Rüdiger Schleifnig

Ein firewall-geschützter Internet-Server unter Windows NT

Diplomarbeit

Bibliografische Information der Deutschen Nationalbibliothek:

Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de/ abrufbar.

Impressum:

Copyright © 1999 GRIN Verlag
ISBN: 9783638067645

Rüdiger Schleifnig

Ein firewall-geschützter Internet-Server unter Windows NT

GRIN Verlag

Fachhochschule Münster

Abteilung Steinfurt

Fachbereich Elektrotechnik

Labor für Technische Informatik

Diplomarbeit

Ein firewall-geschützter Internet-Server unter Windows NT

Diplomand: cand. ing. Rüdiger Schleifnig

0. Vorwort

Immer mehr Menschen nutzen das Internet für private oder geschäftliche Zwecke. Immer mehr Firmen und Behörden wissen die Vorteile des Intranets zu schätzen. An vielen Stellen werden heutzutage die Vorteile von beiden Netzen verknüpft, um möglichst effektives Arbeiten zu ermöglichen; Stichworte sind E-Mail, Online-Shopping, Online-Banking, Internet-Surfing, Datenkonsistenz, verteilte Systeme und Client-Server-Architekturen.
Immer weniger Menschen sind jedoch in der Lage, die komplexen Strukturen, die diese neuen Techniken mit sich bringen oder durch die sie erst möglich werden, zu durchschauen. Auf der Gegenseite der vielen Vorteile, die diese nahezu grenzenlosen Kommunikationsmöglichkeiten bieten, stehen viele nicht zu unterschätzende Sicherheitsrisiken. Anders als bei den positiven Seiten dieser Entwicklung wissen aber viele Benutzer nichts von den Risiken oder unterschätzen und ignorieren diese.

In dieser Diplomarbeit können aufgrund der knapp bemessenen Zeit, vorgesehen für die Diplomarbeit an der Fachhochschule sind etwa drei Monate, keine eigenständigen Untersuchungen über Viren oder andere Bedrohungen von Computersystemen durchgeführt werden. Diese Untersuchungen werden durch eine systematische Recherche, vor allem im Internet, ersetzt.
Die Diplomarbeit soll zeigen, dass es sowohl im homogenen wie auch in einem heterogenen Umfeld - der Windows NT Server steht in einem UNIX-dominierten Netzwerk - möglich ist, mit geringem finanziellen und personellen Aufwand einen „relativ“ sicheren Netzwerkserver mit Internetanbindung aufzubauen, welcher sowohl Angriffen von innen als auch von außen in einem gewissen Rahmen widerstehen kann.

Vollkommene Sicherheit gibt es nicht und maximale Sicherheit wird man in diesem Zeit- und Kostenrahmen nicht erreichen können. Zu erreichen ist aber ein wesentlich höherer Sicherheits-Level als ihn Windows NT standardmäßig mit sich bringt.

1. Danksagung

Mein ganz besonderer Dank gilt meiner Familie, die es mir ermöglicht hat, dieses Studium trotz einiger zwischenzeitlicher Probleme und Tiefpunkte zu beenden.

Weiterhin möchte ich mich bei Herrn Professor Dr.rer.nat. Norbert Witt dafür bedanken, dass er diese Diplomarbeit betreut hat, und dass er es in der ihm eigenen Art und Weise tat. Er war immer da, hat dort wo er konnte Unterstützung angeboten, aber nicht „regulierend“ in die Diplomarbeit eingegriffen, sondern lediglich Ratschläge gegeben.
Herrn Prof. Dr.rer.nat. Manfred Langenberg möchte ich dafür danken, dass er trotz terminlichem Engpass bereit war, meine Diplomarbeit als Koreferent zu betreuen.

Obwohl eine Diplomarbeit den Nachweis erbringen soll, dass der Student in der Lage ist, ein wissenschaftliches Thema in einem angemessenen Zeitrahmen eigenständig zu bearbeiten, kommt wohl keine Diplomarbeit ohne Tips, Ratschläge oder kritische Fragen anderer Personen aus.
Unter diesem Eindruck möchte ich mich auch bei Herr Dipl.Ing. Ulrich Geupel, der sich als Laboringenieur um die Beschaffung der Hardware gekümmert hat, oft den einen oder anderen Rat hatte oder die „dringend“ benötigten Teile aus dem Ärmel zauberte, bedanken.
Auch bei Herrn Dr. Dirk Böhme, der als Leiter der DVZ mit Rat und Tat bei der Realisierung des technischen Umfeldes des Internet-Servers zur Verfügung stand und als Windows-NT-Kenner die eine oder andere Anregung zum Einsatz und zur Optimierung des Betriebssystems gegeben hat, möchte ich mich bedanken.

Steinfurt, im Juni 1999

2. Inhaltsverzeichnis

3. Die Aufgabenstellung

Ziel dieser Diplomarbeit ist die Einrichtung eines firewall-geschützten Internet-Servers unter Windows NT.

Am Anfang der Diplomarbeit steht die Recherche. In Büchern und vor allen Dingen im Internet sollen die aktuellen Sicherheitsrisiken in Bezug auf Intra- und Internets zusammengetragen werden.
Zeitgleich soll ein PC beschafft werden, der in der Lage ist, die an ihn gestellten Anforderungen zu erfüllen, dabei aber ein möglichst günstiges Preis-/Leistungsverhältnis aufweist.

Nach der Beschaffung soll zunächst ein Intranet-Server auf Grundlage des Betriebssystems „Windows NT 4.0“ erstellt werden. Der PC soll sich in das vorhandene heterogene Umfeld, Sparc-Stations mit dem Betriebssystem Unix, PCs mit dem Betriebssystem Linux und PCs mit den Betriebssystemen Windows 3.11, Windows 95 und Windows NT Workstation, einfügen. Das Sicherheitsniveau dieses Intranet-Servers soll durch Veränderung der standardmäßigen Einstellungen des Betriebssystems und frei zugänglicher Software, also Free-Ware oder Evaluation-Versionen von Programmen, angehoben werden.

Anschließend soll, aufbauend auf dem lauffähigen Intranet-Server, ein Internet-Server unter der Software „Windows Internet Information Server 2.0“ eingerichtet werden, der sowohl als WWW-Server als auch als FTP-Server genutzt werden kann.

Auf dem Internet-Server soll eine Homepage eingerichtet werden, auf der sich das Lehrgebiet für „Technische Informatik und Mikrocomputertechnik“ präsentieren soll und von der es möglich ist, Down- und Uploads vorzunehmen. Zum Einsatz kommen hier im wesentlichen HTML, Java, Java-Script und Perl.

Sowohl der Intranet- als auch der Internet-Server sollen unter besonderer Berücksichtigung des Themas „Sicherheit“ aufgebaut werden und ihr Sicherheitsniveau in abschließenden simulierten Angriffen unter Beweis stellen. Um ein Verständnis der verschiedenen Angriffsmethoden zu ermöglichen, umfasst diese Diplomarbeit einen relativ großen theoretischen Teil.

4. Die eingesetzte Hardware

Da der eingesetzte Computer auf der einen Seite in der Lage sein soll, mehrere Anfragen gleichzeitig, sei es über Intranet oder Internet, in akzeptabler Zeit zu bearbeiten, sich aber andererseits innerhalb eines vernünftigen finanziellen Rahmens bewegen soll, fiel die Wahl auf Hardware mit den folgenden Eckdaten:

Prozessor:	INTEL Pentium II 450 MHz
Mainboard:	Asus P2BS; incl. U2W-Controller Adaptec 2940U2W
Arbeitsspeicher:	1 x SDRAM 256MB; Zugriffszeit 7ns
Festplatten:	2 x IBM DDRS-39130; U2W; 9,1GB; 7200U/min; 512kB Cache
Grafikkarte:	Matrox Millenium G200; 8MB
Netzwerkkarte:	3Com 3C905; 10/100MBit
CD-ROM Laufwerk:	Toshiba 6401B; SCSI, 40-fach
Floppy-Laufwerk:	3,5´´; 1,44MB
Betriebssystem:	Windows NT 4.0; Server-Version
Monitor:	vorhandener 20‘‘ Monitor der Marke ELSA

5. Das ISO-OSI Referenzmodell und die wichtigsten Protokolle

Natürlich kann an dieser Stelle keine umfassende Einführung in das ISO-OSI-Referenzmodell und die im Intra- und Internet verwendeten Protokolle gegeben werden. Es soll vielmehr versucht werden, die wichtigsten Eckpunkte, die zum Verständnis der Arbeit notwendig sind, darzustellen.
Als tiefergehende Literatur zu dem ISO-OSI-Modell wird das Buch „Computer Netzwerke“ von Andrew S. Tanenbaum [5] empfohlen.
Erschöpfende Beschreibungen der im Internet verwendeten Protokolle sind in Form von RFCs an vielen Stellen im Internet frei zugänglich.

5.1 Die 7 Schichten des ISO-OSI-Referenzmodells

5.1.1 Schicht 1: Physical Layer

Die Bitübertragungsschicht ist die einzige Schicht, die in direktem Kontakt zum physischen Übertragungsmedium steht. Sie ist für die elektrischen und mechanischen Definitionen, wie zum Beispiel die Pinbelegung des Steckers, die Spannungswerte und die Schnittstellensignale zuständig.
Die Bitübertragungsschicht definiert die physische Verbindung innerhalb des Netzes. Sie hat die Aufgabe der Steuerung des Mediums und des Übertragungsverfahrens sowie der Sicherung der Betriebsbereitschaft. Als einzige Schicht sendet und empfängt sie direkt die unstrukturierten Bitströme.

5.1.2 Schicht 2: Data-Link-Layer

Die Sicherungsschicht ist für die Fehlerfreiheit der Datenübertragung zuständig. Der von den Schichten 3 bis 7 kommende Bitstrom wird in Frames (engl.: Rahmen) zerlegt, da die Einzelübertragung von Datenblöcken besser kontrollierbar und leichter korrigierbar ist als die Übertragung eines längeren, „formlosen“ Bitstroms.
Auf der Empfangsseite übernimmt diese Schicht das Wiederherstellen des Bitstroms aus den von der Bitübertragungsschicht übergebenen Rahmen.
Bei leitungsvermittelten Netzen, wie zum Beispiel ISDN, steuert der Data-Link-Layer überdies den Verbindungsauf- und abbau.

Die Sicherungsschicht wird in zwei Unterschichten eingeteilt, den MAC-Layer und den LLC-Layer. Der Medium-Access-Control-Layer (MAC) regelt den Zugriff auf das Übertragungsmedium, der Logical Link Layer (LLC) verwaltet die logischen Verbindungen, die Fehlererkennung und die Flusskontrolle.
Durch die Aufteilung der Schicht 2 in zwei Teilschichten wird es möglich, mit Bridges Netze mit unterschiedlichen Protokollen zu verbinden, siehe 5.2.2 Bridges.

5.1.3 Schicht 3: Network Layer

Die Vermittlungsschicht übernimmt den Verbindungsaufbau zwischen zwei beliebig miteinander verbundenen Rechnern (engl.: routing). Dies umfasst die Bereitstellung geeigneter Adressierung, die Vermittlung, den Verbindungsaufbau und –abbau, die Rücksetzung, die Unterbrechung, die Fehlererkennung und den transparenten Datentransport zwischen den Verbindungsendpunkten. Unter Transparenz fallen die Anpassungen der Eigenarten verschiedener Sicherungsschichten und die Anpassung an sich ändernde Netzwerktopologien.
Die adressierten Kommunikationspartner müssen nicht zwingend die Verbindungsendpunkte sein, sondern es können auch Netzübergänge der Schicht 3, also Router, sein.

5.1.4 Schicht 4: Transport Layer

Die Transportschicht ist für den Aufbau einer Verbindung zwischen zwei Verbindungsendpunkten, in der Regel zwei Rechnern, verantwortlich. Sie ist die einzige der Transportschichten, die eine Ende-zu-Ende-Verbindung zwischen den physikalischen Endpunkten unterhält.
Als oberste der transportorientierten Schichten bietet sie den Anwendungsschichten 5 bis 7 einen allgemeinen und unabhängigen Übertragungsdienst, sie garantiert den Aufbau und den Unterhalt von Verbindungen. Sie kümmert sich um das Multiplexing, das Ordnen der Daten und um eine eventuell notwendige Fehlerbehandlung. Die Besonderheiten der Netzdienste sind damit für die höheren Schichten ohne Relevanz und transparent. Die Schicht bietet eine vom Netzzugang unabhängige Schnittstelle und ermöglicht hierdurch für die Anwendungsseite die zwingend notwendige Hardwareunabhängigkeit.
Für die von ihr erbrachten Dienste ist das darunterliegenden Netzwerk transparent. Ob die Schichten 1 bis 3 als LAN oder WAN realisiert sind, spielt für die Transportschicht keine Rolle.
Da die Schicht eine Ende-zu-Ende-Verbindung zwischen Prozessen bereitstellt, spricht man hier auch von Ende-zu-Ende-Kommunikation.

5.1.5 Schicht 5: Session Layer

Die Sitzungsschicht stellt im Netz die Verbindung für die darüberliegenden Netzdienste zur Verfügung. Als unterste der anwendungsorientierten Schichten nutzt die Sitzungsschicht als erste die von den Schichten 1 bis 4 bereitgestellten Datentransportdienste. Sie ist die letzte Ebene, auf der mit logischen und nicht mit physikalischen Namen für Netzknoten gearbeitet wird.
Verantwortlich ist die Sitzungsschicht für die Dialogsteuerung zwischen zwei Anwendungsprogrammen; sie stellt hierzu umfangreiche Dienste zur Synchronisation bereit. Ihr obliegt die Steuerung der Kommunikation zwischen zwei Anwendungen.

5.1.6 Schicht 6: Presentation Layer

Die Darstellungsschicht bietet für das Anwendungsprogramm die Schnittstelle zum Netzwerk und legt für das Programm die Zugriffsart auf das Netz fest. Hierzu stellt sie Funktionen für den Datentransport zur Verfügung.
Während sich die unter ihr liegenden Schichten nur noch mit reinen Bitströmem befassen, ist für die Darstellungsschicht auch noch die volle Syntax der Daten relevant. Sie konvertiert die von oben kommenden Daten in ein für Netzwerke gültiges Standardformat. Das Formatieren, Strukturieren, Verschlüsseln und Komprimieren von Daten gehört damit zu ihren Aufgaben.
Auf der Empfangsseite stellt sie aus dem von unten kommenden Bitstrom das plattformspezifische Format her und gibt die umgewandelten Daten an die Anwendungsschicht weiter.

5.1.7 Schicht 7: Application Layer

Die Anwendungsschicht stellt einen Streitfall dar, man kann sich nicht einigen, ob sie eine eigenständige Schicht im Rahmen des ISO-OSI-Modells darstellt oder ob sie bereits zu den Anwendungsprogrammen zählt.
Sie bietet ihre Dienste den Anwendungsprozessen an. Zu diesen gehört der Auf- und Abbau von Anwendungsassoziationen (auf der Schicht 7 spricht man häufig nicht mehr von Verbindungen), die Ausführung entfernter Operationen oder ein zuverlässiger Datentransport.

5.2 Netzübergänge und deren Funktionsweise

5.2.1 Repeater

Repeater sind die einfachsten Netzübergänge, sie sind simple Verstärkungseinrichtungen und dienen ausschließlich der direkten Signalweiterleitung. Ihr Aufbau ist relativ einfach und kommt ohne Software aus.

Repeater arbeiten gemäß ihrer Funktion auf der Bitübertragungsschicht (siehe Abbildung 1). Auf dieser Schicht gibt es keine Daten mit logischen Strukturen, sondern nur einzelne Bits, also auch nur zwei Zustände: Strom oder kein Strom bei asymmetrischer Signalverteilung bzw. Stromfluss in die eine oder andere Richtung bei symmetrischer Signalverteilung. Diese elektrischen Signale werden von Repeatern empfangen, verstärkt und wahllos weitergegeben.

Wahllos bedeutet, dass Repeater keinerlei Filter- oder Routingfunktionen übernehmen können, sie leiten alle Daten unkontrolliert und unabhängig von deren Herkunft oder Ziel weiter.

Durch die auf Ebene 1 des OSI-Modells beschränkte Arbeitsweise des Repeaters werden die Ebenen 2 bis 7 nicht ausgewertet. Dies bedeutet, dass die beiden durch einen Repeater gekoppelten Subnetze ab OSI-Ebene 2 identisch sein müssen. Die Verbindung unterschiedlicher Netzwerktechnologien ist somit durch Repeater nicht möglich.

5.2.2 Bridges

Eine Bridge ist ein Netzübergang, der gemäß der Spezifikationen der Ebene 2 des ISO-OSI-Modells arbeitet (siehe Abbildung 1). Die verwendete Technik ist im Vergleich zu Repeatern aufwendiger und erfordert in der Regel eigene Software. Eine Bridge ist meistens ein kleines Bauteil mit eigener Schaltungslogik und Netzschnittstellen. Sie wird zur Lastverteilung in größeren Netzen eingesetzt, da sie anhand einer Adresstabelle in der Lage ist zu entscheiden, ob sich die Adresse eines Datenpakets innerhalb eines Subnetzes befindet oder ob die Datenpakete in ein anderes Subnetz vermittelt werden müssen. Hierdurch werden die einzelnen Subnetze merklich entlastet, da Datenpakete nur noch dann übertragen werden, wenn es notwendig ist.

Eine Bridge lässt sich zur Verbindung gleichartiger Netze einsetzen. Hierbei unterscheidet man zwei verschiedene Typen:

- Die „normale“ MAC-Layer-Bridge arbeitet im unteren Teil der Schicht 2. Ihre Funktionalität entspricht der ursprünglichen OSI-Spezifikation der Ebene 2. Damit die Bridge eingesetzt werden kann, muss bereits der Medienzugriff der beiden Subnetze übereinstimmen. Die Verbindung von zum Beispiel Ethernet mit Token-Ring ist mit einer solchen Bridge also nicht möglich.
- Die LLC-Layer-Bridge wandelt die MAC-Adressen des ersten Subnetzes in MAC-Adressen des zweiten Subnetzes um und ermöglicht so die Verbindung von zum Beispiel Ethernet und Token-Ring.

5.2.3 Router

Router sind Netzübergänge, die den Bridges ähneln, jedoch „intelligenter“ und komplexer sind. Ihre Funktionalität entspricht der Ebene 3 des ISO-OSI-Modells (siehe Abbildung 1). Damit sind sie vom eingesetzten Protokoll abhängig und im Gegensatz zu Bridges nicht mehr nach oben transparent. Router bieten den auf ihnen aufsetzenden Protokollen eine Schnittstelle zu den Schichten 1 und 2, eignen sich also gut dazu, verschiedene LANs miteinander zu verknüpfen.
Die Hauptaufgabe von Routern ist die Wegwahl, das Routen, vom Sender zum Empfänger. Dazu gehört der Aufbau, das Aufrechterhalten und der Abbau einer geordneten Ende-zu-Ende-Verbindung. Für die Wegwahl muss der Router die eingesetzten Netzwerkprotokolle verstehen, da das Routen von TCP/IP-Paketen anders erfolgt als das für IPX-Pakete oder eines Novell-Netzwerks.
Da Router auf der Ebene 3 des OSI-Modells arbeiten, müssen sie alle Protokolle, die über sie geroutet werden sollen, „verstehen“. Um heterogene Netze mit möglichst wenigen, oft teuren Routern betreiben zu können, hat man sogenannte Multi-Protokoll-Router entwickelt, die mehrere Protokolle verarbeiten können. Anhand der Adresse der eingehenden Pakete wird in den Routern zur entsprechenden Routine verzweigt, die das Routing vornimmt.

5.2.4 Gateways

Ein Gateway ist ein Rechner, meist sogar ein Zentralrechner, der vollkommen unterschiedliche Netze koppeln kann. Je nachdem wie groß der Unterschied der zu koppelnden Netze ist, arbeitet das Gateway in einer der Ebenen 4 bis 7, auf jeden Fall oberhalb der Ebene 3. Entsprechen sich zwei eingesetzte Netzwerke zum Beispiel in den Ebenen 6 und 7, so koppelt das Gateway diese

Netzwerke auf der Ebene 5.

Gateways sind notwendig, um herstellerspezifische Protokolle ineinander umzusetzen und eine herstellerübergreifende Kommunikation zu ermöglichen. Für die angeschlossenen Netzwerke ist das Gateway ein direkt adressierbarer Rechner innerhalb des Gesamtnetzwerks, der die Adress- und Formatumsetzungen, die Konvertierungen, die Flusskontrolle und eventuelle Geschwindigkeitsanpassungen für den Übergang in das jeweils andere Teilnetz übernimmt. Man braucht Gateways beispielsweise zur Ankopplung von PCs an Hostsysteme wie zum Beispiel IBM- oder Siemens-Mainframes oder öffentliche Weitverkehrsverbindungen, zum Beispiel WAN-Verbindungen der Telekom. Im Gegensatz zu Routern und Bridges, die zur Strukturierung und Lastverteilung in Netzen eingesetzt werden, ist die Hauptaufgabe der Gateways die Anpassung verschiedener Netzwelten.

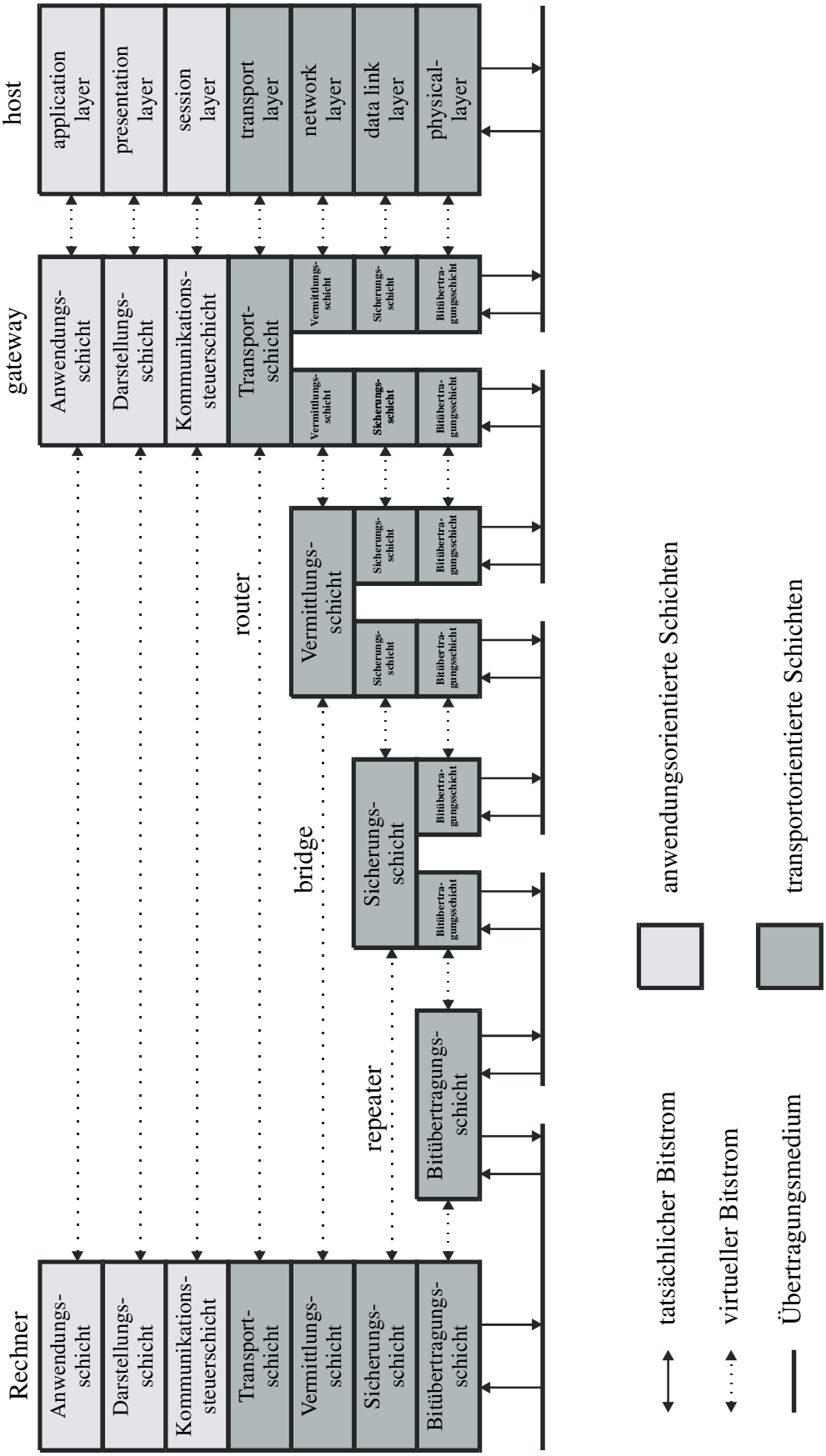

Abb. 1: Verschiedene Geräte im ISO-OSI-Modell