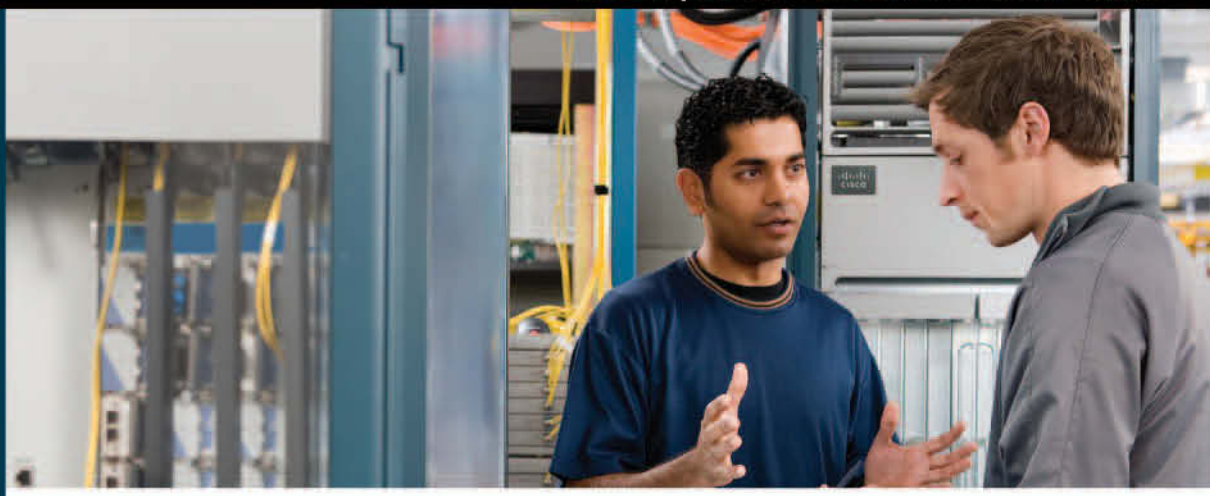
Wendell Odom, CCIE™ Nr. 1624

CCENT/CCNA-PRÜFUNGSHANDBUCH



CCENT/CCNA ICND1 Prüfungshandbuch

Die offizielle Vorbereitung für die Examen
Nr. 640-822 und 640-802
2. Auflage

Testsimulation,
Video-Training

ADDISON-WESLEY ciscopress.com

Kapitel 2

Netzwerkmodelle TCP/IP und OSI

Der Ausdruck *Netzwerkmodell* bzw. *Netzwerkarchitektur* bezieht sich auf eine Reihe von Dokumenten. Jedes dieser Dokumente beschreibt jeweils nur einen kleinen Bereich der Aufgaben, die für ein Netzwerk benötigt werden. Diese Dokumente können zum Beispiel ein Protokoll definieren. Darunter versteht man einen Satz logischer Regeln, die von den beteiligten Geräten bei der Kommunikation befolgt werden müssen. Sie können auch physische Bedingungen für ein Netzwerk festlegen, wie zum Beispiel Spannung- und Strompegel eines bestimmten Kabels. Insgesamt legen die Dokumente eines Netzwerkmodells alle Einzelheiten für die Inbetriebnahme eines funktionierenden Netzwerks fest.

Um ein funktionierendes Netzwerk aufzubauen, müssen alle beteiligten Geräte den Kennwerten entsprechen, die durch ein bestimmtes Netzwerkmodell vorgegeben sind. Nur wenn alle Computer und alle anderen Netzwerkgeräte diese Protokolle, die physischen Spezifikationen sowie Regeln einhalten, und die Geräte korrekt verbunden und konfiguriert sind, können die Computer erfolgreich miteinander kommunizieren.

Stellen Sie sich ein Netzwerkmodell wie den Entwurf eines Architekten zum Bau eines Hauses vor. Sicher können Sie ein Haus auch ohne den Plan eines Architekten bauen, aber es geht einfacher, wenn Sie sich an diesen Plan halten. Weil wahrscheinlich viele verschiedene Handwerker wie Tischler, Elektriker, Maurer oder Maler beim Bau Ihres Hauses mitwirken, ist es hilfreich, wenn alle den gleichen Plan benutzen. Ganz ähnlich könnten Sie Ihr eigenes Netzwerk bauen, Ihre eigene Software schreiben, Ihre eigenen Netzwerkkarten herstellen und so ein Netzwerk erstellen, ohne ein vorhandenes Netzwerkmodell zu verwenden. Allerdings ist es viel leichter, einfach Komponenten zu kaufen und zu verwenden, die bereits einem eingeführten Netzwerkmodell entsprechen. Da die Hersteller von Netzwerkprodukten seit vielen Jahren das gleiche Netzwerkmodell benutzen, werden ihre Komponenten optimal zusammenarbeiten.

Die CCNA-Prüfungen beziehen sich detailliert auf ein Netzwerkmodell – das Transmission Control Protocol/Internet Protocol oder kurz TCP/IP.

TCP/IP ist historisch gewachsen und inzwischen das Netzwerkmodell mit der weitesten Verbreitung. Praktisch jedes heute vorhandene Computer-Betriebssystem unterstützt TCP/IP, vom Mobiltelefon bis zum Supercomputer. Ebenso fast jedes Netzwerk, das unter Verwendung von Cisco-Produkten hergestellt wurde. Kein Wunder also, dass die CCNA-Prüfungen sich besonders auf das Thema TCP/IP konzentrieren.

Die ICND1-Prüfung, wie auch in geringerem Umfang die ICND2-Prüfung, bezieht sich außerdem auf ein zweites Netzwerkmodell, das OSI-Referenzmodell. Historisch betrachtet war OSI der erste ernsthafte Versuch, ein herstellerneutrales Netzwerkmodell zu schaffen, das für eine Benutzung durch jedermann und auf allen Computern der Welt vorgesehen war. Wegen dieser historischen Bedeutung des OSI-Modells sind viele der heute bei der Beschreibung eines Netzwerks verwendeten Fachausdrücke aus dem OSI-Modell abgeleitet.

2.1 Überprüfen Sie Ihren Wissensstand

Dieser Test ermöglicht Ihnen einzuschätzen, ob Sie das gesamte Kapitel lesen sollten. Wenn Sie nicht mehr als eine der acht Fragen falsch beantworten, können Sie zu Abschnitt 2.3, »Prüfungsvorbereitung«, vorblättern. Tabelle 2.1 listet die Hauptüberschriften des Kapitels und die Nummern der dazugehörigen Fragen auf, sodass Sie Ihr Wissen auf diesen Gebieten einschätzen können. Die Antworten finden Sie in Anhang A.

Tabelle 2.1: Zuordnung von Wissensgrundlagen-Abschnitten zu Fragen

Abschnitt	Fragen
Die Architektur von TCP/IP	1 bis 6
Das OSI-Referenzmodell	7 bis 10

1. Welche der folgenden Protokolle sind Beispiele für TCP/IP-Transportschicht-Protokolle (TCP/IP transport layer)?

   a) Ethernet

   b) HTTP

   c) IP

   d) UDP

   e) SMTP

   f) TCP

2. Welche der folgenden Protokolle sind Beispiele für TCP/IP- Netzwerkzugangssschicht-Protokolle (TCP/IP network access layer)?

   a) Ethernet

   b) HTTP

   c) IP

   d) UDP

   e) SMTP

   f) TCP

   g) PPP

3. Wozu dient der HTTP-Prozess, bei dem TCP Daten anfordert und sich dabei von deren korrektem Empfang überzeugt?

   a) Interaktion auf der gleichen Schicht

   b) Interaktion auf einer benachbarten Schicht

   c) Das OSI-Modell

   d) Alle Antworten treffen zu.

4. Wozu dient der Prozess, bei dem TCP auf einem Computer ein Segment als Segment 1 markiert und der Empfangscomputer dann den Empfang von Segment 1 bestätigt?

   a) Datenkapselung

   b) Interaktion auf der gleichen Schicht

   c) Interaktion auf einer benachbarten Schicht

   d) Das OSI-Modell

   e) Keine dieser Antworten trifft zu.

5. Wozu dient der Prozess, bei dem ein Webserver einer Webseite einen TCP-Header hinzufügt, dann einen IP-Header und schließlich einen Sicherungsschicht-Header und einen -Trailer?

   a) Datenkapselung

   b) Interaktion auf der gleichen Schicht

   c) Das OSI-Modell

   d) Jede dieser Antworten trifft zu.

6. Welcher der folgenden Ausdrücke wird speziell zur Kennzeichnung des Objekts verwendet, das bei der Kapselung von Daten auf Schicht 2 zwischen Sicherungsschicht-Headern und -Trailern entsteht?
   a) Daten
   b) Block
   c) Segment
   d) Frame
   e) Datenpaket
   f) Keiner dieser Begriffe. Auf der Sicherungsschicht gibt es keine Kapselung.
7. Welche OSI-Schicht legt die Funktionen für die netzwerkweite logische Adressierung und das Routing fest?
   a) Schicht 1
   b) Schicht 2
   c) Schicht 3
   d) Schicht 4
   e) Schicht 5
   f) Schicht 6
   g) Schicht 7
8. Welche OSI-Schicht legt die Normen für Verkabelung und Stecker fest?
   a) Schicht 1
   b) Schicht 2
   c) Schicht 3
   d) Schicht 4
   e) Schicht 5
   f) Schicht 6
   g) Schicht 7

9. Welche OSI-Schicht legt die Normen für Datenformate und Verschlüsselung fest?
   a) Schicht 1
   b) Schicht 2
   c) Schicht 3
   d) Schicht 4
   e) Schicht 5
   f) Schicht 6
   g) Schicht 7
10. Welche der folgenden Ausdrücke sind als Namen für die sieben OSI-Schichten nicht zulässig?
   a) Anwendung
   b) Sicherung
   c) Übertragung
   d) Darstellung
   e) Internet
   f) Sitzung

2.2 Grundlagen

Es ist heute fast unmöglich, einen Computer zu finden, der das Netzwerkprotokoll TCP/IP nicht beherrscht. In jedem Microsoft-, Linux- oder UNIX-Betriebssystem ist TCP/IP vorhanden. Ebenso in Palmtops und Handys. Da Cisco die Geräte zur Herstellung eben jener Infrastruktur verkauft, mit deren Hilfe diese Computern unter Verwendung von TCP/IP kommunizieren, verfügen natürlich auch die Cisco-Komponenten über weitreichende TCP/IP- Unterstützung.

Die (Netzwerk-)Welt war nicht immer so. Zu der Zeit, als es keine noch Netzwerkprotokolle und kein TCP/IP gab, entwickelten einige Firmen ihre ersten eigenen Netzwerkprotokolle. Diese Protokolle arbeiteten nur auf den Computern des jeweiligen Herstellers, und die technischen Details wurden oft nicht veröffentlicht. Später dann formalisierten und veröffentlichten die Hersteller ihre Netzwerkprotokolle, was die anderen Hersteller in die Lage versetzte, Geräte zu bauen, um mit diesen Computern zu kommunizieren. So veröffentlichte zum Beispiel IBM im Jahr 1974 sein SNA-Netzwerkmodell.

Danach bauten andere Computerhersteller Geräte, die mit IBM-Rechnern unter Verwendung von SNA kommunizieren konnten. Zu den Nachteilen dieser Lösung zählte, dass die größeren Computerhersteller versuchten, den Netzwerkmarkt zu beherrschen.

Eine bessere Lösung bestand in der Bildung eines offenen, standardisierten Netzwerkmodells, das von alle Herstellern akzeptiert wird. Die International Organization for Standardization (ISO) nahm diese Aufgabe in den späten 1970er Jahren in Angriff. Sie begann damals mit der Arbeit an dem, was später als OSI-Netzwerkmodell bekannt werden sollte. ISO hatte ein »vornehmes« Ziel für das OSI-Modell: Netzwerkprotokolle so zu standardisieren, dass eine Zusammenarbeit zwischen allen Computern der Welt möglich wird. Zusammen mit Teilnehmern aus fast allen Industrieländern der Erde, die sich an diesem Projekt beteiligten, arbeitete die ISO auf dieses ehrgeizige Ziel hin.

Ein zweiter, weniger formaler Versuch zur Schaffung eines öffentlichen Standard-Netzwerkmodells entsprang einem Projekt des US-Verteidigungsministeriums. Wissenschaftler verschiedener Universitäten boten sich freiwillig an, bei der Weiterentwicklung der Protokolle zu helfen. Diese Bemühungen führten zu einem konkurrierenden Netzwerkmodell, nämlich TCP/IP.

Am Ende der 1980er Jahre existierten viele konkurrierende, herstellerspezifische sowie zwei standardisierte Netzwerkmodelle, die miteinander im Wettbewerb standen. Schließlich siegte TCP/IP. Herstellerspezifische Protokolle werden zwar heute auch noch in einigen Netzwerken verwendet, jedoch viel seltener als in den 1980er und 1990er Jahren. Das OSI-Modell, dessen Entwicklung auch an einem im Vergleich zu TCP/IP langsameren Fortschritt der Standardisierung krankte, setzte sich am Markt nicht durch. So wurde das fast völlig von einer Hand voll freiwilliger Enthusiasten entwickelte Netzwerkmodell TCP/IP die produktivste Familie von Netzwerkprotokollen.

In diesem Kapitel erfahren Sie etwas über die Grundlagen von TCP/IP. Sie werden dabei einige interessante Dinge über TCP/IP lernen. Doch das eigentliche Ziel dieses Kapitels ist es, ein Verständnis zu vermitteln, was Netzwerkmodelle und Netzwerkarchitekturen sind und wie sie arbeiten.

Außerdem lernen Sie in diesem Kapitel einiges über die bei OSI verwendete Fachterminologie. Wahrscheinlich wird niemand unter Ihnen jemals mit einem Computer arbeiten, der das komplette OSI-Protokoll anstelle von TCP/IP verwendet. Aber dennoch werden Sie oft Fachausdrücke verwenden, die sich auf OSI beziehen. Auch die ICND1-Prüfung beinhaltet OSI-Grundlagen, weshalb Sie in diesem Kapitel auch auf Prüfungsfragen zu OSI vorbereitet werden.

2.2.1 Die Architektur von TCP/IP

TCP/IP definiert eine umfangreiche Sammlung von Protokollen, die Computern die Kommunikation untereinander erlauben. Dabei werden die Einzelheiten dieser Protokolle in Dokumenten niedergelegt, die Request for Comment (RFC) genannt werden. Nach Implementierung der erforderlichen, in TCP/IP-RFCs festgelegten Protokolle kann ein Computer verhältnismäßig leicht mit anderen Computern kommunizieren, auf denen ebenfalls TCP/IP vorhanden ist.

Man kann Telefone mit Computern vergleichen, die TCP/IP verwenden. Sie gehen in ein Geschäft und kaufen ein Telefon von einem der vielen verschiedenen Hersteller. Wenn Sie zu Hause das Telefon an das gleiche Kabel anschließen, an dem auch Ihr altes Telefon angeschlossen war, so wird auch das neue Telefon funktionieren. Der Telefon-Hersteller kennt die Normen Ihres Landes und konstruiert bzw. konfiguriert seine Telefone so, dass diesen den Normen entsprechen. In ähnlicher Weise kann ein Computer, der mit den von TCP/IP genormten Netzwerkprotokollen arbeitet, mit anderen Computern, die diese Normen ebenfalls verwenden, kommunizieren.

Ebenso wie andere Netzwerkarchitekturen klassifiziert TCP/IP die verschiedenen Protokolle nach unterschiedlichen Kategorien bzw. Schichten. Tabelle 2.2 stellt die Schichten des TCP/IP-Architekturmodells dar.

Tabelle 2.2: TCP/IP-Architekturmodell und Beispiele für Protokolle

TCP/IP-Architekturschicht	Beispiele für Protokolle
Anwendung	HTTP, POP3, SMTP
Transport	TCP, UDP
Internet	IP
Netzwerkzugang	Ethernet, Frame Relay

Die erste Spalte der Tabelle führt die vier TCP/IP-Schichten auf, während die zweite Spalte die dazugehörigen und am weitesten verbreiteten TCP/IP-Protokolle zeigt Die von einer neuen Anwendung unmittelbar verwendeten Protokolle werden als Anwendungsschichtprotokolle bezeichnet. So wurde zum Beispiel bei der Gründung des World Wide Web (WWW) ein neues Anwendungsschichtprotokoll geschaffen, um Webseiten anzufordern und deren Inhalt einzulesen. Ähnlich umfasst die Netzwerkzugangsssschicht Protokolle und Normen wie beispielsweise Ethernet. Bei einem neuen LAN-Typ gelten die zugehörigen Protokolle als Teil der Netzwerkzugangsssschicht. In den nächsten Abschnitten erfahren Sie Grundlegendes über jede dieser vier Schichten der TCP/IP-Architektur und ihr Zusammenwirken.

Die Anwendungsschicht von TCP/IP

Die TCP/IP-Protokolle der Anwendungsschicht stellen Dienste für die Anwendungssoftware bereit, die aktuell auf einem Computer ausgeführt wird. Die Anwendungsschicht legt nicht die eigentliche Anwendung fest, sondern vielmehr die Dienste, die von Anwendungen benötigt werden – beispielsweise bei HTTP die Fähigkeit, eine Datei zu übertragen. Die Anwendungsschicht stellt eine Schnittstelle zwischen der auf einem Computer ausgeführten Software und dem eigentlichen Netzwerk dar.

Die heutzutage am häufigsten genutzte TCP/IP-Anwendung ist der Webbrowser. Viele große Softwarehersteller änderten bereits ihre Software, um die Bedienung ihrer Software über einen Webbrowser zu ermöglichen. Mit jedem Betriebssystem ist es heute möglich, einen Webbrowser zu benutzen. Sie starten ihn auf Ihrem Computer, wählen eine Webseite aus, indem Sie deren Namen eingeben, und die Seite erscheint.

Wodurch wird es nun möglich, dass die Webseite in Ihrem Webbrowser erscheint?

Nehmen Sie an, Bob öffnet seinen Browser. Dieser ist so konfiguriert, dass er automatisch nach der Standardwebseite von Larrys Webserver, seiner *Homepage*, sucht. Den logischen Zusammenhang zeigt Abbildung 2.1.

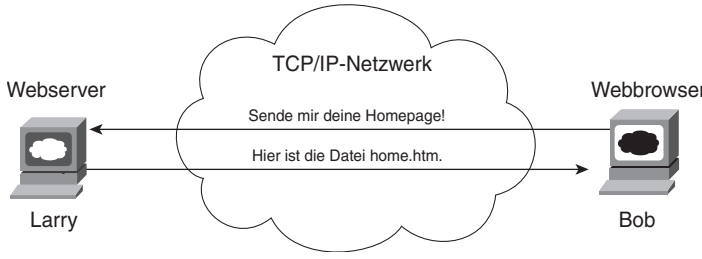


Abbildung 2.1: Anwendung zum Aufruf einer Webseite

Was ist geschehen? Bobs Anforderung ersucht Larrys Server, dessen Homepage an Bob zu senden. Larrys Webserversoftware weiß, dass die Standardwebseite in der Datei namens *home.htm* enthalten ist. Bob erhält die Datei von Larry, ihr Inhalt wird im Fenster des Webbrowsers dargestellt.

Dieses Beispiel benutzt zweimal das TCP/IP-Anwendungsschichtprotokoll. Zunächst werden die Anforderung und die tatsächliche Übertragung der Datei entsprechend dem Hypertext-Transfer-Protocol (HTTP) durchgeführt. Viele von Ihnen haben wahrscheinlich bemerkt, dass die URLs – Universal Resource Locators (häufig als Webadressen bezeichnet) – der meisten

Webseiten mit den Buchstaben »http« beginnen, womit vorausgesetzt wird, dass HTTP für die Übertragung der Webseiten verwendet wird.

Das andere verwendete Protokoll ist die Hypertext Markup Language (HTML). Dies ist eine der Spezifikationen, die bestimmen, wie Bobs Browser mit dem Text der soeben erhaltenen Datei umzugehen hat. Beispielsweise kann die Datei Anweisungen dafür enthalten, einen Text in einer bestimmten Größe oder Farbe darzustellen. Meist gibt es hier auch noch Hinweise auf andere Dateien, die an Bobs Browser zu schicken sind, zum Beispiel Bilder und Animationsdateien. HTTP dient dann dazu, diese zusätzlichen Dateien von Larrys Webserver anzufordern.

Ein genauerer Blick darauf, wie Bobs und Larrys Computer in diesem Beispiel zusammenarbeiten, zeigt einige Einzelheiten über die Funktionsweise von Netzwerkprotokollen. Betrachten Sie Abbildung 2.2 als Ergänzung zu Abbildung 2.1 mit der Darstellung von HTTP-Header und Daten.

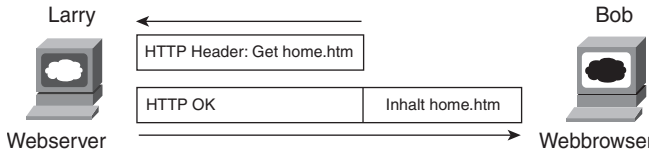


Abbildung 2.2: HTTP-Get-Anweisung und HTTP-Antwort

Um die Webseite von Larry zu erhalten, sendet Bob einen sogenannten HTTP-Header an Larry. Dieser Header enthält den Befehl, eine Datei zu holen (get). Normalerweise enthält die Anforderung den Namen der Datei (hier *home.htm*), oder der Webserver geht davon aus, dass Bob die Standardwebseite angefordert hat.

Larrys Antwort enthält ebenfalls einen HTTP-Header, wobei er einfach OK zurückgibt. Tatsächlich enthält der Header einen HTTP-Rückgabecode, der anzeigt, ob die Anfrage bedient werden kann. Wenn Sie zum Beispiel nach einer nicht aufzufindenden Webseite gesucht haben, erhalten Sie die HTTP-Fehlermeldung »nicht gefunden«. Ihr Rückgabecode lautet 404. Wenn die angeforderte Seite dagegen gefunden wurde, lautet der Rückgabecode 200, was bedeutet, dass die Anforderung ausgeführt wird.

Dieses einfache Beispiel von Bob und Larry stellt eines der wichtigsten Prinzipien dar, die hinter Netzwerkmodellen stehen: Wenn eine Schicht eines Computers mit der entsprechenden Schicht auf einem anderen Computer kommunizieren möchte, so benutzen beide Computer Header mit derjenigen Information, die sie übertragen wollen. Die Header sind ein Teil von dem, was zwischen den beiden Computern übertragen wird. Dieser Vorgang heißt *Interaktion auf derselben Schicht*.

Das Protokoll der Anwendungsschicht (im vorliegenden Fall HTTP) bei Bob kommuniziert mit Larrys Anwendungsschicht. Das geschieht, indem jeweils einer für den anderen einen Header der Anwendungsschicht erzeugt und überträgt, manchmal gefolgt von Anwendungsdaten (siehe Abbildung 2.2). Ungeachtet des gerade verwendeten Protokolls dient dieses Vorgehen der Verständigung mit der Anwendungsschicht des anderen Computers.

Die Protokolle der TCP/IP-Anwendungsschicht stellen Dienste für die Anwendungssoftware bereit, die auf einem Computer ausgeführt wird. Die Anwendungsschicht legt dabei nicht die eigentliche Anwendung fest, sondern lediglich die Dienste, die von den Anwendungen benötigt werden. Beispielsweise bei HTTP die Fähigkeit, eine Datei zu übertragen. Kurz gesagt stellt die Anwendungsschicht eine Schnittstelle zwischen der auf einem Computer ausgeführten Software und dem eigentlichen Netzwerk bereit.

Die Transportschicht von TCP/IP

HTTP ist nur eines von vielen Protokollen, die in der TCP/IP-Anwendungsschicht aktiv sind. Die TCP/IP-Transportschicht dagegen besteht aus zwei Protokollen: dem Transmission Control Protocol (TCP) und dem User Datagram Protocol (UDP). Um wirklich einschätzen zu können, was die TCP/IP-Transportschichtprotokolle leisten, sollten Sie Kapitel 6, »Grundlagen zu TCP/IP-Transport, -Anwendungen und -Sicherheit«, lesen. Jedoch werden Sie schon in diesem Abschnitt eine wichtige Eigenschaft von TCP kennenlernen.

Um einzuschätzen, was die Transportschichtprotokolle leisten, müssen Sie die darüberliegende Schicht, die Anwendungsschicht betrachten. Wieso? Nun, jede Schicht stellt einen Dienst für die darüberliegende Schicht bereit. Beispielsweise wurde in Abbildung 2.2 HTTP für die Übertragung der Homepage von Larry zu Bob verwendet Aber was wäre passiert, wenn Bobs HTTP-Get-Anweisung unterwegs im TCP/IP-Netzwerk verschwunden wäre? Oder wenn Larrys Antwort mit den Inhalten der Homepage verlorengegangen wäre? Wie zu erwarten ist, wäre die Seite in jedem Fall nicht in Bobs Browser erschienen.

Also benötigt TCP/IP einen Mechanismus, der die Datenübertragung über ein Netzwerk sicherstellt. Weil viele Anwendungsschichtprotokolle einen solchen Mechanismus brauchen, stellt TCP für die Anwendungsprotokolle eine Fehlerkorrekturfunktion unter Verwendung von Rückmeldungen bereit. Abbildung 2.3 zeigt das zugrunde liegende Verfahren, das mit Bestätigungen (Acknowledgments) arbeitet.

ANMERKUNG

Die Dateneinheiten in Abbildung 2.3, die den Transportschicht-Header und seine eingekapselten Daten umfassen, werden als *Segment* bezeichnet.

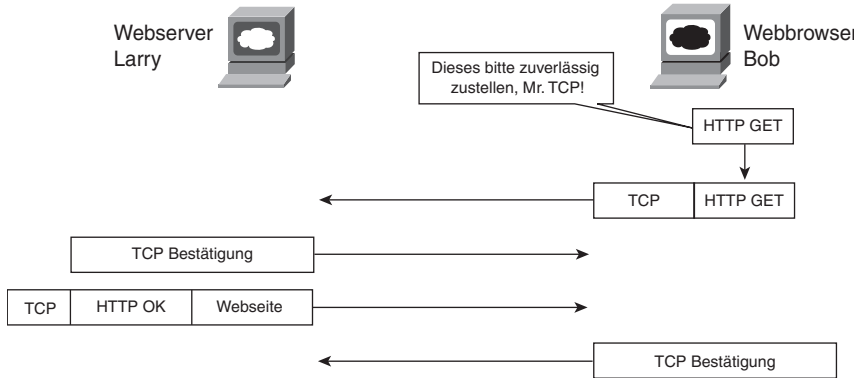


Abbildung 2.3: TCP-Dienste für HTTP

Wie Abbildung 2.3 zeigt, wird TCP von der HTTP-Software aufgefordert, die GET-Anforderung zuverlässig zuzustellen. TCP schickt die HTTP-Daten von Bob zu Larry, wo sie erfolgreich eintreffen. Larrys TCP-Software bestätigt den Erhalt der Daten und übergibt die HTTP-GET-Anforderung an die Software des Webservers. Das Umgekehrte geschieht mit Larrys Antwort, die – ebenfalls erfolgreich – bei Bob eintrifft.

Natürlich bemerkt man die TCP-Fehlerkorrektur nicht, wenn keine Daten verlorengehen. Kapitel 6 zeigt an einem Beispiel, wie TCP verlorengegangene Daten korrigiert. HTTP selbst wird nicht direkt tätig, wenn eine der Übermittlungen in Abbildung 2.3 verlorengeht. Stattdessen sendet TCP diese Daten nochmals und stellt ihren Empfang sicher. Die in diesem Beispiel demonstrierte Funktion wird als Interaktion benachbarter Schichten bezeichnet. Sie legt fest, nach welchen Plänen benachbarte Schichten eines Netzwerkmodells auf demselben Rechner zusammenarbeiten. Das Protokoll der höheren Schicht (HTTP) muss etwas leisten, wozu es nicht in der Lage ist (die Fehlerkorrektur). Also fordert die höhere Schicht bei dem Protokoll der darunterliegenden Schicht (TCP) diesen Dienst an. Die niedrigere Schicht führt ihn anschließend aus. Die niedrigere Schicht stellt also einen Dienst für die Schicht darüber bereit. Tabelle 2.3 fasst die wesentlichen Punkte, wie benachbarte Schichten auf einem einzelnen Rechner mit der entsprechenden Netzwerkschicht eines anderen Rechners zusammenarbeiten, zusammen.

Wichtig!

Tabelle 2.3: Interaktionen gleicher oder benachbarter Schichten

Begriff	Beschreibung
Interaktion in derselben Schicht auf verschiedenen Rechnern	Beide Rechner nutzen ein Protokoll zur Kommunikation mit der gleichen Schicht auf dem anderen Computer. Das von jeder Schicht festgelegte Protokoll benutzt einen zwischen den Rechnern übertragenen Header, um mitzuteilen, was jeder Computer zu tun beabsichtigt.
Nachbarschicht-Interaktion auf demselben Rechner	Auf einem einzelnen Rechner stellt eine Schicht einen Dienst für eine höhere Schicht bereit. Die Soft- oder Hardware, welche die höhere Schicht bildet, fordert die nächstniedrigere Schicht auf, die benötigte Funktion auszuführen.

Die Einzelheiten des physischen Netzwerks wurden in diesen Beispielen zur Beschreibung von Anwendungs- und Transportschicht nicht dargestellt. Die Anwendungs- und Transportschicht arbeiten unabhängig davon, ob sich die Endgeräte im selben LAN befinden oder durch das Internet getrennt sind. Die beiden darunter liegenden Schichten von TCP/IP, die Internet- und die Netzwerkzugangsschicht, müssen über das zugrunde liegende physische Netzwerk informiert sein, da sie die zum Datentransport verwendeten Protokolle festlegen.

Die Internetschicht von TCP/IP

Nehmen Sie an, Sie haben gerade einen Brief an einen Bekannten am anderen Ende des Landes geschrieben, und außerdem einen Brief an einen Freund am anderen Ende der Stadt. Beide sollen abgeschickt werden. Gibt es einen Unterschied, wie Sie beide Briefe behandeln? Natürlich nicht. Sie schreiben auf jeden Umschlag eine Adresse, weil beide Briefe an verschiedene Orte gelangen sollen. Sie versehen beide Briefe mit Briefmarken und werfen sie in den gleichen Briefkasten. Die Post kümmert sich dann darum, wie jeder Brief an den richtigen Zielort gelangt. Das geschieht unabhängig davon, ob der Transport nur durch die Stadt oder quer durch das Land erfolgt.

Wenn die Post den Überlandbrief bearbeitet, sendet sie ihn zu einem anderen Postamt, dann zu einem weiteren usw., bis der Brief am anderen Ende des Landes ausgeliefert wird. Der Ortsbrief geht zum Postamt in Ihrer Stadt, und wird dann direkt Ihrem Freund zugestellt, ohne dass vorher ein anderes Postamt beteiligt ist.

Was hat das mit dem Netzwerkbetrieb zu tun? Nun, die Internetschicht des TCP/IP-Netzwerkmodells, die sich durch das Internetprotokoll (IP) definiert, arbeitet fast so wie der Postdienst. IP bestimmt Adressen so, dass jeder Hostcomputer eine eigene, eindeutige IP-Adresse hat. Genauso legt die Post die Adressierung der Briefe so fest, dass eindeutige Anschriften für Häuser, Wohnungen und Geschäfte vorhanden sind. Ähnlich wird der Weiterlei-

tungsvorgang von IP so organisiert, dass ein sogenannter Router auswählt, wie die Datenpakete gesendet werden müssen, damit sie am richtigen Bestimmungsort ankommen. Genauso wie die Post die notwendige Infrastruktur geschaffen hat, um die Zustellung von Briefen zu ermöglichen – Postämter, Sortiermaschinen, Lastwagen, Flugzeuge und Personal –, definiert die Internetschicht, wie die Einzelheiten einer Netzwerkinfrastruktur beschaffen sein müssen, damit das Netzwerk Daten übertragen kann.

Kapitel 5, »Grundlagen von IP-Adressierung und Routing«, beschreibt die Internetschicht von TCP/IP genauer, wobei weitere Details in diesem Buch und im *CCNA ICND2-Prüfungshandbuch* besprochen werden. Zum besseren Verständnis der Grundlagen der Internetschicht betrachten Sie Bobs Anforderung von Larrys Homepage in Abbildung 2.4, jetzt aber mit Ihren Kenntnissen über IP. Die Details der LAN-Verkabelung sind für diese Abbildung unwichtig, daher werden beide LANs einfach schematisch als Linien dargestellt. Wenn Bob Daten sendet, übermittelt er ein IP-Paket, das aus dem IP-Header, dem Transportschicht-Header (in diesem Fall: TCP), dem Anwendungs-Header (hier HTTP) und verschiedenen Anwendungsdaten (im vorliegenden Fall: keine) besteht. Der IP-Header enthält sowohl ein Adressfeld mit Larrys IP-Adresse (1.1.1.1) als Empfängeradresse als auch Bobs IP-Adresse (2.2.2.2) als Absenderadresse.

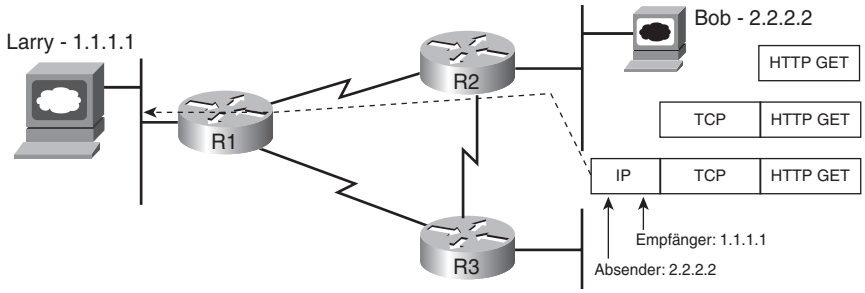


Abbildung 2.4: IP-Dienste für TCP

Anmerkung

Die Dateneinheit ganz unten in Abbildung 2.4, die aus dem Internetschicht-Header und seinen eingekapselten Daten besteht, wird als *Paket* bezeichnet.

Bob schickt das Paket an Router R2. R2 prüft dann die IP-Zieladresse (1.1.1.1) und entscheidet, das Paket an R1 weiterzuleiten. Dazu ist er in der Lage, weil er genügend Informationen über die Netzwerktopologie hat, um zu wissen, dass sich 1.1.1.1 (Larry) auf der anderen Seite von R1 befindet.

Entsprechend leitet R1 das Paket, wenn er es erhält, über das Ethernet-Netzwerk an Larry weiter. Wenn die Verbindung zwischen R2 und R1 gestört ist, informiert IP den Router R2 über den alternativen Weg durch R3, um 1.1.1.1. zu erreichen.

IP definiert logische Adressen, sogenannte *IP-Adressen*. Jedes mit TCP/IP arbeitende Gerät (IP-Host genannt) benötigt eine IP-Adresse, damit über IP kommuniziert werden kann. IP steuert auch das Routing. Das ist der Prozess, nach dem ein Router Datenpakete weiterzuleiten hat.

Alle CCNA-Prüfungen befassen sich ziemlich gründlich mit IP. Für die ICND1-Prüfung enthält Kapitel 5 dieses Buches die wesentlichen Zusammenhänge, während die Kapitel 11 bis 15 IP sehr viel detaillierter beschreiben.

Die Netzwerkzugangsschicht von TCP/IP

Die Netzwerkzugangsssschicht definiert die notwendigen Protokolle und die erforderliche Hardware, um Daten über ein physisches Netzwerk hinweg zu übermitteln. Der Ausdruck *Netzwerkzugangsschicht* bezieht sich darauf, dass diese Schicht die Art und Weise festlegt, wie ein Rechner physisch mit dem Medium zu verbinden ist, damit die Daten übermittelt werden können. Ethernet ist zum Beispiel ein solches Protokoll aus der TCP/IP-Netzwerkzugangsschicht. Es definiert Verkabelung, Adressierung und benötigte Protokolle zur Herstellung eines Ethernet-LAN. Stecker, Kabel, Spannungspegel und Protokolle von WAN-Verbindungen fallen mit einer Vielzahl von anderen Protokollen ebenfalls unter den Begriff der Netzwerkzugangsssschicht. Die Kapitel 3 und 4 behandeln die Grundlagen von LAN bzw.WAN.

So wie jede Schicht eines Netzwerkmodells stellt auch die Netzwerkzugangsschicht von TCP/IP Dienste für die darüberliegende Schicht bereit. Am besten versteht man die Funktion der Netzwerkzugangsschicht von TCP/IP, indem man die Dienste genauer betrachtet, die sie für IP bereitstellt. IP ist auf die Netzwerkzugangsschicht angewiesen, um IP-Pakete über ein physisches Netzwerk zu transportieren. IP kennt die Netzwerktopologie, weiß wie beispielsweise die Router untereinander verbunden sind, wie Hostrechner mit dem physischen Netzwerk verbunden sind und wie das IP-Adressierungsverfahren aussieht. Jedoch enthält das IP-Protokoll absichtlich keine Einzelheiten über die einzelnen zugrunde liegenden physischen Netzwerke. Daher benutzt die Internetschicht von IP die Dienste der Netzwerkzugangsschicht, um die Pakete über die entsprechenden einzelnen physischen Netzwerke zu transportieren.

Zur Netzwerkzugangsschicht gehört eine große Anzahl von Protokollen. Zum Beispiel umfasst sie alle Varianten von Ethernet-Protokollen sowie die

anderen LAN-Standards. Zu dieser Schicht gehören auch die verbreiteten WAN-Standards, wie etwa das Point-to-Point Protocol (PPP) oder Frame Relay. In Abbildung 2.5 sehen Sie das schon bekannte Netzwerk, wobei Ethernet und PPP als die beiden Protokolle der Netzwerkzugangsschicht genutzt werden.

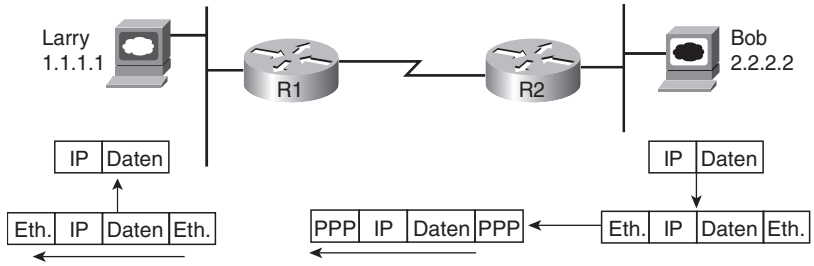


Abbildung 2.5: Ethernet- und PPP-Dienst für IP

Wichtig!

ANMERKUNG

Die in Abbildung 2.5 dargestellten Dateneinheiten – die Ethernet-Header/-Trailer und PPP-Header/-Trailer enthalten –, werden als *Frames* bezeichnet.

Um Abbildung 2.5 richtig einzuschätzen, denken Sie zuerst etwas genauer darüber nach, wie IP sein Ziel erreicht, das Paket von Bob zu Larry zu transportieren. Um ein Paket zu Larry zu senden, sendet Bob das IP-Paket an den Router R2. Dies geschieht mittels Ethernet, weshalb die Ethernet-Regeln einzuhalten und das IP-Paket (IP-Header und Daten) zwischen je einen Ethernet-Header und -Trailer zu setzen ist.

Weil der IP-Routing-Prozess zum Ziel hat, das IP-Paket (IP-Header und Daten) an den Zielrechner zu übergeben, benötigt R2 den von Bob erhaltenen Ethernet-Header und -Trailer nicht mehr. Daher entfernt er sie, wobei das originale IP-Paket übrigbleibt. Um dieses an R1 zu schicken, setzt R2 einen PPP-Header voran und einen PPP-Trailer ans Ende und sendet diesen Datenblock über die WAN-Verbindung an R1.

Entsprechend entfernt R1, nachdem er das Paket erhalten hat, PPP-Header und -Trailer, weil die Aufgabe von PPP nur darin besteht, das IP-Paket über die serielle Verbindung zuzustellen. R1 entscheidet dann, dass er das Paket über Ethernet zu Larry weiterleiten muss. Dazu fügt R1 dem Paket einen neuen Ethernet-Header und -Trailer an und übermittelt es an Larry.

Im Wesentlichen benutzt IP die Protokolle der Netzwerkzugangsschicht, um ein IP-Paket an den nächsten Router oder Host zu übergeben, wobei jeder Router diesen Prozess wiederholt, bis das Paket an seinem Ziel eintrifft. Um die zur erfolgreichen Übermittlung der Daten über das physikalische Netzwerk notwendige Information zu codieren, verwendet jedes Netzwerkzugangsprotokoll Header. Das geschieht in derselben Weise, wie andere Schichten das zur Erreichung ihrer Ziele ebenfalls tun.

Anmerkung

Häufig wird die Netzwerkzugangsschicht des TCP/IP-Modells in Form von zwei Schichten beschrieben, nämlich als Sicherungsschicht und Bitübertragungsschicht oder physische Schicht. Die Gründe für die Beliebtheit dieser Terminologie werden im Abschnitt über OSI erläutert, da diese Ausdrücke aus dem OSI-Modell hervorgehen.

Die Netzwerkzugangschicht von TCP/IP umfasst Protokolle, Verkabelungsstandards, Header und Trailer, die festlegen, wie die Daten über die verschiedenen Typen physischer Netzwerke zu übermitteln sind.

Terminologie zur Datenkapselung

Anhand der Art und Weise wie HTTP, TCP, IP sowie die Protokolle der Netzwerkzugangsschicht Ethernet und PPP arbeiten, können Sie erkennen, dass jede Schicht ihre eigenen Header (und manchmal Trailer) zu den von der höheren Schicht bereitgestellten Daten hinzufügt. Der Ausdruck *Kapselung* beschreibt diesen Vorgang, Daten zwischen Header und Trailer zu setzen. Beispielsweise hat der Webserver die Homepage in Abbildung 2.2 in einen HTTP-Header eingekapselt. In Abbildung 2.3 hat die TCP-Schicht den HTTP-Header und die Daten in einem TCP-Header eingekapselt, in Abbildung 2.4 schliesst IP die TCP-Header und Daten innerhalb eines IP-Headers ein. Schließlich hat die Netzwerkzugangsschicht das IP-Paket noch zwischen einem Header und einem Trailer in Abbildung 2.5 gekapselt.

Der Vorgang, mit dem ein TCP/IP-Host Daten überträgt, kann als Prozess mit fünf Schritten betrachtet werden. Die ersten vier Schritte betreffen die Kapselung, die durch die vier TCP/IP-Schichten vorgenommen wird, während der fünfte Schritt in der tatsächlichen physischen Übertragung der Daten durch den Host besteht. Die Schritte sind in der nachstehenden Liste zusammengefasst:

Schritt 1: Erzeuge die Anwendungsdaten und kapsele sie mit den dazu nötigen Headern der Anwendungsschicht. Zum Beispiel wird die HTTP-OK-Meldung in einem HTTP-Header zurückgegeben, dem Teile des Inhalts einer Webseite folgen.

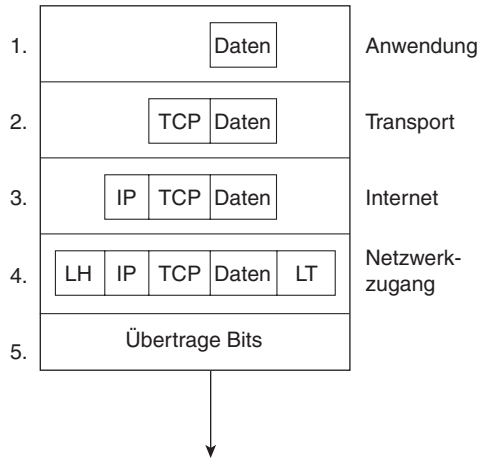
Schritt 2: Kapsele die Daten, die von der Anwendungsschicht geliefert wurden, in einem Transportschicht-Header. Für Endbenutzer-Anwendungen wird üblicherweise ein TCP- oder UDP-Header verwendet.

Schritt 3: Kapsele die Daten, die von der Transportschicht geliefert wurden, in einem Header der Internetschicht (IP-Header). IP ist das einzige auf dieser Schicht im TCP/IP-Netzwerkmodell verfügbare Protokoll.

Schritt 4: Kapsele die Daten, die von der Internetschicht geliefert wurden, in einem Header und -Trailer der Netzwerkzugangsschicht. Dies ist die einzige Schicht, die sowohl einen Header als auch einen Trailer verwendet.

Schritt 5: Sende die Bits. Die physische Schicht codiert das Signal auf dem Medium zur Übertragung des Frames.

Die Zahlen in Abbildung 2.6 entsprechen den fünf Schritten in der Liste. Sie stellen den Vorgang graphisch dar. Beachten Sie, dass die Abbildung keinen Anwendungsschicht-Header zeigt, da die Anwendungsschicht häufig keinen benötigt.



* Die Buchstaben LH und LT bedeuten Link-Header bzw. Link-Trailer und stehen für Header und Trailer der Sicherungsschicht (Data Link Layer).

Abbildung 2.6: Fünf Schritte der Datenkapselung – TCP/IP

Achten Sie schließlich auch noch besonders darauf, sich die Ausdrücke Segment, Paket und Frame und die jeweilige Zuordnung zu merken. Jeder Ausdruck steht für die durch die jeweilige Schicht definierten Header und möglicherweise Trailer sowie die gekapselten Daten, die dem betreffenden Header folgen. Es bezieht sich jeder dieser Ausdrücke auf eine andere Schicht: Segment für die Transportschicht, Paket für die Internetschicht und Frame für die Netzwerkzugangsschicht. Abbildung 2.7 zeigt jede Schicht zusammen mit dem zugehörigen Ausdruck.

Wichtig!

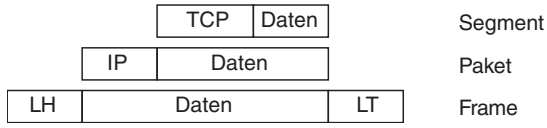


Abbildung 2.7: Zuordnung von Kapselung und »Daten«

Beachten Sie, dass Abbildung 2.7 auch die gekapselten Daten einfach als »Daten« bezeichnet. Wenn die Funktion einer einzelnen Schicht im Mittelpunkt steht, sind die gekapselten Daten normalerweise nicht von Interesse. Zum Beispiel kann bei einem IP-Paket tatsächlich ein TCP-Header hinter dem IP-Header, ein HTTP-Header hinter dem TCP-Header und Daten für eine Webseite erst nach dem HTTP-Header folgen. Aber beim Erläutern von IP müssen Sie nur auf den IP-Header achten und alles, was danach kommt, einfach als »Daten« betrachten. Daher wird bei der grafischen Darstellung von IP-Paketen alles hinter dem IP-Header üblicherweise einfach als »Daten« bezeichnet.

2.2.2 Das OSI-Referenzmodell

Um die ICND1-Prüfung zu bestehen, müssen Sie mit einer Protokollspezifikation vertraut sein, mit der Sie wahrscheinlich noch niemals direkte Erfahrungen gemacht haben – dem OSI-Referenzmodell. Heutzutage besteht die Schwierigkeit beim Erörtern der OSI-Protokollspezifikationen darin, dass es keinen Bezugspunkt gibt. Es ist praktisch nicht möglich, einen Rechner zu finden, dessen Haupt- oder auch nur optionale Netzwerkprotokolle vollständig dem OSI-Modell entsprechen.

OSI ist das »Open System Interconnection«-Referenzmodell für Kommunikation. Es war als Ganzes am freien Markt nie erfolgreich, obwohl einige Originalprotokolle, die das OSI-Modell beinhalten, noch immer in Gebrauch sind. Warum ist es also überhaupt notwendig, sich im Zusammenhang mit der CCNA-Prüfung über OSI Gedanken zu machen?

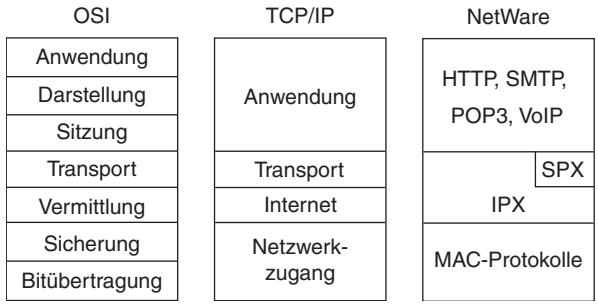
Sie sollten Kenntnisse über OSI haben, weil das OSI-Modell jetzt vor allem als Referenz bei der Beschreibung anderer Protokollspezifikationen benötigt

wird. Und weil von Ihnen als CCENT oder CCNA erwartet wird, dass Sie eine Vorstellung von den Begriffen und Fachausdrücken haben, die hinter Netzwerkarchitektur und Modellen stehen. Und schließlich weil andere Protokolle (TCP/IP eingeschlossen) fast immer mit OSI verglichen werden, wobei dabei oft die OSI-Terminologie benutzt wird.

OSI und TCP/IP im Vergleich

Das OSI-Referenzmodell ist aus sieben Schichten aufgebaut. Jede Schicht definiert eine Vielzahl typischer Netzwerkfunktionen. Als sich OSI während der 1980er und 1990er Jahre in der aktiven Entwicklung befand, haben die OSI-Komitees neue Protokolle und Spezifikationen für die Funktionen der einzelnen Schichten geschaffen. In anderen Fällen, so für TCP/IP, taten sie das nicht, sondern verwiesen stattdessen auf bereits definierte Protokolle. Zum Beispiel werden Ethernet-Standards durch IEEE definiert, sodass die OSI-Komitees keine Zeit damit vergeudeten, einen neuen Ethernet-Typ zu definieren, sondern einfach auf die IEEE-Ethernet-Standards verwiesen.

Heutzutage kann das OSI-Modell als Vergleichsstandard für andere Netzwerkmodelle dienen. Abbildung 2.8 vergleicht das siebenschichtige OSI-Modell mit dem vierschichtigen TCP/IP-Modell. Außerdem zeigt die Abbildung zur Verdeutlichung noch einige Beispielprotokolle sowie die entsprechenden Schichten.



Wichtig!

Abbildung 2.8: OSI-Schichten als Referenz für andere Protokolle

Beim OSI-Modell ist mit jeder der sieben Schichten eine sehr gut spezifizierte Anzahl von Funktionen verbunden. Man kann jedes Netzwerkprotokoll oder jede Spezifikation untersuchen und bestimmen, mit welcher OSI-Schicht eine Übereinstimmung besteht. Beispielsweise entspricht die Internetschicht von TCP/IP, da sie hauptsächlich IP enthält, am besten der OSI-Vermittlungsschicht. Daher wird unter Verwendung von OSI-Terminologie und -Nummerierung meistens gesagt, IP sei ein Vermittlungsschicht- oder Layer-3-Protokoll. Natürlich wäre IP eigentlich in Schicht 2 anzusiedeln,

wenn man das TCP/IP-Modell von unten durchnummerieren würde. Aber jeder Netzwerktechniker verwendet den OSI-Standard zur Beschreibung der Protokolle. Daher gilt IP als Vermittlungsschichtprotokoll.

Während man aus Abbildung 2.8 schließen kann, die OSI-Netzwerkschicht und die TCP/IP-Internetschicht seien zumindest ähnlich, gibt sie keinen Hinweis darauf, warum sie ähnlich sind. Um einschätzen zu können, warum die TCP/IP-Schichten einer OSI-Schicht entsprechen, müssen Sie die Funktionsschichten von OSI genauer betrachten. Zum Beispiel definiert die OSI-Vermittlungsschicht (Schicht 3) die logische Adressierung und das Routing, wie es auch bei der TCP/IP-Internetschicht der Fall ist. Während die Einzelheiten sich in wesentlichen Punkten unterscheiden, entspricht die Funktion der TCP/IP-Internetschicht der der OSI-Vermittlungsschicht, da beide ähnliche Ziele und Eigenschaften definieren. Genauso definiert die TCP/IP-Transportschicht zahlreiche Funktionen, darunter die Fehlerkorrektur, in derselben Weise wie die OSI-Transportschicht. Daher wird TCP als Transportschicht- oder Layer-4-Protokoll bezeichnet.

Nicht alle TCP/IP-Schichten entsprechen einer einzelnen OSI-Schicht. So definiert die TCP/IP-Netzwerkzugangssschicht sowohl die Spezifizierung des physischen Netzwerks als auch die Protokolle zur Steuerung desselben. OSI verlegt die Spezifizierung in die physische Schicht (Bitübertragungsschicht) und die Steuerungsfunktionen in die Sicherungsschicht (Schicht 2). Tatsächlich stellt man sich TCP/IP häufig als Fünf-Schichten-Modell vor, wobei die Netzwerkzugangsschicht von TCP/IP, um OSI zu entsprechen, durch zwei Schichten ersetzt wird, und zwar durch eine physische Schicht sowie eine Sicherungsschicht.

Anmerkung

Merken Sie sich für die Prüfungen, dass TCP/IP entweder eine einzelne Netzwerkzugangsschicht oder zwei untere Schichten (Sicherungsschicht und physische Schicht) besitzt

OSI-Schichten und ihre Funktionen

Cisco erwartet, dass CCNAs ein Grundverständnis der Funktionen in den einzelnen OSI-Schichten haben und die Schichtbezeichnungen und Schichtnummerierung kennen. Außerdem ist es wichtig, dass Sie wissen, welche Schichten des OSI-Modells am besten den in diesem Buch beschriebenen Geräten oder Protokollen entsprechen. Die oberen Schichten des OSI-Referenzmodells (Anwendung, Darstellung und Sitzung – Schichten 7, 6 und 5) beziehen sich auf Funktionen der Anwendungsebene. Die unteren vier Schichten (Transport, Vermittlung, Sicherung und Bitübertragung –

Schichten 4, 3, 2 und 1) legen dagegen Funktionen für den Ende-zu-Ende-Datentransfer fest. Die CCNA-Prüfungen konzentrieren sich auf Themen der unteren Schichten, insbesondere auf Schicht 2 (LAN-Switching) und auf Schicht 3 (Routing). Tabelle 2.4 definiert die sieben Schichten.

Tabelle 2.4: Schichtdefinitionen des OSI-Referenzmodells

Schicht	Beschreibung der Funktionen
7	Schicht 7 stellt eine Schnittstelle zwischen der Kommunikationssoftware und einer Anwendung bereit, die extern kommunizieren möchte. Sie definiert auch Prozesse für die Benutzer-Authentifizierung.
6	Hauptzweck dieser Schicht sind die Definition und das Aushandeln der Datenformate wie zum Beispiel ASCII-Text, EBCDIC-Text, binäre Dateien, BCD und JPEG. Auch die Verschlüsselung wird von OSI als Dienst der Darstellungsschicht definiert.
5	Die Sitzungsschicht definiert Start, Steuerung und Beendigung von Dialogen (sogenannte Sessions oder Sitzungen). Das schließt Steuerung und Management mehrfacher bidirektionaler Nachrichten ein, sodass die Anwendung benachrichtigt werden kann, wenn nur ein Teil der Nachrichten vollständig ist. Dies erlaubt der Darstellungsschicht eine direkte Übersicht über den eingehenden Datenstrom.
4	Protokolle der Schicht 4 stellen eine große Zahl von Diensten bereit, die in Kapitel 6 dieses Buches beschrieben werden. Während die OSI-Schichten 5 bis 7 auf die Kommunikation in der Anwendungsebene ausgerichtet sind, löst Schicht 4 die Probleme bei der Datenübergabe an den anderen Rechner, so zum Beispiel die Fehlerkorrektur und die Ablaufsteuerung.
3	Die Vermittlungsschicht definiert drei Hauptfunktionen: logische Adressierung, Routing (Weiterleitung) und Wegbestimmung. Die Routing-Konzepte legen fest, wie Geräte (meist Router) Pakete an ihr Ziel weiterleiten. Die logische Adressierung weist jedem Gerät eine für den Routing-Prozess nutzbare Adresse zu, und die Wegbestimmung bezieht sich auf die Funktion der Routing-Protokolle, aus den möglichen Pfaden zum Ziel den besten auszuwählen.
2	Die Sicherungsschicht definiert die Protokolle und Regeln, nach denen ein Gerät seine Daten über ein bestimmtes Medium senden darf. Protokolle der Sicherungsschicht definieren auch das Format für Header und Trailer, die den am Medium angeschlossenen Geräten die erfolgreiche Übermittlung von Daten erlauben. Der Sicherungs-Trailer, der den gekapselten Daten folgt, beinhaltet ein Frame-Check-Sequence-Feld (FCS), das es dem Empfangsgerät ermöglicht, Übertragungsfehler zu finden.
1	Diese Schicht arbeitet normalerweise mit den Normen anderer Organisationen. Diese Normen behandeln die physischen Eigenschaften des Übertragungsmediums, zum Beispiel Stecker, Pins, Pinbelegung, Spannungs- bzw. Strompegel, Codierung, Modulation von Licht und die Regeln für das Aktivieren und Deaktivieren des physischen Mediums.

Tabelle 2.5 listet die meisten Geräte und Protokolle auf, die in den CCNA-Prüfungen vorkommen, sowie die dazugehörigen OSI-Schichten. Beachten Sie, dass viele Geräte die Protokolle mehrerer OSI-Schichten verstehen müssen, sodass die in der Tabelle aufgeführte Schicht in Wirklichkeit die höchste ist, auf der das Gerät arbeitet. Beispielsweise sind Router hauptsächlich auf der Schicht 3 tätig. Funktionen der beiden Schichten 1 und 2 muss der Router aber auch beherrschen.

Tabelle 2.5: OSI-Referenzmodell – Beispielgeräte und Protokolle

Schichtbezeichnung	Protokolle und Spezifikationen	Geräte
Anwendung (Application), Darstellung oder (Presentation), Sitzung oder Kommunikationssteuerug (Session) (Schichten 7 bis 5)	Telnet, HTTP, FTP, SMTP, POP3, VoIP, SNMP	Firewall, Intrusion-Detection-Systeme
Transport (Schicht 4)	TCP, UDP	
Vermittlung oder Netzwerk (Network) (Schicht 3)	IP	Router
Sicherung (Data Link) (Schicht 2)	Ethernet (IEEE 802.3), HDLC, Frame-Relay, PPP	LAN-Switch, drahtloser Zugangspunkt (Accesspoint), Kabelmodem, DSL-Modem
Physische Schicht (Schicht 1)	RJ-45, EIA/TIA-232, V.35, Ethernet (IEEE 802.3)	LAN-Hub, Repeater

Neben den Grundeigenschaften jeder OSI-Schicht (siehe Tabelle 2.4) und einigen Beispielprotokollen und Geräten zu jeder Schicht (Tabelle 2.5) sollten Sie auch die Bezeichnungen der Schichten im Gedächtnis behalten. Sie können sie einfach auswendig lernen, aber manche Menschen nutzen lieber einen mehr oder weniger sinnvollen Text, um sich das Auswendiglernen zu erleichtern.

Bei den folgenden drei Sätzen sind die ersten Buchstaben jedes Wortes die gleichen wie die der (englischen) OSI-Schichtbezeichnung, und zwar in der in Klammern angegebenen Reihenfolge:

- Alle praktischen Studenten trauen niemals dem Professor (Schichten 7 bis 1).
- All People Seem To Need Data Processing (Schichten 1 bis 7).
- Prima! Der neue Text sieht problemlos aus (Schichten 1 bis 7).

Das Prinzip der OSI-Schichten und seine Vorteile

Es hat viele Vorteile, wenn man die Funktionen oder Aufgaben des Netzwerks in kleinere Einheiten, die sogenannten *Schichten,* zerlegt und dazwischen Standardschnittstellen definiert. Die Schichten teilen eine große, nicht leicht zu überschauende Vielfalt von Funktionen und Protokollen in kleinere Teile auf, wodurch das Verständnis der Funktionen, die Hard- und Softwareinstallation und die Fehlersuche erleichtert werden. Die folgende Liste fasst die Vorteile der nach Schichten geordneten Protokollspezifikationen zusammen:

Wichtig!

- **Weniger komplex** Netzwerkmodelle zerlegen Konzepte und Funktionen in kleinere Teile.
- **Standardschnittstellen** Die Definition von Standardschnittstellen zwischen jeder Schicht erlaubt es mehreren Herstellern, Produkte für eine gegebene Funktion zu schaffen, mit allen Vorteilen des freien Wettbewerbs.
- **Leichter zu lernen** Netzwerktechniker können viel leichter Einzelheiten einer Protokollspezifikation lernen.
- **Einfachere Entwicklung** Eine verringerte Komplexität gestattet leichter Programmänderungen und eine schnellere Produktentwicklung.
- **Interoperabilität zwischen Produkten verschiedener Hersteller** Die Herstellung von Produkten für denselben Netzwerkstandard führt dazu, dass Rechner und Netzwerktreiber von vielen Herstellern im selben Netzwerk zusammenarbeiten können.
- **Modulare Konstruktionsweise** Von einem Hersteller kann Software für die höheren Schichten implementiert werden (z. B. ein Webbrowser), während ein anderer Hersteller die Software für die Implementierung niedrigerer Schichten schreibt, z. B. die in Microsoft-Betriebssystemen integrierte TCP/IP-Software.

Die Vorteile der Schichten kann man bei der besprochenen Analogie zur Post erkennen. Wer einen Brief schreibt, muss sich keine Gedanken darüber machen, wie die Post ihn quer durch das Land zustellt. Der Postangestellte im Land muss den Inhalt des Briefes nicht beachten. Dementsprechend ermöglichen die Schichten einem Softwarepaket oder Hardwaregerät, die Funktionen einer Schicht zu realisieren und darauf zu vertrauen, dass die anderen Funktionen von den jeweils zuständigen Schichten ausgeführt werden. Zum Beispiel kann einem Webbrowser die Netzwerktopologie gleichgültig sein, die Ethernet-Karte im PC muss sich nicht für den Inhalt einer Webseite interessieren, und ein Router im Netzwerk muss nicht den Inhalt einer Webseite kennen oder gar »wissen«, ob der absendende Rechner eine Ethernetkarte oder eine sonstige Netzwerkkarte benutzt hat.

Kapselung bei OSI

Wie bei TCP/IP gibt es auch bei OSI Prozesse, bei denen eine höhere Schicht Dienste von der nächstniedrigeren Schicht anfordert. Zur Bereitstellung der Dienste kapselt die niedrigere Schicht die Daten der höheren Schicht mit einem Header. Das letzte Thema dieses Kapitels erklärt Terminologie und Konzepte der OSI-Kapselung.

Im TCP/IP-Modell werden Ausdrücke wie Segment, Paket und Frame benutzt, um die verschiedene Schichten und ihre entsprechenden gekapselten Daten zu bezeichnen (siehe Abbildung 2.7). OSI verwendet dagegen einen allgemeineren Ausdruck: Protokolldateneinheit oder PDU (Protocol Data Unit). Eine PDU steht für die Bits, die Header und Trailer sowie auch die gekapselten Daten für diese Schicht enthalten. Zum Beispiel ist ein IP-Paket, wie es in Abbildung 2.7 gezeigt wird, eine PDU. Genauer handelt es sich bei einem IP-Paket um eine Layer-3-PDU, weil IP ein Protokoll der Schicht 3 ist. Der Ausdruck *L3PDU* ist eine Kurzfassung der Bezeichnung *Layer-3-PDU*. So bezieht man sich einfach auf die »Schicht-x-PDU«, anstatt die Ausdrücke Segment, Paket oder Frame zu benutzen, wobei »x« für die Nummer der Schicht steht, die gerade betrachtet wird.

OSI definiert Kapselung ähnlich wie TCP/IP. Alle Schichten mit Ausnahme der niedrigsten definieren einen Header, wobei die Daten der nächsthöheren Schicht hinter dem Header eingefügt werden. Die Sicherungsschicht definiert sowohl einen Header als auch einen Trailer und platziert die Layer-3-PDU zwischen beiden. Abbildung 2.9 stellt den typischen Kapselungsprozess dar. Sie sehen ganz oben die Anwendungsdaten und Anwendungsschicht-Header und ganz unten die L2PDU, die zur physischen Verbindung gesendet wird.

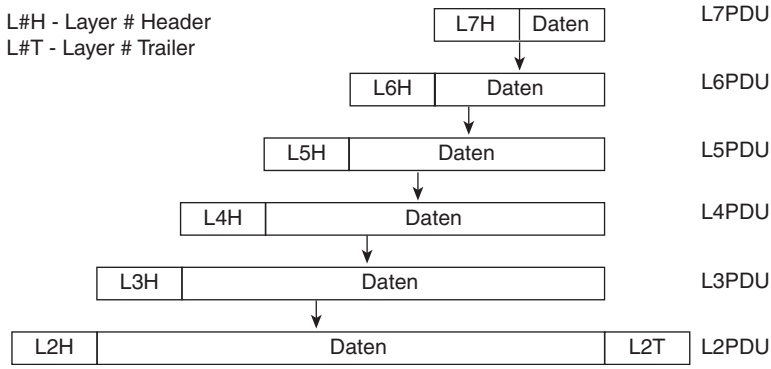


Abbildung 2.9: OSI-Kapselung und PDUs

2.3 Prüfungsvorbereitung

2.3.1 Wiederholung

Wiederholen Sie die wichtigsten Themen innerhalb der Kapitel, die mit diesem Symbol am äußeren Seitenrand gekennzeichnet sind.

Tabelle 2.6 enthält eine Übersicht der wichtigen Themen mit den jeweiligen Seitenzahlen.

Tabelle 2.6: Schlüsselthemen in Kapitel 2

Element	Inhalt	Seite
Tabelle 2.3	Definitionen für die Interaktion auf gleichen und auf benachbarten Schichten.	68
Abbildung 2.5	Zeigt den Dienst der Sicherungsschicht (Schicht 2), der für IP die IP-Pakete von Host zu Host zu überträgt.	71
Abbildung 2.7	Erklärt die Bedeutung der Ausdrücke Segment, Paket und Frame.	74
Abbildung 2.8	Vergleicht die Netzwerkmodelle OSI und TCP/IP miteinander.	75
Liste	Nennt die Vorteile der Verwendung eines Schichtenmodells in einem Netzwerk	79

2.3.2 Vervollständigen Sie die Listen und Tabellen

Drucken Sie eine Kopie von Anhang H, »Tabellen zur Übung« (zu finden auf der CD-ROM), zumindest aber den Abschnitt zu diesem Kapitel, und vervollständigen Sie die Tabellen und Listen aus dem Gedächtnis.

Anhang I, »Lösungen zu den Übungen«, ist ebenfalls auf der CD-ROM zu finden und enthält die vollständigen Tabellen und Listen als Lösung.

2.3.3 Wichtige Definitionen

Beschreiben Sie die folgenden Begriffe dieses Kapitels und überprüfen Sie Ihre Antworten mit den Erläuterungen im Glossar:

Interaktion benachbarter Schichten, Entkapselung, Kapselung, Frame, Netzwerkmodell, Paket, Protokolldateneinheit (PDU), Interaktion auf der gleichen Schicht, Segment.

2.3.4 OSI-Referenz

Die Schichtbezeichnungen im OSI-Modell sollten Sie auswendig lernen. Tabelle 2.7 listet eine Zusammenfassung von OSI-Funktionen zu jeder Schicht auf, zusammen mit jeweils einigen Beispielprotokollen.

Tabelle 2.7: OSI-Modell (Zusammenfassung)

Schicht	Beschreibung der Funktionen
Anwendung (Application, 7)	Schnittstelle zwischen Netzwerk und Anwendungssoftware Authentifizierungsdienste
Darstellung (Presentation, 6)	Definiert Format und Aufbau von Daten. Verschlüsselung
Sitzung (Kommunikationssteuerung, Session, 5)	Richtet Ende-zu-Ende-Datenströme zwischen Endpunkten ein und hält sie aufrecht. Umfasst die Verwaltung von Transaktionsflüssen.
Transport (4)	Stellt eine Vielzahl von Diensten zwischen zwei Hostrechnern zur Verfügung, unter anderem Verbindungseinrichtung und Verbindungsbeendigung, Flusssteuerung, Fehlerkorrektur und das Zerlegen großer Datenblöcke in kleinere Teile zur Übertragung.
Vermittlung (Network, 3)	Logische Adressierung, Routing, Wegermittlung
Sicherung (Data Link, 2)	Formatiert Daten in Frames, die zur Übertragung auf einem physischen Medium geeignet sind. Definiert Regeln dafür, wann das Medium benutzt werden darf, und Mittel zur Erkennung von Übertragungsfehlern.
Bitübertragung (Physisch, physical, 1)	Beschreibt die zur Bitübertragung notwendigen elektrischen und optischen Spezifikationen für die Verkabelung, die Verbindungen sowie die Prozeduren zur Umwandlung des Bitstroms in eine Energieform, die über das physische Medium transportiert wird.