geräte miteinander zu einem Internetwork verbunden werden können:

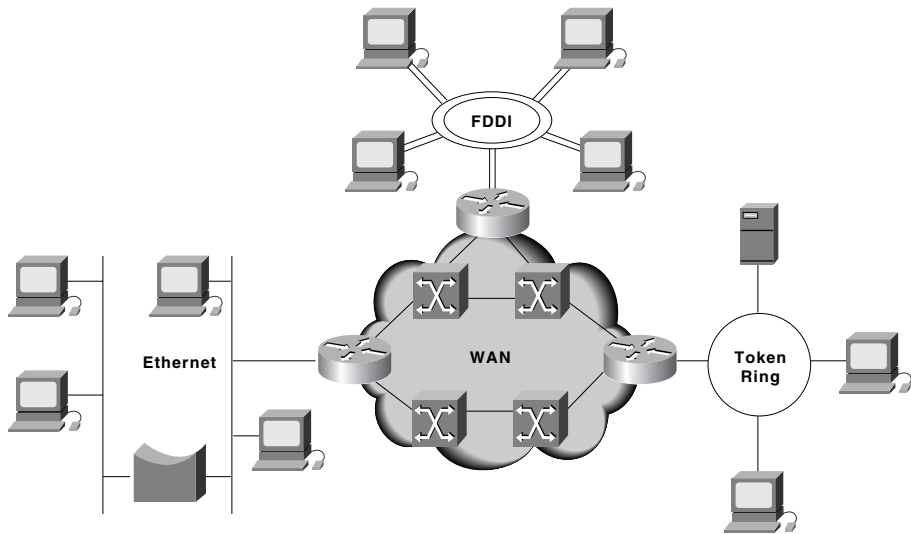


Bild 1.1: Verschiedene Netzwerk-Technologien können zu einem Internetnetwork verbunden werden

1.1.1 Die Geschichte des Internetworking

Die ersten Netzwerke waren Netzwerke im Teilnehmerbetrieb, bei denen Großrechner (Mainframes) mit angeschlossenen Terminals zum Einsatz kamen. Solche Umgebungen wurden mit der System Network Architecture (SNA) von IBM und der Netzwerk-Architektur von Digital eingerichtet.

ANMERKUNG

Hier scheint man sich auf die nordamerikanische Welt zu beschränken, denn Siemens hat/hatte mit seinem Großrechner-Betriebssystem BS2000 und dem zugehörigen Transdata-Netz Gleiches zu bieten.

Lokale Netzwerke (Local Area Network – LAN) entstanden während der PC-Revolution. In einem LAN konnten viele Benutzer, die räumlich nicht zu weit voneinander entfernt waren, Dateien und Nachrichten austauschen und auf Ressourcen gemeinsam zugreifen, z. B. auf Datei-Server.

Weitverkehrsnetze (Wide Area Network – WAN) verbinden LANs mit räumlich weiter voneinander entfernten Benutzern. Zu den für die Verbindung von LANs verwendeten Methoden gehören z. B. T1, T3, ATM, ISDN, ADSL, Frame Relay oder Funkverbindungen. Beinahe täglich entstehen neue Methoden zur Verbindung entfernter LANs.

Heute sind Hochgeschwindigkeits-LANs und vermittelte Internetworks weit verbreitet und häufig im Einsatz, weil die Übertragungsgeschwindigkeiten sehr hoch sind und sehr bandbreiten-intensive Anwendungen wie Multimedia und Video-Konferenzen unterstützt werden.

Das Internetworking entwickelte sich als Lösung der folgenden drei Schlüsselprobleme: voneinander isolierte LANs, doppelte Haltung von Ressourcen und fehlende Netzwerk-Verwaltung. Aufgrund der abgeschlossenen LANs war es unmöglich, dass verschiedene Büros oder Abteilungen elektronisch miteinander kommunizierten. Bei der doppelten Haltung von Ressourcen musste die gleiche Hard- bzw. Software in jedem Büro und in jeder Abteilung vorhanden sein und vom eigenen Support eingerichtet und verwaltet werden. Für die Netzwerk-Verwaltung gab es keine zentralisierte Verwaltung und Verfahren für die Fehlerbehebung.

1.1.2 Die Herausforderungen des Internetworking

Ein funktionierendes Internetwork zu implementieren ist keine leichte Aufgabe. Dabei sind eine Vielzahl von Anforderungen zu berücksichtigen, insbesondere was die Connectivity, die Zuverlässigkeit, das Netzwerk-Management und die Flexibilität betrifft. Jeder dieser Bereiche ist ein Schlüssel für den Aufbau eines effizienten und effektiven Internetworks.

Eine der Herausforderungen beim Verbinden verschiedener Systeme stellt die Unterstützung der Kommunikation zwischen unterschiedlichen Technologien dar. So können in verschiedenen Niederlassungen z.B. verschiedene Medien mit verschiedenen Datenraten verwendet werden oder auch verschiedene Systeme, die miteinander kommunizieren müssen.

Eine weitere wichtige Überlegung betrifft die Betriebszuverlässigkeit eines Internetworks. Sowohl einzelne Benutzer als auch ein Unternehmen benötigen konsistenten, zuverlässigen Zugriff auf die Netzwerk-Ressourcen.

Unternehmen sind heute sehr auf Datenaustausch angewiesen – Internetworks müssen daher eine gewisse Zuverlässigkeit aufweisen. Da wir nun einmal nicht in einer perfekten Welt leben, weisen viele große Internetworks Redundanzen auf, um die Kommunikation auch noch im Falle von Problemen aufrecht erhalten zu können.

Des Weiteren muss das Netzwerk-Management über einen zentralen Support und Möglichkeiten der Fehlerbeseitigung im Internetwork verfügen. Konfiguration, Sicherheit, Performance und weitere Anforderungen müssen ausreichend berücksichtigt werden, um die Funktionalität eines Internetworks gewährleisten zu können. Sicherheit ist unentbehrlich – viele Leute denken bei Netzwerk-Sicherheit an den Schutz des privaten Netzwerks ge-

gen Angriffe von außen. Jedoch ebenso wichtig ist es, das Netzwerk gegen Angriffe von innen abzusichern, schon deshalb, weil die meisten Sicherheitsverstöße intern auftreten. Netzwerke müssen außerdem davor geschützt werden, als Werkzeug für Angriffe auf externe Sites verwendet zu werden.

Anfang des Jahres 2000 wurden viele größere Websites Opfer von Distributed Denial Of Service (DDOS)-Attacken. Diese Angriffe wurden möglich, weil eine große Zahl der zu dieser Zeit an das Internet angeschlossenen privaten Netzwerke nicht ausreichend geschützt waren. Diese privaten Netzwerke wurden von den Angreifern als Werkzeuge benutzt.

Da nichts in dieser Welt bleibt wie es ist, müssen Internetworks flexibel genug sein, um sich mit neuen Anforderungen verändern zu können.

1.2 Das Open System Interconnection-Referenzmodell

Das OSI-Referenzmodell (Open System Interconnection – OSI) beschreibt den Weg, den Daten von einer Software-Anwendung auf einem Computer über das Netzwerk-Medium bis zu einer Anwendung auf einem anderen Rechner nehmen. Das OSI-Referenzmodell ist ein Konzept, das diesen Weg in sieben Schichten unterteilt, die jeweils eine einzelne Netzwerk-funktion spezifizieren. Dieses Modell wurde 1984 von der International Standardization Organization (ISO) entwickelt und wird heute als das primäre Architekturmodell für die Kommunikation zwischen Computern betrachtet. Das OSI-Modell unterteilt die Aufgaben, die beim Transport von Daten über ein Netzwerk anfallen, in sieben kleinere, überschaubare Gruppen. Dabei wird jeder der sieben OSI-Schichten eine Aufgabe oder eine Gruppe von Aufgaben zugeordnet. Jede Schicht ist sinnvollerweise in sich abgeschlossen, sodass die der Schicht zugeordnete Aufgabe unabhängig von anderen implementiert werden kann. So kann die Implementation für eine Schicht aktualisiert werden, ohne dass andere Schichten davon betroffen sind. Die folgende Liste nennt die sieben Schichten des OSI-Referenzmodells:

- Schicht 7 – Application (Anwendung)
- Schicht 6 – Presentation (Darstellung)
- Schicht 5 – Session (Kommunikation, Sitzung)
- Schicht 4 – Transport (Transport)
- Schicht 3 – Network (Vermittlung, Netzwerk)
- Schicht 2 – Data Link (Sicherung, Verbindung)
- Schicht 1 – Physical (physikalische Schicht)

ANMERKUNG

Eine praktische Eselsbrücke, um sich die sieben Schichten zu merken, ist der Satz »All people seem to need data processing«. Der Anfangsbuchstabe jedes Wortes bezieht sich auf eine Schicht.

- All – Application Layer
- People – Presentation Layer
- Seem – Session Layer
- To – Transport Layer
- Need – Network Layer
- Data – Data link Layer
- Processing – Physical Layer

Bild 1.2 stellt das sieben-schichtige OSI-Referenzmodell grafisch dar.

7	Anwendung
6	Darstellung
5	Kommunikation
4	Transport
3	Netzwerk
2	Sicherung
1	Physikalisch

Bild 1.2: Das OSI-Referenzmodell besteht aus sieben voneinander unabhängigen Schichten

1.2.1 Eigenschaften der OSI-Schichten

Die sieben Schichten des OSI-Referenzmodells können in zwei Gruppen unterteilt werden: höhere bzw. *obere Schichten* und niedrige bzw. *untere Schichten*.

Die *oberen Schichten* des OSI-Modells betreffen Anwendungen und sind im Allgemeinen nur als Software implementiert. Die höchste Schicht, die An-

wendungsschicht, ist die dem Benutzer nächste Schicht. Sowohl die Benutzerschicht als auch die Anwendungsschicht interagieren mit Software-Anwendungen, die eine Kommunikationskomponente enthalten. Wenn von höherer Schicht die Rede ist, dann wird damit manchmal auch nur die nächsthöhere Schicht im OSI-Modell bezeichnet.

Die *unteren Schichten* eines OSI-Modells betreffen den Datentransport. Die physikalische Schicht und die Verbindungsschicht sind als Hard- und Software implementiert. Die restlichen unteren Schichten sind nur als Software implementiert. Die unterste Schicht, die physikalische, ist dem physikalischen Netzwerk-Medium (z.B. der Netzwerk-Verkabelung) am nächsten und ist für das Absetzen der Daten auf das Medium zuständig.

Bild 1.3 zeigt die Unterteilung in untere und obere OSI-Schichten.

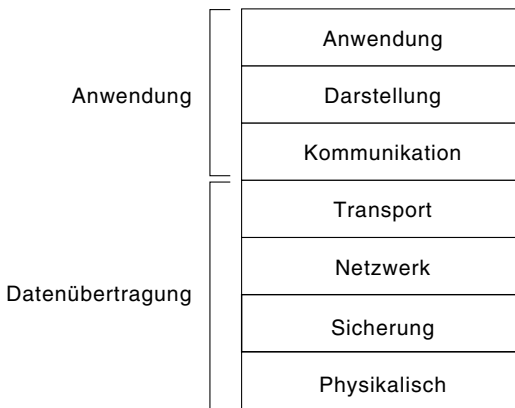


Bild 1.3: Die OSI-Schichten lassen sich in zwei Gruppen unterteilen

1.2.2 Protokolle

Das OSI-Modell bietet einen konzeptionellen Rahmen für die Kommunikation zwischen Computern, wobei das Modell an sich keine Methode für die Kommunikation ist. Die tatsächliche Kommunikation wird erst durch den Einsatz von Protokollen möglich. Im Kontext von Datennetzwerken ist ein *Protokoll* eine formale Zusammenstellung von Regeln und Konventionen, mit denen der Austausch von Daten zwischen Computern über ein Netzwerk-Medium geregelt wird. Mit einem Protokoll werden die Funktionen einer oder mehrerer OSI-Schichten implementiert. Es gibt eine Vielzahl an Kommunikationsprotokollen, die sich jedoch alle in eine der folgenden Gruppen einordnen lassen: *LAN-Protokolle*, *WAN-Protokolle*, *Netzwerk-*

Protokolle und *Routing-Protokolle*. *LAN-Protokolle* arbeiten auf der Ebene der physikalischen und der Verbindungsschicht des OSI-Modells und definieren die Kommunikation über verschiedene LAN-Medien. *WAN-Protokolle* arbeiten auf der Ebene der drei untersten Schichten des OSI-Modells und definieren die Kommunikation über die verschiedenen Weitverkehrsmedien. *Routing-Protokolle* sind Protokolle der Vermittlungsschicht, die die Pfadfestlegung und das Verkehrs-Switching regeln. Die *Netzwerk-Protokolle* schließlich sind verschiedene Protokolle der oberen Schichten, die zu einer bestimmten Protokollfamilie gehören. Viele Protokolle bauen auf anderen auf, um ihre Aufgabe zu erfüllen. Routing-Protokolle benutzen z.B. Netzwerk-Protokolle, um Informationen zwischen Routern auszutauschen. Dieses Konzept des Aufbaus auf bereits vorhandene Schichten ist der Ursprung des OSI-Modells.

1.2.3 Das OSI-Modell und die Kommunikation zwischen Systemen

Daten, die von einer Software-Anwendung des einen Computers zur Software-Anwendung eines anderen Computers übertragen werden sollen, müssen jede OSI-Schicht passieren. Wenn z.B. eine Anwendung auf System A Daten an eine Anwendung auf System B übertragen will, übergibt das Anwendungsprogramm auf System A diese Daten an die Anwendungsschicht (Schicht 7) des Systems A. Dann reicht die Anwendungsschicht die Daten an die Darstellungsschicht (Schicht 6) weiter, die die Daten der Kommunikationsschicht (Schicht 5) übergibt usw. bis hinunter zur physikalischen Schicht (Schicht 1). Von der physikalischen Schicht werden die Daten in das physikalische Netzwerk-Medium eingespeist und darüber zum System B übertragen. Die physikalische Schicht des Systems B entfernt vom physikalischen Medium hinzugefügte Daten und gibt seine Daten an die Verbindungsschicht (Schicht 2) weiter, von wo sie an die Vermittlungsschicht (Schicht 3) übergeben werden usw. bis hinauf zur Anwendungsschicht (Schicht 7) des Systems B. Die Anwendungsschicht des Systems B schließlich übergibt die Daten an das Programm, das als Empfänger bestimmt ist, womit der Kommunikationsprozess abgeschlossen ist.

1.2.4 Interaktion zwischen den Schichten des OSI-Modells

Jede Schicht des OSI-Modells kommuniziert mit drei anderen OSI-Schichten: mit der nächsthöheren Schicht, mit der nächstniedrigeren und mit der gleichen Schicht auf dem anderen, vernetzten Computer. So kommuniziert z.B. die Verbindungsschicht des Systems A mit der Vermittlungs- und der

physikalischen Schicht seines Systems und mit der Verbindungsschicht des Systems B. Bild 1.4 veranschaulicht dieses Beispiel.

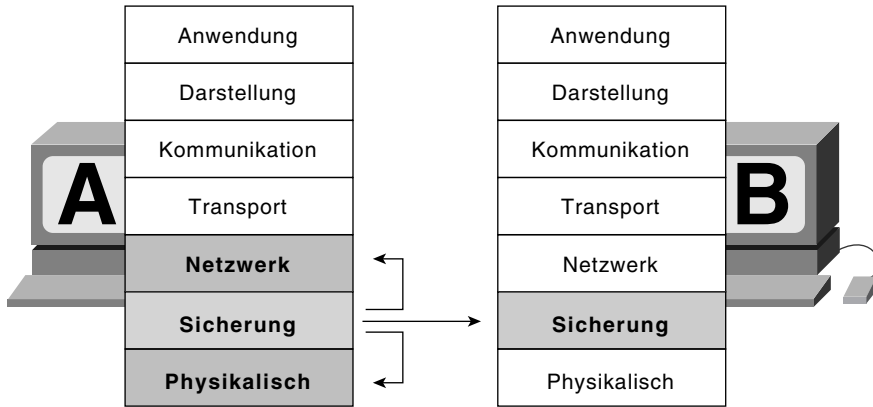


Bild 1.4: Die Schichten des OSI-Modells kommunizieren mit anderen Schichten

1.2.5 Dienste der OSI-Schichten

Die aufeinander folgenden OSI-Schichten kommunizieren miteinander, um ihre Dienste gegenseitig zu nutzen. Die Dienste der benachbarten Schichten dienen zur Kommunikation zwischen einer OSI-Schicht und der gleichen Schicht auf einem anderen Computer. Zu den Diensten der Schichten zählen drei grundlegende Elemente: der Dienstbenutzer, der Dienstanbieter und der Dienstzugriffspunkt (Service Access Point – SAP).

In diesem Zusammenhang ist der *Dienstbenutzer* die OSI-Schicht, die von der benachbarten Schicht einen Dienst anfordert. Der *Dienstanbieter* ist die Schicht, die diesen Dienst dem Dienstbenutzer anbietet. OSI-Schichten können Dienste mehreren Dienstbenutzern gleichzeitig anbieten. Beim SAP handelt es sich um einen konzeptionell bestimmten Ort, an dem eine OSI-Schicht den Dienst einer anderen Schicht anfordern kann.

Bild 1.5 stellt dar, wie diese drei Elemente auf der Vermittlungs- und Verbindungsschicht interagieren.

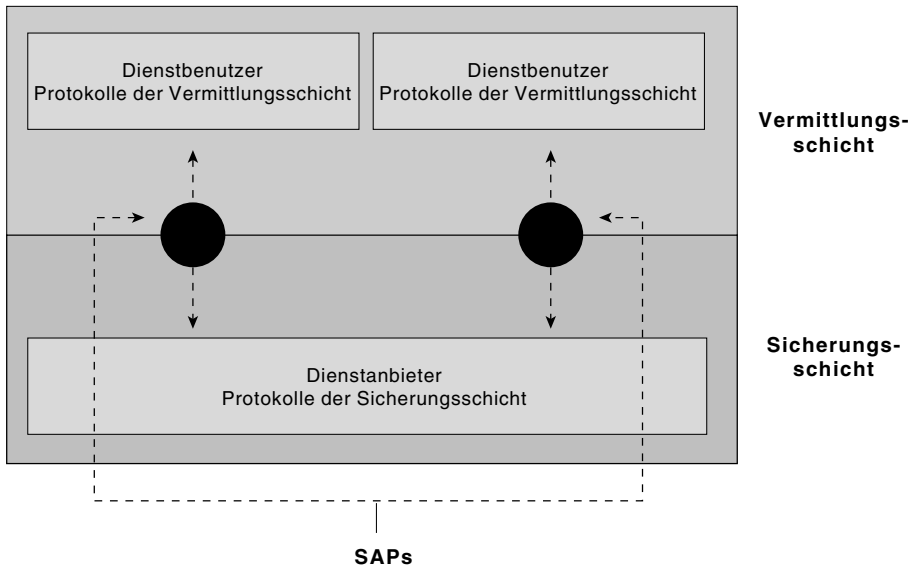


Bild 1.5: Dienstbenutzer, -anbieter und SAPs interagieren auf Ebene der Vermittlungs- und Verbindungsschicht

1.2.6 Schichten des OSI-Modells und der Datenaustausch

Die sieben OSI-Schichten setzen verschiedene Formen von Steuerdaten ein, um mit der gleichen Schicht auf einem anderen Computer zu kommunizieren. Diese *Steuerdaten* bestehen aus bestimmten Anforderungen und Anweisungen, die zwischen Partnerschichten des OSI-Modells ausgetauscht werden.

Für Steuerdaten gibt es zwei Formen: den Header (Kopf) oder Trailer (Anhang). Der Header wird den von der höheren Schicht heruntergereichten Daten vorangestellt. Ein Trailer wird diesen Daten angehängt. Es ist allerdings nicht unbedingt erforderlich, dass eine OSI-Schicht den heruntergereichten Daten einen Header oder Trailer hinzufügt.

Die Bezeichnung Header, Trailer und Daten ist relativ zu verstehen, in Abhängigkeit von der Schicht, die die Informationseinheit analysiert. Für die Vermittlungsschicht besteht die Informationseinheit z.B. aus dem Header der Schicht 3 und den Daten. Auf Ebene der Verbindungsschicht wird jedoch alles, was von der Vermittlungsschicht heruntergereicht wird, als Daten behandelt (also der Header der Schicht 3 und die Daten).

Mit anderen Worten: Der Datenteil einer Informationseinheit auf Ebene einer bestimmten OSI-Schicht kann die Header, Trailer und Daten sämtlicher

darüber liegenden Schichten enthalten. Genau dies wird als *Kapselung* bezeichnet. Bild 1.6 zeigt, wie Header und Daten einer Schicht vom Header der darunter liegenden Schicht gekapselt werden.

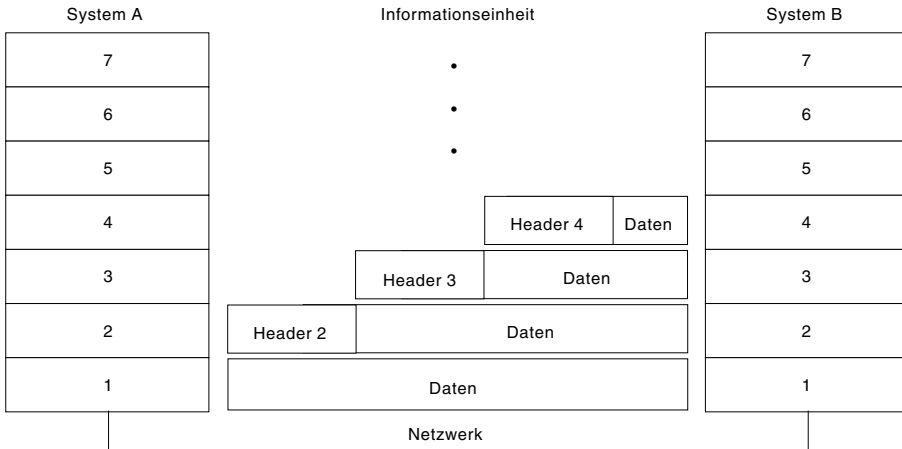


Bild 1.6: Header und Daten können während des Datenaustauschs gekapselt werden

Verfahren des Datenaustauschs

Der Datenaustausch erfolgt zwischen den Partnerschichten des OSI-Modells. Jede Schicht des Quellsystems fügt den eigentlichen Daten seine Steuerdaten hinzu. Jede Schicht des Zielsystems analysiert die Steuerdaten und entfernt diese wieder.

Wenn System A Daten einer Anwendung an System B senden will, müssen die Daten an die Anwendungsschicht übergeben werden. Die Anwendungsschicht des Systems A transportiert dann alle von der Anwendungsschicht des Systems B angeforderten Steuerdaten, indem sie den Daten einen Header voranstellt. Die sich daraus ergebende Informationseinheit (Header und Daten) wird an die Darstellungsschicht weitergegeben, die wiederum ihren eigenen Header voranstellt, der Steuerinformationen für die Darstellungsschicht des Systems B enthält. Die Informationseinheit wächst von Schicht zu Schicht mit Steuerdaten für die Partnerschichten im System B an, da jede Schicht ihren Header anfügt (oder ihren Trailer). Von der physikalischen Schicht wird die gesamte Informationseinheit in das Netzwerk-Medium eingespeist.

Die physikalische Schicht des Systems B empfängt die Informationseinheit und reicht sie an die Verbindungsschicht. Diese liest die Steuerdaten aus dem

Header, der von der Verbindungsschicht des Systems A hinzugefügt wurde. Der Header wird entfernt und der Rest der Informationseinheit wird an die Vermittlungsschicht übergeben. Jede Schicht führt die gleichen Aktionen aus: Sie liest den Header der Partnerschicht, entfernt diesen und übergibt den Rest der Informationseinheit an die nächsthöherliegende Schicht. Nachdem die Anwendungsschicht diese Aktionen ausgeführt hat, werden die Daten an die Anwendung des Systems B übergeben, für die die Daten bestimmt sind, und zwar genau in der Form, wie sie von der Anwendung des Systems A übertragen wurden.

1.2.7 Die physikalische Schicht des OSI-Modells

Die physikalische Schicht definiert die elektrische, mechanische, prozedurale und funktionale Spezifikation für die Aktivierung, Aufrechterhaltung und Deaktivierung der physikalischen Verbindung zwischen kommunizierenden Netzwerk-Systemen. Die Spezifikationen der physikalischen Schicht betreffen Eigenschaften wie die Spannung, zeitliche Vorgaben für Spannungsänderungen, physikalische Übertragungsraten, die maximale Übertragungstrecke und die Stecker und Buchsen. Die Implementationen der physikalischen Schicht können unterteilt werden in LAN- oder WAN-Spezifikationen. Bild 1.7 zeigt einige der gängigsten LAN- und WAN-Implementationen der physikalischen Schicht.

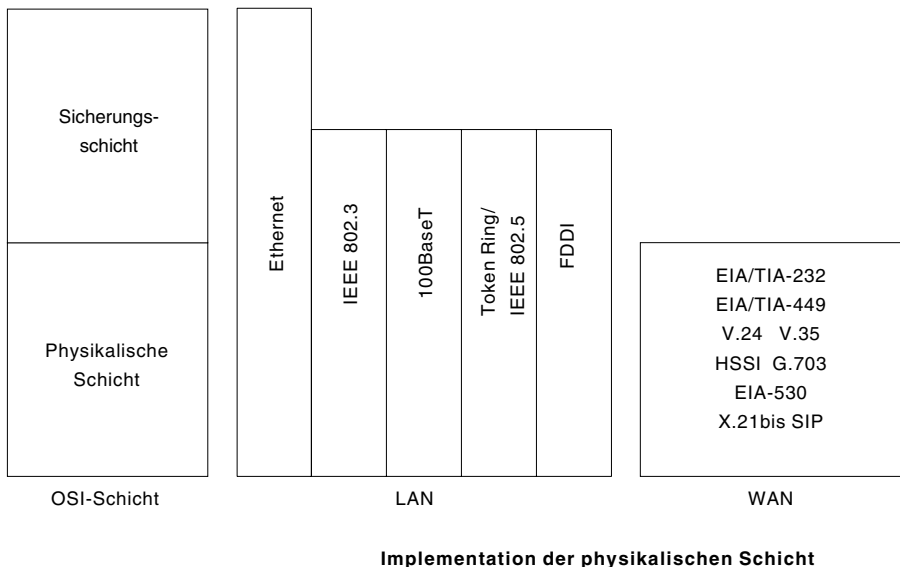


Bild 1.7: Implementierungen der physikalischen Schicht können LAN- oder WAN-Spezifikationen sein

1.2.8 Die Verbindungsschicht des OSI-Modells

Die Verbindungsschicht sorgt für die zuverlässige Übertragung der Daten über eine physikalische Netzwerk-Verbindung. Die verschiedenen Spezifikationen der Verbindungsschicht definieren unterschiedliche Netzwerk- und Protokolleigenschaften, einschließlich der physikalischen Adressierung, Netzwerk-Topologie, Fehlererkennung, Frame-Abfolge und Flusssteuerung. Bei der physikalischen Adressierung (im Gegensatz zur Netzwerk-Adressierung) wird definiert, wie Geräte auf Ebene der Verbindungsschicht adressiert werden. Die Netzwerk-Topologie wird von Spezifikationen der Verbindungsschicht bestimmt, die definiert, wie Geräte physikalisch miteinander verbunden werden, z.B. über einen Bus oder einen Ring. (Die Fehlererkennung alarmiert die Protokolle der oberen Schichten, wenn ein Übertragungsfehler auftritt, und die Sequenzierung der Daten-Frames sortiert Frames, falls diese nicht in der richtigen Reihenfolge eingehen.) Die Flusssteuerung schließlich regelt die Übertragung der Daten, sodass das empfangende Gerät nicht mit Daten überlastet wird.

Das Institute of Electrical and Electronics Engineers (IEEE) hat die Verbindungsschicht noch in zwei Subschichten aufgeteilt: die Logical Link Control (LLC – logische Verbindungssteuerung) und die Media Access Control (MAC – Medium-Zugriffssteuerung). Bild 1.8 zeigt die IEEE-Subschichten der Verbindungsschicht.

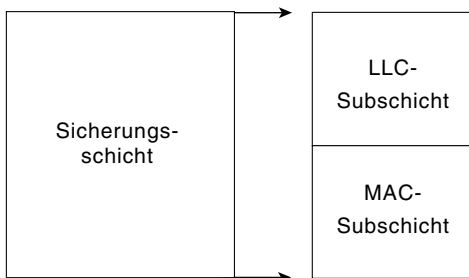


Bild 1.8: Die Verbindungsschicht besteht aus zwei Subschichten

Die Subschicht *Logical Link Control (LLC)* verwaltet die Kommunikation zwischen Geräten eines Netzwerks, die über eine einzige Leitung läuft. LLC ist in der Spezifikation IEEE 802.2 definiert und unterstützt sowohl die verbindungslosen als auch die verbindungsorientierten Dienste der Protokolle höherer Schichten. IEEE 802.2 definiert mehrere Felder in Frames der Verbindungsschicht, sodass es mehreren Protokollen der höheren Schichten möglich ist, eine einzige physikalische Datenverbindung gemeinsam zu nutzen. Die Subschicht *Media Access Control (MAC)* verwaltet den Protokoll-

zugriff auf das physikalische Netzwerk-Medium. Die IEEE-MAC-Spezifikation definiert MAC-Adressen, anhand derer mehrere Geräte auf Ebene der Verbindungsschicht eindeutig identifizierbar sind.

1.2.9 Die Vermittlungsschicht des OSI-Modells

Die Vermittlungsschicht legt die Netzwerk-Adresse fest, die sich von der MAC-Adresse unterscheidet. Manche Netzwerk-Schicht-Implementierungen, wie das Internet Protokoll (IP), legen Netzwerk-Adressen auf eine Weise fest, die es erlaubt, die Route systematisch durch Vergleich der Quellnetzadresse mit der Zielnetzadresse unter Berücksichtigung der Netzwerkmaske zu bestimmen. Weil diese Schicht den logischen Aufbau des Netzwerkes festlegt, können Router sie benutzen, um zu bestimmen, wie Pakete weitergeleitet werden. Deshalb wird viel Planungs- und Konfigurationsarbeit für Internetworks auf Schicht 3 – der Vermittlungsschicht – verwendet.

1.2.10 Die Transportschicht des OSI-Modells

Die Transportschicht nimmt Daten von der Kommunikationsschicht entgegen und teilt die Daten für den Transport über das Netzwerk auf. Grundsätzlich ist die Transportschicht für die Sicherstellung einer fehlerfreien und in der richtigen Reihenfolge stattfindenden Datenübertragung verantwortlich. Flusssteuerung findet grundsätzlich in der Transportschicht statt.

Die Flusssteuerung verwaltet die Datenübertragung zwischen Geräten so, dass das sendende Gerät nicht mehr Daten übermittelt als das empfangende Gerät verarbeiten kann. Mit dem Multiplexing können mehrere Anwendungen ihre Daten über eine einzelne physikalische Verbindung übertragen. Virtuelle Verbindungen werden von der Transportschicht aufgebaut, aufrechterhalten und abgebaut. Zur Fehlerprüfung gehört das Aufsetzen von Mechanismen zur Fehlererkennung in der Datenübertragung, während es Aufgabe der Fehlerbehebung ist, dass fehlerhafte Daten ggf. erneut angefordert werden.

Im Internet werden die Transport-Protokolle TCP und UDP benutzt.

1.2.11 Die Kommunikationsschicht des OSI-Modells

Diese Kommunikationsschicht baut Sitzungen zwischen Einheiten der Darstellungsschicht auf, verwaltet und beendet diese. Kommunikationsverbindungen bestehen aus Dienstanforderungen und Dienstantworten, die zwischen Anwendungen in verschiedenen Netzwerk-Geräten ausgetauscht werden. Diese Anforderungen und Antworten werden von Protokollen ko-

ordiniert, die in der Kommunikationsschicht implementiert sind. Einige Implementationen der Kommunikationsschicht enthalten das Zone Information Protocol (ZIP), das AppleTalk-Protokoll, das den Name-Binding-Prozess koordiniert, und das Session Control Protocol (SCP), das Vermittlungsschicht-Protokoll der DECnet Phase IV.

1.2.12 Die Darstellungsschicht des OSI-Modells

Die Darstellungsschicht bietet eine Vielzahl von Kodier- und Konvertierfunktionen, die auf Daten der Anwendungsschicht angewandt werden. Diese Funktionen stellen sicher, dass die Daten, die von der Anwendungsschicht des einen Systems kommen, von der Anwendungsschicht eines anderen Systems gelesen werden können. Zu den Kodier- und Konvertierverfahren der Darstellungsschicht gehören z.B. die gängigen Datendarstellungsformate, die Konvertierung von Zeichendarstellungsformaten, gängige Datenkompressionsverfahren und übliche Datenverschlüsselungen.

Übliche Datendarstellungsformate oder der Einsatz von standardisierten Bild-, Klang- und Videoformaten ermöglichen den Austausch von Anwendungsdaten zwischen verschiedenartigen Computersystemen. Konvertierverfahren werden dazu verwendet, Daten zwischen Systemen auszutauschen, die mit unterschiedlichen Text- und Datendarstellungen arbeiten, z.B. mit EBCDIC und ASCII. Mit Standard-Datenkompressionen können Daten, die an der Quelle komprimiert wurden, problemlos vom Zielgerät dekomprimiert werden. Gleiches gilt für den Einsatz von Verschlüsselungen.

Die Implementationen der Darstellungsschicht sind normalerweise nicht mit einem bestimmten Protokoll-Stack verbunden. Zu den weit verbreiteten Standards für Video gehören QuickTime und Motion (MPEG). Bei QuickTime handelt es sich um eine Spezifikation für Video- und Audiodaten am Apple-Computer, während MPEG ein Standard für die Komprimierung und Kodierung von Videodaten ist.

Zu den bekanntesten Grafikformaten zählen Graphics Interchange Format (GIF), Joint Photographic Experts Group (JPEG) und Tagged Image File Format (TIFF). GIF und JPEG sind ein Standard für die Komprimierung und Kodierung von Grafikdaten, TIFF ist ein Standard-Kodierformat für Grafikdaten.

1.2.13 Die Anwendungsschicht des OSI-Modells

Die Anwendungsschicht des OSI-Modells ist dem Benutzer am nächsten, d.h. dass die Anwendungsschicht und der Benutzer direkt mit der Software interagieren.

Diese Schicht interagiert mit Software-Anwendungen, die eine kommunizierende Komponente implementieren. Solche Anwendungen gehören nicht mehr in den Rahmen des OSI-Modells. Zu den Funktionen der Anwendungsschicht gehören die Identifizierung des Kommunikationspartners, das Ermitteln der Ressourcen-Verfügbarkeit und die Synchronisierung der Kommunikation.

Beim Identifizieren der Kommunikationspartner ermittelt die Anwendungsschicht für die Anwendung, die Daten übertragen will, die Identität und Verfügbarkeit des Kommunikationspartners. Bei der Ermittlung der Ressourcen-Verfügbarkeit muss die Anwendungsschicht entscheiden, ob ausreichende Netzwerk-Ressourcen für die angeforderte Kommunikation vorhanden sind. Von der Synchronisierung ist jegliche Kommunikation zwischen Anwendungen betroffen, die von der Anwendungsschicht koordiniert werden muss.

Beispiele für die Umsetzung der Anwendungsschicht sind Telnet, File Transfer Protocol (FTP) und Simple Mail Transfer Protocol (SMTP).

1.3 Datenformate

Die Daten und Steuerdaten, die in Internetworks übertragen werden, können in den unterschiedlichsten Formaten vorliegen. Die Begriffe, mit denen diese Formate bezeichnet werden, sind nicht immer konsistent und können gegeneinander ausgetauscht werden. Zu den gängigen Datenformaten gehören Frame-, Paket-, Datagramm-, Segment-, Nachrichten-, Zell- und Dateneinheiten. Ein Frame ist eine Informationseinheit, deren Quelle und Ziel Entitäten der Verbindungsschicht sind. Ein Frame setzt sich aus dem Header der Verbindungsschicht (und ggf. einem Trailer) und den Daten der höheren Schicht zusammen. Header und Trailer enthalten Steuerdaten, die für die Verbindungsschicht des Zielsystems bestimmt sind. Die Daten der höheren Schicht werden vom Header und Trailer der Verbindungsschicht gekapselt. Bild 1.9 zeigt die grundlegenden Komponenten eines Frames der Verbindungsschicht.

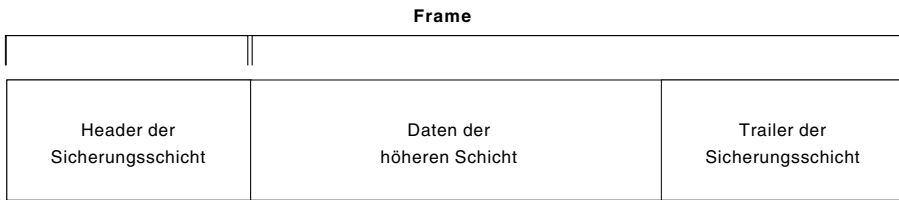


Bild 1.9: Die Daten der höheren Schichten bilden den Frame der Verbindungsschicht

Ein *Paket* ist eine Informationseinheit, deren Quelle und Ziel die Vermittlungsschicht ist. Ein Paket setzt sich aus dem Header der Vermittlungsschicht (und ggf. einem Trailer) und den Daten der höheren Schicht zusammen. Header und Trailer enthalten Steuerdaten, die für die Vermittlungsschicht des Zielsystems bestimmt sind. Die Daten der höheren Schichten sind vom Header und Trailer der Vermittlungsschicht gekapselt. Bild 1.10 zeigt die grundlegenden Komponenten eines Pakets der Vermittlungsschicht.

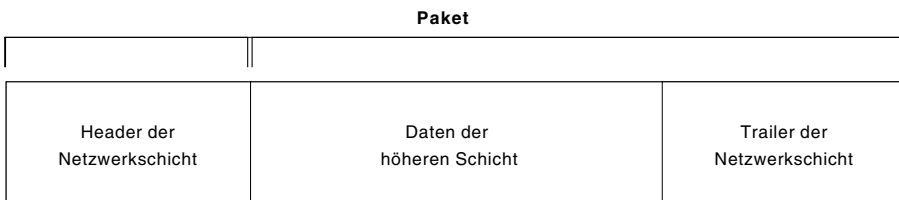


Bild 1.10: Drei grundlegende Komponenten bilden ein Paket der Vermittlungsschicht

Der Begriff *Segment* wird normalerweise auf Informationseinheiten bezogen, deren Quelle und Ziel Entitäten der Transportschicht sind.

Eine *Nachricht* ist eine Informationseinheit, deren Quelle und Ziel Entitäten sind, die oberhalb der Vermittlungsschicht liegen (oft die Anwendungsschicht).

Eine *Zelle* ist eine Informationseinheit mit fester Größe, deren Quelle und Ziel die Verbindungsschicht ist. Zellen werden in vermittelten Umgebungen verwendet, z.B. in Netzen mit Asynchronous Transfer Mode (ATM) und Switched Multimegabit Data Service (SDMS). Eine Zelle besteht aus einem Header und den Nutzdaten. Der Header enthält Steuerdaten, die für die Verbindungsschicht des Zielsystems bestimmt sind; der Header ist 5 Byte lang. Zu den Nutzdaten gehören die Daten der höheren Schicht (48 Byte), die vom Zell-Header gekapselt werden.

Die Länge des Header- und Nutzdatenfelds ist für alle Zellen immer gleich. Bild 1.11 zeigt die Komponenten einer typischen Zelle.

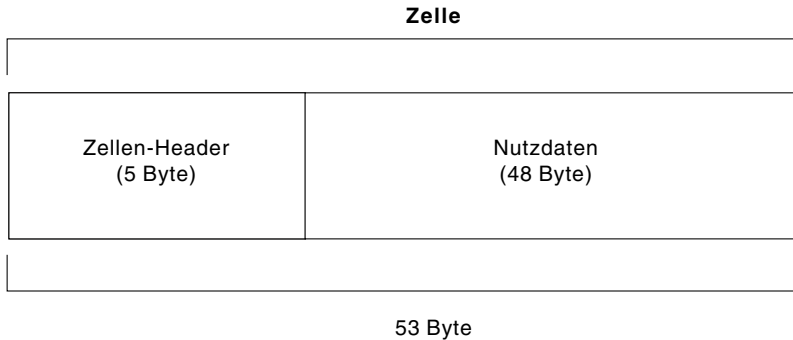


Bild 1.11: Eine typische Zelle besteht aus zwei Komponenten

Dateneinheit ist ein Oberbegriff, der eine Vielzahl von Informationseinheiten umfasst. Zu den gängigen Dateneinheiten gehören Service Data Unit (SDU), Protocol Data Unit (PDU) und Bridge Protocol Data Unit (BPDU). SDUs sind Informationseinheiten der Protokolle höherer Schichten, mit denen Dienstanforderungen an die niedrigeren Schichten gestellt werden. PDU ist der OSI-Begriff für ein Paket. BPDUs werden vom Spanning-Tree-Algorithmus als Hallo-Nachricht verwendet.

1.4 Die ISO-Hierarchie von Netzwerken

Große Netzwerke sind normalerweise hierarchisch organisiert. Ein solcher Aufbau bietet verschiedene Vorteile: beim Management, der Flexibilität und der Reduzierung überflüssigen Datenverkehrs. Deshalb hat die International Organization for Standardization (ISO) eine Vielzahl terminologischer Konventionen für die adressierenden Einrichtungen eines Netzwerks angepasst. Schlüsselwörter in diesem Abschnitt sind *End-System* (ES), *intermediäres System* (IS), *Bereich* und *autonomes System* (AS).

Ein ES ist ein Netzwerk-Gerät, das keinerlei Routing- oder Weiterleitungsfunktion ausführt. Zu ES gehören z.B. Terminals, Personalcomputer und Drucker. Ein IS ist ein Netzwerk-Gerät, das Routing- oder Weiterleitungsfunktionen ausführt. Zu IS gehören z.B. Router, Switches und Bridges. IS-Netzwerke können in zwei Arten unterteilt werden: Intradomain-IS und Interdomain-IS. Ein Intradomain-IS kommuniziert innerhalb eines einzigen autonomen Systems, während ein Interdomain-IS innerhalb und zwischen autonomen Systemen kommuniziert. Ein *Bereich* ist eine logische Gruppe

von Netzwerk-Segmenten und den daran angeschlossenen Geräten. Bereiche sind unterteilt in autonome Systeme. Ein AS sind mehrere Netzwerke, die gemeinsam administriert werden und eine gemeinsame Routing-Strategie haben. Autonome Systeme lassen sich in Bereiche unterteilen, wobei ein AS manchmal als eine *Domain* bezeichnet wird. Bild 1.12 zeigt ein hierarchisches Netzwerk mit seinen Komponenten.

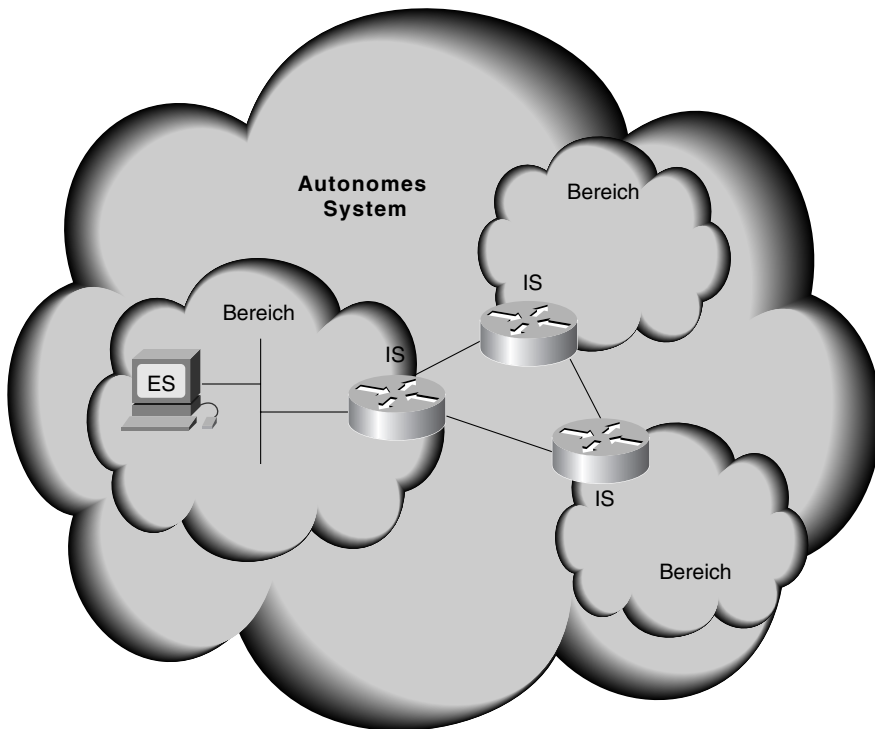


Bild 1.12: Ein hierarchisches Netzwerk besteht aus einer Vielzahl von Komponenten

1.5 Verbindungsorientierte und verbindungslose Netzwerk-Dienste

Allgemein können Transportprotokolle in verbindungsorientierte und verbindungslose Protokolle aufgeteilt werden. Verbindungsorientierte Dienste müssen zuerst eine Verbindung mit dem gewünschten Dienst aufbauen, bevor sie irgendwelche Daten übermitteln können. Ein verbindungsloser Dienst kann Daten ohne einen vorherigen Verbindungsaufbau übertragen. Grundsätzlich bieten verbindungsorientierte Dienste im Gegensatz zu den verbindungslosen eine gewisse Garantie, dass die Daten zugestellt wurden.

Verbindungsorientierte Verfahren verwenden einen bestimmten Pfad (Leitungsweg), der für die Dauer einer (logischen) Verbindung besteht. Verbindungslose Verfahren übertragen die Daten über eine fest aufgebaute (logische) Verbindung.

Während des Verbindungsaufbaus können die Endknoten Ressourcen für die Verbindung reservieren. Die Endknoten können außerdem bestimmte Kriterien für die Übertragung aushandeln und festlegen, wie beispielsweise die bei TCP-Verbindungen benutzte Fenstergröße. Diese Reservierung von Ressourcen ist Bestandteil bestimmter Denial Of Service (DOS)-Angriffe. Ein angreifendes System sendet viele Anfragen für Verbindungsaufbauten, baut die Verbindungen aber nie fertig auf. Der angegriffene Rechner hat jetzt Ressourcen für eine Menge nicht fertig aufgebauter Verbindungen zur Verfügung gestellt. Wenn nun ein Endknoten versucht, eine tatsächliche Verbindung herzustellen, sind nicht genug Ressourcen für diese berechnete Verbindung übrig.

Der Eintritt in die Phase der Datenübertragung erfolgt, wenn die eigentlichen Daten über die Verbindung gesendet werden. Während der Datenübertragung prüfen die meisten verbindungsorientierten Dienste auf verlorene Pakete und sorgen für die erneute Versendung derselben. Grundsätzlich ist das Protokoll ebenfalls dafür verantwortlich, die Pakete in die richtige Reihenfolge zu bringen, bevor die Daten im Protokollstapel weitergegeben werden.

Wenn die Datenübertragung abgeschlossen ist, beenden die Endknoten die Verbindung und geben die für die Verbindung reservierten Ressourcen wieder frei.

Verbindungsorientierte Netzwerkdienste haben mehr Overhead als verbindungslose. Die verbindungsorientierten Dienste müssen eine Verbindung aushandeln, Daten übertragen und die Verbindung wieder abbauen, während bei einer verbindungslosen Übertragung die Daten ohne den zusätzlichen Overhead von Verbindungsauf- und -abbau einfach gesendet werden können. Jedes der Verfahren hat seine Berechtigung in Internetworks.

1.6 Adressierung im Internetwork

Adressen in einem Internetwork kennzeichnen ein einzelnes Gerät oder ein Gerät als ein Mitglied einer Gruppe. Die Adressierungsverfahren sind abhängig von der Protokollfamilie und der OSI-Schicht. Die folgenden drei Adressarten werden am häufigsten verwendet: Adressen der Verbindungs-

schicht, Medium-Zugriffssteuerung-(MAC-)Adressen und Adressen der Vermittlungsschicht.

1.6.1 Verbindungsschicht

Die Adresse der Verbindungsschicht kennzeichnet jede physikalische Netzwerkverbindung von Netzwerk-Geräten eindeutig. Diese Adressen werden manchmal auch als *physikalische* oder *Hardware*-Adressen bezeichnet. Die Adressen der Verbindungsschicht liegen in einem ebenen Adressraum und stehen in vordefinierter und fester Beziehung zu einem bestimmten Gerät.

Endsysteme sind im Allgemeinen mit nur einer physikalischen Verbindung an das Netzwerk angeschlossen, weshalb sie nur eine Verbindungsschichtadresse benötigen. Router und andere Internetworking-Geräte verfügen normalerweise über mehrere physikalische Netzwerk-Verbindungen und haben deshalb auch mehrere Verbindungsadressen. Bild 1.13 zeigt, wie jede Schnittstelle eines Geräts anhand der Verbindungsschichtadresse eindeutig identifiziert ist.

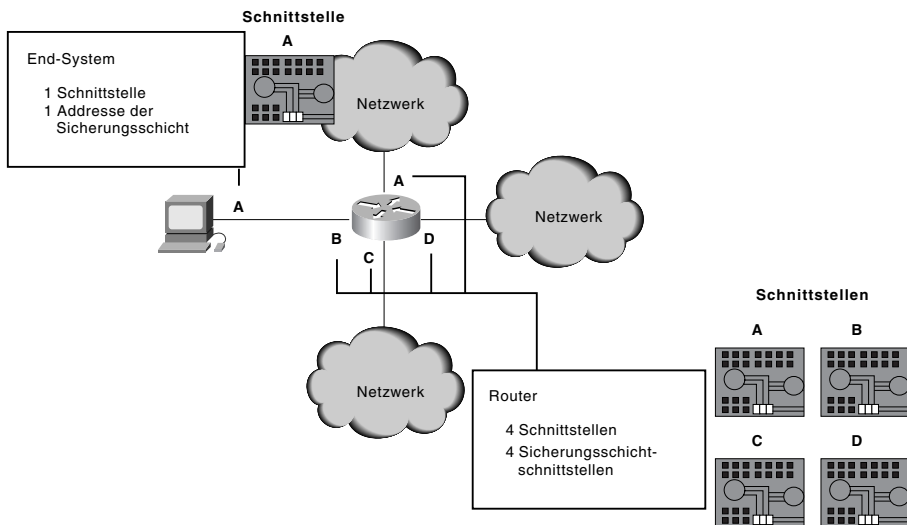


Bild 1.13: Jede Schnittstelle eines Geräts ist anhand der Verbindungsschichtadresse eindeutig gekennzeichnet

1.6.2 MAC-Adressen

Eine Media Access Control-Adresse (MAC – Medium-Zugriffssteuerung) bildet einen Teil der Verbindungsschichtadresse. MAC-Adressen kennzeichnen eine Netzwerk-Entität in einem LAN, das die IEEE-MAC-Adressen der

Verbindungsschicht implementiert. Wie die meisten Adressen der Verbindungsschicht sind auch die MAC-Adressen für jede LAN-Schnittstelle eindeutig. Bild 1.15 zeigt den Zusammenhang zwischen MAC-Adresse, Verbindungsschichtadresse und IEEE-Subschichten der Verbindungsschicht.

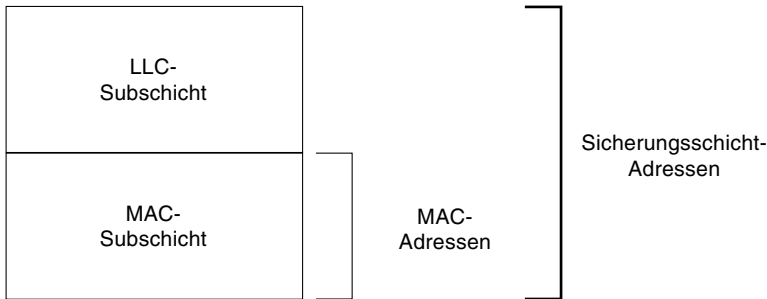


Bild 1.14: Beziehung zwischen MAC-Adresse, Verbindungsschichtadresse und den IEEE-Subschichten der Verbindungsschicht

MAC-Adressen sind 48 Bit lang und werden als zwölf hexadezimale Ziffern geschrieben. Die ersten sechs hexadezimalen Ziffern, die vom IEEE festgelegt sind, kennzeichnen den Hersteller. Dabei handelt es sich um den Organizational Unique Identifier (OUI). Die letzten sechs hexadezimalen Ziffern geben die Seriennummer der Schnittstelle an oder einen anderen Wert, den der Hersteller festlegt. MAC-Adressen werden auch als Burned-in Adresses (BIAs – eingebrannte Adressen) bezeichnet, da sie in das ROM gebrannt sind. Beim Initialisieren der Schnittstellenkarte wird die Adresse ausgelesen und ins RAM kopiert. Bild 1.15 stellt das MAC-Adressenformat dar.

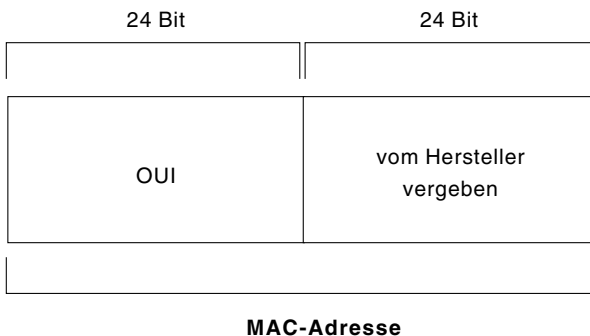


Bild 1.15: Die MAC-Adresse ist eine eindeutige Adresse aus hexadezimalen Ziffern

1.6.3 Adressabbildung

Da Internetworks allgemein Netzwerk-Adressen verwenden, um Datenverkehr im Netzwerk zu routen, ist es nötig, Netzwerk-Adressen auf MAC-Adressen abzubilden. Wenn die Netzwerk-Schicht die Netzwerk-Adresse der Zielstation ermittelt hat, muss es die Daten mithilfe der MAC-Adresse über ein physikalisches Netzwerk schicken. Verschiedene Protokollfamilien benutzen unterschiedliche Methoden, um diese Abbildung zu realisieren, aber die bekannteste ist das Address Resolution Protocol (ARP).

Die verschiedenen Protokollfamilien verwenden unterschiedliche Verfahren, um die MAC-Adresse eines Geräts zu ermitteln. Die folgenden drei Verfahren werden am häufigsten eingesetzt: Das Address Resolution Protocol (ARP – Adressauflösungsprotokoll) bildet Netzwerk-Adressen auf MAC-Adressen ab. Das Hello-Protokoll ermöglicht es Netzwerk-Geräten, die MAC-Adressen anderer Netzwerk-Geräte zu ermitteln. MAC-Adressen sind entweder in die Adresse der Vermittlungsschicht eingebettet oder werden von einem Algorithmus generiert.

In der TCP/IP-Familie wird das Address Resolution Protocol (ARP) verwendet. Muss ein Netzwerk-Gerät Daten zu einem anderen Gerät senden, sind ihm die Quell- und Zielnetzwerkadresse für die Datenübertragung bekannt. Bevor die Daten nun geschickt werden können, muss die Zieladresse einer MAC-Adresse zugeordnet werden. Zuerst überprüft die sendende Station ihre ARP-Tabelle, um festzustellen, ob die MAC-Adresse des Ziels bereits bekannt ist. Falls das nicht der Fall ist, wird ein Broadcast, der die IP-Adresse des Ziels enthält, an das Netzwerk geschickt. Jede Station im Netzwerk empfängt den Broadcast und vergleicht die enthaltene IP-Adresse mit der eigenen. Nur die Station mit der entsprechenden IP-Adresse antwortet der sendenden Station mit einem Paket, das ihre MAC-Adresse enthält. Die erste Station fügt diese Information ihrer ARP-Tabelle für spätere Verwendung hinzu und fährt mit der Datenübertragung fort.

Liegt das Ziel in einem entfernten Netzwerk hinter einem Router, ist der Vorgang im Prinzip derselbe, nur schickt die sendende Station eine ARP-Anfrage für die MAC-Adresse des Standard-Gateways. Die Anfrage wird dann zu diesem Gerät geschickt. Das Standard-Gateway schickt nun die Anfrage über die Netzwerke, die nötig sind, um das Paket in das Netzwerk, in dem sich das Ziel-Gerät befindet, zuzustellen. Der Router im Netzwerk des Ziel-Gerätes benutzt dann ARP, um die MAC-Adresse des eigentlichen Ziel-Gerätes zu erhalten, und stellt das Paket zu.

Mit dem Hello-Protokoll (einem Protokoll der Vermittlungsschicht) können sich Netzwerk-Geräte gegenseitig identifizieren und feststellen, ob der Partner noch in Betrieb ist. Beim Einschalten eines Geräts sendet dieses Hello-Nachrichten an alle Geräte im Netzwerk (Broadcast). Die Netzwerk-Geräte senden eine Hello-Antwort zurück. In bestimmten zeitlichen Abständen sendet jedes Gerät Hello-Nachrichten, um bekannt zu geben, dass es noch in Betrieb ist. Dabei können die Netzwerk-Geräte die MAC-Adressen anhand der Hello-Protokoll-Pakete ermitteln.

Von drei Protokollen werden berechenbare MAC-Adressen verwendet. In diesen Protokollfamilien sind die MAC-Adressen berechenbar, weil die Vermittlungsschicht entweder die MAC-Adresse einbettet oder einen Algorithmus zur Bestimmung verwendet. Diese drei Protokolle sind: Xerox Network Systems (XNS), Novell Internetwork Packet Exchange (IPX) und DECnet Phase IV.

1.6.4 Adressen der Vermittlungsschicht

Mit einer Adresse der Vermittlungsschicht wird eine Entität in dieser Schicht des OSI-Referenzmodells identifiziert. Vermittlungsschichtadressen liegen in einem hierarchischen Adressraum und werden auch als *virtuelle* oder *logische Adressen* bezeichnet.

Die Beziehung zwischen einem Netzwerk-Gerät und einer Netzwerk-Adresse ist eine logische und keine feste. Diese Adresse basiert entweder auf den physikalischen Netzwerkeigenschaften (das Gerät ist an ein bestimmtes Segment angeschlossen) oder auf Gruppierungen, die ohne physikalische Grundlage sind (das Gerät ist Teil einer AppleTalk-Zone). Die End-Systeme benötigen für jedes von ihnen unterstützte Protokoll der Vermittlungsschicht eine eigene Adresse (wobei davon ausgegangen wird, dass jedes Gerät nur über eine physikalische Verbindung zum Netzwerk verfügt). Router und andere Internetworking-Geräte benötigen für jede physikalische Netzwerkverbindung eine Vermittlungsschichtadresse. Ein Router, der z.B. mit drei Schnittstellen ausgestattet ist, die jede mit AppleTalk, TCP/IP und OSI betrieben wird, muss für jede Schnittstelle drei Vermittlungsschichtadressen aufweisen. Daraus ergibt sich, dass dieser Router über neun Vermittlungsschichtadressen verfügt. Bild 1.16 illustriert, wie jeder Netzwerk-Schnittstelle eine Vermittlungsschichtadresse für jedes unterstützte Protokoll zugewiesen wird.

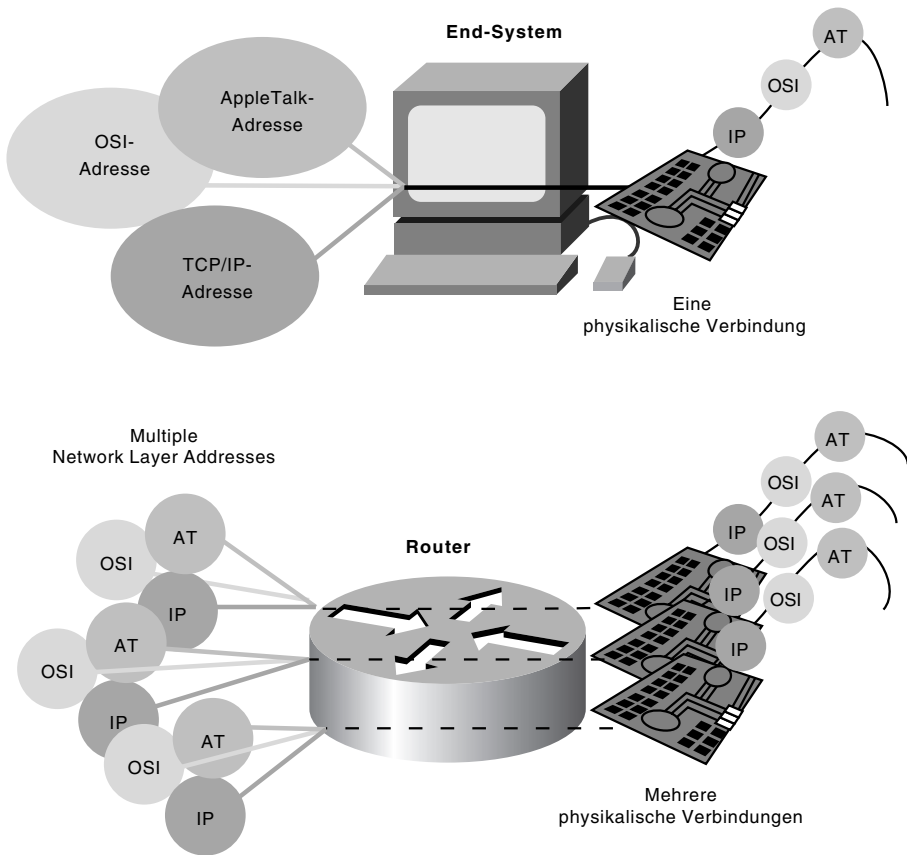


Bild 1.16: Jeder Netzwerk-Schnittstelle muss für jedes unterstützte Protokoll eine Vermittlungsschichtadresse zugewiesen sein

1.6.5 Hierarchischer oder ebener Adressraum

Der Internetworking-Adressraum ist in einer der beiden folgenden Formen abgebildet: hierarchisch oder eben.

Ein hierarchischer Adressraum ist unterteilt in zahlreiche Untergruppen, mit denen die Adresse immer weiter angenähert wird, bis sie auf ein einziges Gerät weist (ähnlich einer Anschrift). Ein ebener Adressraum besteht aus nur einer einzigen Gruppe (ähnlich der Sozialversicherungsnummer in den USA).

Die hierarchische Adressierung bietet gewisse Vorteile gegenüber dem ebenen Adressschema. So kann die Adressensortierung und -wiederholung relativ einfach durch Vergleichsoperationen erreicht werden. In Irland z.B. ist jede Straße eindeutig gekennzeichnet und kann in keinem anderen Land lie-

gen. Bild 1.17 zeigt die Unterschiede zwischen hierarchischem und ebenem Adressraum.

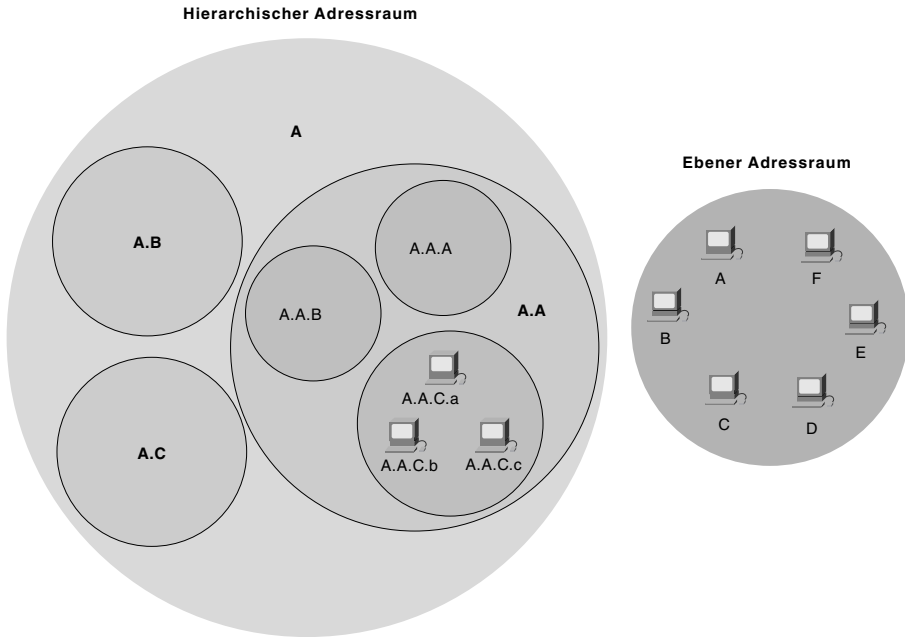


Bild 1.17: Unterschiede zwischen hierarchischem und ebenem Adressraum zeigen sich bei Vergleichsoperationen

1.6.6 Adresszuordnung

Adressen können Geräten auf zwei verschiedene Weisen zugeordnet werden: *statisch* oder *dynamisch*. *Statische Adressen* werden von einem Netzwerk-Administrator nach einem vorgefertigten Adressierungsplan vergeben. Eine statische Adresse ändert sich nicht, es sei denn, der Netzwerk-Administrator nimmt eine manuelle Änderung vor. *Dynamische Adressen* werden Geräten anhand protokollspezifischer Verfahren zugeordnet, wenn sie an das Netzwerk angeschlossen werden. Ein Gerät, das über eine dynamische Adresse angesprochen wird, erhält meistens bei jeder neuen Anbindung an das Netzwerk (z.B. beim Einschalten) eine andere Adresse. In manchen Netzwerken wird ein Server für die Adresszuordnung verwendet. Die Adresszuordnung durch einen Server erfolgt, wenn ein Gerät an das Netzwerk angeschlossen wird. Vom Server zugeordnete Adressen werden für andere Geräte weiterverwendet, wenn das Gerät die Verbindung zum Netzwerk beendet. So kann ein Gerät bei jedem Anschluss an das Netzwerk eine andere Adresse erhalten.

1.6.7 Adressen oder Namen

An Internetworking-Geräte werden normalerweise sowohl Adressen als auch Namen vergeben. Der Name ist dabei meistens ortsunabhängig und bleibt dem Gerät auch bei einem Standortwechsel zugeordnet. Hingegen sind die Internetworking-Adressen ortsgebunden; sie ändern sich, wenn ein Gerät »umgezogen« ist (wobei die MAC-Adresse eine Ausnahme von dieser Regel bildet). So wie Netzwerk-Adressen auf MAC-Adressen abgebildet werden, werden Namen üblicherweise mittels eines Protokolls auf Netzwerk-Adressen abgebildet. Im Internet wird das Domain Name System (DNS) verwendet, um den Namen eines Gerätes auf seine IP-Adresse abzubilden. Z.B. ist es einfacher für Sie, sich `www.cisco.com` anstatt der IP-Adresse zu merken. Folglich tippen Sie `www.cisco.com` in ihrem Browser ein, wenn Sie die Webseite von Cisco besuchen möchten. Ihr Computer führt einen DNS-Lookup auf die IP-Adresse für den Cisco-Webserver durch und benutzt dann für die Kommunikation mit selbigem die Netzwerk-Adresse.

1.7 Grundlagen der Flusststeuerung

Die Flusststeuerung ist eine Funktion, die dem Datenstau im Netzwerk vorbeugt, indem sie sicherstellt, dass ein sendendes Gerät nicht mehr Daten übermittelt, als das empfangende Gerät annehmen bzw. verarbeiten kann. Es gibt unzählige Ursachen für einen Datenstau: Wenn z.B. ein schneller Computer mehr Daten auf das Netzwerk überträgt, als dieses überhaupt vermitteln kann, oder das empfangende Gerät mit diesem Datenschwall überschüttet wird, den es gar nicht abarbeiten kann. Drei Verfahren stehen zur Verfügung, um dem Datenstau vorzubeugen: Pufferung, Drosselung der Datenquelle und Windowing.

Gepuffert wird von Netzwerk-Geräten, um Daten mit besonders hoher Übertragungsrate zwischenspeichern, bis diese verarbeitet werden können. Gelegentlich hohe Übertragungsraten können durch die Pufferung problemlos abgefangen werden. Dauert dieser Zustand aber zu lange an, wird der Speicher zu stark beansprucht, und alle weiterhin eingehenden Datagramme werden abgewiesen.

Nachrichten zur Drosselung der Datenquelle werden vom empfangenden Gerät gesendet, damit dessen Puffer nicht überlaufen. Das empfangende Gerät sendet eine Drosselungsnachricht an das sendende Gerät, damit dieses seine Übertragungsrate reduziert. Zuerst verweigert das empfangende Gerät weitere Daten, wenn die Puffer überlaufen. Dann sendet es an das sendende Gerät für jedes verweigte Paket eine Drosselungsnachricht. Das sendende Gerät reduziert daraufhin schrittweise die Übertragungsrate, bis es keine

Drosselungsnachrichten mehr erhält. Schließlich steigert das sendende Gerät wieder nach und nach die Übertragungsrate, bis wieder Drosselungsnachrichten eingeht.

Windowing ist ein Verfahren zur Flusssteuerung, bei dem das Quellgerät vom Zielgerät nach einer bestimmten Anzahl gesendeter Pakete eine Quittung anfordert. Bei einer Window-Größe von 3 fordert das Quellgerät eine Quittung an, nachdem es drei Pakete gesendet hat. Zuerst sendet das Quellgerät drei Pakete an das Zielgerät. Nach Eingang der drei Pakete sendet das Zielgerät eine Quittung an das Quellgerät. Wenn das Quellgerät die Quittung empfängt, sendet es weitere drei Pakete. Erreichen das Zielgerät aus irgendeinem Grund nicht alle drei Pakete (z. B. Pufferüberlauf), sendet es keine Quittung. Vom Quellgerät werden dann die letzten drei Pakete mit einer niedrigeren Übertragungsrate erneut gesendet.

1.8 Grundlagen der Fehlerprüfung

Die Verfahren der Fehlerprüfung ermitteln, ob die Daten während der Übertragung zerstört wurden. Die Fehlerprüfung ist in vielen OSI-Schichten implementiert.

Eine der üblichen Fehlerprüfungen ist der Cyclic Redundancy Check (CRC), der zerstörte Daten erkennt und ausscheidet. Funktionen zur Fehlerbehebung (z. B. wiederholte Übertragung) bleiben Protokollen der höheren Schichten vorbehalten. Vom Quellgerät wird ein CRC-Wert aus den zu übertragenden Daten berechnet. Das Zielgerät berechnet auf die gleiche Weise einen solchen Wert und vergleicht ihn mit dem Übertragenen, um festzustellen, ob während der Übertragung ein Fehler auftrat. Sind die Werte gleich, wird das Paket als gültig betrachtet. Sollten die Werte unterschiedlich sein, ist ein Fehler während der Übertragung aufgetreten, und das Paket wird ausgeschieden.

1.9 Grundlagen des Multiplexing

Beim Multiplexing werden vom Quellgerät mehrere Datenkanäle auf einem Kanal oder auf einer physikalischen Leitung zusammen übertragen. Dieses Verfahren kann auf jeder Schicht des OSI-Referenzmodells implementiert sein. Auf der Gegenseite, beim Zielgerät, erfolgt das Demultiplexing, das die Datenkanäle wieder separiert. Multiplexing findet z. B. statt, wenn Daten mehrerer Anwendungen auf ein einzelnes Datenpaket der unteren Schichten multiplext wird. Bild 1.18 zeigt dieses Beispiel.

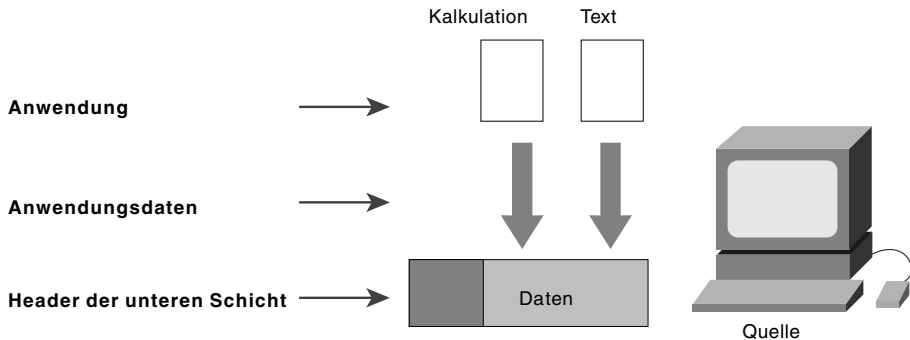


Bild 1.18: Die Daten mehrerer Anwendungen können in ein Paket der unteren Schichten multiplext werden

Ein weiteres Beispiel für Multiplexing ist die Übertragung der Daten mehrerer Geräte über einen physikalischen Kanal (wobei ein als Multiplexer bezeichnetes Gerät zum Einsatz kommt). Bild 1.19 veranschaulicht dieses Beispiel.

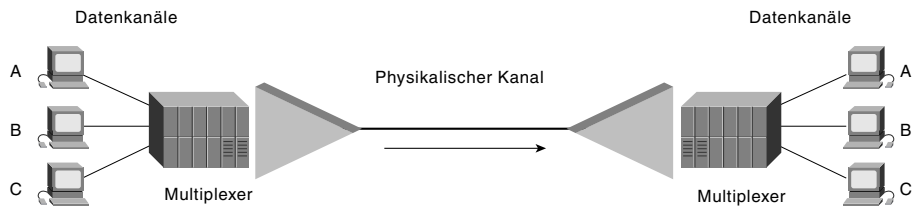


Bild 1.19: Die Daten mehrerer Geräte können auf einen physikalischen Kanal multiplext werden

Ein Multiplexer ist ein Gerät der physikalischen Schicht, das mehrere Datenströme auf einem oder mehreren Ausgangskanälen am Quellgerät zusammenfasst. Auf der Gegenseite multiplext ein Multiplexer die Kanäle wieder und maximiert die Nutzung der Bandbreite des physikalischen Mediums, indem es für mehrere Datenquellen gleichzeitig zur Verfügung steht.

Es gibt verschiedene Multiplex-Verfahren: Zeitmultiplex (TDM – Time-Devision Multiplexing), asynchrones Zeitmultiplexing (ATDM – Asynchronous Time-Devision Multiplexing), Frequenz-Multiplex (FDM – Frequency Multiplexing) und das statistische Multiplexing.

Beim TDM wird jedem Datenkanal anhand einer Zeitscheibe die Bandbreite zugeordnet, unabhängig davon, ob zu dieser Zeit Daten zu übertragen sind oder nicht. Beim ATDM wird die Bandbreite nach Bedarf über eine dynami-

sche Zeitscheibe zugewiesen. Beim FDM wird jedem Datenkanal in Abhängigkeit seiner Signalfrequenz die Bandbreite zugeordnet. Beim statistischen Multiplexing wird die Bandbreite dynamisch jedem Kanal zugeordnet, der Daten zu übertragen hat.

1.10 Organisationen für Standardisierung

Eine Vielzahl von Organisationen trägt zu Internetworking-Standards bei, indem sie Diskussionsforen anbieten, aus diesen informellen Diskussionen formale Spezifikationen erstellen und für die Verbreitung dieser Spezifikationen sorgen, wenn diese zum Standard erklärt wurden.

Die meisten Standardisierungsorganisationen nutzen bestimmte Vorgehensweisen, um einen formalen Standard zu erstellen: Organisieren von Ideen, Diskussion der Umsetzung, Entwicklung eines Entwurfs, Abstimmung über den gesamten Standard oder über Teile und schließlich die formelle Bekanntgabe des vollständigen Standards.

Zu den bekanntesten Organisationen, die sich mit Internetworking-Standards befassen, zählen die folgenden:

- *International Organization for Standardization (ISO)* – ISO ist eine internationale Standardisierungsorganisation, die für einen weiten Bereich von Standards verantwortlich zeichnet, zu denen viele Standards gehören, die Netzwerke betreffen. Am bekanntesten sind das OSI-Referenzmodell und die OSI-Protokollfamilie.
- *American National Standards Institute (ANSI)* – ANSI ist ein Mitglied der ISO und koordiniert freiwillige Gruppen in den USA. ANSI entwickelte das Fiber Distributed Data Interface (FDDI) und weitere Kommunikationsstandards.
- *Electronic Industries Association (EIA)* – EIA spezifiziert elektrische Übertragungsstandards, zu denen auch solche aus dem Netzwerkbereich gehören. Von der EIA wurde der sehr häufig verwendete Standard EIA/TIA-232 (früher als RS-232 bekannt) entwickelt.
- *Institute of Electrical and Electronic Engineers (IEEE)* – IEEE ist eine professionelle Organisation, die Netzwerk-Standards und andere Standards definiert. Vom IEEE wurden die sehr häufig eingesetzten LAN-Standards IEEE 802.3 und IEEE 802.5 entwickelt.
- *International Telecommunication Union Telecommunication Standardization Sector (ITU-T)* – Früher trug diese Organisation die Bezeichnung Committee for International Telegraph and Telephone (CCITT). ITU-T

ist heute eine internationale Organisation, die Kommunikationsstandards entwickelt. Unter anderem wurde von der ITU-T das X.25-Protokoll entwickelt.

- *Internet Activities Board (IAB)* – IAB ist eine Gruppe von Internetworking-Forschern, die neue Aspekte zum Internet diskutieren und Internet-Regeln verabschieden und Arbeitsgruppen einsetzen. Einige Dokumente mit dem Status Request For Comments (RFC) wurden vom IAB als Internet-Standards herausgegeben, wozu auch das Transmission Control Protocol/Internet Protocol (TCP/IP) und das Simple Network Management Protocol (SNMP) gehören.

1.11 Zusammenfassung

Diese Kapitel führte die Grundelemente ein, aus denen Internetworks aufgebaut sind. Zu verstehen, wo die Teile von Internetworks in das OSI-Modell passen, hilft die Konzepte besser zu verstehen. Internetworks sind zusammengesetzte Systeme, die als Ganzes betrachtet zu komplex sind, um sie verstehen zu können. Nur durch das Aufteilen des Netzwerkes in die Grundbausteine kann es auf einfache Weise verstanden werden. Versuchen Sie, während Sie lesen und Netzwerke kennen lernen, in den Kategorien der OSI-Schichten und Grundbausteine darüber nachzudenken.

Das Verstehen des Zusammenwirkens zwischen verschiedenen Schichten und Protokollen macht das Entwerfen, Konfigurieren und die Diagnose von Internetworks möglich. Ohne das Verstehen der Grundbausteine ist das Verstehen des Zusammenwirkens kaum möglich.

1.12 Fragen zum Kapitel

F: Welche Schichten hat das OSI-Modell?

A: Application (Anwendung), Presentation (Darstellung), Session (Kommunikation, Sitzung), Transport (Transport), Network (Vermittlung), Data Link (Sicherung, Verbindung), Physical (physikalische Schicht).

F: Welche Schicht ist für die Wahl des Pfades in einem Internetwork zuständig?

A: Schicht 3, die Vermittlungsschicht.

F: Was wird in der physikalischen Schicht festgelegt?

A: Spannungsniveaus, Zeit für Spannungsänderungen, physikalische Datenraten, maximale Entfernungen für die Übertragung, physikalische Verbindungen und die Art des Mediums.

F: *Nennen Sie eine Methode zur Abbildung von Netzwerk-Adressen auf MAC-Adressen.*

A: ARP, Hello, Berechenbarkeit.

F: *Was beinhaltet mehr Overhead, verbindungsorientierte oder verbindungslose Dienste?*

A: Verbindungsorientierte.

1.13 Weiterführende Informationen

- Die Webseite von Cisco (www.cisco.com) ist eine hervorragende Quelle für weitere Informationen zu diesen Themen. Der Dokumentationsabschnitt enthält eingehende Diskussionen über viele der in diesem Kapitel angesprochenen Themen.
- Teare, Diane: *Designing Cisco Networks*. Indianapolis: Cisco Press, Juli 1999.