

Netzwerke

Stand: **September 2009 / Axel Wagner**

Vorbemerkungen

Dieses knappe Skript stützt sich auf vielfältige im Internet frei zugängliche Informationen (siehe Linkliste). Es ist für den Unterricht Informatik ab Klasse 10 konzipiert und soll elementare Grundbegriffe und technische Zusammenhänge vermitteln.

Oft sind bei Schülern nur punktuelle und wenig strukturierte Kenntnisse (wenn überhaupt) über Netzwerke vorhanden.

Mit diesem Skript soll ein Einstieg in die Funktionsweise des Internet und seiner Dienste gegeben werden.

Das Skript stellt ein Gerüst zur Vorbereitung dar und ist für den Unterricht entsprechend zu kürzen.

Inhaltsverzeichnis

Einführung.....	3
Architektur eines Netzwerks.....	4
Netzwerkprotokolle.....	7
Domain, DNS, URL.....	8
Adressierung.....	10
IP-Adressen.....	10
IP-Adressklassen.....	11
Protokolle & Dienste.....	14
Protokolle und Dienste in der Anwendungsschicht.....	16
Router, Routing.....	18
IP-Routingtabelle.....	19
Grundlagen TCP/IP.....	21
Das Schichtenmodell.....	21
TCP (Transport Control Protocol).....	24
IP (Internet Protocol)	28
Die Netzzugangsschicht.....	29
Sicherheit in Netzwerken.....	30
Firewall.....	30
Firewall-Technologien.....	31
TCP/IP-Hilfsprogramme.....	35
DMZ - Demilitarisierte Zone.....	42
DMZ-Host.....	42
Quellen & Literatur.....	44

Grundlagen Netzwerke

Einführung

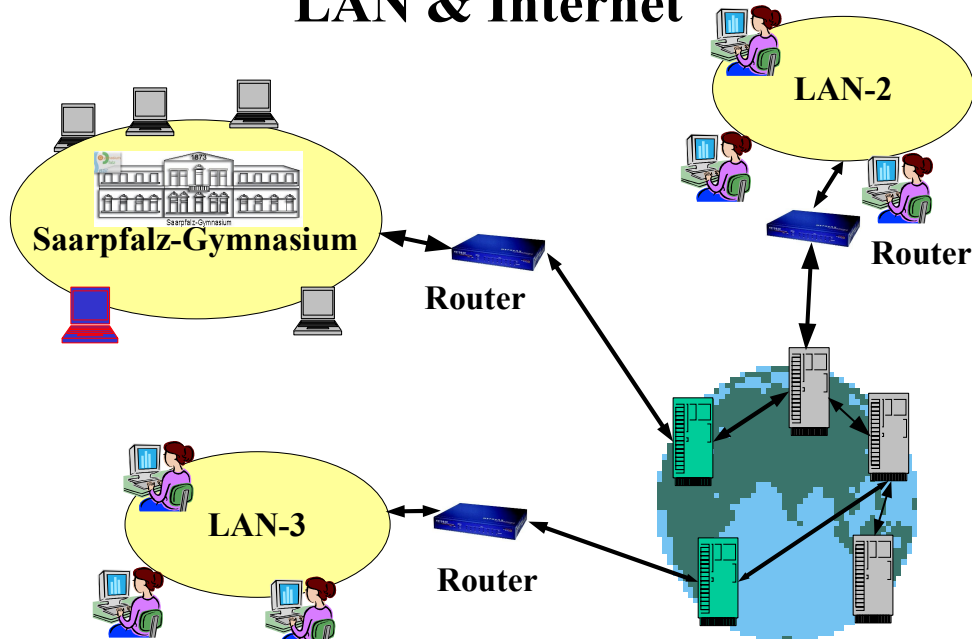
Als Folge des Sputnik-Schocks 1957 wurde Ende der 60er-Jahre von einer Projektgruppe des amerikanischen Verteidigungsministeriums (ARPA) ein Computer-Netz konstruiert, das viele Teilnetze ohne zentrale Kontrolle zu einem weltumspannenden Netzwerk verbinden kann. Bis Anfang **1970 waren 4 Netzknoten installiert**. In den Jahren 1974 bis 1978 wurde das **TCP/IP-Protokoll** entwickelt: Das Internet war geboren.

Das Internet ist ein offener Computer-Verbund, der seinen Anfang an US-amerikanischen Universitäten und Forschungsstätten nahm. Es war so gestaltet, dass bei Zerstörung eines Teiles der Rest weiterhin funktionieren sollte. Es gibt kein "Hauptkabel" und keinen "Zentralcomputer". Es wurde von Wissenschaftlern und Universitäten, kommerziellen Unternehmen weiterentwickelt. Heute ist es jedermann über sog. Provider zugänglich. Es handelt sich nicht um ein einheitliches Netzwerk, sondern um einen Zusammenschluss unterschiedlichster Rechner und Netzwerke. Jedes einzelne Netz wird separat verwaltet und unterliegt somit auch keiner globalen Kontrolle.

Jede Information wird in Form von Datenpaketen zum Empfänger transportiert. Der Weg ist dabei nicht vorgegeben. Die Übertragungswegen können Kupferkabel, optische Kabel, Telefonleitungen oder Satellitenverbindungen sein.

Damit dieses Netz weltweit funktioniert, müssen **Standards** für die Kennung von Rechnern und Standards für die Übertragungstechnologie definiert sein.

LAN & Internet



Architektur eines Netzwerks

[3]

Die Architektur beschreibt die Art des Zusammenwirkens der Netzwerkrechner.

Peer-to-Peer-Netzwerk

Bei dieser Netzwerkart ist jeder Rechner gleichberechtigt.

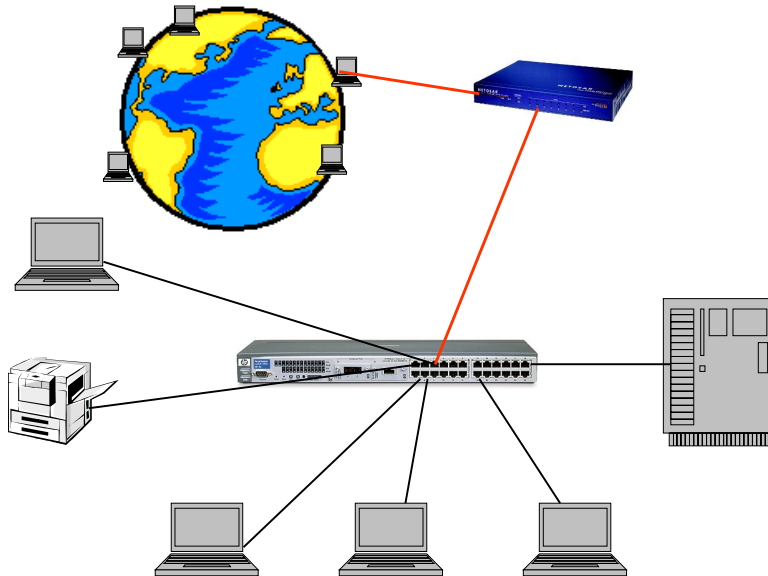
Client-Server-Netzwerk

Server: Sie stellen sog. Dienste (von anderen nutzbare Betriebsmittel) bereit. Dienste können Programme, gemeinsamen Speicherplatz, Drucker oder Zugriff auf das Internet ermöglichen

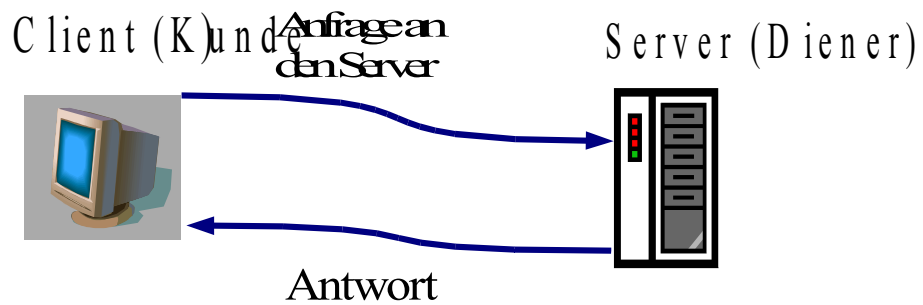
Beispiele: Webserver, Mailserver, Druckserver

Clients (Workstations) sind Nutzer der Dienste.

LAN (Local Area Network)



Client-Server



Ein Server ist ein Programm, welches eine Datenanfrage von einem Client (-Programm) empfängt und Antwortdaten liefert.

LAN (Local Area Network)

Gruppe von Computern, die innerhalb einer eng begrenzten Ausdehnung, z.B. innerhalb eines Hauses oder mehrerer Gebäude vernetzt sind. Die Computer besitzen meistens einen gemeinsamen Adressbereich.

WAN (Wide Area Network)

Verbindet man Netzwerke über sog. Router, dann entsteht ein Weitverkehrsnetz (WAN). Ein WAN ist in seiner Ausdehnung nicht begrenzt. Ein Beispiel für ein WAN ist das Internet.

Clients, Server, Drucker, Router sind über Datenkabel (TP-Kabel, Glasfaser) miteinander verbunden. **Anmeldungen am Netz, Daten- und Programmanforderungen, Druckaufträge** sowie **Internetzugriffe** werden vom Netzwerkbetriebssystem kontrolliert und bearbeitet.

Das Netzwerkbetriebssystem verwaltet die **Benutzer und ihre Rechte**. Es gibt Lese-, Schreib- und Ausführungsrechte für Dateien und für Verzeichnisse, Druckrechte oder Rechte für den Internetzugriff. Über diese Rechte lässt sich ein Netzwerk sicher einrichten.

Netzwerkprotokolle

Damit Computer im Netzwerk sich miteinander verständigen können, müssen Sie die gleiche "Sprache sprechen". Es muss also verbindlich festgelegt sein, wie die Informationen von Computer A zu Rechner B kommen. Diese Aufgabe übernehmen in Netzen die Protokolle. Grundlage ist, dass die beteiligten Geräte über Adressen eindeutig identifizierbar sind.

Das **TCP/IP Protokoll**. Das **T**ransmission **C**ontrol **P**rotocol kontrolliert dabei die **Übertragung**.

Das **Internet Protocol** kontrolliert die **Adressierung**. Wie sprechen deshalb auch von IP-Adresse.

Adressierung

Alle Geräte im Netzwerk benötigen eine Adresse

IP-Adressen bestehen aus 4 Dezimalzahlen zwischen 0 und 255, die durch je einen Punkt getrennt sind (*dotted decimal notation*).

Beispiel: 192.109.53.23

Routing

Die Daten suchen sich mit Hilfe der Router ihren Weg zum Ziel selbstständig.

Domain, DNS, URL

Da IP-Adressen nur schwer zu merken sind, gibt es zusätzlich Domännennamen, die den IP-Adressen eindeutig zugeordnet sind.

Eine **Domain** (dt. Domäne) identifiziert einen Computer eindeutig ohne Verwendung der **IP-Adresse**.

Im obigen Beispiel ist 192.109.53.23 gleichbedeutend mit der Domain **saar.de**

Der sog. **Domain Name Service** (DNS) im Internet ist für die Umsetzung von Namen in IP-Adressen zuständig.

DNS ist vergleichbar mit einem Telefonbuch, das die Namen der Teilnehmer in ihre Telefonnummer auflöst.

Vorteil: Der Benutzer kann mit Namen arbeiten, der Computer verwendet die zugehörige Adresse.

Aufgabe: Wie kann man einen DNS-Error mit Hilfe des Browsers erzeugen?

URL

Normalerweise tippt man den Domännennamen als Teil einer Webadresse (URL) im Browser ein.

Jeder Name einer Domain besteht aus einer Folge von durch Punkten getrennte Namen.

Die englische Bezeichnung **Top Level Domain (TLD)** bezeichnet dabei den letzten Namen dieser Folge.

Beispiele für TLD

de	Deutschland
fr	Frankreich
ch	Schweiz
edu	USA (Computer im US-Bildungssystem)
com	USA (Computer in US-Firmen)
gov	USA (Computer in der US-Verwaltung)

Beispiele für Domains saar.de frweb.cs.uni-sb.de

Übung: Domäne über IP-Adresse und Domainname ansprechen (Ping-Befehl oder Browser)

Über den Domainnamen kann man einen Computer (eine Computergruppe) eindeutig identifizieren. Damit auch eine einzelne HTML-Datei ansprechbar sein soll, muss eine vollständige Adressangabe, die URL (Uniform Resource Locator) angegeben werden.

Beispiel: Beim Aufruf der URL <http://www.saar.de/~awa/infsek1/infsek1.htm>

wird die URL in seine Bestandteile zerlegt:

Protokoll: http (für Webseiten)

Nach dem Doppelpunkt folgt // Dies ist der **Beginn einer absoluten Adressangabe.**

Domainname: [saar.de](http://www.saar.de)

Verzeichnis: ~awa

Unterverzeichnis infsek1

Datei: infsek1.htm

Oft (nicht zwingend) steht vor dem Domänennamen die Angabe "www". Dies ist ein Verzeichnis, in dem sich die öffentlichen Dokumente befinden.

Root Zone Database

<http://www.iana.org/domains/root/db/>

Adressierung

Quelle: [10]

Das Internet besteht aus Millionen von Computern, welche miteinander verbunden sind. Ist ein LAN mit dem Internet verbunden, wird es damit auch zu einem Teil des Internet.

Damit alle LAN's miteinander Daten austauschen können, müssen sie voneinander **unterscheidbar** sein.

1981 wurde das IP-Protokoll eingeführt. Jedes System im Internet besitzt eine eindeutige 32-Bit-Adresse.

- IP-Adressen sind weltweit eindeutig
- InterNIC (*Inter Network Information Center*) ist die zentrale Vergabestelle
- DENIC ist für Deutschland zuständig
- Es gibt unterschiedliche Adressklassen für verschiedene Anzahlen von IP-Adressen

IP-Adressen

Jede Quelle oder Ziel von IP-Paketen muss eine IP-Adresse besitzen. IP-Adressen besitzen eine Länge von 32 Bit.

IP-Adressen können nicht beliebig gewählt werden

IP-Adressen bestehen aus 4 Dezimalzahlen, die durch je einen Punkt getrennt sind (*dotted-decimal notation*)

Beispiel: 192.168.1.19

Binär: 11000000.10101000.00000001.00010011

Der vordere Teil (*192.168.1*) gibt an, zu welchem Netz der Rechner gehört (*Netzwerk-ID*)

Der hintere Teil (*.19*) beschreibt den Rechner (*Host-ID*)

Zur Unterscheidung von Netzwerk-ID und Host-ID dient die **Subnetzmaske**. Die auf 1 gesetzten Bit der Subnetzmaske markieren in der 32-Bit-Adresse die Netzwerk-ID.

Beispiel: 255.255.255.0

Binär: 11111111. 11111111. 11111111. 00000000

Die Binärstellen, die das Netzwerk kennzeichnen, werden mit der Subnetzmaske angegeben. Die 0-Bit der Subnetzmaske geben an, dass die Bit der IP-Adresse ignoriert werden.

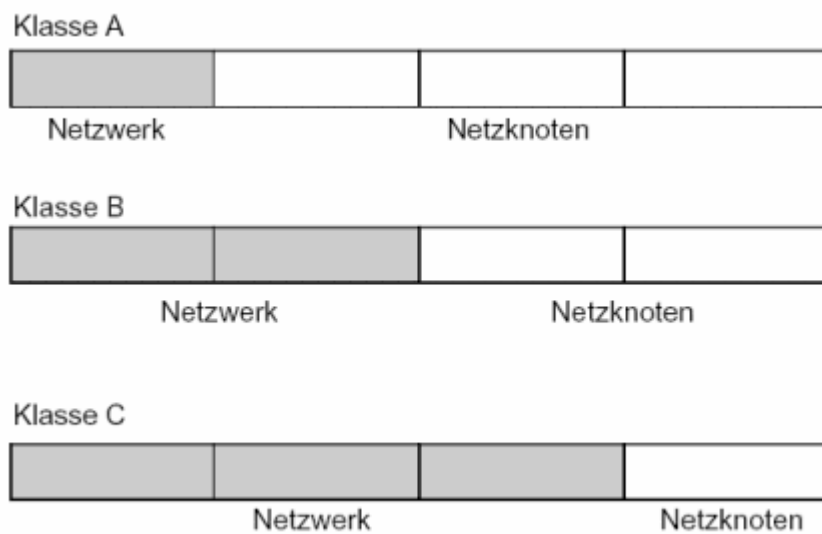
Aufgaben

Wie viele Geräte (Rechner, Router, ...) lassen sich theoretisch mit IPv4 adressieren?

Wie viele Geräte (Rechner, Router, ...) lassen sich theoretisch mit IPv6 (128 Bit) adressieren?

Wie viele IP-Adressen sind dies pro m² der Erdoberfläche? (Erdradius = 6.378.000 m)

IP-Adressklassen



Alle Adressen haben die Form **Netzwerk-ID gefolgt von Host-ID**

Jedes LAN besitzt eine Netzwerk-ID und jeder darin befindliche Computer (Knoten) eine sog. Host-ID.

Übersicht über die Adressklassen A - C

- Netzwerk- und Host-ID können unterschiedlich lang sein.
- Weder Netzwerk-ID noch Host-ID dürfen nur Nullen und Einsen enthalten

In den Klassen A - C besitzen die niedrigste und höchste Host-ID eine besondere Bedeutung:

Die niedrigste Host-ID 0 ist nicht erlaubt (alle Bit der Host-ID sind 0).

Die höchste Host ID 255 (alle Bit der Host-ID sind 1) ist die sog **Broadcastadresse, mit der alle Host erreicht werden können**. Auch die Host-ID 255 darf nicht vergeben werden.

Netzklasse	Netz-ID	Host-ID	Subnetz-Maske	Anzahl Netze/max. Netzgröße
A	0... 127	.x.y.z	255.0.0.0	125 /16,777,214 Rechner (nicht 128 Netze, s. Ausnahmen)
B	128.0... 191.255	.y.z	255.255.0.0	16.384/65.534 Rechner
C	192.0.0... 223.255.255	.z	255.255.255.0	2.097.152/254 Rechner

Klasse A

Das erste Bit ist 0.

Das Netzwerkpräfix umfasst **8Bit**: (0.x.y.z) bis (127.x.y.z). Es gibt 125 A-Klassen, da die Klassen 0.x.y.z und 10. x.y.z nicht vergeben sind und 127.x.y.z für andere Zwecke reserviert ist.

Für die Host-ID verbleiben 24 Bit. Somit sind $2^{24} - 2 = 16,777,214$ Hostadressen möglich.

Klasse B

Die beiden ersten Bit sind 10, der Rest (14 Stellen) ist beliebig.

Das Netzwerkpräfix ist **16 Bit** lang: 128.0.x.y bis 191.255.x.y. Es können $2^{14} = 16384$ B-Klassen verwaltet werden. Die Zahl der Hosts beträgt $2^{16} - 2 = 65534$.

Klasse C

Die drei ersten Bit sind 110, der Rest der drei Bytes ist beliebig.

Das Netzwerkpräfix ist **24 Bit** lang 192.0.0.x bis 223.255.255.x.. Dies ergibt $2^{21} = 2,097,152$ unterschiedliche Netzwerke. Es können $2^8 - 2 = 254$ Rechner verwaltet werden.

Klasse D erste 4 Bits "1110"

Klasse E erste 4 Bits "1111"

Reservierte IP-Adressen

In lokalen Netzwerken kann man dafür reservierte IP-Adressen vergeben. Diese sind im „freien“ Internet nicht erlaubt.

Adresse	Bedeutung
0.0.0.0	Keine Netzadresse im eigentlichen Sinne. Diese Adresse wird für das Routing verwendet.
10.0.0.0 bis 10.255.255.255	Dieser Bereich des Klasse A Netzes wird nicht geroutet ("private" Adressen für lokale Netze).
127.0.0.1	Diese IP-Adresse bezeichnet den lokalen Rechner.
172.16.0.0 - 172.31.255.255	Wie 10.x.y.z, jedoch für ein Klasse B Netz.
192.168.x.y	Wie 10.x.y.z, jedoch für ein Klasse C Netz.

Die Adresse 0.0.0.0 Alle Pakete mit unbekannter Adresse werden an einen Default-Router gesendet.

Durch die Kombination von Netzwerk- und Hostadresse ist der Rechner eindeutig identifiziert.

Beispiel: 194.95.249.240

Die Adresse gehört zum Klasse-C-Netzwerk 194.95.249 und besitzt die Host-ID 240

Protokolle & Dienste

Quellen: [7] und [8]

Die Bedeutung des Wortes Protokoll im Alltag:

Zusammenfassung wichtiger Ergebnisse, Strafzettel, Niederschrift einer Aussage, Stundenprotokoll, diplomatisches Zeremoniell, internationales Abkommen und **Übertragungsprotokoll**.

Wenn wir das Medium **Telefonleitung** betrachten, fällt auf, dass es verschiedene Möglichkeiten gibt, es zu nutzen:

Es gibt die Dienste Telefon, Fax und „Internet“.

Als **Dienste** bezeichnet man spezielle Programme, um den Datentransport in einem Netzwerk abzuwickeln. Dienste wickeln die Datenübertragung nach einem genormten **Protokoll** ab.

Beispiele für Dienste: WWW, E-Mail, FTP, Internetradio, ...

Was ist ein Protokoll und wozu wird es benötigt?

Um Daten zwischen zwei Geräten senden zu können, muss der Ablauf der Übertragung normiert sein: Man spricht von einem Protokoll.

Mit Protokollen wird sichergestellt, dass die

- richtigen Partner miteinander kommunizieren.
- die Daten korrekt übertragen werden.
- die Zustellung der Daten bestätigt wird.
- die Daten nicht unendlich im Netz herum wandern (Zeitkontrolle).
- Fehler erkannt und korrigiert werden.

Beispiel 1: Abfolge beim Telefonieren

1. Aufbau der Verbindung: Anrufer startet die Kommunikation; der Angerufene meldet sich mit Namen; der Anrufende meldet sich (Handshake)
2. Führen des Gesprächs
3. Verabschiedung und Abbau der Verbindung

Im Protokoll wird auch eine **Fehlerbehandlung** vereinbart:

Die Telefonverbindung wird unterbrochen. Wenn beide Gesprächsteilnehmer gleichzeitig einen Rückruf starten, führt dies zu keiner Verbindungsaufnahme.

Lösung: Der **Anrufer** startet im Falle einer Unterbrechung den Rückruf.

Definition

Ein Protokoll ist eine Sammlung von Regeln, die elektronische Kommunikation zwischen zwei Systemen (Rechnern) ermöglicht. Es muss auch festgelegt sein, wie z.B. Übertragungsfehler behandelt werden.

Beispiel 2: Funkverkehr (siehe Heiko Holtkamp, Einführung in TCP/IP)

Im Funkverkehr bestätigen die Kommunikationspartner den Empfang der Nachricht mit 'Roger' und signalisieren den Wechsel der Sprechrichtung mit 'Over'. Zum Beenden der Verbindung wird die Nachricht 'Over and out' verwendet.

Aufgabe: Fülle die Tabelle aus.

Medium	Dienst
Funkwellen (irdisch)	
Deutsche Post	
Straße	
Satellit	
Fernsehkabel	
Stromkabel	

Protokolle und Dienste in der Anwendungsschicht

Quellen: [7], [6], [9]

Hinweis: Oft werden die Begriffe Protokoll und Dienst synonym gebraucht.

Abgrenzung Protokoll – Dienst

Eng verwandt mit dem Konzept des **Protokolls** ist das Konzept des Kommunikations**dienstes**. Während Protokolle sich auf das interne Verhalten aus Sicht der beteiligten Protokollinstanzen beziehen, beschreibt der zugehörige Kommunikationsdienst das abstrakte Verhalten aus Sicht der Dienstanutzer im Sinne einer Schnittstellenbeschreibung. Das Protokoll macht Annahmen über die Dienste der tieferen Schicht, der Dienst über die Dienstanutzer. Genutzt wird ein Dienst von der nächst höheren Schicht, die diesen verfeinert und qualitativ verbessert wiederum bereitstellt. Die Schicht n stellt der Schicht (n+1) Dienste, unter Verwendung von Diensten der Schicht (n-1), zur Verfügung.

Dienste, Protokolle und Programme (Werkzeuge)

Dienst	www	E-Mail	DNS
Protokoll	http	POP3, SMTP	Meistens UDP
Programm	Browser	Mailprogramm	(Browser)

- WWW-Dienst mit dem Protokoll HTTP Hypertext Transfer Protocol
- E-Mail-Dienst mit den Protokollen SMTP und POP3 (Simple Mail Transfer Protocol, Post Office Protocol 3)
- DNS (Domain Name Service)

HTTP oder „Hypertext Transfer Protocol“ wird zum Übertragen von Webseiten benutzt.

SMTP ist ein elektronischer Dienst zum Versenden der Mail.

POP3 oder „Post Office Protocol 3“ wird dazu verwendet, E-Mails abzuholen.

Mit DNS werden Domainnamen mit einer IP Adresse verknüpft.

Wichtig: WWW ist nicht gleichbedeutend mit Internet!

Frage: Was ist das Internet?

Antworten:

Das Internet ist ein weltweiter Verbund von Computern, die miteinander Daten austauschen. Das Netzwerk mit Millionen von angeschlossenen Rechnern ist dezentral organisiert. Es gibt also keinen Zentralrechner, der das Internet steuert (!!! DNS hat zentrale Instanzen !!!)

Das Internet besteht aus einem Netz von miteinander verbunden Teilnetzen ('Netz der Netze').

Wichtig:

Daten werden in Pakete zerlegt und diese transportiert. Daten werden beim Sender in viele kleine nummerierte Pakete verpackt und verschickt. Nicht alle Pakete müssen denselben Weg zum Empfänger nehmen!

Router, Routing

http://www.netgear.de/Support/Basiswissen/router_grundlagen.html

Datenverkehr ist zunächst nur innerhalb der LAN's möglich. Die Verbindungsstellen zwischen den LAN's sind die Router. Die Router sorgen für den Datenaustausch zwischen den LAN's.

Ein Router ist mit zwei Netzwerken verbunden und besitzt mindestens zwei Netzwerkanschlüsse und damit mindestens zwei IP-Adressen.

Ein Vergleich mit der Briefpost

Die LAN's sind die Städte, die Router stellen die Briefzentren dar. Ein Brief in eine andere Stadt wird zum Briefzentrum der Zielstadt (zum Router des Zielnetzes) geschickt.

Der Transport zum Empfänger (zum Zielrechner) erfolgt innerhalb der Stadt (innerhalb des LAN's).

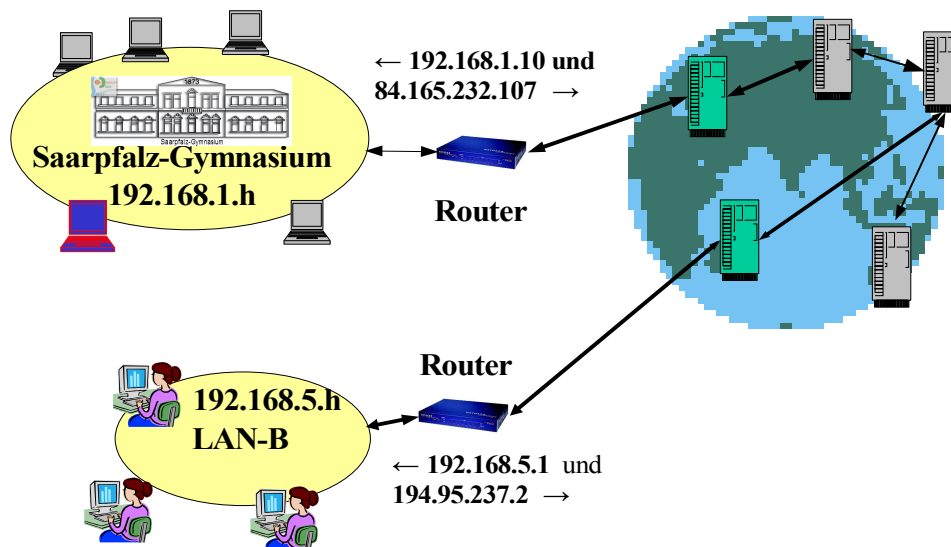
Ähnlich verläuft das Routing in Netzwerken:

Beispiel: Das Saarpfalz-Gymnasium besitzt die Netzwerk-ID des SPG (192.168.1). Der Router hat die lokale IP-Adresse 192.168.1.10 und die vom Internetprovider (z.B. Telekom) zugewiesene Adresse **84.165.232.107**

Das LAN-B besitzt die lokale Netzwerk-ID 192.168.5 und der Router besitzt die im Internet gültige Adresse **194.95.237.2**

Ein Paket aus dem LAN des SPG soll an das LAN-B mit der im Internet sichtbaren Adresse **194.95.237.2** gesendet werden. Da die Netzwerk-ID verschieden von 192.168.1 ist, geht das Paket an den Router, der das SPG mit dem Internet verbindet.

Routing



IP-Routingtabelle

Jeder Knoten, der das TCP/IP-Protokoll verwendet, verfügt über eine Routingtabelle.

Routingtabellen befinden sich in jedem IP-Knoten. Die Routingtabelle speichert Informationen zu IP-Zielen und möglichen Verbindungen zu den Zielen.

Jede Tabelle enthält eine Reihe von Standardeinträgen und Werte, die von anderen Routern stammen.

Mit Hilfe der Routingtabelle wird die IP-Adresse des nächsten Knotens ermittelt:

Direkte Zustellung: Der Zielhost ist in demselben Netz und ist über seine Host-ID erreichbar.

Indirekte Zustellung: Es muss eine Route zum Ziel ermittelt werden. Dies erfolgt mit Hilfe der Routing-Tabelle.

Die Einträge lassen sich mit dem Befehl `netstat -rn` auslesen.

```
axel@info1:~> netstat -rn
```

Kernel IP Routentabelle

Ziel	Router	Genmask	Flags	MSS	Fenster	irtt	Iface
192.168.0.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0
127.0.0.0	0.0.0.0	255.0.0.0	U	0	0	0	lo
0.0.0.0	192.168.0.1	0.0.0.0	UG	0	0	0	eth0

G Die Route geht durch ein Gateway.

U Das zu verwendende Interface ist aktiv.

Multicast Adresse

Multicast bedeutet man das Versenden des selben Datenstroms an mehrere Empfänger (genannt Multicast-Gruppe). Der Bereich **224.0.0.0/24** ist für das lokale Netz reserviert und wird von Routern nicht weitergeleitet (geforwarded). Eine typische Anwendung ist das Senden von Multimediainformationen (Echtzeitaudio oder -Video) zu Hosts.

Grundlagen TCP/IP

Das Schichtenmodell

Quelle: [9], [11], [12]

Netzwerke sind in Schichten (Layers) organisiert. Jede Schicht "abstrahiert" bzw. kapselt eine bestimmte Aufgabe. Jede Protokollschicht führt die ihr zugewiesene Teilaufgabe bei der Datenübertragung aus.

Vorteile:

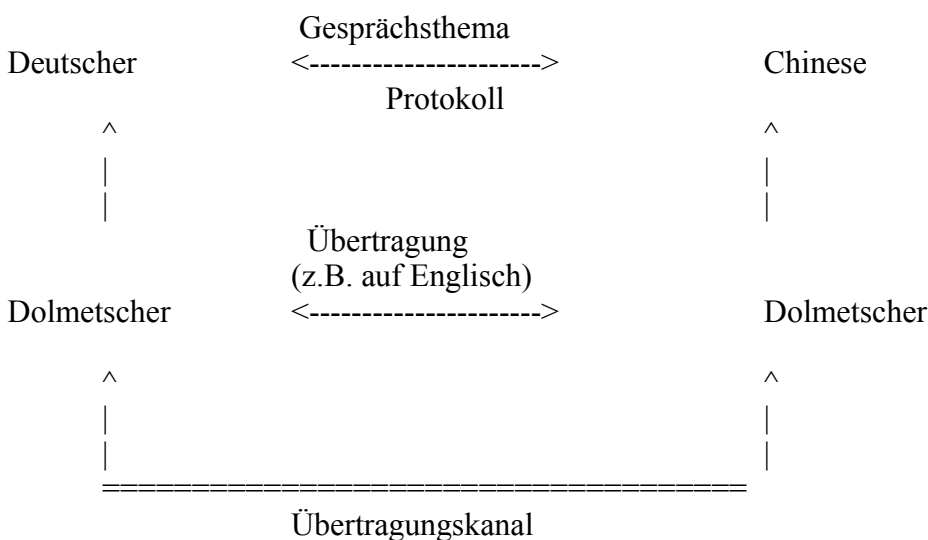
Eine Netzwerkanwendung, wie etwa der Web-Browser, muss nichts über die zu Grunde liegende Netzwerk-Hardware wissen.

Für den Browser ist ohne Bedeutung, ob er über Modem oder Netzwerkkarte mit dem Internet kommuniziert. Er verwendet nur die oberste Schicht, die Anwendungsschicht.

Die Software einer Schicht kann ohne Beeinflussung anderer Schichten gewartet werden.

Ein Beispiel

Wenn sich zwei Partner verständigen wollen und jeder die Sprache des anderen nicht beherrscht, kann folgendes Schichtenmodell das Problem lösen.

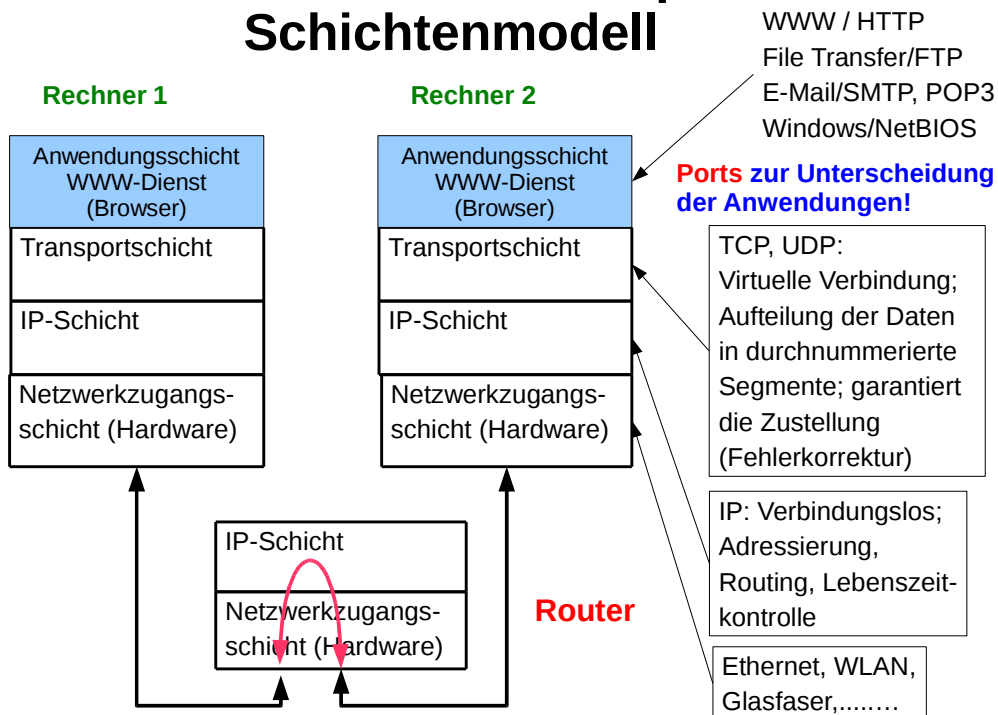


In jeder Schicht läuft eine horizontale Kommunikation ab

Anwendungsschicht			
HTTP für Internet-Browser	POP zum Abholen der Mail	SMTP Versenden der Mail	FTP File Transfer Protocol
Transportschicht TCP			
Internetschicht IP			
Netzwerkschicht Verbindung zur Netzwerkkarte: „Physik, Elektrotechnik“			

Die **Transportschicht** sorgt dafür, dass die Daten ankommen. Hier findet eine weitere „Adressierung“ durch **Ports** statt. Ports identifizieren einen Dienst, der auf dem Rechner läuft.

TCP/IP-Protokollstapel Schichtenmodell



Anmerkung

Router bearbeiten nur die beiden unteren Protokollschichten – die IP- und die Netzwerkschicht. Solange ein Router keinen eigenen Datenverkehr erzeugt oder aufnimmt, braucht er weder Transport- noch Anwendungsschicht

Anwendungen in der obersten Schicht

Auf der obersten Ebene (Anwendungsschicht) sind die sogenannten Anwendungsprotokolle implementiert. Beispiele sind HTTP, SMTP, POP3 und FTP.

Diese Anwendungsprotokolle kommunizieren einerseits mit dem Benutzer, andererseits mit der TCP-Schicht.

TCP (Transport Control Protocol)

Quelle: [7]

Ports

Da auf einem Rechner, d.h. unter einer IP-Adresse, gleichzeitig **mehrere Anwendungen** laufen können, muss es zusätzlich zur IP-Adresse ein weiteres Unterscheidungsmerkmal geben.

Jeder Anwendung ist eindeutig eine **Portnummer** zugeordnet. Der ankommende Datenstrom kann mit Hilfe der Portnummer zur richtigen Anwendung gelangen.

Ein Vergleich

Wenn die IP-Adresse die Hausnummer darstellt, adressiert die Portnummer die Zimmernummer innerhalb des Hauses, um den richtigen Bewohner (das Anwendungsprogramm) zu erreichen.

Ein Brief mit einer Adresse wird am korrekten Gebäude ankommen, aber ohne die Zimmernummer wird er nicht zum gewünschten Empfänger gelangen.

Ports arbeiten analog: Ein Datenpaket wird an die korrekte IP Adresse ausgeliefert: Aber nur mit der Portnummer wird das Paket der richtigen Anwendung zugestellt.

Bei TCP/IP können auf einem Host mehrere Dienste laufen. So kann ein Web-Server ebenso aktiv sein, wie ein Mail-Server oder ein Dienst für Netzwerkdrucker. Die einzelnen Dienste werden dabei über Ports, bzw. Portnummern (16 Bit) identifiziert.

Eine TCP/IP-Kommunikation hat immer einen Quellport und einen Zielport.

Der Quellport identifiziert das Programm, das die Anfrage sendet. Dies kann etwa ein Port sein, den der Webbrowser nutzt. Der Zielport gibt den Port des Hosts an, der die Anfrage abarbeitet. Auf diesem Port läuft dann beispielsweise der Web-Server (Port 80).

SMTP: 25 POP3: 110 FTP: 20 und 21

Zusatzinformationen

Die Portnummern unter 256 sind für so genannte Well-Known-Services, wie FTP (Port 21) oder TELNET, reserviert. Die Werte zwischen 256 und 1024 werden für systemspezifische Dienste genutzt. Alle anderen über 1024 sind frei nutzbar. Sie dienen zum Beispiel für ausgehende Verbindungen als Quellports. Ports sind für die Sicherheit wichtig und müssen beobachtet werden, da sie von Angreifern benutzt werden. Ein erster Hinweis auf einen Angriff ist ein sogenannter Portscan. Ein Hacker lässt dabei eine Software (Port-Scanner) auf den Computer los, die durchtestet, welche Ports offen sind. Solche Angriffe sind nur durch korrekt konfigurierte Firewalls abzuwehren.

TCP

TCP bündelt den Datenstrom aus der Anwendungsschicht in **Segmente**. In den Segmenten sind Zusatzinformationen gespeichert, um folgende Ziele zu erreichen:

Steuerung des Datenflusses

Um zu vermeiden, dass große Datenmengen das Netz für andere blockieren, werden die Daten in **TCP-Segmente** aufgeteilt und durchnummeriert.

Jedes TCP-Segment enthält: TCP-Quellport, TCP-Zielpport, Sequenznummer (sequence number), Bestätigungsnummer (**ACK Acknowledgement number**).

Jedes zu übertragende Datenbyte ist nummeriert. Mit der **Sequenznummer** wird die Nummer des ersten Datenbytes des jeweiligen TCP- Segments gespeichert.

TCP garantiert die richtige Reihenfolge der Segmente

Damit kann kontrolliert werden, ob alle Segmente beim Zielrechner ankommen. Das TCP-Protokoll im Zielrechner setzt die Segmente wieder in der richtigen Reihenfolge zusammen, sofern Segmente später eintreffen.

Die **Bestätigungsnummer (ACK Acknowledgement number)** signalisiert dem Empfänger die nächste erwartete Sequenznummer.

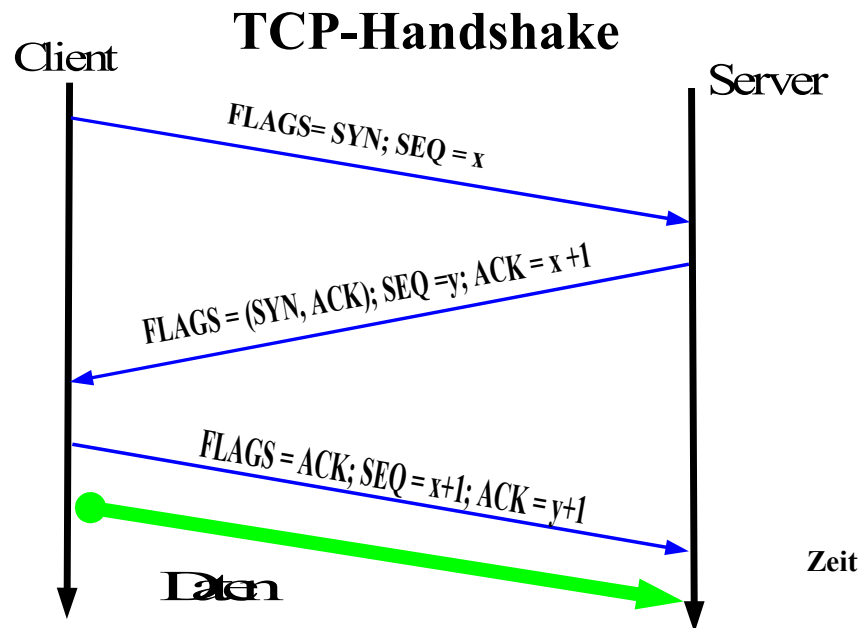
Erkennung von Übertragungsfehlern

TCP-Segmente müssen bestätigt werden. Fehlende Segmente werden vom sendenden Rechner erneut übertragen.

Aufbau der Verbindung: TCP Handshake

Quellen: [13],[14], [15]

TCP ist ein verbindungsorientiertes Protokoll. Verbindungen werden über ein *Dreiwegen-Handshake (three-way handshake)* aufgebaut.



Zum Aufbau einer Verbindung sendet der Client dem Server, mit dem er eine Verbindung aufbauen will, ein Segment, in dem das SYN-Bit (Synchronize-Bit) gesetzt ist. Mit diesem Segment teilt der Client dem Server mit, dass der Aufbau einer Verbindung gewünscht wird.

Der Server kann die Verbindung nun annehmen oder ablehnen. Nimmt er die Verbindung an, wird ein Bestätigungssegment gesendet. In diesem Segment sind das SYN-Bit und das ACK-Bit (Acknowledge-Bit) gesetzt. Im Feld ACK bestätigt der Server die Sequenznummer des Client dadurch, dass die um Eins erhöhte Sequenznummer des Client 1 gesendet wird.

Der Server antwortet mit gesetztem SYN-Bit, zusätzlich ist das ACK-Bit (Acknowledge-Bit) gesetzt.

Der Client bestätigt mit einem ACK-Bit die Aufnahme der Verbindung.

Zum Beenden der Verbindung wird statt des SYN-Bit wird das FIN-Bit (Finalize-Bit) gesetzt.

Aufgaben

Nenne drei wichtige Funktionen von TCP

Lösung: Sitzungseinrichtung, Sitzungsbeendigung, Garantie der Zustellung der Daten

IP (Internet Protocol)

IP ist zuständig für

- das Versenden der Pakete an die richtige Adresse
- die Wahl des dafür notwendigen Weges (Routing)

- Hierzu ergänzt das IP-Protokoll die Datenpakete um **Absender-** und **Zieladressen**.
- Der sendende Rechner leitet die Pakete an den nächsten bekannten Vermittlungsrechner (= Router) weiter: Jeder Rechner verfügt über eine sog. Routingtabelle, die die Adressen erreichbarer Rechner im Netz enthält.
- Falls dieser Rechner nicht der Zielrechner ist, sorgt er für die **Weiterleitung** der Pakete (die Übertragung erfordert keine durchgehende Verbindung).
- Dieser Routingvorgang wird auf jedem Rechner beim Empfang eines IP-Pakets durchgeführt, bis das Paket am Zielort angekommen ist.
- IP-Pakete können verloren gehen, dupliziert werden und in anderer Reihenfolge als gesendet eintreffen.

Um diesen Forderungen gerecht zu werden, umfasst das Internet Protokoll im wesentlichen folgende Funktionen:

- Wegwahl (Routing)
- Lebenszeitkontrolle
- Adressierung
-

IP garantiert nicht die Zustellung der Daten. Dies wird durch TCP garantiert.

Beispiel

Ein Brief ist mit Absender- und Empfängeradresse versehen und wird zum nächsten Postschalter gebracht. Eine korrekte Zustellung ist aber nur dann gewährleistet, wenn sich beide Kommunikationspartner zusätzliche Bestätigungsdaten schicken (im Sinne von Dreifach-TCP-Handshake).

IP ist ein so genanntes "verbindungsloses" Protokoll. Es tauscht keine Kontrollinformationen mit der Gegenstelle im Netzwerk aus (Handshaking). Für das IP-Protokoll ist es gleichgültig, ob der Kommunikationspartner überhaupt bereit ist, Daten zu empfangen.

Der Empfang der Daten wird durch TCP geregelt. IP erfüllt nur die Aufgabe, Daten von der Transportschicht in einheitliche Datenpakete zu packen und diese an die Netzzugangsschicht weiterzuleiten und umgekehrt.

Die Netzzugangsschicht

(Quelle: Wikipedia)

Netzzugangsschicht (*engl.: link layer*): Die Netzzugangsschicht sorgt für die physikalische Datenübertragung zwischen zwei Systemen (Rechner, Router, ...).

Die Internet-Protokolle wurden mit dem Ziel entwickelt, verschiedene Subnetze zusammenzuschließen. Daher kann die Host-an-Netz-Schicht durch Protokolle wie Ethernet, FDDI (Glasfaser) oder 802.11 (WLAN) realisiert werden.

ARP arbeitet auf der Netzwerkschicht und setzt IP-Adressen in MAC-Adressen. Die MAC-Adresse (Media Access Control) ist die fest eingetragene Hardware-Adresse der Netzwerkkarte. Die MAC-Adresse hat eine Länge von 48 Bit und wird hexadezimal geschrieben.

Die eigentliche Adressierung im Ethernet erfolgt anhand der MAC-Adressen.

Bevor ein IP-Paket verschickt werden kann, muss die MAC-Adresse des Zielrechners bekannt sein. Dazu versendet ARP einen Broadcast (Rundruf) mit der Frage "who has <IP-Adresse>". Ist der Ziel-Host erreichbar, antwortet dieser mit einem an den Absender gerichteten ARP-Reply "<IP-Adresse> is at <MAC-Adresse>". Diese Antwort speichert der Rechner temporär im ARP-Cache. Wird die Hardware neu gestartet oder ausgeschaltet, wird der ARP-Cache gelöscht.

Frage: Welche unterschiedliche Funktion erfüllen MAC-Adresse und IP-Adresse?

Sicherheit in Netzwerken

Firewall

Eine Firewall ist ein Gerät, das ein Netzwerk gegenüber einem anderen Netzwerk schützt und gleichzeitig die Kommunikation zwischen diesen Netzwerken **kontrolliert zulässt**.

Firewalls schränken den Austausch von Datenpaketen zwischen den beiden gekoppelten Netzen ein.

Beispiel: Mittelalterliche Burg

- Besucher werden zunächst identifiziert und notiert (protokolliert)
- Die Besucher werden kontrolliert, welche Gegenstände sie ein- und ausführen
- Alle Personen müssen die Burg an einer bestimmten, besonders gesicherten Stelle betreten
- Die Burg verhindert, dass sich Angreifer an anderen Stellen nähern können (Burggraben)
- Personen können die Burg nur an bestimmten Stellen verlassen
- Alle passierenden Personen werden registriert.

Die Besucher = Datenpakete

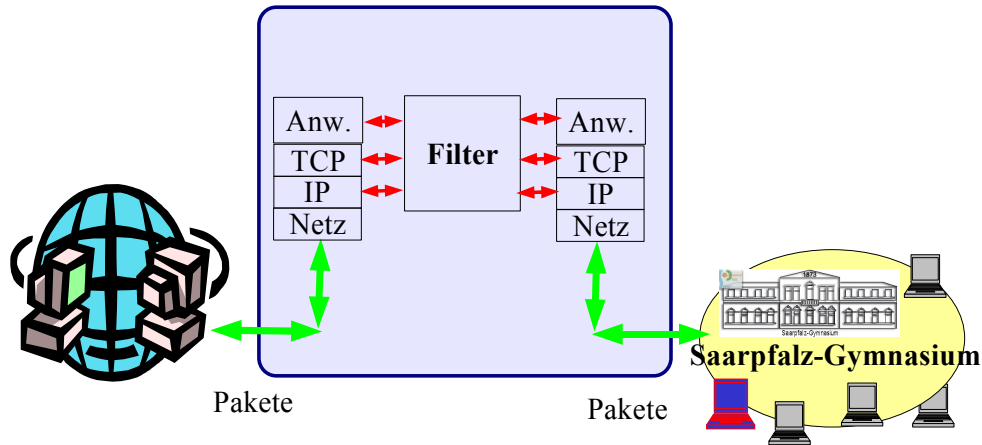
'Verbindungswünsche' (=Angriffe) von außen werden unterbunden.

Nur „registrierte“ Programme dürfen Verbindungen ins Internet starten

Antworten aus dem Internet werden nur für registrierte Programme zum PC durchgelassen

Trojaner (nicht genehmigt) dürfen keine Verbindung ins Internet aufnehmen.

Firewall



Firewall-Technologien

Grundsatz: Default-Deny-Prinzip

Es wird nur das erlaubt was erwünscht ist. Die restlichen Verbindungen sind per Default verboten.

Paketfilterung

Paketfilter arbeiten auf der TCP- oder IP-Schicht. Pakete werden anhand ihrer Quell- und Ziel-IP-Adresse und der Portnummern untersucht, ob sie passieren dürfen oder nicht. Dabei wird zwischen ein- oder ausgehenden Paketen unterschieden. Unzulässige Pakete werden protokolliert und verworfen.

SPI - Stateful Packet Inspection

SPI ist eine dynamische Paketfilterung: Die statische Paketfilterung wird um zusätzliche Regeln erweitert.

Beispiel: SPI überprüft, ob eingehende Datenpakete zu zuvor gesendeten Datenpaketen in Beziehung stehen, also zu einer Sitzung gehören, die durch das sichere lokale Netzwerk ausgelöst wurden.

Nur Pakete dürfen das LAN betreten, wenn sie **Antwortpakete** einer ausgehenden Nachricht sind.

Das Filter merkt sich die Zieladresse und vergleicht sie im zurück kommenden IP-Paket mit der Quelladresse.

Datenpakete, die sehr häufig eintreffen, werden identifiziert. Liegt der Verdacht nahe, dass es sich um eine DoS-Attacke (Denial-of-Service) handelt, werden diese Datenpakete automatisch verworfen.

Erlaubte Kommunikation:

In den eigens definierten Regeln sind die freizuschaltenden Ports und Wege festgelegt. So kann z.B. der Zugriff auf einen internen Webserver erlaubt werden: Anfragen auf Port 80 werden auf eine spezielle interne IP-Adresse weitergeleitet.

Dienstefilterung

Sie beobachtet die Portnummern, die im System verwendet werden.

Dadurch kann man mittels Paketfilterung Pakete bestimmter Protokolle zulassen oder blockieren. Es dürfen z.B. nur Pakete zum HTTP-Protokoll passieren, Pakete für Chat werden unterbunden.

Was geht nicht?

Die Kontrolle der Verbindungen von bestimmten Benutzern ist nicht möglich, da die Pakete keine Benutzerinformationen enthalten.

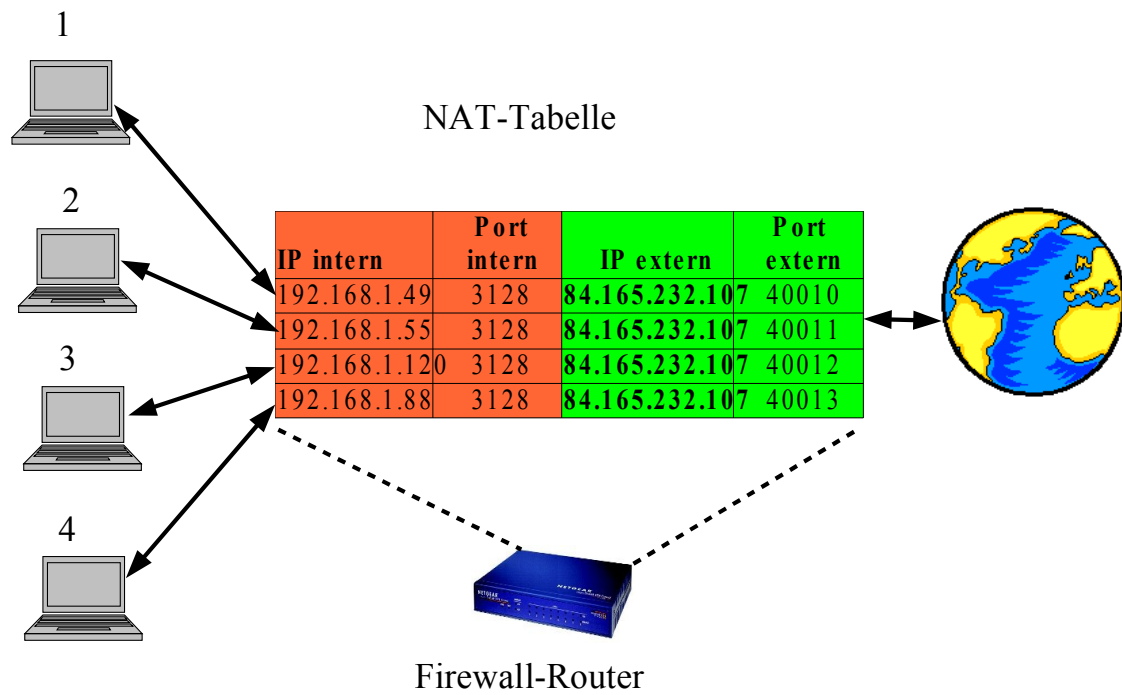
NAT (Network Address Translation)

NAT ist das Umschreiben von IP-Adressen und Port-Nummern in IP-Paketen durch Firewalls, um die Adressen in internen Netzen zu verschleiern. Diese Verschleierung (Mascerading) kann zur Geheimhaltung der internen Adressen dienen oder auch durch die Verwendung sog. privater IP-Adressbereiche notwendig sein.

NAT -manchmal auch als **NPAT** (*Network and Port Address Translation*) bezeichnet - bildet **alle** Adressen eines privaten Netzwerkes auf **eine** einzelne öffentliche (dynamische) IP-Adresse ab. Dies geschieht dadurch, dass bei einer existierenden Verbindung zusätzlich zu den Adressen auch die Portnummern ausgetauscht werden. Auf diese Weise benötigt ein gesamtes privates Netz nur eine einzige IP-Adresse.

Das Umschreiben der IP-Adressen im Firewall-Router geschieht mittels einer Tabelle.

Firewall



Beispiel

Client 2 (Absenderadresse 192.168.1.55, Port 3128) schickt ein Paket ins Internet.

Der Router modifiziert das Paket zu Absenderadresse
84.165.232.107, Port 40011

Der Server im Internet sendet sein Antwortpaket an 84.165.232.107, Port 40011.

Im Antwortpaket aus dem Internet (an 84.165.232.107, Port 40011) werden die Router-Änderungen wieder rückgängig gemacht, d.h. das Paket wird dem Client 2 mit der Adresse 192.168.1.55 zugestellt.

Weder Client 2 noch der Internet-Server merken etwas von diesen Adress- und Port-Tausch:

Für den Client ist der Firewall-Router die übliche Schnittstelle zum Internet.

Für den Internet-Server scheinen die Pakete vom Router zu kommen.

Der Internet-Server erhält keine Informationen über die Clients im Netz, da er nur den Router „sieht“.

Mehrere Clients können eine offizielle IP-Adresse gemeinsam nutzen.

Quelle: http://www.bfd.bund.de/technik/Ori_int2/ohint_3.html

Ein **Application Level Gateway** ist ein speziell konfigurierter Rechner, über den die gesamte Kommunikation zwischen dem zu schützenden und dem unsicheren Netz stattfindet. Ein Application Level Gateway arbeitet im Gegensatz zum Packet-Filter auf der Anwendungsschicht, d. h. die Kontrolle der Kommunikationsbeziehungen findet auf Anwendungsebene statt. Für jeden Dienst (Telnet, FTP usw.) werden **Security Proxys** eingeführt, die den direkten Zugriff auf den Dienst verhindern. Hierbei bestehen z. B. die Möglichkeiten einer ausführlichen Protokollierung (Audit) und einer benutzerbezogenen Authentisierung für die unterschiedlichen Dienste

TCP/IP-Hilfsprogramme

arp Erlaubt die Einträge des ARP-Cache (Address Resolution Protocol) anzuzeigen und zu ändern.

Das Address Resolution Protocol setzt IP-Adressen in MAC-Adressen (= Physikalische Adresse) um. Damit nun ein IP-Paket sein Ziel findet, muss die Hardware-Adresse des Ziels bekannt sein.

Jede Netzwerkkarte besitzt eine eindeutige Hardware-Adresse, die fest auf der Karte eingestellt ist.

Quelle: <http://www.elektronik-kompodium.de/sites/net/0901061.htm>

```
infotux:~ # arp -vn 192.168.0.1
```

Address	Hwtype	Hwaddress	Flags Mask	Iface
192.168.0.1	ether	00:14:6C:03:DB:DC	C	eth0

netstat Ist ein Tool, mit dem sich alle aktiven TCP-, UDP- und IP-Verbindungen, die Routing-Tabelle und eine Statistik der TCP/IP-Daten abrufen lassen.

```
infotux:~ # netstat -a
```

Active Internet connections (servers and established)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	localhost:36544	*.*	LISTEN
tcp	0	0	*:6881	*.*	LISTEN
tcp	0	0	localhost:55918	*.*	LISTEN
tcp	0	0	*:sunrpc	*.*	LISTEN
tcp	0	0	*:37395	*.*	LISTEN
tcp	0	0	localhost:48503	*.*	LISTEN
tcp	0	0	localhost:ipp	*.*	LISTEN
tcp	0	0	localhost:smtp	*.*	LISTEN
tcp	0	0	localhost:49786	*.*	LISTEN
tcp	0	0	localhost:57552	localhost:49786	ESTABLISHED
tcp	0	0	192.168.0.4:50655	www.opensuse.o:www-http	ESTABLISHED
tcp	0	1	192.168.0.4:56509	192.168.:pdl-datastream	SYN_SENT
tcp	0	0	localhost:49786	localhost:57553	ESTABLISHED
tcp	0	0	localhost:49786	localhost:57552	ESTABLISHED
tcp	0	0	localhost:57553	localhost:49786	ESTABLISHED
tcp	0	0	*:ssh	*.*	LISTEN
tcp	0	0	localhost:ipp	*.*	LISTEN
tcp	0	0	localhost:smtp	*.*	LISTEN
udp	0	0	*:filenet-tms	*.*	
udp	0	0	*:35000	*.*	
udp	0	0	*:35000	*.*	
udp	0	0	*:35000	*.*	
udp	0	0	*:35000	*.*	
udp	0	0	*:bootpc	*.*	
udp	0	0	*:mdns	*.*	

```
udp    0    0 *:sunrpc      *:*
udp    0    0 *:ipp        *:*
hostname    Zeigt den Hostnamen des Computers an.
```

ifconfig (Linux) bzw ipconfig (Windows)

Zeigt die aktuellen TCP/IP-Konfigurationseinstellungen an.

ping Überprüft IPv4- oder IPv6-Verbindungen mit anderen IP-Knoten.

route Zeigt die Einträge der lokalen IPv4- und IPv6-Routingtabelle an und ermöglicht Ihnen, die lokale IPv4-Routingtabelle zu ändern.

Beispiel:

```
infol:~ # route
Kernel IP routing table
Destination      Gateway          Genmask         Flags Metric Ref
Use Iface
192.168.0.0      *                255.255.255.0   U        0      0
0 eth0
loopback        *                255.0.0.0       U        0      0
0 lo
default         192.168.0.1     0.0.0.0         UG       0      0
0 eth0
```

Flags zur näheren Bestimmung der Route - U für Up (aktiv), H für Host (Ziel ist ein Rechner) und G für Gateway (Ziel ist z.B. ein Router)

traceroute Verfolgt den Pfad, den ein IPv4- oder IPv6-Paket zu einem bestimmten Ziel zurücklegt.

```
infotux:~ # traceroute saar.de
traceroute to saar.de (192.109.53.23), 30 hops max, 40 byte packets
 1 p54A5F954.dip.t-dialin.net (84.165.249.84) 2.822 ms 2.854 ms 4.471 ms
 2 * * *
```

3 217.0.67.170 (217.0.67.170) 58.947 ms 57.266 ms 54.827 ms
4 193.159.226.218 (193.159.226.218) 56.896 ms 56.287 ms 54.562 ms
5 core2-sb.intersaar.de (213.135.0.93) 54.638 ms 54.352 ms 56.800 ms
6 fw1.intersaar.de (213.135.0.247) 57.939 ms 58.234 ms 57.477 ms
7 bellona.wg.saar.de (192.109.53.23) 56.945 ms 57.655 ms 56.403 ms

TCPdump/Wireshark

Tcpdump erlaubt Netzwerkschnittstellen abzuhören. **Wireshark** erlaubt eine grafische Analyse des Netzwerkverkehrs

Mit folgender Befehlszeile weist man **Tcpdump** an, alle Pakete zu protokollieren, die an oder von dem Host 192.168.0.1 kommen:

```
inf01:~ # tcpdump host 192.168.0.1
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
21:18:38.049670 IP 192.168.0.10.8637 > 192.168.0.1.domain: 37890+ AAAA?
googleads.g.doubleclick.net. (45)
21:18:38.050239 IP 192.168.0.10.23237 > 192.168.0.1.domain: 1263+ PTR? 1.0.168.192.in-
addr.arpa. (42)
21:18:38.113424 IP 192.168.0.1.domain > 192.168.0.10.8637: 37890 1/1/0 (131)
21:18:38.113565 IP 192.168.0.10.18941 > 192.168.0.1.domain: 56656+ A?
googleads.g.doubleclick.net. (45)
21:18:38.121525 IP 192.168.0.1.domain > 192.168.0.10.23237: 1263 NXDomain 0/0/0 (42)
21:18:38.121866 IP 192.168.0.10.5140 > 192.168.0.1.domain: 64438+ PTR? 10.0.168.192.in-
addr.arpa. (43)
21:18:38.174801 IP 192.168.0.1.domain > 192.168.0.10.18941: 56656 5/0/0[[domain]
21:18:38.184020 IP 192.168.0.1.domain > 192.168.0.10.5140: 64438 NXDomain 0/0/0 (43)
21:18:43.046559 arp who-has 192.168.0.1 tell 192.168.0.10
21:18:43.047192 arp reply 192.168.0.1 is-at 00:14:6c:03:db:dc (oui Unknown)
21:19:27.175457 IP 192.168.0.10.14997 > 192.168.0.1.domain: 39727+ AAAA?
static.cache.l.google.com. (43)
21:19:27.236901 IP 192.168.0.1.domain > 192.168.0.10.14997: 39727 0/1/0 (91)
21:19:27.237059 IP 192.168.0.10.elm-momentum > 192.168.0.1.domain: 41771+ AAAA?
static.cache.l.google.com. (43)
21:19:27.298162 IP 192.168.0.1.domain > 192.168.0.10.elm-momentum: 41771 0/1/0 (91)
21:19:27.298592 IP 192.168.0.10.17345 > 192.168.0.1.domain: 54266+ A?
static.cache.l.google.com. (43)
21:19:27.359542 IP 192.168.0.1.domain > 192.168.0.10.17345: 54266 1/0/0 (59)
21:19:32.174565 arp who-has 192.168.0.1 tell 192.168.0.10
21:19:32.175223 arp reply 192.168.0.1 is-at 00:14:6c:03:db:dc (oui Unknown)
```

```
21:19:42.360064 IP 192.168.0.10.4505 > 192.168.0.1.domain: 15982+ AAAA? www.google.de.  
(31)  
21:19:42.432656 IP 192.168.0.1.domain > 192.168.0.10.4505: 15982 2/1/0 CNAME[[domain]  
21:19:42.432815 IP 192.168.0.10.tivoconnect > 192.168.0.1.domain: 11775+ A? www.google.de.  
(31)  
21:19:42.506870 IP 192.168.0.1.domain > 192.168.0.10.tivoconnect: 11775 6/0/0 CNAME[[  
domain]  
21:19:42.507194 IP 192.168.0.10.23528 > 192.168.0.1.domain: 30866+ AAAA? www.google.com.  
(32)  
21:19:42.587989 IP 192.168.0.1.domain > 192.168.0.10.23528: 30866 1/1/0 CNAME  
www.l.google.com. (100)  
21:19:42.588199 IP 192.168.0.10.5161 > 192.168.0.1.domain: 50001+ A? www.google.com. (32)  
21:19:42.658237 IP 192.168.0.1.domain > 192.168.0.10.5161: 50001 5/0/0 CNAME  
www.l.google.com.,[[domain]
```

Quellen: Wikipedia und <http://www.nwlab.net/tutorials/wireshark/>

Ethereal ist ein Programm zur Analyse von Netzwerk-Kommunikationsverbindungen. Ein Packet-Sniffer ist eine Software, die den Datenverkehr im Netzwerk aufzeichnet, die Inhalte der Datenpakete dekodiert und lesbar darstellt.

Sniffer untersuchen und analysieren den Netzwerkverkehr. So haben Administratoren die Chance, Schwachstellen und Sicherheitslücken zu erkennen. Umgekehrt können Angreifer per Sniffer das Netz nach Schwachstellen absuchen.

nslookup

Nslookup erlaubt die direkte Abfrage eines Nameservers.

Beispiel

```
info1:~ # nslookup www.saarpfalz-gymnasium.de  
Server:      192.168.0.1  
Address:     192.168.0.1#53
```

Non-authoritative answer:

```
www.saarpfalz-gymnasium.de    canonical name = lincoln.teresto.net.  
Name:  lincoln.teresto.net  
Address: 212.88.134.26
```

dig (Domain-Name-Server-Information-Grabber)

dig ist ein Kommandozeilen-Tool zur Abfrage von DNS-Name-Servern.

Beispiel info1:~ # dig

```

; <<>> DiG 9.4.2-P1 <<>>
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48394
;; flags: qr rd ra; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 14

;; QUESTION SECTION:
;
      IN      NS

;; ANSWER SECTION:
.      19094 IN    NS     B.ROOT-SERVERS.NET.
.      19094 IN    NS     C.ROOT-SERVERS.NET.
.      19094 IN    NS     D.ROOT-SERVERS.NET.
.      19094 IN    NS     E.ROOT-SERVERS.NET.
.      19094 IN    NS     F.ROOT-SERVERS.NET.
.      19094 IN    NS     G.ROOT-SERVERS.NET.
.      19094 IN    NS     H.ROOT-SERVERS.NET.
.      19094 IN    NS     I.ROOT-SERVERS.NET.
.      19094 IN    NS     J.ROOT-SERVERS.NET.
.      19094 IN    NS     K.ROOT-SERVERS.NET.
.      19094 IN    NS     L.ROOT-SERVERS.NET.
.      19094 IN    NS     M.ROOT-SERVERS.NET.
.      19094 IN    NS     A.ROOT-SERVERS.NET.

;; ADDITIONAL SECTION:
C.ROOT-SERVERS.NET. 30384 IN    A      192.33.4.12
D.ROOT-SERVERS.NET. 30384 IN    A      128.8.10.90
E.ROOT-SERVERS.NET. 30384 IN    A      192.203.230.10
F.ROOT-SERVERS.NET. 44604 IN    A      192.5.5.241
F.ROOT-SERVERS.NET. 48876 IN    AAAA   2001:500:2f::f
G.ROOT-SERVERS.NET. 30084 IN    A      192.112.36.4
H.ROOT-SERVERS.NET. 33085 IN    A      128.63.2.53
H.ROOT-SERVERS.NET. 33278 IN    AAAA   2001:500:1::803f:235
I.ROOT-SERVERS.NET. 32785 IN    A      192.36.148.17
J.ROOT-SERVERS.NET. 40074 IN    A      192.58.128.30
J.ROOT-SERVERS.NET. 61188 IN    AAAA   2001:503:c27::2:30
K.ROOT-SERVERS.NET. 29067 IN    A      193.0.14.129
K.ROOT-SERVERS.NET. 32310 IN    AAAA   2001:7fd::1
L.ROOT-SERVERS.NET. 44604 IN    A      199.7.83.42

```

Erläuterungen

A – IPv4-Adresse (für die Abbildung eines Namens auf eine IPv4-Adresse)

AAAA – IPv6-Adresse

NS – Autoritativer Name-Server

Für die Abbildung eines Namen zu einem für die jeweilige Domain zuständigen Name-Server, der autoritative Informationen liefern kann.

Weitere Tools: <http://sectools.org/>

Whois (umfangreicher: gnome-nettool)

Liefert Informationen über den Domain-Inhaber

Angry IP Scanner <http://www.angryip.org/w/Download>

Aufgaben

Beschreibe 2 Vorteile eines Computernetzes!

Beschreibe 2 typische Serverdienste im Internet.

Bestimme die IP-Adresse der WebSite *www.spiegel.de* . Zu welcher Netzwerkkategorie gehört der Server?

Gib statt des ping-Befehls den Befehl *tracert www.spiegel.de* ein. Welche Daten liefert das Programm?

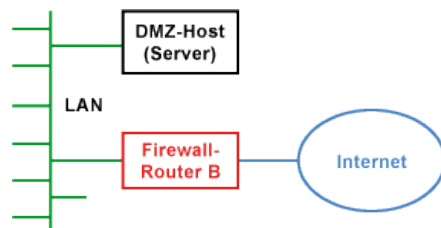
Weitere Informationen

DMZ - Demilitarisierte Zone

Die Demilitarisierte Zone ist ein eigenständiges Subnetz, welches das lokale Netzwerk (LAN) durch Firewall-Router (A und B) vom Internet trennt. Die Firewall-Router sind so konfiguriert, dass sie Datenpakete, für die es keine vorhergehende Aufforderung gab, verwerfen (Stateful Packet Inspection). Wird also aus dem Internet ein Datenpaket an den Server geschickt, wird es vom Firewall-Router A verworfen. Sollte ein Hacker doch auf einen Server innerhalb DMZ Zugriff erhalten und Datenpakete in das LAN zum Schnüffeln oder Hacken schicken wollen, werden diese vom Firewall-Router B verworfen.

In beiden Firewall-Routern müssen statische Routen konfiguriert werden, damit die eingehenden Datenpakete an die richtige Station im LAN geschickt werden. Diese Vorgehen hat noch den Vorteil, dass es den Datenverkehr vom Internet kommend aus dem LAN fern hält und deshalb im LAN nur der interne Datenverkehr und die Internet-Verbindungen ablaufen. Das LAN ist dann weniger anfällig für Überlastungen, die durch den Datenverkehr aus dem Internet kommen.

DMZ-Host



Die Kosten für einen zweiten Router und der Konfigurationsaufwand sind nicht unerheblich. Wer hier sparen will, kann auch eine Demilitarisierte Zone (DMZ) mit einem zentralen Host einrichten.

Diese Sparlösung einer Demilitarisierten Zone (DMZ) sieht die Konfiguration eines Standard-Empfängers im Firewall-Router vor. Dabei gibt es zwei Ansätze. Die **intelligente** Lösung leitet alle Pakete mit einer NAT-Vorgabe (Port-Forwarding) zum DMZ-Host. Dabei wird das Datenpaket abhängig vom TCP-Port an den DMZ-Host weitergeleitet oder verworfen.

Eine **ungünstige** Lösung ist es, alle von außen initiierte Verbindungen an den DMZ-Host weiterzuleiten. Dadurch kann der DMZ-Host mit Datenpaketen überschwemmt werden und ein Ausfall provoziert werden. Diesen Vorgang nennt man Denial-of-Service (DoS).

In einem solchen Fall empfiehlt sich zumindest die Installation einer Software-Firewall (z.B. Personal-Firewall) auf dem DMZ-Host und das Aktivieren von Stateful Packet Inspection (SPI) im Firewall-Router.

In jedem Fall muss der Router das Network Address Translation (NAT) beherrschen, damit eine Verbindung in das Internet möglich ist. Da der Router im Internet mit einer eigenen IP-Adresse erreichbar ist und im LAN der private IP-Adressraum verwendet wird, übernimmt NAT die Umsetzung von öffentlicher IP-Adresse in die privaten IP-Adressen. Anhand der Sender-IP-Adresse kann NAT eingehende Datenpakete dem richtigen Empfänger zuordnen.

Vorteil des DMZ-Hosts

Er lässt sich als Proxy-Server (Vermittler) zwischen lokalem Netz und den Servern im Internet nutzen. Den Stationen im lokalen Netz tritt er als zuständiger Server entgegen. Den Servern im Internet spielt er einen Client vor. Auf diese Weise lässt sich die Kommunikation zwischen den Stationen und dem Internet protokollieren und filtern.

Quellen & Literatur

Technische Informatik mit Delphi: für Unterricht und Selbststudium
von Eckart Modrow; emu-online

- [1] Unterrichtsentwurf: Zur Funktionsweise des Internet
<http://bebis.cidsnet.de/weiterbildung/sps/informatik/umaterial/internlp.htm>
- [2] Internet-Lexikon: <http://www.weihenstephan.org/~wschwarz/netlex/i-net-lexikon.html>
- [3] TCP/IP, Architektur
<http://www.kl.unibe.ch/sec2/gymbield/unterricht/Faecher/Informatik/>
- [4] Kommunikation
<http://www.mrsison.com/ch-2.ppt>
- [5] Protokolle
http://www.jonietz.de/personen/daniel/publikationen/protokolle_infos2003.pdf
- [6] Wellenreiten auf der Datenautobahn
<http://www.internet-kompetenz.ch/einstieg/studium/download/>
- [7] Protokolle und Ports
http://www.hackerhighschool.org/lessons/HHS_de3_Protokolle_und_Ports.pdf
- [8] Pädagogische Hausarbeit zur zweiten Staatsprüfung für das Lehramt an Gymnasien,
Kaiserslautern
http://www.jonietz.de/personen/daniel/publikationen/protokolle_infos2003.pdf
- [9] Andreas Rittershofer
<http://www.rittershofer.de/info/bagindra/tcpip.htm>
- [10] Datenübertragung
<http://www.sn.schule.de/~dvt/lpe14/1412prot.htm#tcpip#tcpip>
- [11] Informatik Klasse 11, Netzwerke, Schichtenmodell
<http://www.walko.de/schule/info/klasse11/gk/vorbereitung/index.htm>
- [12] <http://www.rvs.uni-bielefeld.de/~heiko/tcpip/>