Netzwerke

Protokolle und Dienste

(Stand 2024)

Dipl.-Ing. (FH) Oliver Gauer, Andreas Dittfurth

1. Ausgabe, November 2024

ISBN 978-3-98569-226-2

NWPD_2024

Plus

HERDT

Bevor Sie beginnen …

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*

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.

1

Protokolle und Dienste – Definition und Unterschiede

1.1 Protokolle

Allgemeine Umschreibung

Ein Protokoll legt – ganz allgemein ausgedrückt – Verhaltens- oder Verfahrensregeln fest. Haben Sie schon einmal ein weibliches Mitglied der britischen Königsfamilie anlässlich eines offiziellen Anlasses ohne Hut gesehen? Sicher nicht, denn das royale Protokoll schreibt seit den 1950er Jahren vor, dass weibliche Familienmitglieder nicht ohne Hut erscheinen dürfen.

Protokolle in der IT

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 meist mehrere Protokolle beteiligt.

Protokolle in Netzwerken lassen sich grob in drei Gruppen unterteilen:

- Protokolle für die physische Datenübertragung
- Protokolle für die Wegermittlung und den Pakettransport
- Protokolle für den Datentransport

Protokolle für die physische Datenübertragung

Diese Gruppe von Protokollen beschreibt Verfahren, wie Daten über ein bestimmtes Medium transportiert werden müssen. Die Protokolle definieren die Spannungspegel der Signalströme, die detaillierte Aderbelegungen oder die Spannungswerte ab/ bis eine logische Null oder eine logische Eins dargestellt werden.

Im Ethernet-Protokoll wird die Art des Zugriffs auf ein WLAN (CSMA/CA = Carrier Sense, Multiple Access with Collision Avoidance; etwa: Leitungsabfrage bei vielfachem Zugriff mit Kollisionsvermeidung) festgelegt.

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)
  Beispiel: RIP, OSPF
- Protokolle zum Transport von Paketen zwischen Netzwerken (geroutete Protokolle)
  Beispiel: IP, AppleTalk

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.

1.2 Dienste in der IT

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 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.

Dienste in Netzwerken lassen sich – wie die oben genannten Protokolle – grob in drei Gruppen unterteilen:

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

Netzwerk-Dienste für den Netzwerkbetrieb

Netzwerk-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.

Netzwerk-Dienste für Betriebssysteme

Es gibt eine ganze Reihe von Netzwerk-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 (Anmelde-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 Anwendungs-Servern 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.

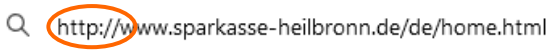
Lastenverteilung (Load balancing)

Neben der Ausfallsicherheit bieten Cluster den Vorteil, die Leistungsfähigkeit von Systemen zu erhöhen. Werden Dienste auf mehrere Systeme verteilt, kann dem Entstehen von Ressourcen-engpässen (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 Empfang und Versand von E-Mails zur Verfügung. In Firmennetz-werken bieten die Dienste Zugriff von Programmen auf Remote-Drucker oder das Speichern von Daten auf Datei-Servern.

Nutzen Dienste kryptografische Verfahren, sorgen diese dafür, dass beim Einkaufen über das Internet Informationen verschlüsselt werden, um sie vor dem Zugriff durch Dritte zu schützen. Bei einem Zugriff auf eine Website via *HTTP* ändert sich die URL zu *HTTPs.* Die Kommunikation zwischen dem Browser und dem Webserver (Übertragung von Passwörten etc.) wird verschlüsselt:



URL während der Eingabe

URL nach der Eingabe auf HTTPs geändert

1.3 Gegenüberstellung Protokoll – Dienst

	Protokoll	Dienst
Definition	Ein Satz von Regeln und Standards, die bestimmen, wie Daten zwischen Geräten oder Systemen über ein Netzwerk übertragen werden	Eine Funktion oder Anwendung, die auf einem Server bereitgestellt wird und über ein Netzwerk von Clients verwendet werden kann
Funktion	Regelt die Kommunikation und Datenübertragung	Bietet spezifische Funktionen oder Ressourcen an
Beispiel	HTTP (Hypertext Transfer Protocol), TCP (Transmission Control Protocol), FTP (File Transfer Protocol)	Webserver (z. B. Apache, Nginx), E-Mail-Server (z. B. Microsoft Exchange), DNS-Server
Schicht im Netzwerkmodell	Meistens auf der Kommunikations- oder Transportschicht des OSI-Modells angesiedelt	Meistens auf der Anwendungs-schicht des OSI-Modells anzutreffen
Zweck	Stellt sicher, dass Daten korrekt und zuverlässig zwischen Systemen über-tragen werden	Bietet eine bestimmte Dienst-leistung oder Ressource für Benutzer oder andere Systeme an

	Protokoll	Dienst
Beziehung zueinander	Protokolle werden von Diensten verwendet, um Daten zu übertragen oder zu empfangen.	Dienste nutzen Protokolle, um ihre Funktionen über Netzwerke bereitzustellen.
Beispielhafte Nutzung	HTTP wird verwendet, um Webseiten von einem Webserver zu einem Webbrowser zu übertragen.	Ein Webserver-Dienst hostet Webseiten und verwendet das HTTP-Protokoll zur Kommunikation mit Webbrowsern.
Konfiguration	Wird oft in Netzwerkkonfigurationen und Systemen spezifiziert (z. B. Portnummern, Sicherheitseinstellungen)	Wird auf Servern konfiguriert, um die spezifischen Funktionen bereitzustellen (z. B. Einrichten von E-Mail-Konten, Hosting von Websites)

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.

1.4 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 in SOHO- uns Unternehmensnetzwerken Übertragungsraten von 10 Mbit/s, 100 Mbit/s (Fast Ethernet), 1000 Mbit/s (Gigabit-Ethernet), 10, 40 und 100 Gbit/s üblich. Im Bereich von Rechenzentren oder großen Netzwerk-Provider sind Verbindungen mit 200, 400 und seit Oktober 2022 800 Gbit/s (DE-CIX in Frankfurt/ Main) verfügbar.

In seiner ursprünglichen Form erstreckt sich das LAN dabei nur über ein Gebäude; Ethernet über Glasfaser hat zwischenzeitlich eine Reichweite von 10 km und mehr erreicht.

Die Ethernet-Protokolle umfassen Festlegungen für Kabeltypen und Stecker sowie für Übertragungsformen. Im OSI-Modell 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 (Payload) zu übermittelnden Informationen des Protokolls) deutlich geringer ausfallen, als wenn eine Differenzierung von Knoten und Netzen in jedem Header mit enthalten sein muss.

1.5 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 Netzwerk-Computer mit einem „sprechenden Namen“ versehen werden. So kann dieser statt mit seiner für uns Menschen unhandlichen IP-Adresse mit seinem Namen angesprochen werden.

Beispiel 1:

Dieses Buch können Sie unter 13.95.212.204 bestellen – nicht leicht zu merken? Tippen Sie stattdessen in Ihren Browser *herdt.de* und nutzen Sie die Namensauflösung des Internets!

Beispiel 2:

Für den in der Berliner Hauptverwaltung stehenden ersten Druckserver könnte der Name BE-HV-DRSVR-01 vergeben werden. 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 BEISPIELFIRMA im Namen enthalten sein. Für den Druckserver der Hauptverwaltungsstelle ergäbe dies einen Namen wie HV-DRSRV-01.BERLIN.BEISPIELFIRMA.DE. Domänen und Unterdomänen werden mit einem Punkt voneinander getrennt. Die Top-Level-Domain, also die oberste Hierarchieebene, stellt in diesem Beispiel die Domäne „DE“ für Deutschland dar. Ihr untergeordnet ist die Domäne „BEISPIELFIRMA“, dieser ist die Domäne „BERLIN“ untergeordnet. So kann eine hierarchische Unternehmensstruktur in der Benennung der einzelnen Geräte im Netzwerk anhand der Namensvergabe erreicht werden. An diesem Beispiel ist gut zu erkennen, dass spätere Fusionen eine Umbenennung von Geräten notwendig machen können. Dies zieht erheblichen Verwaltungs- und Konfigurationsaufwand nach sich und sollte daher unbedingt vermieden werden.

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 (IP-)Adressen, die sich aus Netzwerkadresse und Knotenadresse zusammensetzen. Damit das Netzwerk in der Lage ist, auf Anforderung eines Benutzers Daten von FORSCHUNG-WKS-215.Hamburg. BEISPIELFIRMA.DE (WKS steht hier für Workstation) in der Hauptverwaltung in Berlin zu drucken, also an HV-DRSRV-01.BERLIN.BEISPIELFIRMA.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 im Netzwerk, 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, mittlerweile wird DNS stillschweigend immer als dynamisches DNS verstanden.

Kommt zur IP-Adressvergabe ein DHCP-Server zum Einsatz, verändern sich im Laufe der Nutzung die an die Clients vergebenen IP-Adressen. Der (dynamische) DNS-Server und der DHCP-Server tauschen diese Änderungen an den IP-DNS-Name-Paar untereinander aus. 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)

DNSSEC ist ein Sicherheitsprotokollerweiterung von DNS. Mit DNSSEC werden die Authentizität und Integrität von Antworten auf DNS-Abfragen gesichert. Dies schützt vor bestimmten Arten von Cyberangriffen, insbesondere vor DNS-Spoofing oder Cache Poisoning, bei denen Angreifer gefälschte DNS-Antworten senden, um Benutzer auf falsche Websites umzuleiten. 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.

Exkurs: Asymmetrische Verschlüsselung

Funktionsweise der asymmetrischen Verschlüsselung (Public-Key-Verschlüsselung)

Im Gegensatz zur symmetrischen Verschlüsselung existiert bei den asymmetrischen Verschlüsselungen für jeden Teilnehmer ein Schlüsselpaar. Dieses Schlüsselpaar setzt sich aus einem geheimen Schlüssel (Private Key) und einem öffentlichen Schlüssel (Public Key) zusammen.

Der geheime Schlüssel wird niemals weitergegeben und darf nur dem Besitzer zugänglich sein. Der öffentliche Schlüssel dagegen muss frei zugänglich sein. Öffentlicher und privater Schlüssel stehen in einem bestimmten Verhältnis zueinander.

Mittels komplexer mathematischer Funktionen wird aus dem ersten Schlüssel der zweite Schlüssel berechnet und umgekehrt. Die beiden Schlüssel stehen also in einer mathematischen Abhängigkeit zueinander.

Wichtig:

Das Verfahren zur Erzeugung des Schlüsselpaares muss so komplex sein, dass es für Unbefugte keine effiziente Möglichkeit geben darf, nachträglich aus dem öffentlichen Schlüssel den privaten Schlüssel zu berechnen.

„Effizient“ bedeutet in diesem Zusammenhang, dass der zu erwartende Ertrag durch das Knacken des Schlüssels in keinem sinnvollen Verhältnis zum notwendigen Aufwand steht.

Ablauf der asymmetrischen Verschlüsselung

- Alice will an Bob eine asymmetrisch verschlüsselte Nachricht senden.
- Bob stellt Alice seinen Public Key (seinen öffentlichen Schlüssel) zur Verfügung, z. B. durch Veröffentlichung im Internet.
- Alice verschlüsselt die Nachricht mit dem Public Key von Bob und verschickt die Nachricht. Nur Bob kann die Nachricht mit seinem Private Key (seinem privaten Schlüssel) wieder entschlüsseln.