Netzwerke

Protokolle und Dienste

(Stand 2020)

Andreas Dittfurth

1. Ausgabe, März 2021

ISBN 978-3-86249-963-2

NWPD_2020

Plus

HERDT

Bevor Sie beginnen …

Empfohlene Vorkenntnisse

- Grundwissen zu Computernetzwerken
- Grundwissen zu Betriebssystemen (Linux, Windows)
- Grundwissen über Hardware (PC, Netzwerkkomponenten)

Hinweise zu Soft- und Hardware

Zum besseren Verständnis der Protokolle empfiehlt sich der Einsatz eines Netzwerkanalysators (auch „Netzwerksniffer“ genannt) wie Wireshark (siehe: *https://www.wireshark.org/*), um selbst die Funktionen und Kommunikationsabläufe bestimmter Protokolle und Dienste nachvollziehen zu können. Das Programm sollte auf einem Rechner mit Netzwerkzugang installiert werden. Sollen darüber hinaus Dienstkonfigurationen nachvollzogen werden, wird ein Server mit installierten Netzwerkdiensten wie DNS, DHCP und RAS/VPN benötigt.

Typografische Konventionen

Damit Sie bestimmte Elemente auf einen Blick erkennen und zuordnen können, werden diese im Text durch eine besondere Formatierung hervorgehoben. So werden beispielsweise Bezeichnungen für Programmelemente wie Register oder Schaltflächen immer *kursiv* geschrieben und wichtige Begriffe **fett** hervorgehoben.

Kursivschrift	kennzeichnen alle vom Programm vorgegebenen Bezeichnungen für Schaltflächen, Dialogfenster, Symbolleisten etc., Menüs bzw. Menüpunkte (z. B. *Datei - Schließen*), Internetadressen und vom Benutzer angelegte Namen (z. B. Rechner-, Domänen-, Benutzernamen).
`Courier`	wird für Systembefehle sowie für Datei- und Verzeichnisnamen verwendet. In Syntaxangaben werden Parameter kursiv ausgezeichnet (z. B. `cd` *`Verzeichnisname`*). Eckige Klammern `[]` kennzeichnen optionale Elemente. Alternative Eingaben sind durch einen senkrechten Strich `|` getrennt. Benutzereingaben auf der Konsole werden **`fett`** hervorgehoben.

Symbole

 Hilfreiche Zusatzinformation

 Praxistipp

 Warnhinweis

HERDT BuchPlus – unser Konzept:

Problemlos einsteigen – Effizient lernen – Zielgerichtet nachschlagen

Nutzen Sie dabei unsere maßgeschneiderten, im Internet frei verfügbaren Medien:

Wie Sie schnell auf diese BuchPlus-Medien zugreifen können, erfahren Sie unter ***www.herdt.com/BuchPlus***.

1 Übersicht über gängige Kommunikations-protokolle

1.1 Die Aufgaben von Protokollen und Diensten in der IT

Protokolle und Dienste

Protokolle dienen in der IT dazu, den Transport von Daten zu gewährleisten. Sie stellen die „Sprachen“ dar, mit denen verschiedene Systeme miteinander kommunizieren. An jedem Kommunikationsprozess sind mehrere Protokolle beteiligt.

Dienste stellen den Protokollen eine Umgebung zur Verfügung, in der Aufgaben, wie etwa die Konfiguration von Netzwerkinformationen oder die Bereitstellung von Daten auf entfernten Systemen, bewältigt werden können. Die Trennlinie zwischen Diensten und Protokollen zu finden ist nicht immer ganz einfach. So basiert der Dienst des Internets (WWW) auf einem eigenen Protokoll (HTTP), der namensauflösende Dienst DNS (Domain Name System) jedoch verwendet das Protokoll DNS.

Generell gilt, dass kein Dienst ohne ein geeignetes Protokoll seine Aufgaben erledigen kann. Denn jede Kommunikation basiert in der IT auf einer Vielzahl von unterschiedlichen Möglichkeiten, die jeweils eine genaue Anpassung der Umgebung erfordern. Diese Anpassungen werden als Regelsätze von exakt für diese Aufgaben entworfenen Protokollen beschrieben.

Protokolle für die physikalische Datenübertragung

Eine Gruppe von Protokollen beschreibt das Verfahren, wie Daten über ein bestimmtes Medium transportiert werden müssen. So wird etwa im Ethernet-Protokoll die Art des Zugriffs auf das Übertragungsmedium (CSMA/CD = Carrier Sense, Multiple Access with Collision Detection; etwa: Leitungsabfrage bei vielfachem Zugriff mit Kollisionserkennung) festgelegt; es werden aber auch Definitionen der Ströme, Aderbelegungen, Spannungen, die eine Null oder eine Eins darstellen, usw. beschrieben.

Andere Protokolle dienen dazu, die Daten aus einem Netzwerk in die Daten einer Telefonverbindung einzubinden, um so den Transport zwischen den Netzwerken zu ermöglichen. Definitionen zur Telefonverbindung selbst fallen hierbei in den Grenzbereich der Netzwerkprotokolle. Zwar kann eine WAN-Verbindung mittels ISDN aufgebaut werden, es handelt sich dabei jedoch um die Nutzung eines netzwerkfremden Dienstes.

Der Einsatz von hardwarenahen Protokollen wird durch die verwendete Hardware bestimmt und lässt keinen Spielraum für individuelle Anpassungen.

Protokolle für die Wegermittlung und den Pakettransport

Eine weitere Gruppe von Protokollen hat die Aufgabe, den Transport von Datenpaketen zwischen Netzen zu gewährleisten. Diese Protokolle lassen sich in zwei Gruppen fassen:

- Protokolle zur Ermittlung der möglichen Wege zwischen Netzwerken (Routing-Protokolle)
- Protokolle zum Transport von Paketen zwischen Netzwerken (geroutete Protokolle)

Protokolle für den Datentransport

Auf einem Computer nehmen meist mehrere Anwendungen gleichzeitig Dienste des Netzwerkes in Anspruch. Zwischen diesen Anwendungen und dem Netzwerk müssen vermittelnde Protokolle eingesetzt werden, die die Daten in transportgerechte Segmente unterteilen und beim Zusammensetzen an die jeweils richtige Anwendung weiterleiten. Die Datensegmente, die von den Transportprotokollen an die Netzwerkprotokolle weitergereicht werden, bezeichnet man als Datagramme.

Da Datagramme auf unterschiedlichen Pfaden durch das Netzwerk transportiert werden können, muss darauf geachtet werden, dass sie in der richtigen Reihenfolge zusammengesetzt und an die Anwendungen weitergereicht werden.

Ein Grund, warum Daten in Segmenten und nicht im Ganzen übertragen werden, ist, dass bei einer Beschädigung oder einer teilweise fehlerhaften Übertragung nicht das gesamte Datenpaket neu gesendet werden muss. Das beteiligte Protokoll nimmt bei jedem zusätzlichen Verarbeitungsprozess zu diesem Zweck eine weitere Unterteilung der Daten in kleinere Stücke vor. Viele Protokolle können dann bei einer Beschädigung oder einem Datenverlust geeignete Reaktionen in die Wege leiten, um die Daten erneut zu übertragen. Andere Protokolle verlassen sich darauf, dass weitere am Kommunikationsprozess beteiligte Protokolle oder Dienste die Datenintegrität sicherstellen.

Generell benötigt jede zusätzliche Funktionalität beim Datentransport auch die Bandbreite des Netzwerkes und die Verarbeitungskapazität der CPU. Daher gilt es immer, einen Kompromiss zwischen Sicherheit der Übertragung und Effektivität der Ressourcen-Nutzung zu finden.

Dienste

Aktuelle Dienste umfassen unterschiedlichste Aufgaben. Viele dieser Aufgaben werden nicht von einem einzelnen Dienst gewährleistet, sondern werden durch mehrere unterschiedliche Dienste abgedeckt. Dies ist teilweise auf sich verändernde Ansprüche und Leistungsfähigkeiten von Netzwerken, Betriebssystemen, Benutzern und Anwendungen zurückzuführen, zum Teil handelt es sich bei alternativen Diensten um Produkte verschiedener Hersteller.

Dienste in Netzwerken lassen sich grob in drei Gruppen unterteilen:

- Dienste für den Netzwerkbetrieb
- Dienste für Betriebssysteme
- Dienste für Anwender und Anwendungen

Dienste für den Netzwerkbetrieb

Dienste für den Netzwerkbetrieb haben die Aufgabe, den einwandfreien und benutzerfreundlichen Betrieb von Netzwerken sicherzustellen. Sie übernehmen Dienste wie Adressauflösung und -zuweisung, Zeitsynchronisation, Sicherheitsfilterung von Daten und Paketen oder die Bereitstellung zwischengespeicherter Informationen zur Entlastung von Weitverkehrsverbindungen.

Teilweise ist dabei die Grenze zu den anderen Gruppen von Netzwerkdiensten fließend. So kann etwa die Zeitsynchronisation sowohl von Netzwerkkomponenten als auch von Betriebssystemen oder Benutzern verwendet werden.

Dienste für Betriebssysteme

Es gibt eine ganze Reihe von Diensten, die betriebssystemspezifische Aufgaben erfüllen. In der Folge finden Sie eine Übersicht über gängige Betriebssystemaufgaben, die von Netzwerkdiensten gewährleistet werden:

- **Benutzerauthentifizierung**: Die Anmeldeinformationen von Benutzern werden bei modernen Netzwerken nicht mehr von lokalen Systemen abgelegt. Die Verwaltung erfolgt in einer zentralen Datenbank für das gesamte Netzwerk, die Authentifizierung übernimmt ein zentraler Server.
- **Bereitstellung verteilter Dienst**: Um Systemressourcen effizienter zu nutzen, können beispielsweise Datenbanken auf mehrere Rechner verteilt werden. Auch Anwendungen laufen nicht immer auf dem lokalen System, sondern werden zunehmend auf sogenannten Anwendungsservern ausgeführt. Dies bietet Einsparungspotenzial für Hardware und Lizenzen. Zudem kann der administrative Aufwand für die Netzwerkwartung deutlich verringert werden.
- **Ausfallsicherheit**: Indem beispielsweise Dokumentationen mittels verteilter Dateisysteme auf mehreren Servern im Netzwerk gespeichert werden, kann erreicht werden, dass bei Ausfall kompletter Systeme das Netzwerk einsatzbereit bleibt. Durch geografische Verteilung von Systemen – z. B. Clusterung über Weitverkehrsleitungen – kann ein wirksamer Schutz vor Datenverlust bei Katastrophen wie Erdbeben, Flugzeugabstürzen oder Bränden errichtet werden.
- **Lastenverteilung**: Neben der Ausfallsicherheit bieten Cluster den Vorteil, die Leistungsfähigkeit von Systemen zu erhöhen. Werden Dienste auf mehrere Systeme verteilt, kann dem Entstehen von Ressourcenengpässen (sog. „Flaschenhälsen“) vorgebeugt werden.

Dienste für Anwender und Anwendungen

Diese Gruppe von Netzwerkdiensten stellt Benutzern und Anwendungen Dienste wie das World Wide Web, Newsgroups oder E-Mail zur Verfügung. In Firmennetzwerken bieten die Dienste Zugriff von Programmen auf Remote-Drucker oder das Speichern von Daten auf Datei-Servern.

Dienste sorgen dafür, dass beim Einkaufen über das Internet Informationen verschlüsselt werden, um sie vor dem Zugriff durch Dritte zu schützen. Bei einem einzigen Zugriff auf eine Website kommen neben HTTP etwa Cookies, Skripte, Active-X-Steuerdaten usw. zum Tragen, die größtenteils wiederum auf eigene Netzwerkdienste zurückgreifen.

1.2 Protokolle in lokalen Netzwerken

Netzwerkprotokolle

Eine ganze Reihe von Protokollen, die in lokalen Netzwerken Verwendung finden, soll hier kurz vorgestellt werden. Diese sind aus Gründen der Übersichtlichkeit in folgende Gruppen unterteilt:

- Übertragungsprotokolle
- Übermittlungsprotokolle

Die Gruppe der Übertragungsprotokolle bezieht sich dabei auf die Übertragung von Daten und betrifft den hardwarenahen Bereich.

Die Übermittlungsprotokolle beschäftigen sich mit der korrekten Zustellung von Daten über das Netzwerk. Sie gewährleisten, dass Daten vom korrekten Empfänger ausgewertet werden, dass die Weiterverarbeitung im System fehlerfrei und effizient vollzogen wird und dass beschädigte oder verloren gegangene Daten erneut übertragen werden.

Übertragungsprotokolle

Die Gruppe der verwendeten Übertragungsprotokolle in modernen Netzwerken ist nicht mehr so groß wie noch vor wenigen Jahren. Neben Ethernet kommt heutzutage kaum ein kabelbasiertes Protokoll mehr zum Einsatz. Nachdem IBM Anfang 2002 die Produktion von Komponenten für Token-Ring-Netzwerke eingestellt hat, war dessen Verschwinden aus modernen Netzwerken absehbar.

Auch Verfahren wie VG-AnyLAN findet man in kaum einem Netzwerk mehr vor. Gründe hierfür sind neben den Kosten vor allem eine Tendenz des Marktes zur Vereinheitlichung. Dabei muss sich nicht das beste Verfahren durchsetzen, sondern vielleicht das mit der breitesten Unterstützung durch die Hersteller.

Ethernet

Ethernet spezifiziert Software (u. a. Protokolle) und Hardware (u. a. Kabel, Verteiler, Netzwerkkarten) für kabelgebundene Datennetze. Ursprünglich war Ethernet für lokale Datennetze (LANs) gedacht, wird daher auch als LAN-Technik bezeichnet. Daten werden in Form von Datenframes zwischen den im lokalen Netzwerk verbundenen Geräten ausgetauscht. Derzeit sind Übertragungsraten von 10 Mbit/s, 100 Mbit/s (Fast Ethernet), 1000 Mbit/s (Gigabit-Ethernet), 10, 40 und 100 Gbit/s spezifiziert. In seiner ursprünglichen Form erstreckt sich das LAN dabei nur über ein Gebäude; Ethernet über Glasfaser hat eine Reichweite von 10 km und mehr.

Die Ethernet-Protokolle umfassen Festlegungen für Kabeltypen und Stecker sowie für Übertragungsformen. Im OSI-Modell (siehe Kapitel 3) ist mit Ethernet sowohl OSI-Schicht 1 und 2 festgelegt. Ethernet entspricht weitestgehend der IEEE-Norm 802.3. Es wurde ab den 90er Jahren zur meistverwendeten LAN-Technik und hat andere LAN-Standards wie Token Ring verdrängt. Ethernet kann die Basis für Netzwerkprotokolle, z. B. AppleTalk, DECnet, IPX/SPX oder TCP/IP, bilden.

Eine ausführliche, stets aktuelle Übersicht über die vielen verschiedenen Ethernet-Spezifikationen finden Sie unter der Adresse *https://de.wikipedia.org/wiki/Ethernet*.

Übermittlungsprotokolle

Übermittlungsprotokolle stellen sicher, dass Daten auf einem geeigneten Weg vom Sender zum Empfänger übermittelt werden. Sie sind generell in zwei Gruppen zu fassen:

- routingfähige Protokolle
- nicht routingfähige Protokolle

Routingfähige Protokolle enthalten Informationen über logische Strukturen von Netzwerken. Diese Strukturen werden in Form von Netzen und Subnetzen gebildet, die über Router miteinander in Verbindung stehen. Sie dienen dazu, eine Hierarchie im Netzwerk zu implementieren, und können dabei Broadcast-Domänen segmentieren. Werden Daten innerhalb eines logischen Netzes übermittelt, spielt die Hierarchie keine große Rolle. Soll Datenverkehr aber die Grenzen eines Netzes überschreiten, muss im routingfähigen Protokoll eine Information über das Zielnetzwerk enthalten sein, die es den vermittelnden Geräten (Routern) erlaubt, einen geeigneten Weg zu wählen.

In der Vergangenheit wurden verschiedene routingfähige Protokolle verwendet, heutzutage spielen nur noch IPv4 und IPv6 eine Rolle.

Nicht routingfähige Protokolle spielen keine Rolle für den Datenverkehr zwischen Netzwerken. Sie unterstützen keine Untergliederung in logische Netze, sondern gehen davon aus, dass sich alle physikalisch ansprechbaren Knoten eines Netzwerkes im selben logischen Verbund befinden. Daher können sie auch nicht eingesetzt werden, um Datenverkehr zwischen Netzen zu ermöglichen.

Diesem Nachteil steht auf der anderen Seite gegenüber, dass der Konfigurationsaufwand des Protokolls und sein Overhead (der Anteil an zusätzlich zu den Nutzdaten zu übermittelnden Informationen des Protokolls) deutlich geringer ausfallen, als wenn eine Differenzierung von Knoten und Netzen in jedem Header mit enthalten sein muss.

1.3 Namensauflösende Dienste

Rechnernamen und Domänen

Je größer ein Netzwerkverbund ist, desto wichtiger ist es, dass Systeme von den Benutzern in einer nachvollziehbaren Art und Weise adressiert werden können. Darum kommt einer sauberen Nomenklatur (Namensgebungsregel) eine bedeutende Rolle zu.

Es fällt Benutzern und Administratoren deutlich leichter, sich im Netzwerk zurechtzufinden, wenn etwa der Druckserver der Hauptverwaltung in Berlin B-HV-DrSrv01 heißt, als wenn das Gerät als 24Bv27Ssr254 oder über seine IP-Adresse angesprochen werden muss. Hierfür sollten im gesamten Netzwerkverbund eindeutige Regeln verwendet werden, die möglichst in entsprechenden Pflichtenheften definiert und zur Information der Benutzer in öffentlich zugänglichen Dateien dokumentiert werden.

Wird das Netz größer und umfasst es möglicherweise sogar mehrere Länder oder Firmen eines Konsortiums, kommt als weiterer Namensbestandteil die Domäne hinzu. Domänen stellen für Gruppen von Rechnern und Benutzern zentrale Authentifizierungsinstanzen zur Verfügung. So kann etwa die Standortinformation BERLIN als Unterdomäne von FIRMA im Namen enthalten sein. Für den Druckserver der Hauptverwaltungsstelle ergäbe dies einen Namen wie HV-DrSrv01.Berlin.Firma.de.

Namensauflösende Protokolle

Der Wichtigkeit von Namen für Benutzer steht auf Netzwerkseite die Übermittlung von Informationen zwischen logischen Netzen gegenüber. Die Adressierung der Systeme erfolgt über eindeutige Adressen, die sich aus Netzwerkadresse und Knotenadresse zusammensetzen. Damit das Netzwerk in der Lage ist, auf Anforderung eines Benutzers Daten von Forschung-Wks215.Hamburg.Firma.de (Wks steht hier für Workstation) an Produktion-Filer02.Berlin.Firma.de zu übermitteln, muss das System den Namen einer Adresse zuordnen.

Dies kann generell auf mehrere Arten erfolgen. Die Arten der Namensauflösung sind einerseits vom eingesetzten Netzwerkprotokoll abhängig und betreffen andererseits die Betriebssystemumgebung. Die folgende Aufzählung gibt einen Überblick über die gängigen Arten der Namensauflösung:

- namensauflösende Broadcast-Anfragen
- Namenszuordnungen über Dateien
- statische oder dynamische Datenbanken auf Servern

Dienste veröffentlichen

Neben Namen werden in Netzwerken auch Informationen über die Verfügbarkeit von Diensten benötigt. Auch diese Informationen werden über Mechanismen der Namensauflösung publiziert und sollen hier nicht getrennt betrachtet werden, da sie im Prinzip nur eine Sonderform der Namensauflösung darstellen.

Namensauflösende Broadcasts

Innerhalb kleiner Netzwerkverbunde ist es möglich, die Namensauflösung über Broadcasts zu regeln. Gibt ein Benutzer oder eine Anwendung einem System den Auftrag, eine Datenübermittlung mit einem anderen System zu initialisieren, sendet das System als Erstes eine Anfrage an alle anderen Systeme, in der der Empfänger aufgefordert wird, seine Adresse bekannt zu geben.

Diese Art der Namensauflösung belastet das Netzwerk, da die gesamte zur Verfügung stehende Bandbreite durch die Broadcasts nicht mehr für die eigentliche Datenübermittlung genutzt werden kann, und führt dazu, dass alle Netzwerkkarten stets mit der Auswertung von Paketen belastet werden, auch wenn sie in der Regel nicht für sie bestimmt sind. Broadcasts können nur innerhalb logischer und physikalischer Netze oder Subnetze verwendet werden, da diese nicht geroutet werden können, da sonst alle Netze von Broadcasts geflutet würden (sog. Broadcast-Sturm).

Broadcasts zur Namensauflösung werden von NetBIOS, einem proprietären namensauflösenden Dienst von Microsoft, verwendet. Sie unterstützen neben gerouteten Netzwerken auch keine hierarchischen Domänen-Konzepte und werden daher kaum noch eingesetzt.

Namenszuordnungen über Dateien

Eine weitere Möglichkeit der Zuordnung von Rechner-Namen oder Diensten zu Adressen besteht in der Verwendung vorkonfigurierter Dateien, die entsprechende Einträge enthalten. Durch die lokale Verfügbarkeit von Netzwerkinformationen wird die Bandbreite deutlich entlastet, aber es werden andererseits erhebliche manuelle Wartungsarbeiten für das administrative Personal fällig. Daher bietet sich die Arbeit mit Zuordnungsdateien nur dann an, wenn etwa einzelne entfernte Ressourcen in einer gerouteten Umgebung angesprochen werden sollen, in der lokale Rechner-Namen über Broadcasts aufgelöst werden können. Ein weiterer Einsatzbereich von Dateien zur Namenszuordnung ergibt sich, wenn Dienste wie DNS (Domain Name System) verwendet werden, die keine Broadcasts unterstützen.

Die Textdateien `Hosts` und `LMHosts`

Die Informationen werden als Adress-Namenspaare in Textdateien festgehalten und können vom System nur ausgewertet werden, wenn sie an bestimmten Orten im Dateisystem unter einem festen Namen gespeichert sind. Dieser Name ist für NetBIOS-Informationen *LMHosts* und für DNS-Informationen *Hosts*. Der Speicherort ist betriebssystemabhängig. Bei aktuellen Microsoft-Betriebssystemen und UNIX-Systemen ist dies in der Regel das Verzeichnis etc/. Bei der Größe aktueller Netzwerke haben diese Dateien stark an Bedeutung verloren und werden nur in Ausnahmefällen verwendet. Server übernehmen an zentraler Stelle komplett die dynamische Verwaltung der Daten für das gesamte Netzwerk.

Alle NetBIOS-Namensdienste haben durch fehlende IPv6-Unterstüzung stark an Bedeutung verloren.

Statische oder dynamische Datenbanken auf Servern

In großen Netzwerken lassen sich die Informationen über Namens-Adress-Paare nur dann verwalten, wenn diese an zentraler Stelle für das gesamte Netzwerk bereitgestellt werden. Diese Datenbanken können entweder dynamisch von den Betriebssystemen oder weiteren Netzwerkdiensten aktualisiert werden oder sie müssen als statische Einträge von Serveroperatoren gepflegt werden.

Domain Name System (DNS)

Das weltweit am weitesten verbreitete System zur Auflösung von Namens-Adress-Paaren ist das **Domain Name System**. DNS-Server unterstützen dabei ein hierarchisches Namenssystem, das auf Namensräumen mit Domänen und Unterdomänen basiert.

Im Beispiel

server3.buchhaltung.herdt.de

steht der Rechner *server3* in der Unterdomäne *buchhaltung* der Domäne *herdt* im Namensraum *de*. Dieser Namensraum wird auch als „Top-Level-Domain“ bezeichnet.

Adressen in DNS können entweder für lokale Systeme genutzt werden oder im Internet eingebunden sein und so zur weltweiten Adressauflösung verwendet werden. Im Internet sind unterhalb des Stammes ROOT (der bei DNS-Namen durch einen finalen Punkt gekennzeichnet ist) die Namensräume von Staaten und Organisationen angelegt. Diese werden von InterNIC (International Network Information Center), der internationalen Verwaltung für das Internet, oder den nationalen Unterorganisationen (für Deutschland DeNIC; genauer: für alle Domains mit der Länderendung .de) verwaltet. Bei diesen – oder stellvertretend bei Internetserviceprovidern – können sich dann Firmen oder auch Privatpersonen einen Namensraum zuweisen lassen, dessen Verwaltung ihnen dann selbst obliegt.

DNS basiert ursprünglich auf einer statischen Adressdatenbank, in der Zonen für bestimmte Namensräume eingerichtet werden. Diese enthalten untergeordnete Einträge für Rechnernamen, Dienste und Unterdomänen. Insgesamt gibt es etwa 20 unterstützte Eintragstypen. Neben Namen können z. B. auch Diensteinträge (SRV) verwendet werden, die angeben, welche Server bestimmte Dienste für das Netz bereitstellen.

Ein weiteres Merkmal von DNS ist, dass die Datenbank an weitere Server repliziert werden kann. Somit kann in Netzen mit mehreren Standorten die Namensauflösung lokal erfolgen, und WAN-Verbindungen werden entlastet. Allerdings ist es in den meisten Implementierungen von DNS nicht möglich, an den Replikaten Änderungen vorzunehmen. Diese Replikate (sog. sekundäre Zonen) sind schreibgeschützte Kopien der originalen, aktiven Datenbank (der primären Zone). Es handelt sich hierbei um eine Master/Slave-Konfiguration.

Aktuelle Implementierungen des DNS-Serverdienstes erlauben darüber hinaus die Errichtung von Zonen im Multi-Master-Modell, bei denen mehrere aktive DNS-Server die Konfigurationsinformationen zu einer einzelnen Zone gegenseitig aktualisieren können und Änderungen der Zone auf jedem beliebigen beteiligten Server erfolgen können.

Dynamisches DNS (D-DNS)

Zwar basiert DNS ursprünglich auf statischen Datenbanken, aktuelle Implementierungen unterstützen aber auch dynamische Einträge. Zusätzlich kann ein dynamischer DNS-Server von einem DHCP-Server Informationen über die dynamische Vergabe von Adressen an Clients erhalten. Damit wird der Verwaltungsaufwand von DNS deutlich verringert. D-DNS wird beispielsweise von Microsoft-Betriebssystemen ab Windows 2000 oder den aktuellen Linux-Versionen unterstützt.

Einer der Vorteile von dynamischem DNS ist dabei, dass die Daten nicht über eine Datenbankdatei repliziert werden müssen, sondern in einer Datenbank mit Einzelattributreplikation verwaltet werden. Dadurch ist die Belastung des Netzwerkes für die DNS-Replikation deutlich reduziert.

Domain Name System Security Extensions (DNSSEC)

Mit DNSSEC werden die Authentizität und Integrität von Antworten auf DNS-Abfragen gesichert. Übermittelte DNS-Zonendaten werden überprüft, ob sie vom erwarteten, vertrauenswürdigen Absender stammen und ob sie inhaltlich identisch sind mit den Daten, die der Ersteller der Zone autorisiert hat. Zur Erfüllung dieser Aufgaben kommen asymmetrische Verschlüsselungstechniken und Zertifikate zum Einsatz.

Asymmetrische Verschlüsselung bedeutet, dass zwei unterschiedliche Schlüssel verwendet werden: ein privater Schlüssel des Eigentümers, der für die Verschlüsselung oder Echtheitsbestätigung (im Fall von DNSSEC) verwendet wird, und ein zweiter (öffentlicher) Schlüssel, mit dem die Echtheit bestätigt werden kann oder die Daten entschlüsselt werden können. Im Gegensatz dazu stehen symmetrische Verschlüsselungen, bei denen beide Parts den identischen Schlüssel für Ver- und Entschlüsselung verwenden.

Windows Internet Name Service (WINS)

Der Windows Internet Name Service von Microsoft dient dazu, NetBIOS-Namen und -Dienste in einem lokalen Netzwerk für Clients verfügbar zu machen, indem die Namens-Adress-Zuordnung in einer zentralen Datenbank gehalten wird. Jeder WINS-Client ist einem primären WINS-Server zugeordnet, dem er beim Start des Netzwerkadapters seine IP-Adresse, seinen Systemnamen sowie eine Vielzahl weiterer NetBIOS-Informationen mitteilt. Allerdings unterstützt WINS im Gegensatz zu DNS keine hierarchischen Konzepte und ist damit für den Einsatz in sehr großen Systemen nur bedingt geeignet.

WINS wird schon länger als veraltet angesehen. Microsoft empfiehlt – sofern möglich – eine Umstellung auf DNS. Mit der Entdeckung sicherheitsrelevanter Lücken in der WINS-Implementierung aktueller Windows-Versionen im Juni 2017 und der Tatsache, dass Microsoft diese Lücke nicht patchen wird, verbietet sich ein Einsatz von WINS in Produktivumgebungen. Dennoch ist WINS in manchen Unternehmen weiterhin im Einsatz.

1.4 Protokolle aus dem Weitverkehrsbereich

Übersicht

Im Weitverkehrsbereich unterliegt Netzwerkkommunikation grundsätzlich anderen Regeln als in lokalen Netzwerken. Dies hat vor allem damit zu tun, dass im Weitverkehrsbereich hauptsächlich verbindungsorientierte Kommunikation auftritt, die sich deutlich von der auf dem Medium konkurrierenden Kommunikation in lokalen Netzen unterscheidet. Entsprechend bestehen auch andere Anforderungen an WAN-Protokolle als an LAN-Protokolle.

Auf logischer Ebene dagegen ähnelt die Kommunikation im WAN der in komplexen LAN-Umgebungen. Auch im WAN muss üblicherweise zwischen diversen Netzen vermittelt werden und entsprechend kommen hier auch bekannte Netzwerkprotokolle wie IP und IPX (bis etwa 2010) zum Einsatz.

Im Folgenden werden WAN-Dienste kurz vorgestellt. Hier soll nur ein genereller Überblick gegeben werden. Eine Auflistung der einzelnen Protokolle, die diverse Aufgaben im Hintergrund der Dienste erfüllen, würde den Rahmen dieser Übersicht sprengen.

Gängige WAN-Protokoll-Familien

Protokoll	Beschreibung
Asynchronous Transfer Mode (ATM)	Bei ATM handelt es sich um ein Hochgeschwindigkeits-Datenübertragungsverfahren, das im LAN-Backbone-Bereich, in Telefonnetzen und im Internet sowie bei dedizierten Standortanbindungen zum Einsatz kommt. Im ATM-Netzwerk wird eine virtuelle Verbindung zwischen Endsystemen aufgebaut, über die in einem konstanten Strom von 53 Byte großen Zellen Daten verschiedener Anwendungen übertragen werden können. Dabei kommen unterschiedliche Übertragungsgeschwindigkeiten zum Einsatz.
Frame Relay	Frame Relay wurde als Zubringerdienst für ISDN entwickelt und ist ebenfalls ein Hochgeschwindigkeits-Datenübertragungsverfahren im WAN-Bereich. Es ist ein Packet-Switching-Verfahren, d. h., Daten werden entsprechend ihrer Zieladresse über virtuelle Leitungen vermittelt. Die Größe der übertragenen Daten ist dabei unterschiedlich.
Integrated Services Digital Network (ISDN)	Der digitale Telefondienst ISDN spielt auch in Netzwerken eine bedeutende Rolle für Weitverkehrsverbindungen. Hier kommen neben Wählleitungen auch Standleitungen infrage. Im Gegensatz zu den zuvor genannten Diensten werden nur geringere Geschwindigkeiten unterstützt. ISDN war lange Zeit der am weitesten verbreitete WAN-Dienst. Inzwischen ist er weitestgehend durch DSL verdrängt worden. Die Daten, die über ISDN übertragen werden, müssen allerdings in der Regel gekapselt werden. Diese Kapselung kann mittels unterschiedlicher Protokolle wie etwa PPP, L2TP oder PPTP erfolgen.
Digital Subscriber Line (DSL)	DSL erfreut sich großer Beliebtheit. Dies ist vor allem auf die vielfältigen Einsatzmöglichkeiten des Internets im Heimbereich (wie Musik- oder Videostreaming) zurückzuführen. Hier kommt vor allem das Asymetric DSL (ADSL) zum Einsatz, bei dem eine hohe Download-Rate einer niedrigen Upload-Rate gegenübersteht. Bei der Anbindung von Firmennetzen dagegen kommt vor allem symmetrisches DSL (SDSL) zum Einsatz. Neuere Technologien mit höheren Übertragungsraten sind unter den Kürzeln ADSL2+, HDSL oder VHDSL bekannt. Einer der Hauptgründe für die weite Verbreitung von DSL-Verfahren ist, dass bestehende Vernetzungen für die Hochgeschwindigkeits-Datenübertragung genutzt werden können und damit die Kosten für den Umstieg relativ niedrig ausfallen können. Im Zusammenhang mit DSL kommt es häufig zu einer fehlerhaften Namensgebung, wenn von DSL-Modems die Rede ist. In Wirklichkeit handelt es sich bei einem DSL-Modem üblicherweise um eine ATM-Bridge.

1.5 Neue Protokolle an der Grenze zwischen WAN und LAN

Steigender Bandbreitenbedarf im LAN

Mit dem stetigen steigenden Bandbreitenbedarf in lokalen Netzwerken drängen immer mehr Techniken aus dem Weitverkehrsbereich in lokale Netze. Dies verursacht Probleme, da sich Kommunikation zwischen Netzen generell anders verhält als konkurrierende Kommunikation im LAN. Grund für den wachsenden Bandbreitenbedarf sind vor allem die immer größer werdenden Datenmengen, die für heutige Applikationen benötigt werden, und dabei besonders der Trend zu multimedialer Ausschmückung von Dokumenten sowie die Verbreitung von Video- und Audiostreaming. Beim Vergleich der Dateigröße eines reinen Textdokumentes mit einer PowerPoint-Folie wird deutlich, warum heute im Netzwerk Übertragungsgeschwindigkeiten von 10 Mbit/s oder auch 100 Mbit/s oft nicht mehr ausreichen.

Eine Vielzahl von Clients greift z. B. auf wenige Fileserver zu, was bei guter Anbindung (etwa mit Gigabit-Ethernet) für den Einzelnen ausreichend wäre. Da sich aber alle Beteiligten bei erhöhtem individuellen Bedarf die Bandbreite des Servers teilen müssen, kann am Server u. U. keine ausreichende Bandbreite gewährleistet werden.

LANE

Eine der Techniken, die heute zunehmend Einzug ins LAN gefunden hat, ist die ATM-LAN-Emulation (ATM-LANE). Dabei geht es um die Aufgabe, auf einem verbindungsorientierten Medium den quasi verbindungslosen Verkehr und die Namensauflösungsstrategien lokaler Netzwerke zu simulieren.

Die Umsetzung dieser Problematik erfordert vollkommen neue Netzwerkfunktionalitäten, die das LAN im ATM-Netz abbilden. Dazu gehören neue Servertechnologien wie etwa Broadcast-Emulatoren über ATM.

Steigender Adressbedarf

Ein weiteres Problem, das sowohl lokale Netze als auch den WAN-Bereich (und dabei besonders das Internet) betrifft, ist der stetig steigende Bedarf an gültigen IP-Adressen. Durch die Umstellung der Adressen von 32 Bit (IPv4) auf 128 Bit (IPv6) ist dieses Problem prinzipiell gelöst.

Allerdings ist nach wie vor der Einsatz von IPv6 im LAN mit Mehrkosten für neue Hardware (Router und Layer-3-Switches) verbunden. Da außerdem der Verwaltungsaufwand steigt und IPv4 intern nach wie vor funktioniert, wird in den meisten Netzwerken intern nach wie vor IPv4 eingesetzt. Für den internen Netzwerkbetrieb stehen mit den privaten Netzwerkadressen fast 17 Millionen Adressen bereit, die eine Adressierung aller Systeme ermöglichen. IPv6 bedingt seinerseits steigende Bandbreiten, denn der Header von IPv6 ist deutlich größer als der von IPv4.

An IPv6 führt kein Weg vorbei, auch wenn die Ablösung von IPv4 nach wie vor recht schleppend voranschreitet. Im Dezember 2020 fanden etwa 30 % aller Zugriffe auf Google über IPv6 statt. Zu erwarten ist wohl, dass IPv4 und IPv6 häufig und noch längere Zeit parallel eingesetzt werden, wie das in modernen Betriebssystemen unterstützt wird.

Sicherheitsbedarf

Da firmenkritische Daten für den Zugriff über Weitverkehrsverbindungen verfügbar gemacht werden und ein großer Teil der Korrespondenz über Mail stattfindet, kommt dem Thema der Sicherheit eine große Bedeutung zu.

Im Bereich der Zugangskontrolle über WAN-Verbindungen finden Authentifizierungsmechanismen wie etwa RADIUS (Remote Authentication Dial-In User Service) in Verbindung mit Zertifikaten und hardwarebasierten Einmal-Passwortgeneratoren Einsatz. Mit der schnellen Verbreitung von WLANs gewinnen die Verschlüsselung von Daten sowie die geschützte und gesicherte Übertragung an Einfluss. Verschlüsselungen sind durch eine Vielzahl von Faktoren – wie etwa Schlüssellängen, verwendete Algorithmen und Lebensdauer der Schlüssel – für den normalen Anwender meist schwer nachvollziehbar. Gleichzeitig werden auch die Angriffsmethoden immer ausgefeilter, was zu einer Art Wettrüsten zwischen angreifenden und abwehrenden Instanzen führt. Neben Firmenrechnern müssen auch Privatanwender der stetig wachsenden Problematik der Kriminalität im Netz begegnen, indem sie ihre Rechner mit aktueller Schutzsoftware ausstatten.

Der umfangreiche Bereich der Netzwerksicherheit kann in diesem Buch nur gestreift werden, doch sollte sich jeder der Brisanz des Themas bewusst sein und entsprechend handeln. Mails können verschlüsselt versendet werden, Einkäufe im Internet sollten nur über SSL-Verschlüsselung erledigt werden, Vorsicht ist bei Dateidownload und Mailanhängen geboten u.v.m. Diese Maßnahmen erhöhen die Sicherheit, eliminieren aber nicht vollständig die Gefahren. Weiterführende Informationen finden Sie u. a. im HERDT-Buch *Netzwerke – Sicherheit*.

Funkübertragung

In heutigen LANs kommt es vermehrt zum vermischten Einsatz von kabelbasierten Übertragungstechniken und kabellosem Netzwerkverkehr. Waren Richtfunkverfahren noch vor wenigen Jahren vor allem für die Vernetzung von Gebäuden im Einsatz, werden heutzutage oft Notebooks mit WLAN-Adaptern ausgestattet, und auch Bluetooth findet eine immer stärkere Verbreitung. Zusätzlich werden zunehmend tragbare Computer, Tablets und Smartphones eingesetzt, die sich über die Mobiltelefonnetze mittels Hochgeschwindigkeitsverbindungen (z. B. UMTS, HSDPA, LTE) mit dem Internet oder Firmennetzwerken verbinden.

Da immer mehr mobile Geräte mit Computern synchronisiert werden sowie eine stetige Verfügbarkeit von Netzwerken (z. B. Internet) vom Benutzer als selbstverständlich angesehen wird, wird die Funkkommunikation nach und nach zum erwarteten Standard. Da die Frequenzbänder, die zur Datenübertragung verwendet werden können, beschränkt sind, kann es zu Konflikten zwischen Geräten kommen. In größeren Firmen können aus diesem Grund Funknetze überlastet sein, so dass sich Benutzer z. B. zu Hauptgeschäftszeiten nicht mehr einloggen können.

Ausblick

Die Implementierung von IP in lokalen Netzen oder DNS im Intranet ist genau genommen eine Portierung von Weitverkehrstechniken aus dem Internet in den Einsatzbereich lokaler Netze. Klassische, mittlerweile veraltete LAN-Techniken wie etwa NetBEUI oder NetBIOS, die für den Einsatz in kleinen Netzen deutlich effizienter waren, wurden verdrängt. Diese Tendenz – Einsatz eines Standards für alle Bereiche – wird sich in der Zukunft weiter verstärken.

2 Netzwerkmodelle

2.1 Überblick Netzwerkmodelle

Einleitung

Nehmen Sie an, jemand möchte über das Internet auf die HTML-Seite eines Hardwareherstellers zugreifen, um dort einen Treiber für seine Grafikkarte mittels FTP herunterzuladen. Das Betriebssystem des Downloadrechners unterscheidet sich deutlich von dem des Hardwareherstellers. Vielleicht sind auch noch veraltete Geräte und ein Webbrowser eines anderen Herstellers im Spiel.

Im Internet wird seine Anfrage über ATM-Leitungen, Frame-Relay-Verbindungen oder ISDN-Leitungen bis zum Rechner des Herstellers übermittelt, wobei unter Umständen diverse Protokolle zum Einsatz kommen.

Aufgrund der Vielzahl an beteiligten Hard- und Softwarekomponenten wird eine klare Strukturierung der Kommunikation über das Netzwerk benötigt. Nur so kann gewährleistet sein, dass die diversen Produkte an den Schnittstellen zwischen Netzhardware, Kommunikationsprotokollen und Software fehlerfrei miteinander kommunizieren.

Schichten

Um die Schnittstellen zwischen Komponenten der Kommunikation zu vereinheitlichen, wird ein theoretisches Modell verwendet, das die einzelnen Komponenten und Aufgaben bestimmten Schichten zuordnet. Diese Schichten weisen standardisierte Schnittstellen zu den benachbarten Schichten auf. Im Einzelfall können bestimmte Pakete von Schichten zusammengefasst werden, wenn es z. B. nur um Hardware geht oder nur Softwareanwendungen betroffen sind. Es ist jedoch aus Kompatibilitätsgründen notwendig, ein generelles Modell zur Standardisierung zu verwenden.

Heute werden vor allem drei Modelle zur Darstellung von Netzwerkkommunikation verwendet. Sie unterscheiden sich vor allem durch die Genauigkeit, mit der dabei die einzelnen Schichten definiert sind. Außerdem gibt es Unterschiede in der Generalisierung der Modelle. Dabei gilt: Je allgemein gültiger ein Modell sein soll, desto exakter muss jede einzelne Funktion beschrieben werden, die auf einer Schicht liegt.

Die drei gängigsten Modelle sind:

- das ISO/OSI-Modell
- das DoD-Modell
- das TCP/IP-Modell

2.2 Das OSI-Modell

Geschichte

Das OSI-Modell (auch ISO/OSI-Modell) wurde 1984 von der International Organization for Standardization (ISO), einem Zusammenschluss von Normungsorganisationen, entwickelt, um Kommunikationsabläufe in Computernetzen in einem normierenden, theoretischen Modell (auch Referenzmodell genannt) abzubilden. Der Modellname OSI (Open Systems Interconnection) weist auf den Ansatz hin, mit dem Modell die Kommunikation über unterschiedlichste technische Systeme zu ermöglichen.