Kapitel 3

LANs

3.1 Einführung

Sie sollten das OSI-Referenzmodell nun grundsätzlich verstanden haben und wissen, was mit Datenpaketen passiert, wenn diese durch die verschiedenen Schichten wandern. Nun wollen wir uns den grundlegenden Netzwerkgeräten zuwenden. Wir werden sehen, welche Geräte bei der Abarbeitung der einzelnen OSI-Schichten eingesetzt werden. In diesem Kapitel wollen wir uns hauptsächlich den LANs (Local Area Networks) widmen.

Wie Sie bereits wissen, handelt es sich bei LANs um Hochgeschwindigkeitsnetzwerke mit geringer Fehlerrate, die sich auf vergleichsweise kleine geografische Gebiete (mit einem Durchmesser von maximal wenigen tausend Metern) beschränken. LANs verbinden Workstations, Peripheriegeräte, Terminals und andere Geräte innerhalb eines Gebäudes oder eines anderen räumlich begrenzten Bereichs miteinander.

Zwar funktioniert das Senden von Daten an alle Geräte innerhalb eines kleinen Netzwerks ohne Probleme, es ist aber einleuchtend, dass umso mehr Datenverkehr stattfindet, je größer ein Netzwerk ist. Dieser Umstand kann ein schwerwiegendes Problem darstellen, da auf einem Kabel immer nur ein Paket zur selben Zeit transportiert werden kann. Wenn also alle Geräte in einem Netzwerk nur an einem gemeinsamen Kabel angeschlossen sind, verlangsamt das den Datenfluss im Netzwerk beträchtlich.

Netzwerkgeräte sind Komponenten, die zur Verbindung von Netzwerken eingesetzt werden. Nicht nur Umfang und Komplexität von Computernetzwerken nehmen kontinuierlich zu; dies gilt gleichermaßen für die Netzwerkgeräte, die für ihre Verbindung eingesetzt werden. Netzwerkgeräte können den Kommunikationsumfang innerhalb eines Netzwerks steuern und den Datenfluss beschleunigen.

In diesem Kapitel werden Sie Netzwerktopologien, einfache LAN-Geräte und die Entwicklung der Netzwerkgeräte kennen lernen. Ferner werden Sie ein wenig über die Netzwerkgeräte erfahren, die in den einzelnen Schichten des OSI-Referenzmodells eingesetzt werden. Außerdem werden Sie sehen, wie Pakete durch die einzelnen Geräte geleitet werden, wenn sie die Schichten des OSI-Modells durchwandern. Abschließend werden Sie die grundlegenden Schritte bei der Einrichtung von LANs kennen lernen.

3.2 Topologien

Der Begriff Topologie definiert die Struktur eines Netzwerks. Die Topologiedefinition besteht aus zwei Teilen: der physikalischen Topologie (d. h. der tatsächlichen Anordnung von Leitungen oder anderen Übertragungsmedien) und der logischen Topologie (diese bestimmt, wie die Hosts auf die Übertragungsmedien zugreifen). Gängige physikalische Topologien sind Bus-, Ring-, Stern-, erweiterte Stern-, hierarchische und vermaschte Topologien (Abbildung 3.1).

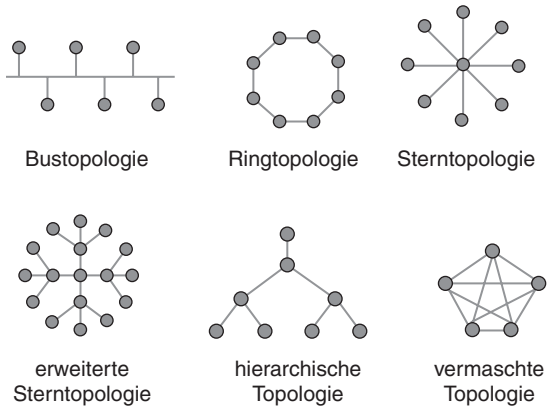

Abbildung 3.1: Der physikalische Aufbau, der festlegt, wie ein LAN tatsächlich aussieht, wird als Topologie bezeichnet.

Die gängigen physikalischen Topologien sind die folgenden:

- **Bustopologie.** Hier wird ein einzelnes Backbone-Segment (Kabel) verwendet, an das alle Hosts direkt angeschlossen sind.
- **Ringtopologie.** Hier wird jeder Host mit dem jeweils nächsten Host verbunden, und der letzte Host dieser Kette wird wieder an den ersten angeschlossen. Das Ergebnis ist ein physikalischer Leitungsring.
- **Sterntopologie.** In diesem Fall werden alle Kabel an ein zentrales Gerät angeschlossen, z. B. einen Hub oder einen Switch (diese Geräte werden im Verlauf dieses Kapitels noch beschrieben).
- **Erweiterte Sterntopologie.** Diese Topologie basiert auf der Sterntopologie. Es werden einzelne Sterne durch Verknüpfung von Hubs oder Switches miteinander verbunden. Auf diese Weise lassen sich Umfang und Größe des Netzwerks erweitern.
- **Hierarchische Topologie.** Dieses System ähnelt der erweiterten Sterntopologie. Hier allerdings werden Hubs oder Switches nicht direkt miteinander verbunden, sondern die Kommunikation sekundärer (d. h. untergeordneter) Systeme wird von einem Zentralcomputer innerhalb der Topologie gesteuert.
- **Vermaschte Topologie.** Diese Topologie wird eingesetzt, wenn die Kommunikation keinesfalls unterbrochen werden darf (dies ist beispielsweise bei den Steuer-

systemen eines Atomkraftwerks der Fall). Man erkennt in Abbildung 3.1, dass bei einer komplett vermaschten Topologie jeder Host über eigene Verbindungen zu allen anderen Hosts verfügt. Eine teilweise vermaschte Topologie ähnelt der Struktur des Internets, welches über zahlreiche Pfade zu jedem beliebigen Host verfügt (wenn auch natürlich nicht von jedem Host zu jedem anderen Host).

Abbildung 3.2 zeigt mehrere Topologien. Sie sehen hier ein LAN mit geringer Komplexität, wie es etwa in Schulen oder kleinen Unternehmen vorkommen kann. Die Abbildung beinhaltet eine Menge Symbole und stellt viele Netzwerkkonzepte dar, die Sie im Verlauf dieses Buchs kennen lernen werden.

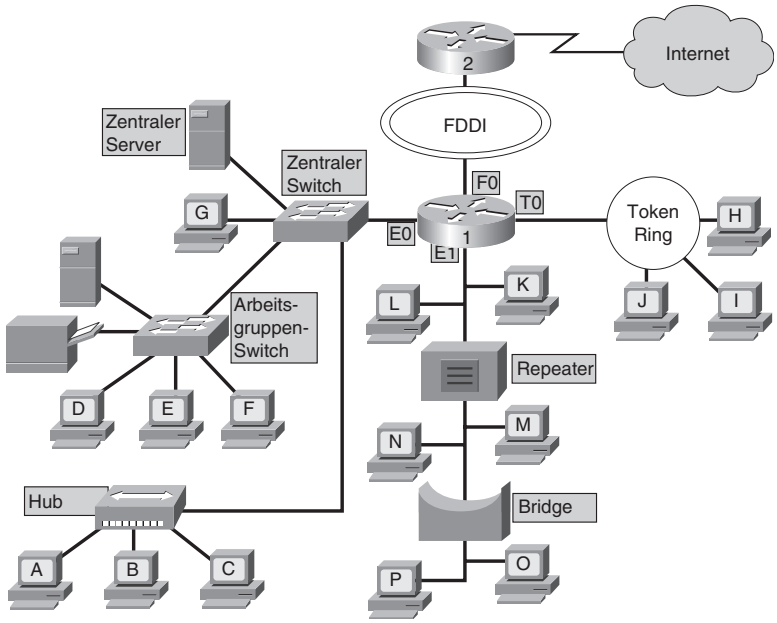

Abbildung 3.2: Dieses LAN ist typisch für ein Schulnetzwerk; es enthält viele der Geräte, die Sie im CCNA-Curriculum kennen müssen.

3.2.1 LAN-Geräte in einer Topologie

Geräte, die direkt an ein Netzwerksegment angeschlossen sind, werden häufig als Hosts bezeichnet. Zu diesen Hosts gehören Computer (und zwar Clients wie auch Server), Drucker, Scanner und viele andere Anwendergeräte. Die Hosts sind auch ohne Netzwerk funktionsfähig, allerdings sind ihre Fähigkeiten dann stark eingeschränkt.

Hostgeräte gehören keiner Schicht an. Sie verfügen über eine physikalische Verbindung zum Netzwerkmedium in Form der Netzwerkkarte, während die Funktionen der anderen OSI-Schichten über eine Software realisiert werden, die auf dem Host ausgeführt wird. Das bedeutet, dass Hosts auf allen sieben Schichten des OSI-Modells gleichermaßen agieren. Hostgeräte führen zum Beispiel alle Kapselungs-

und Entkapselungsvorgänge selbst aus, um Mails zu versenden, Dokumente zu drucken, Bilder einzuscannen oder auf Datenbanken zuzugreifen. Wenn Sie mit den inneren Vorgängen eines PC vertraut sind, dann können Sie sich den PC selbst als ein sehr kleines Netzwerk vorstellen, in dem der Bus und die Erweiterungssteckplätze an CPU, RAM und ROM angeschlossen sind.

Es gibt für Hosts keine Symbole, die in der Netzwerkindustrie zum Standard geworden sind, aber trotzdem sind Hosts meist recht leicht zu erkennen. Wie Sie Abbildung 3.3 entnehmen können, werden sie vorwiegend so dargestellt, wie sie in Wirklichkeit aussehen, so dass sie auf den ersten Blick erkannt werden können.

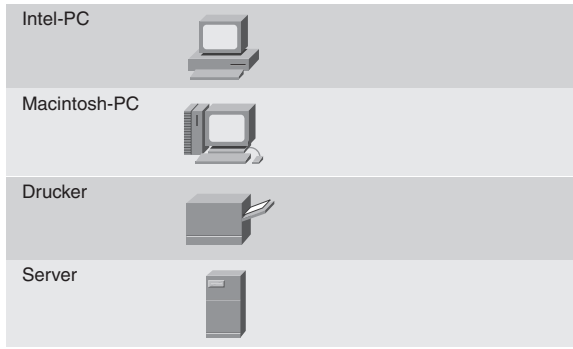

Abbildung 3.3: Diese Geräte können ihren Benutzern eine Netzwerkverbindung bereitstellen, über die Daten oder Ressourcen gemeinsam genutzt werden können.

Der Hauptgrund für den Anschluss eines Computers an das LAN besteht darin, dem Benutzer den Zugriff auf eine Vielzahl von Daten und Anwendungen zu gestatten. Mit moderner Software, Mikroelektronik und einer vergleichsweise geringen Summe Geld können Sie Textverarbeitung, Tabellenkalkulation, Präsentationen und Datenbankzugriffe realisieren. Ferner können Sie einen Webbrowser verwenden, um praktisch unmittelbar auf Daten im World Wide Web zuzugreifen. Sie können Mails verschicken, Grafiken bearbeiten, Daten in Datenbanken ablegen, Computerspiele ausführen und mit anderen Computern in aller Welt kommunizieren usw. Die Liste der Anwendungen wächst täglich.

3.2.2 Netzwerkkarten

Bislang ging es in diesem Kapitel in erster Linie um Geräte und Konzepte der OSI-Schicht 1. Mit der Beschreibung der Netzwerkkarte bewegen wir uns nun zu Schicht 2 (Sicherungsschicht) des OSI-Referenzmodells. Netzwerkkarten werden als zur Schicht 2 gehörig betrachtet. Jede einzelne Karte verfügt weltweit über einen eindeutigen Code: die MAC-Adresse (Media Access Control). Wir werden uns in Kapitel 6 eingehender mit dieser Adresse beschäftigen; an dieser Stelle sei lediglich gesagt, dass sie zur Steuerung der Datenkommunikation des Hosts im Netzwerk verwendet wird.

Die Netzwerkkarte (gelegentlich auch als »Netzwerkadapter« bezeichnet) verbindet den Host mit dem Medium und steuert den Zugriff des Hosts auf dieses Medium. Physikalisch gesehen handelt es sich bei ihr um eine Erweiterungsplatine (Abbildung 3.4), die in einem Steckplatz auf der Hauptplatine eines Computers oder Peripheriegeräts montiert wird. Bei Laptops und Notebooks sind Netzwerkkarten normalerweise als PCMCIA-Karten ausgeführt.

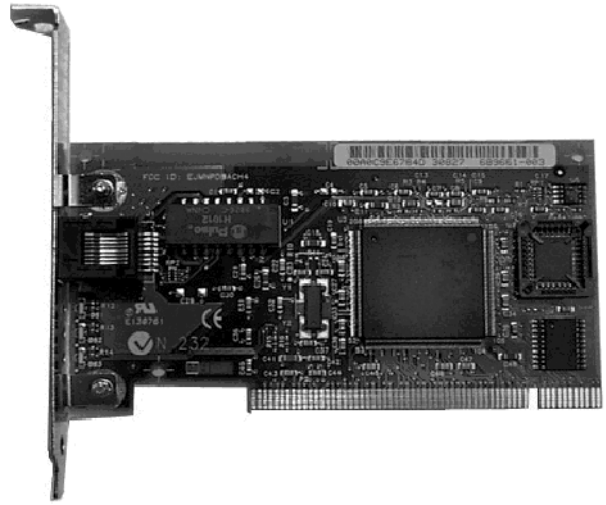

Abbildung 3.4: Die Netzwerkkarte bereitet die Daten nicht nur auf die Übertragung im Medium vor, sondern ist auch für die Steuerung des Datenflusses zwischen Computer und Medium und für den Empfang eingehender Daten verantwortlich.

Die Netzwerkkarte ist die wesentliche Hardwarekomponente bei der Netzwerkkommunikation. Sie übersetzt die parallelen Daten, die der Computer erzeugt, in ein serielles Format, das dann über das Netzwerkkabel übertragen wird. Die Nullen und Einsen der Binärkommunikation werden in elektrische Impulse, Lichtimpulse, Radiowellen oder andere Signalkodierungen gewandelt, die das Medium transportieren kann.

Ein wichtiges Element der Netzwerkkarte ist der Transceiver (Kunstwort aus *Transmitter* und *Receiver*, also Sender und Empfänger). Heute sind bei allen Karten – z. B. solchen, die in 10Base2- oder 10/100BaseT-Netzwerken eingesetzt werden – die Transceiver auf der Karte selbst enthalten. Früher verfügten beispielsweise Karten für 10Base5-Netzwerke über einen AUI-Anschluss (Attachment Unit Interface), über den mittels eines externen Kabels ein Transceiver angeschlossen wurde. Der Transceiver dient der Sendung und dem Empfang von Daten.

Es gibt Fälle, in denen der Anschlusstyp auf der Netzwerkkarte nicht zu dem Medium passt, das an die Karte angeschlossen werden soll. Ein gutes Beispiel hierfür ist der Router Cisco 2500. Auf dem Router befinden sich z. B. nur AUI-Anschlüsse. Soll

der Router nun an ein Category-5-UTP-Ethernetkabel (Kabel mit unabgeschirmten, verdrillten Aderpaaren; kurz »CAT5 UTP«) angeschlossen werden, so wird dafür ein Transceiver benötigt. Dieser wandelt einen Signal- und/oder Anschlusstyp in einen anderen um (z. B. kann über einen Transceiver eine 15-polige AUI-Schnittstelle mit einem RJ45-Anschluss verbunden werden, oder elektrische Impulse können in optische Signale konvertiert werden). Ein Transceiver gilt als Gerät der Schicht 1, da er ausschließlich Bits verarbeitet und mit Adressdaten oder Protokollen höherer Ebene nichts anfangen kann.

Für Netzwerkkarten gibt es keine Standardsymbole. Es wird vielmehr vorausgesetzt, dass, wenn Netzwerkgeräte an Netzwerkmedien angeschlossen sind, immer irgendeine Art von Netzwerkkarte oder einer ähnlichen Komponente vorhanden ist, auch wenn diese im Allgemeinen nicht darstellt ist. Ein Endpunkt in einer Netzwerktopologie ist deshalb entweder eine Netzwerkkarte oder eine (physikalische) Schnittstelle, die zumindest teilweise Aufgaben einer Netzwerkkarte übernimmt.

3.3 Medien

Wie aus Abbildung 3.5 zu ersehen ist, können die Symbole für Übertragungsmedien variieren. Das Ethernetsymbol etwa ist normalerweise eine gerade Linie, von der andere Linien senkrecht abgehen; das Token-Ring-Netz wird durch einen Kreis symbolisiert, an den die Hosts angeschlossen sind; und FDDI-Netze werden durch zwei konzentrische Kreise dargestellt, an die die Geräte angeschlossen sind.

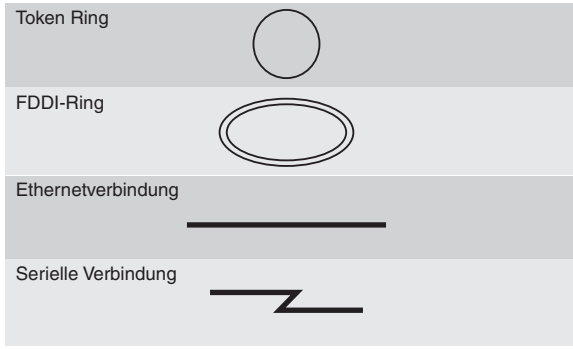

Abbildung 3.5: Das Netzwerkmedium ist die Komponente, über die die Signale von einem Netzwerkgerät zum anderen wandern.

Die Hauptfunktion von Medien besteht darin, einen bitförmigen Datenstrom in einem LAN zu übertragen. Mit Ausnahme drahtloser LANs (die die Atmosphäre oder den Weltraum als Medium verwenden) und der neuartigen PANs (Personal Area Networks; diese verwenden als Medium den menschlichen Körper!) beschränken sich die Übertragungsmedien in LANs auf Leiterkabel (z. B. Kupferdrähte) und Glasfaserkabel. Übertragungsmedien werden als LAN-Komponenten der Schicht 1 betrachtet.

Computernetzwerke können mit verschiedenen Medientypen aufgebaut werden. Dabei hat natürlich jedes Medium seine Vor- und Nachteile, und der Vorteil eines Mediums kann gleichzeitig der Nachteil eines anderen Mediums sein (man vergleiche einmal die Kosten für CAT5-Kabel mit denen für Glasfaserkabel). Zu den möglichen Vor- oder Nachteilen gehören die folgenden Faktoren:

- Kosten
- einfache Installation
- maximale Kabellänge

Netzwerksignale können auch über Koaxialkabel, Glasfaserkabel und sogar im freien Raum übertragen werden. Wir werden uns hier allerdings hauptsächlich auf das CAT5-UTP-Kabel konzentrieren, denn dieses Kabel ist das meistverwendete Medium bei Netzwerkinstallationen.

3.4 Repeater

Wie gerade erwähnt, gibt es bei den verschiedenen Medientypen zahlreiche Vor- und Nachteile. Einer der Nachteile des von uns bevorzugten CAT5-UTP-Kabels ist die auf 100 Meter begrenzte Maximallänge des Kabels. Wenn Sie also ein Netzwerk aufbauen, in dem diese Grenze überschritten werden kann oder wird, dann benötigen Sie ein neues Gerät in Ihrem Netzwerk: den Repeater.

Der Begriff »Repeater« (dt. etwa »Wiederholer«) stammt aus den frühen Tagen der visuellen Kommunikation: Ein Mann stand auf einem Hügel und empfing von einem anderen Mann, der auf einem anderen Hügel zur Linken stand, ein visuelles Signal; er wiederholte dieses Signal in Richtung eines dritten Mannes, der auf einem Hügel zu seiner Rechten stand. Ein Gerät dieses Namens gab es übrigens auch schon in der Telegrafie, dem Telefon, der Nachrichtentechnik und der optischen Kommunikation, und überall besteht der Sinn darin, den Signalverlust in längeren Leitungen durch Neuverstärkung auszugleichen.

Häufige Probleme in der Netzwerktechnik sind eine zu große Zahl von angeschlossenen Geräten und zu große Entfernungen. Beide Probleme können durch den Einsatz eines Repeaters gelöst werden.

Wie Netzwerkmedien sind auch Repeater Netzwerkgeräte der Schicht 1 (Bitübertragungsschicht) des OSI-Modells. Um verstehen zu können, wie ein Repeater funktioniert, ist es wichtig zu wissen, dass Daten in elektrische oder in Lichtimpulse gewandelt werden, bevor Sie einen Absender verlassen und dann im Netzwerkmedium versandt werden. Diese Impulse werden als Signale bezeichnet. Wenn Signale den Absender verlassen, sind sie klar und eindeutig zu erkennen. Je größer jedoch die Strecke ist, die sie im Netzwerkmedium zurückgelegt haben, desto schwächer und verzerrter werden sie. Wie bereits gesagt, hat ein CAT5-Ethernetkabel eine maximal zulässige Länge von 100 Metern. Wenn ein Signal nun eine größere Distanz zurücklegt, dann ist nicht mehr sichergestellt, dass die Netzwerkkarte beim Empfänger das Signal korrekt lesen kann. Ein Repeater stellt eine einfache Lösung dieses Problems dar.

Der Zweck eines Repeaters ist die Neugenerierung und Neutaktung von Netzwerksignalen auf der Bitebene, damit diese eine größere Strecke im Medium zurücklegen können. Für 10-MBit/s-Ethernetnetze gilt eine Regel, die bei der Erweiterung von LAN-Segmenten beachtet werden muss: die »5-4-3-Regel« oder »Vier-Repeater-Regel«. Diese Regel besagt, dass Sie maximal fünf Netzwerksegmente seriell mit Hilfe von vier Repeatern verbinden können, aber nur drei Segmente dürfen Hosts (Computer) beinhalten.

Ursprünglich bezeichnete der Begriff »Repeater« ein Gerät mit jeweils genau einem Eingang und einem Ausgang. Es gibt jedoch auch Repeater mit mehreren Anschlüssen. Repeater werden als Geräte in der Schicht 1 des OSI-Modells klassifiziert, da sie lediglich auf der Bitebene agieren und andere Daten transparent weiterleiten. Das Symbol für Repeater ist nicht standardisiert.

3.5 Hubs

Allgemein gesprochen wird der Begriff Hub immer dann anstelle des Terms Repeater verwendet, wenn von einem Gerät die Rede ist, das als zentrales Element eines Netzwerks verwendet wird (Abbildung 3.6). Obwohl ein Hub in einer physikalischen Sterntopologie eingesetzt wird, verhält er sich wie eine Bustopologie: Wenn ein Gerät sendet, lauschen alle anderen Geräte, wodurch ein logischer Bus erzeugt wird.

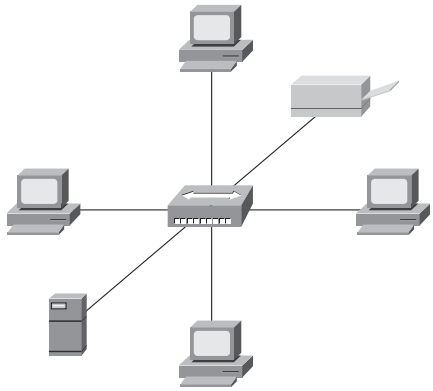

Abbildung 3.6: In Ethernet- und Token-Ring-Netzwerken werden normalerweise Sterntopologien verwendet. Im Zentrum solcher Netze steht immer ein Hub, ein Repeater oder ein Konzentrator.

Der Zweck eines Hubs besteht in der Neugenerierung und Neutaktung von Netzwerksignalen. Dies geschieht auf der Bitebene für eine große Anzahl von Hosts (vier, acht oder vielleicht sogar 24 Hosts). Man bezeichnet diesen Vorgang als Konzentration. Hier eine Liste der wichtigsten Eigenschaften von Hubs:

- Sie generieren und wiederholen Signale.
- Sie senden Signale an das gesamte Netzwerk.
- Sie können Netzwerkdaten nicht gezielt filtern.

– Sie sind nicht in der Lage, den optimalen Pfad zu bestimmen.
– Sie werden als Netzwerkkonzentrationspunkte eingesetzt.

Sie werden bemerken, dass die Eigenschaften eines Hubs denen eines Repeaters ähneln; aus diesem Grund bezeichnet man einen Hub manchmal auch als »Multiport-Repeater«. Der Unterschied besteht in der Anzahl der an das Gerät anschließbaren Kabel. Während ein Repeater normalerweise nur zwei Anschlüsse aufweist, hat ein Hub zwischen vier und 20 oder mehr Ports (Abbildung 3.7). Und während ein Repeater an einem Anschluss Daten empfängt und am anderen wieder verstärkt ausgibt, empfängt ein Hub zwar auch Daten an einem Port, leitet sie dann aber an alle anderen weiter.

Hubs werden in der Regel in Ethernet-10BaseT- oder -100BaseT-Netzwerken verwendet. Die Rolle des Hubs in einem Token-Ring-Netzwerk wird von einer MAU (Media Access Unit) gespielt. Zwar ähnelt diese physikalisch einem Hub, aber die Token-Ring-Technologie arbeitet, wie Sie in Kapitel 7 werden sehen, ganz anders. Bei FDDI-Netzwerken schließlich heißt das Verbindungsgerät Konzentrator. Auch MAUs und Konzentratoren sind Geräte der OSI-Schicht 1.

Abbildung 3.7: Hubs werden auch als Konzentratoren bezeichnet, da sie auch als zentrale (»konzentrierende«) Verbindungspunkte verwendet werden.

Zwei der Gründe zur Verwendung von Hubs sind die Erstellung eines zentralen Verbindungspunkts für den Anschluss von Medien und die Erhöhung der Netzwerkzuverlässigkeit. Letztere ergibt sich logisch, denn nun kann ein beliebiges Kabel ausfallen, ohne dass gleich das gesamt Netzwerk gestört wird; hier liegt ein Unterschied zur Bustopologie, wo die Unterbrechung eines einzigen Kabels das gesamte Netzwerk stilllegen kann. Hubs werden als Geräte der Schicht 1 betrachtet, denn sie verstärken das Signal lediglich und geben es dann an all ihren Anschlüssen aus.

Es gibt in der Netzwerktechnik verschiedene Klassifizierungen für Hubs (Abbildung 3.8; da es kein standardisiertes Symbol gibt, werden wir in diesem Buch durchgehend das dort gezeigte Symbol verwenden). Zunächst einmal kann man Hubs in aktive und passive Versionen unterteilen. Die meisten modernen Hubs sind aktiv, d. h. sie werden von einer Stromquelle versorgt, um die Netzwerksignale regenerieren zu können. Sehr selten verwendet man passive Hubs, deren Aufgabe in erster Linie darin besteht, Signale an mehrere Benutzer zu verteilen. Passive Hubs verstärken die Signale nicht, können also auch nicht zur Verlängerung der maximalen Leitungslänge verwendet werden.

Eine spezielle Version des aktiven Hubs ist der intelligente Hub. Er erzeugt nicht nur das Signal neu, sondern verfügt über einen integrierten Prozessor, der Ihnen Diagno-

sefunktionen bereitstellt, damit Sie gegebenenfalls Probleme mit einem bestimmten Port einschränken können.

Abbildung 3.8: Das Symbol für einen Hub ist nicht standardisiert.

3.6 Bridges

Eine Bridge ist ein Schicht-2-Gerät, welches zur Erzeugung zweier oder mehrerer LAN-Segmente dient, die jeweils eine separate Kollisionsdomäne darstellen. Dies geschieht zum Zweck der Bandbreitenerhöhung, denn Bridges filtern die Datenkommunikation in einem LAN – etwa, um lokale Daten auch nur lokal zu versenden – und ermöglichen gleichzeitig Verbindungen zu anderen Teilen (Segmenten) des LAN, damit Daten, die in diese anderen Teile übertragen werden sollen, auch dorthin gelangen. Vielleicht fragen Sie sich jetzt, woher die Bridge weiß, welche Daten lokal sind und welche nicht. Die Antwort entspricht der auf die Frage, woher ein Postangestellter bei der Verteilung weiß, welche Briefe in seiner Stadt bleiben und welche woanders hin müssen: Die Bridge merkt sich die lokalen Adressen. Wie bereits erwähnt, haben die Netzwerkkarten aller Netzwerkgeräte eine eigene, eindeutige MAC-Adresse. Die Bridge speichert die MAC-Adressen, die an ihren beiden Anschlüssen auftreten, und entscheidet auf der Basis dieser Adressliste, welche Daten wohin gelangen können.

Aufgrund ihrer Fähigkeit, Netzwerkkommunikation auf der Basis der MAC-Adresse auszufiltern, können Bridges Daten beliebiger Netzwerkprotokolle sehr schnell weiterleiten – denn mit diesen Protokollen müssen sie sich ja gar nicht erst auseinander setzen. Es geht also nur darum, Frames entweder weiterzuleiten oder eben nicht weiterzuleiten, je nach MAC-Adresse. Hier eine Liste wichtiger Merkmale von Bridges:

- Bridges sind »intelligenter« als Hubs, d. h. sie können eingehende Frames analysieren und auf der Basis der Adressdaten weiterleiten (oder auch nicht).
- Sie sammeln Pakete und leiten diese dann zwischen zwei oder mehr LAN-Segmenten weiter.
- Sie erstellen mehrere Kollisionsdomänen und erlauben es so mehreren Geräten, Daten gleichzeitig zu übertragen, ohne dass es zu einer Kollision kommt.
- Sie erstellen Adresstabellen.

Abbildung 3.9 zeigt ein Beispiel für den Einsatz einer Bridge. Das Aussehen von Bridges kann von Typ zu Typ sehr stark variieren. Zwar haben Router und Switches eine Reihe der Funktionen von Bridges übernommen, aber Bridges spielen nichtsdestoweniger in vielen Netzwerken eine wichtige Rolle. Wenn man also Router und Switches verstehen will, dann muss man sich erst einmal die Funktionsweise von Bridges klarmachen. In Abbildung 3.9 ist das Symbol einer Bridge zu sehen, welches ein wenig an eine Hängebrücke erinnert. Der Begriff »Bridge« bezeichnet immer ein Gerät mit genau zwei Anschlüssen (obwohl in der Literatur auch Bridges mit drei oder mehr Anschlüssen erwähnt werden).

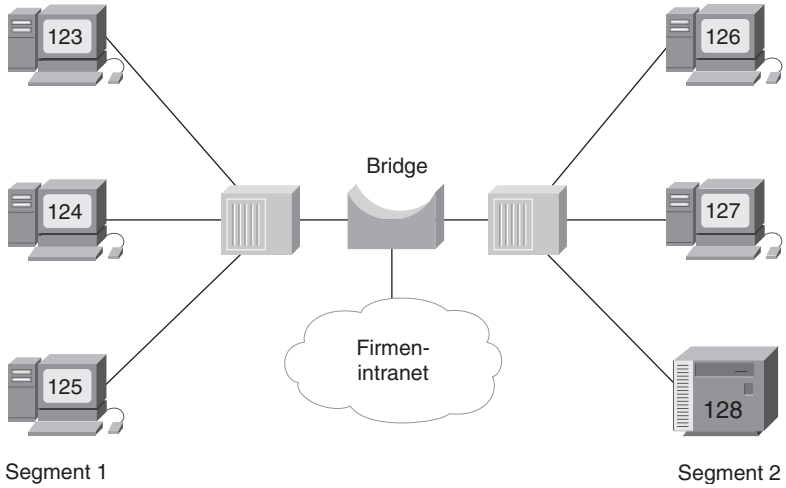

Abbildung 3.9: Bridges agieren in der Schicht 2 (Sicherungsschicht) des OSI-Referenzmodells und beachten keine Daten, die für darüber liegende Schichten gedacht sind.

3.7 Switches

Ein Switch ist ebenso wie eine Bridge ein Gerät der Schicht 2. Tatsächlich werden Switches auch hin und wieder als »Multiport-Bridge« bezeichnet (ähnlich, wie ein Hub auch »Multiport-Repeater« genannt wird); der Unterschied zwischen Hub und Switch ist der gleiche wie der zwischen einer Bridge und einem Repeater: Switches treffen auf der Basis der MAC-Adressen Entscheidungen, während Hubs überhaupt keine Entscheidungen treffen.

Dank der Fähigkeit, Entscheidungen zu treffen, können Switches die Effizienz in einem LAN drastisch erhöhen. Dies erreichen sie durch das Switching; dieser Begriff bezeichnet die Fähigkeit, Daten gezielt an den Anschluss zu senden, mit dem der Zielhost verbunden ist. Ein Hub hingegen sendet seine Daten an *alle* Ports, d. h. alle Hosts müssen alle Daten überprüfen und verarbeiten (also annehmen oder nicht annehmen).

Auf den ersten Blick sehen Switches oft wie Hubs aus: Beide Gerätetypen verfügen über mehrere Anschlüsse, denn ein Teil ihrer Funktion ist die Verbindungskonzentration (d. h. der Anschluss möglichst vieler Geräte an einem zentralen Punkt im Netzwerk). Die Unterschiede zwischen Hubs und Switches liegen in dem, was *in* den Geräten passiert. Abbildung 3.10 zeigt das Symbol für einen Switch; die Pfeile oben auf dem Gerät stehen für die unterschiedlichen Datenpfade, die ein Switch realisieren kann.

Abbildung 3.10: Switches sind Geräte, die in der Sicherungsschicht des OSI-Referenzmodells agieren.

Stellen Sie sich also einen Switch als ein Gerät vor, welches die Anschlussmöglichkeiten eines Hubs mit den Möglichkeiten verbindet, die eine Bridge zur Kommunikationssteuerung anbietet. Die Frames werden von den Eingangs-Ports (Schnittstellen) auf die Ziel-Ports geschaltet, und jeder dieser Anschlüsse verfügt über die volle Bandbreite. Mehr hierzu werden Sie in Kapitel 7 erfahren.

3.8 Router

Der Router ist das erste hier vorgestellte Gerät, welches in der OSI-Schicht 3 arbeitet. Der Router ist deswegen so definiert, weil er – anders als Geräte der Schicht 2 – Entscheidungen nicht auf der Basis der MAC-Adressen, sondern der Netzwerkadressen fällt. Router können außerdem verschiedene Technologien der Schicht 2 miteinander verbinden, so etwa Ethernet, Token Ring und FDDI. Aufgrund ihrer Fähigkeit, Pakete basierend auf Schicht-3-Daten zu verteilen, sind Router, auf denen das IP-Protokoll ausgeführt wird, zum Rückgrat des Internets geworden.

Der Zweck eines Routers besteht darin, die Schicht-3-Daten eingehender Pakete zu untersuchen, darauf basierend den geeignetsten Pfad im Netzwerk zu wählen und die Daten dann entsprechend auf den passenden Ausgangsanschluss zu schalten. In großen Netzwerken sind Router die wichtigsten Geräte zur Verkehrssteuerung. Es sind die Router, die es praktisch jedem Computer ermöglichen, mit jedem beliebigen anderen Computer in der Welt zu kommunizieren! Router können aber nicht nur diese Grundfunktionen ausführen, sondern erfüllen auch zahlreiche andere Aufgaben, die wir in späteren Kapiteln noch beschreiben werden.

Router unterscheiden sich in vielerlei Hinsicht von Bridges. Zunächst einmal arbeiten Bridges in der Schicht 2 (Sicherungsschicht), während Router in Schicht 3 (Vermittlungsschicht) des OSI-Modells agieren. Zweitens leiten Bridges die Daten auf der Basis der physikalischen Adresse (MAC-Adresse) weiter, Router hingegen setzen hierzu auf ein anderes Adressierungsschema, welches in Schicht 3 auftritt. Sie verwenden Adressen der Vermittlungsschicht, die allgemein als logische Adressen oder IP-Adressen bezeichnet werden. Ein Router vergleicht die erkannte IP-Adresse des Zielrechners mit den Daten in seiner Routingtabelle und schickt empfangene Daten auf dieser Basis entweder an das richtige Netzwerk weiter oder lokal schließlich an den richtigen Zielhost. Da IP-Adressen softwareseitig implementiert sind und auf ein Netzwerk verweisen, in dem sich ein Gerät befindet, werden diese Schicht-3-Adressen manchmal auch als Protokolladressen oder Netzwerkadressen bezeichnet. Physikalische Adressen (MAC-Adressen) werden normalerweise vom Hersteller der Netzwerkkarte vergeben und sind in diese Karte »eingebrannt«; IP-Adressen hingegen weist der Netzwerkadministrator zu.

Das Symbol eines Routers (Abbildung 3.11) signalisiert die beiden primären Verwendungszwecke: Pfadauswahl und Versand der Pakete über die optimale Route. Ein Router kann verschiedene Arten von Schnittstellen aufweisen.

Abbildung 3.11: Das Router-Symbol.

Abbildung 3.12 zeigt die Schnittstellen eines Routers der 2500-Serie mit Ethernet-Anschluss für eine LAN-Anbindung.

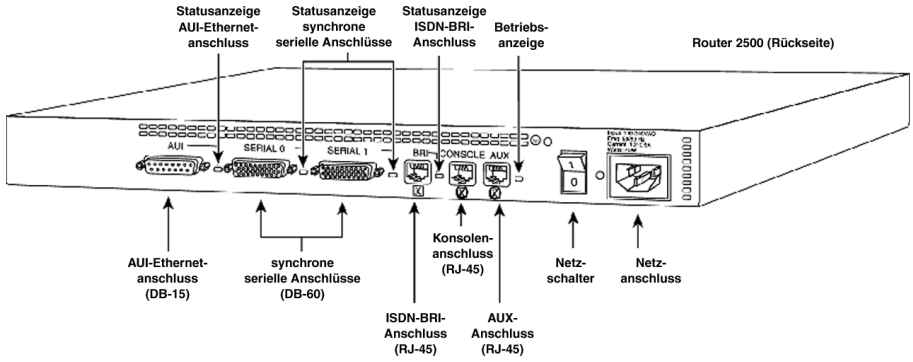

Abbildung 3.12: Der Konsolenanschluss ermöglicht eine direkte Verbindung zum Router; mit diesem Anschluss wird die Konfiguration des Gerätes durchgeführt.

Abbildung 3.13 zeigt die Anschlüsse von Routern der Serien 1603 und 3640.

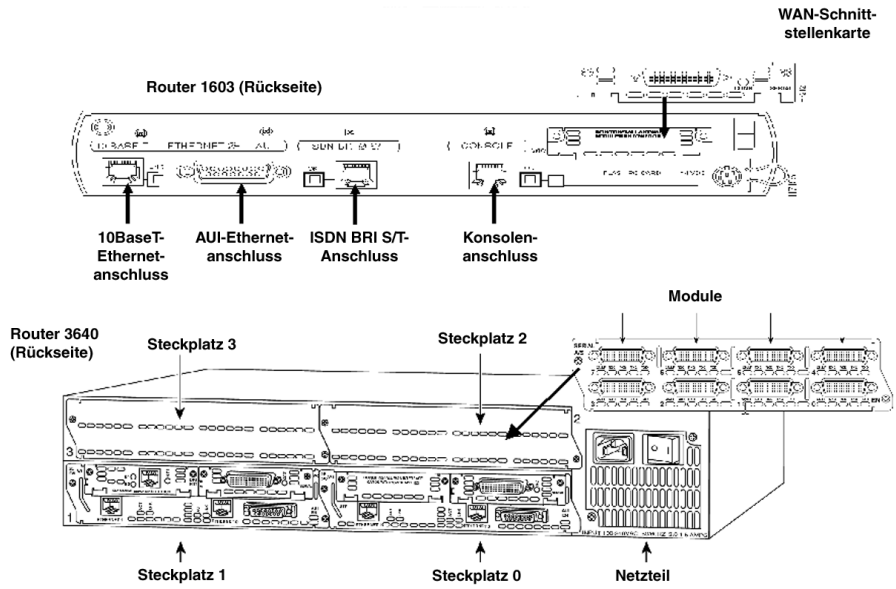

Abbildung 3.13: Diese Router verfügen für Ethernetverbindungen sowohl über 10BaseT- als auch über AUI-Anschlüsse.

3.9 Wolken

Das Wolkensymbol in Abbildung 3.14 repräsentiert in der Regel ein anderes Netzwerk, manchmal auch das Internet. Es zeigt lediglich an, dass eine Möglichkeit zur Verbindung mit diesem anderen Netzwerk (oder dem Internet) vorhanden ist; wie diese Verbindung aussieht oder um was für ein Netzwerk es sich überhaupt handelt, geht aus dem Symbol nicht hervor.

Abbildung 3.14: Die Wolke steht für eine Menge von Detailangaben, die aber in der gegebenen Situation nicht wichtig sind.

Eine Wolke weist viele physikalische Merkmale auf. Stellen Sie sich zum besseren Verständnis einmal all die Geräte vor, über die Ihr Computer mit einem anderen, sehr weit entfernten Computer (vielleicht auf einem anderen Kontinent) verbunden ist. Es gibt kein einzelnes Bild, auf dem all die Vorgänge und Geräte darstellbar wären, die bei der Herstellung dieser Verbindung beteiligt sind.

Es sei an dieser Stelle noch einmal darauf verwiesen, dass wir uns zum gegenwärtigen Zeitpunkt nur dafür interessieren, wie LANs mit größeren WANs und dem Internet (dem *ultimativen* WAN) verbunden werden, so dass jeder Computer mit jedem anderen Computer an jedem Ort zu jeder Zeit kommunizieren kann. Da die Wolke kein einzelnes Gerät ist, sondern eine Sammlung von Geräten repräsentiert, die auf allen Ebenen des OSI-Modells vorhanden sein können, kann die Wolke als Gerät der Schichten 1 bis 7 klassifiziert werden.

3.10 Netzwerksegmente

Der Begriff Segment hat in der Netzwerktechnik zahlreiche Bedeutungen. Die korrekte Definition hängt von der Situation ab, in der das Wort benutzt wird[1]. Historisch gesehen beschreibt ein Segment das Schicht-1-Medium als den normalen Kabelweg für die Datenübertragung in einem LAN. Wie bereits weiter oben unter »Medien« beschrieben, gibt es bei jedem Medientyp eine maximal zulässige Übertragungslänge. Jedes Mal, wenn nun ein elektrisches Gerät eingesetzt wird, um diese Länge zu erweitern oder Daten zu beeinflussen, wird ein neues physikalisches Segment erstellt (Abbildung 3.15).

Eine zweite Definition – die heute bei Cisco gängige – beschreibt ein Segment als eine Kollisionsdomäne. Der Unterschied zwischen der ersten und der zweiten Definition ist sehr subtil; wir werden in Kapitel 7 darauf eingehen, wenn die Kollisionsdomänen beschrieben werden. Eine dritte mögliche Definition besagt, dass ein Segment eine PDU in der OSI-Schicht 4 ist.

---

1. Andere Definitionen des Begriffs »Segment« werden häufig in der Netzwerktechnik eingesetzt; wir werden diese in späteren Kapiteln kennen lernen.

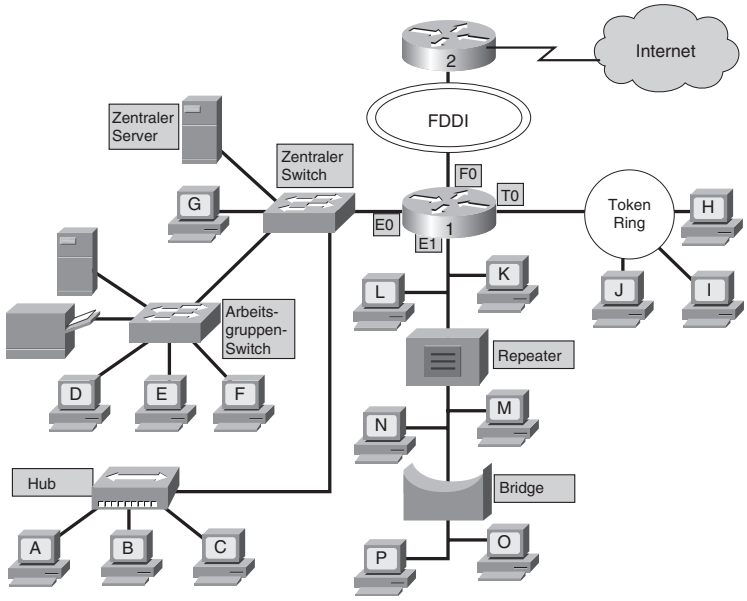

Abbildung 3.15: Ein Netzwerk kann aus mehreren Segmenten bestehen, die durch Netzwerkgeräte miteinander verbunden sind.

3.11 Die Entwicklung der Netzwerkgeräte

Die Geschichte der Computernetzwerke ist sehr komplex, und sehr viele Techniker auf der ganzen Welt haben im Verlaufe der letzten dreißig Jahre daran mitgewirkt. Wir können an dieser Stelle natürlich nur einen sehr groben Überblick darüber geben, wie sich die verschiedenen Geräte, die Sie bereits kennen gelernt haben, der Reihe nach entwickelt haben. Es ist sicher hilfreich zu sehen, welche Probleme von welchen Geräten gelöst wurden – und welche Probleme nach wie vor bestehen.

Die späten Sechziger und die Siebziger Jahre waren die Zeit noch kleinerer Rechner, der so genannten »Mikrocomputer« (auch wenn diese – gemessen an heutigen Standards – immer noch riesig waren). 1978 stellte die Firma Apple dann den Personal Computer vor, und 1981 zog IBM mit einem PC mit offener Architektur nach. Die Benutzerfreundlichkeit des Apple Macintosh, die offene Architektur des IBM-PC und die weitere Miniaturisierung der ICs hatten eine weite Verbreitung von PCs im privaten wie auch im geschäftlichen Bereich zur Folge. In den späten Achtzigern stellten sich die Benutzer von Stand-Alone-Computern dann die Frage, warum man solche Rechner nicht miteinander verbinden sollte; so begann die gemeinsame Nutzung von Daten (Dateien) und Ressourcen (Druckern).

Bereits in den Sechziger Jahren begann das amerikanische Verteidigungsministerium mit dem Aufbau großer, zuverlässiger WANs und setzte diese Maßnahmen bis in die Neunziger fort. Die dabei entwickelten Technologien wurden auch für den Aufbau von LANs eingesetzt, aber wichtiger noch ist die Tatsache, dass sich aus diesen WANs des Verteidigungsministeriums das Internet entwickeln sollte.

Damit Sie den nächsten technologischen Schritt – die Entwicklung der LANs – besser verstehen können, betrachten Sie einmal das folgende Problem: Irgendwo in der Welt gibt es mehrere Computer, die miteinander kommunizieren wollen. Zu diesem Zweck benötigen die Rechner ein Gerät, das in der Lage sein muss, sowohl mit dem Gerät als auch mit dem Medium zu kommunizieren (die Netzwerkkarte); ferner muss es eine Möglichkeit geben, die Meldungen physikalisch zu übertragen (das Medium). Nehmen wir ferner an, dass diese Computer mit anderen Computern kommunizieren wollen, die weiter entfernt sind. Die Lösung dieses Problems waren Repeater und Hubs: Repeater konnten die Übertragungsentfernung von Computerdatensignalen verlängern. Hubs (Multiport-Repeater) ermöglichten einer Gruppe von Benutzern die gemeinsame Nutzung von Dateien, Servern und Peripheriegeräten. Man könnte diese Konstellation als »Arbeitsgruppennetzwerk« bezeichnen.

Solche Arbeitsgruppen (»Workgroups«) wollten schon bald auch mit anderen Gruppen kommunizieren können. Aufgrund der Funktionalität von Hubs (diese senden alle Daten ohne Ansehen des Empfängers an alle Ports) wuchs das Datenaufkommen umso stärker, je größer die Anzahl der Hosts und Workgroups wurde. Um hier Abhilfe zu leisten, erfand man die Bridge, mit der ein Netzwerk in mehrere Kollisionsdomänen unterteilt werden konnte. Auf diese Weise ließ sich die Verkehrslast in einer Domäne verringern.

Die besten Eigenschaften des Hubs (Konzentration und Konnektivität) wurden mit dem wesentlichen Merkmal der Bridge (Segmentierung) zum Switch kombiniert. Ein Switch hat viele Anschlüsse, die sich alle so verhalten, als hätten Sie eine direkte Verbindung zur anderen Seite der Bridge; auf diese Weise lassen sich mehr Benutzer anschließen und größere Datenströme steuern.

In den mittleren Achtzigern wurden Spezialcomputer entwickelt, die man zunächst als Gateways, später dann als Router bezeichnete. Diese Geräte erlaubten die Verbindung mehrerer LANs. Internetworks wurden aufgebaut. Das amerikanische Verteidigungsministerium verfügte bereits über ein sehr ausgedehntes Internetwork, aber erst die flächendeckende Einführung von Routern, die automatisch den optimalen Pfad für Daten ermittelten und Daten vieler verschiedener Protokolle gezielt weiterleiten konnten, ermöglichte die explosionsartige Zunahme von Netzwerken, wie wir sie heute kennen. Dieses Wachstum wird durch die Wolke symbolisiert.

Am Beginn des neuen Jahrhunderts besteht nun der nächste Schritt in der Zusammenführung von Computer- und Kommunikationstechnologien (und hier insbesondere der Zusammenführung von Sprache, Video und Daten, die traditionell durch unterschiedliche Systeme übermittelt werden) zu einem einheitlichen Informationsstrom.

3.11.1 Die Entwicklung der Netzwerkgeräte und die OSI-Schichten

Hosts und Server agieren in den Schichten 1 bis 7 und führen dort die Kapselung durch. Abbildung 3.16 zeigt die Symbole der einzelnen Netzwerkgeräte, die den jeweiligen Schichten des OSI-Referenzmodells zugeordnet sind. Transceiver, Repeater und Hubs werden als aktive Schicht-1-Geräte betrachtet, da sie lediglich Bits über-

tragen und einen Stromanschluss benötigen. Patchkabel, Patchfelder und andere Verbindungskomponenten hingegen sind passive Schicht-1-Komponenten, da sie lediglich eine Art »Leitung« bereitstellen.

Abbildung 3.16: Jedes Gerät verfügt über spezielle Funktionen, die in den einzelnen Schichten des OSI-Modells verwendet werden.

Netzwerkkarten gelten als Geräte der Schicht 2, da auf ihnen die MAC-Adresse gespeichert ist; da sie aber auch häufig Signalisierungs- und Kodierungsaufgaben haben, sind sie ebenso Schicht-1-Geräte. Bridges und Switches sind Schicht-2-Komponenten, da sie auf der Basis der MAC-Adresse (d. h. der Daten in Schicht 2) Entscheidungen zur Weiterleitung von Paketen treffen. Sie agieren aber ebenso in Schicht 1, um Bits die Interaktion mit dem Medium zu ermöglichen.

Router sind Schicht-3-Geräte, denn sie wählen auf der Basis der Netzwerkadressen (Schicht-3-Adressen) die optimalen Pfade aus und weisen Paketen dann die passende Route zu. Router-Schnittstellen agieren nicht nur in Schicht 3, sondern auch in den Schichten 2 und 1. Wolken, in denen Router, Switches, Server und viele andere Geräte enthalten sein können, die wir noch nicht vorgestellt haben, sind den Schichten 1 bis 7 zugeordnet.

3.11.2 Grundlagen zum Datenfluss in LANs

Damit die in einem Netzwerk auftretende Kommunikation zuverlässig abläuft, müssen die übertragenen Daten in Blöcke aufgeteilt werden, die leicht zu bearbeiten und zu identifizieren sind. Dies erfolgt über den in Kapitel 2 beschriebenen Prozess der Kapselung.

Rufen wir uns diesen Prozess noch einmal kurz ins Gedächtnis, so sehen wir, dass die oberen drei Schichten – die Anwendungs-, die Darstellungs- und die Sitzungsschicht – die Daten für die Übertragung vorbereiten, indem sie ein gemeinsames Übertragungsformat erstellen. Die Transportschicht unterteilt die Daten dann in handlichere Einheiten, die als Segmente bezeichnet werden. Ferner werden den einzelnen Segmenten hier Sequenznummern zugewiesen, damit der Empfänger die Daten später wieder in der richtigen Reihenfolge zusammensetzen kann.

Die Vermittlungsschicht kapselt das Segment und erstellt auf diese Weise ein Paket. Diesem werden dann die Netzwerkadressen des Empfängers und des Absenders (in der Regel IP-Adressen) hinzugefügt. In der Sicherungsschicht wird das Paket durch Kapselung nachfolgend zum Frame, und die lokalen Adressen (d. h. MAC-Adressen) von Absender und Empfänger werden hinzugefügt. Die Sicherungsschicht überträgt die Binärdaten des Frames dann über die Medien der Bitübertragungsschicht.

Wenn die Daten lediglich innerhalb eines LAN übertragen werden, bezeichnen wir die Dateneinheiten immer als Frames, weil für die Übertragung des Pakets vom Absender zum Empfänger lediglich die MAC-Adresse benötigt wird. Müssen wir die Daten jedoch über ein Intranet oder das Internet an den Zielhost senden, dann werden die Daten als Pakete oder Datagramme bezeichnet. Zur Zustellung wird hier die im Paket enthaltene Netzwerkadresse mit der endgültigen Zieladresse des Hosts verwendet. Die Daten der Sicherungsschicht dagegen sind lokaler Natur – sie ändern sich, während das Paket durch die einzelnen Netzwerke wandert. Es sind die unteren drei Schichten des OSI-Modells – die Vermittlungs-, die Sicherungs- und die Bitübertragungsschicht, die für den Transport von Daten in einem Intranet oder im Internet zuständig sind.

3.11.3 Paketfluss durch Geräte der Schicht 1

Der Paketfluss durch Geräte der Schicht 1 ist unkompliziert. Als Komponenten dieser Schicht werden zunächst physikalische Medien klassifiziert, die lediglich Bits (z. B. als Spannungs- oder Lichtimpulse) verarbeiten. Wenn die Geräte der Schicht 1 passiv sind (z. B. Stecker, Anschlüsse, Buchsen, Patchfelder oder physikalische Medien), dann wandern die Bits einfach durch diese Komponenten – und zwar am besten so, dass sie nicht verändert werden. Bei aktiven Geräten der Schicht 1 (z. B. Repeatern oder Hubs) werden die erkannten Bits neu generiert und getaktet. Transceiver – auch sie sind aktive Geräte – senden und empfangen nicht nur Daten von den Medien, sondern können als Schnittstellenwandler (AUI-Anschluss auf RJ45-Anschluss) oder als Medienwandler (z. B. RJ45 auf ST optisch) fungieren; in allen Fällen agieren Transceiver jedoch als Schicht-1-Geräte. Kein Gerät der Schicht 1 verarbeitet die Header oder Daten eines gekapselten Pakets. Diese Geräte arbeiten nur mit Bits.

3.11.4 Paketfluss durch Geräte der Schicht 2

Es ist wichtig, sich klar zu machen, dass Pakete *in* Frames enthalten sind, denn in Schicht 2 wird mit Paketen in ihrer gekapselten Form gearbeitet: eben diesen Frames. Denken Sie auch immer daran, dass alles, was mit einem Frame geschieht, gleichermaßen auch mit dem Paket passiert.

Netzwerkkarten, Bridges und Switches verwenden zur Lenkung der Frames die MAC-Adressen (d. h. die Adressen der Sicherungsschicht), weswegen sie als Geräte der Schicht 2 betrachtet werden. Die MAC-Adresse ist auf der Netzwerkkarte gespeichert und in jedem Fall eindeutig. Sie ist die Grundlage des Frames.

Bridges untersuchen die MAC-Adressen eingehender Frames. Wenn der Frame lokal ist (d. h. eine MAC-Adresse enthält, die sich im gleichen Netzwerksegment befindet wie der Empfangsanschluss der Bridge), dann wird er nicht über die Bridge weitergeleitet; ist der Frame nicht lokal (d. h. die MAC-Adresse ist einem anderen Segment zugeordnet als der Empfangsanschluss der Bridge), dann wird er zum nächsten Netzwerksegment weitergeleitet. Einen Switch kann man sich als Hub mit Einzelanschlüssen vorstellen, die wie Bridges funktionieren. Switches lesen die MAC-Adresse eines empfangenen Daten-Frames aus und leiten den Frame dann an den passenden Anschluss weiter.

3.11.5 Paketfluss durch Geräte der Schicht 3

Das wichtigste Gerät, welches dieser Schicht zugeordnet ist, ist der Router. Router agieren eigentlich gleichermaßen in Schicht 1 (d. h. Bits werden an Router-Anschlüssen aus dem Medium empfangen), Schicht 2 (Frames werden auf der Basis der im Paket gespeicherten Daten von einem Eingang gezielt an einen Ausgang geleitet) und Schicht 3 (Entscheidungen zu Weiterleitung und Routing).

Der Paketfluss durch Router (d. h. die Auswahl des optimalen Pfades und das tatsächliche Senden des Pakets über den richtigen Ausgangsanschluss) erfolgt mit Hilfe der Schicht-3-Netzwerkadressen. Wenn der richtige Port ausgewählt ist, kapselt der Router das Paket wieder in einem Frame, um es an seinen nächsten Bestimmungsort weiterzuleiten. Dieser Vorgang geschieht bei jedem Router auf dem Weg vom Absender zum Empfänger.

3.11.6 Paketfluss durch Geräte der Schichten 1 bis 7

Es gibt Geräte (wie etwa Ihren PC), die als Komponenten der Schichten 1 bis 7 betrachtet werden, d. h. sie führen Vorgänge aus, die mit jeder Schicht des OSI-Modells in Verbindung gebracht werden können. Das Gateway (eigentlich ein Computer, der Daten von einem Protokoll in ein anderes umwandelt) kann sowohl in einer als auch in mehreren Schichten aktiv sein. Ein Beispiel für ein Gateway ist ein Computer in einem LAN, der den Anschluss des Netzwerks an einen IBM-Mainframecomputer oder ein netzwerkweites Faxsystem ermöglicht. Bei beiden Beispielen müssten die Daten den gesamten OSI-Stapel durchwandern, um in das Datenformat des Empfängergeräts – Mainframe bzw. Faxgerät – konvertiert zu werden.

3.11.7 Paketfluss durch Wolken

Wolken können verschiedene Arten von Elementen enthalten, z. B. Netzwerkkarten, Bridges, Router, Gateways und andere Netzwerkgeräte. Da eine Wolke eigentlich kein einzelnes Gerät darstellt, sondern eine ganze Gruppe verschiedener Geräte, die auf allen Ebenen des OSI-Modells aktiv sind, kann auch sie als ein Gerät der Schichten 1 bis 7 betrachtet werden.

Sie können den Pfad der Daten zum Ziel prüfen, indem Sie den Befehl `ping` verwenden. Dieser Befehl sendet kurze IP-Pakete an das im Befehl spezifizierte Gerät. Wenn dieses Gerät korrekt konfiguriert ist, antwortet es. Wenn Sie also eine Antwort be-

kommen, dann wissen Sie, dass das Gerät irgendwo existiert und auch aktiv ist. Erhalten Sie keine Antwort, dann können Sie davon ausgehen, dass irgendwo zwischen Ihrem Host und dem Zielgerät ein Problem aufgetreten ist.

3.12 Wie man ein einfaches Netzwerk aufbaut

Sie sollten nicht gleich mit dem Aufbau eines komplexen LAN beginnen, sondern erst einmal eine einfache Variante entwickeln. Das nachfolgend vorgestellte Netzwerk zeigt bereits, vor welchen Aufgaben Sie stehen werden, wenn Sie einmal ein größeres Netzwerk entwickeln müssen. Hier einige Übungsaufgaben, die Sie lösen sollten, bevor Sie mit der Planung richtig anfangen:

- Stellen Sie fest, wie Sie die MAC-Adressen (physikalische Adressen, Ethernet-Adressen) und die IP-Adressen der auf Ihrem Computer installierten Netzwerkadapter ermitteln können.
- Wie können Sie diese Einstellungen ändern? Beschreiben Sie, wo Sie diese Änderungen vornehmen können und welche Änderungen Sie überhaupt vornehmen können.
- Zeichnen Sie die Symbole der grundlegenden Netzwerkgeräte (Repeater, Hubs, Bridges, Switches, PCs, Server und Wolken) aus dem Gedächtnis heraus auf.
- Zeichnen Sie mit zehn Knotenpunkten sechs verschiedene Topologien auf (denken Sie dabei an Abbildungen in diesem Kapitel) und beschreiben Sie die Vor- und Nachteile der verschiedenen Topologien.
- Zeichnen Sie Diagramme der folgenden Netzwerke: Verbindung zweier PCs, Verbindung von vier PCs mit einem Hub, Verbindung von vier PCs mit einem Switch, Netzwerk mit zwei Gruppen mit je vier PCs, die jeweils an einen Router angeschlossen sind.
- Zeichnen Sie einen Hub auf und beschriften Sie alle Anzeigen und Anschlüsse.
- Skizzieren Sie ein Straight-Through-Kabel (CAT5 UTP). Beschriften Sie die Farbkodierungen an den Steckern an beiden Enden des Kabels.
- Skizzieren Sie eine Verbindungsleitung (CAT5 UTP). Beschriften Sie die Farbkodierungen an den Steckern an beiden Enden des Kabels.
- Erläutern Sie alle Anschlüsse und Anzeigen einer installierten Netzwerkkarte.

Wir wollen zunächst eine einfache Arbeitsgruppe erstellen. Verbinden Sie also erst einmal, wie in Abbildung 3.17 gezeigt, zwei PCs miteinander.

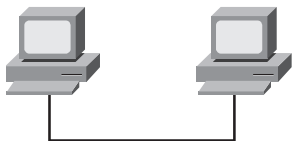

Abbildung 3.17: Ein einfaches, aus zwei Knoten bestehendes Netzwerk.