


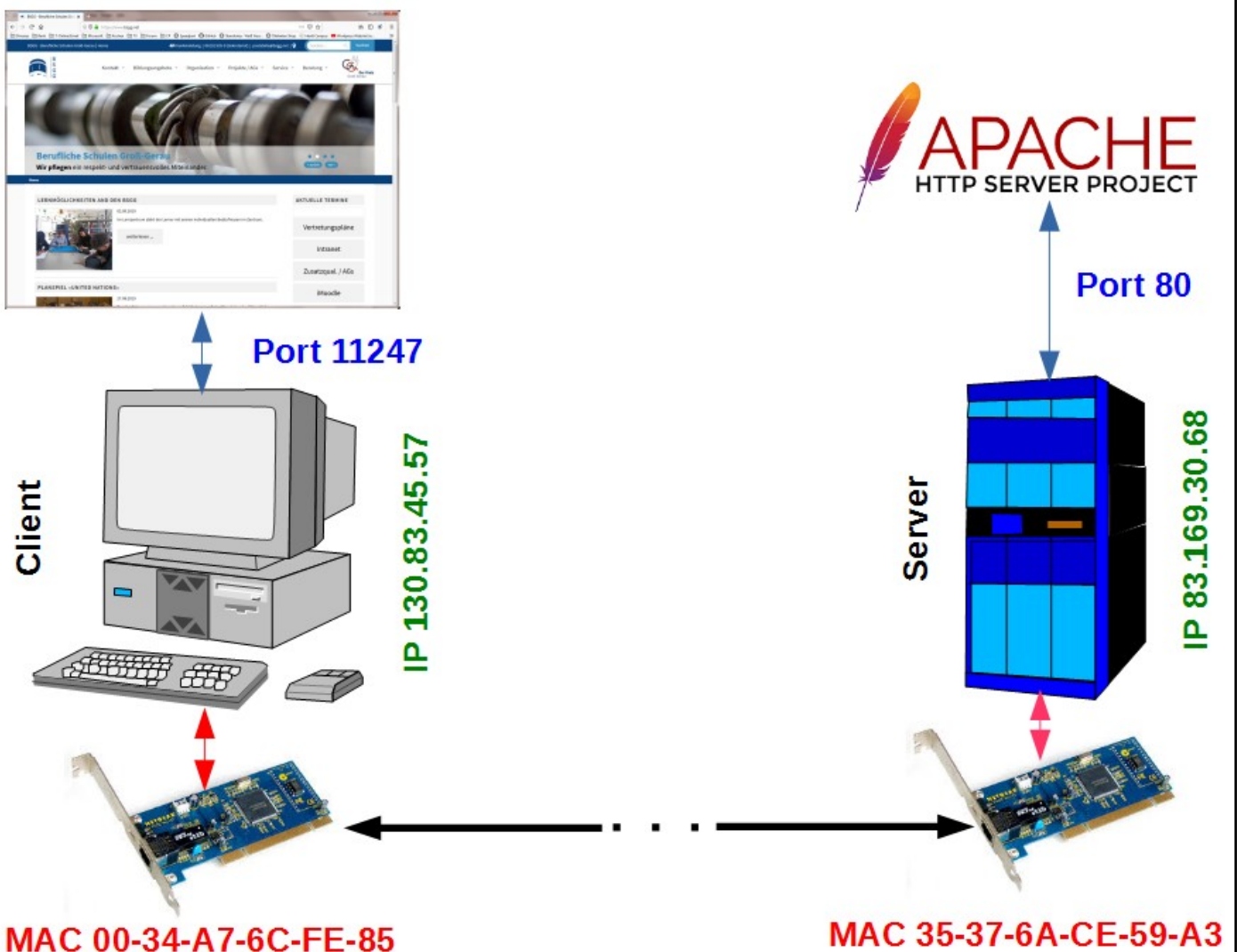
Arbeitsblatt Nr. 8	Q2 Technologie: Vernetzte IT-Systeme		B S G G
Datum:	Thema: Adressschemata bei TCP/IP		
Seite 1 von 4	Name:		

Adressierung in TCP/IP-Netzwerken

Die Daten, die ein bestimmtes Programm, welches auf einem Rechner (Client) in einem TCP/IP-Netzwerk versendet, sollen von einem bestimmten Programm, welches auf einem anderen Rechner (Server) läuft, empfangen und verarbeitet werden.


Nutzen wir als Beispiel hierzu den Abruf einer Webseite. Der Benutzer eines Client-PC (links) will sich mit dem Browser Firefox die Startseite der Homepage der Beruflichen Schulen Groß-Gerau anzeigen lassen. Diese Seite wird von einem Webserver (rechts) ausgeliefert.

Zur Vereinfachung hat der Client-PC eine sogenannte „öffentliche IP-Adresse“, in diesem Fall 130 . 83 . 45 . 57. Der Webserver ist unter der öffentlichen IP-Adresse 83 . 169 . 30 . 68 erreichbar.



Sie sehen für jeden der beiden miteinander kommunizierenden Rechner drei Nummern:

- eine Portnummer (dies ist eine 16 Bit-Integerzahl im Bereich 0...65535)
- eine IPv4-Adresse (dies ist eine 32 Bit-Integerzahl, die byteweise in dezimaler Form geschrieben wird. Jedes Byte hat einen Wert von 0...255)
- eine MAC-Adresse (dies ist eine 48 Bit-Integerzahl, die in hexadezimaler Form geschrieben wird, wobei die einzelnen Bytes optisch voneinander getrennt werden)

Arbeitsblatt Nr. 8	Q2 Technologie: Vernetzte IT-Systeme		B S G G
Datum:	Thema: Adressschemata bei TCP/IP		
Seite 2 von 4	Name:		

Portnummer

Jedes Mal, wenn ein Prozess (d.i. ein in Ausführung befindliches Programm) mit Hilfe des Netzwerks kommunizieren soll, bekommt es automatisch vom Betriebssystem eine sogenannte Portnummer zugewiesen. Diese Portnummer ist variabel. Werden von einem Prozess mehrere Kommunikationsverbindungen benötigt, erhält jede dieser Verbindungen eine eigene Portnummer zugewiesen.

Durch diese Portnummer kann das Betriebssystem den jeweiligen Prozess bzw. Thread¹ eindeutig identifizieren.

Auf der Serverseite wartet ein Service (z.B. der Webservice) auf den Verbindungswunsch durch einen Client. Deshalb sind die Portnummern zur Kontaktierung serverseitiger Dienste festgelegt, damit der jeweilige Service auch erreichbar ist.

Ein Webserver wird für Anfragen per HTTP typisch unter der Portnummer 80 kontaktiert. Per HTTPS verschlüsselte Anfragen werden hingegen an den Port 443 gerichtet.

Standarddienste sind über die Portnummern von 0 bis 1023 erreichbar. Man nennt diese daher auch „Well Known Ports“.

Unter der URL https://de.wikipedia.org/wiki/Liste_der_standardisierten_Ports findet sich eine Liste für diese Zuordnungen.

Zusammengefasst: Jede Kommunikationsverbindung in der Anwendungsschicht erhält vom Betriebssystem eine Portnummer zugewiesen. Sobald durch die betreffende Anwendung (z.B. der Browser Firefox) Daten versendet werden, wird in der Transportschicht im TCP-Header der zu versendenden Daten die Quell-Portnummer (d.i. die datenversendende Anwendung auf dem Client) **und** die Ziel-Portnummer (d.i. die datenempfangende Anwendung auf dem Server) eingetragen.

Das nachfolgende Bild zeigt einen Ausschnitt von Kommunikationsverbindungen. In der ersten Spalte wird das betreffende Transportprotokoll angezeigt (TCP), in der zweiten Spalte wird die Quell-IP (z.B. 192.168.2.100) und die Quell-Portnummer (z.B. 32533) angegeben (durch einen „:“ voneinander getrennt). In der dritten Spalte sieht man die Ziel-IP und die Ziel-Portnummer. Die fünfte Spalte zeigt den Status der Verbindung (z.B. „HERGESTELLT“) und die letzte Spalte zeigt die sogenannte „Process ID“ (kurz: PID). Das ist die Nummer, unter der der betreffende Prozess/Thread vom Betriebssystem verwaltet wird (z.B. ein bestimmtes Browsertab vom Firefox).


TCP	192.168.2.100:32533	136.243.104.235:443	HERGESTELLT	2648
TCP	192.168.2.100:32541	169.51.77.229:5938	HERGESTELLT	2680
TCP	192.168.2.100:32542	34.209.130.220:443	HERGESTELLT	6972
TCP	192.168.2.100:33003	85.10.193.220:443	HERGESTELLT	1252
TCP	192.168.2.100:33005	52.10.184.57:443	WARTEND	0
TCP	192.168.2.100:33008	13.107.136.9:443	HERGESTELLT	3452

Diese Ausgabe erhält man bei Eingabe des Befehls `netstat -n -o` in einer Kommandozeile.

IP-Adresse

Nachdem die Transportschicht die zu versendenden Daten mit einem TCP-Header versehen hat, werden diese Informationen an die Internetschicht (Vermittlungsschicht im OSI-Modell) überge-

¹ Ein Thread ist ein sogenannter „nebenläufiger Prozess“. Jeder Prozess hat einen „Main-Thread“ und aus diesem heraus können zusätzliche Threads erzeugt werden. So kann z.B. ein Druckauftrag aus einer Textverarbeitung im Hintergrund ausgeführt werden und der Benutzer kann an seinem Text weiter arbeiten.

Arbeitsblatt Nr. 8	Q2 Technologie: Vernetzte IT-Systeme		B S G G
Datum:	Thema: Adressschemata bei TCP/IP		
Seite 3 von 4	Name:		

ben. Für den Versand der Daten ist jedoch noch eine weitere Information erforderlich: Die sogenannte „IP-Adresse“.

Eine IP-Adresse ist eine weltweit eindeutige Nummer für ein bestimmtes Rechnersystem.

Jedes Rechnersystem muss also zur Kommunikation über eine IP-Adresse verfügen. Diese IP-Adresse wird entweder lokal durch den Administrator konfiguriert (feste IP) oder durch einen sogenannten DHCP-Server im eigenen Netzwerk bereit gestellt und dem PC im Rahmen des Bootprozesses zugewiesen (dynamische IP). Im heimischen Umfeld enthält der DSL-Router üblicherweise einen DHCP-Server, der den Geräten dann eine IP-Adresse „verleiht“ (im WLAN nach erfolgreicher Authentifizierung).

Die Internetschicht trägt also nun im IP-Header die Quell-IP (Client) und die Ziel-IP (Server) ein. Durch die weltweite Eindeutigkeit dieser beiden IP-Adressen können nun die beiden Anwendungen (Firefox-Browser und Apache Webserver) miteinander kommunizieren.

Sowohl die beiden Portnummern wie auch die beiden IP-Adressen werden auf dem gesamten Transportweg zwischen Empfänger und Ziel (und umgekehrt auf dem Rückweg) nicht verändert!

Im obigen Beispiel werden IPv4-Adressen verwendet. Diese bestehen wie bereits erwähnt aus einer 32 Bit-Integerzahl. Diese Zahl wird in vier Gruppen à 8 Bit (ein Byte) unterteilt. Jedes Byte kann Werte zwischen 0 und 255 annehmen. Die vier Werte werden durch einen Punkt optisch voneinander getrennt.

Beispiel: 192 . 168 . 2 . 100

Da der mit der zunehmenden Anzahl von Rechnersystemen im Internet die freien, nicht vergebenen IPv4-Adressen immer weniger wurden, hat man ein neues IP-Adressschema entwickelt, das auf einer 128 Bit großen Integerzahl beruht: IPv6.

IPv6 Adressen werden allerdings in hexadezimaler Form geschrieben. Jede hexadezimale Ziffer steht für vier Bit; eine IPv6 Adresse besteht also aus 32 hexadezimalen Ziffern. Zur besseren Lesbarkeit werden diese 32 Hex-Ziffern in Vierergruppen geschrieben, die optisch durch einen Doppelpunkt voneinander getrennt werden.

Beispiel: 2003 : 00c0 : d71e : f380 : 7438 : e22a : 1e1e : f442

Aufgrund bestimmter Verkürzungsregeln lassen sich IPv6 Adressen auch kürzer schreiben.

Mit dem Befehl `ipconfig` in einer Befehlszeile lässt sich die IP-Konfiguration an-

```

Verbindungsspezifisches DNS-Suffix:
Verbindungslokale IPv6-Adresse . : fe80::416c:c708:841:7335%16
IPv4-Adresse (Auto. Konfiguration): 169.254.115.53
Subnetzmaske . . . . . : 255.255.0.0
Standardgateway . . . . . :

```

sehen. Ausführliche Informationen erhält man mit dem Befehl `ipconfig /all`.

Zusammengefasst: Die Internetschicht erstellt einen IP-Header, der dem TCP-Header und den Nutzdaten der Anwendung vorangestellt wird. In dem IP-Header befinden sich u.a. eine Quell- und eine Ziel IP. Hierdurch sind die beiden Rechnersysteme weltweit eindeutig bestimmt. Durch die Quell- und Ziel Portnummern sind die jeweiligen Prozesse definiert.

Eine IP-Adresse bezeichnet man als eine **logische Adresse**, da sich ein Rechnersystem durch seine (frei) zugeteilte IP-Adresse mit anderen Rechnersystemen zu einem Netzwerk gruppieren lässt, unabhängig vom tatsächlichen Ort!

MAC-Adresse

Die von der Internetschicht erzeugten Daten (IP-Header + TCP-Header + Anwendungsdaten) werden nun an die Netzzugangsschicht übermittelt. Die Netzzugangsschicht „enthält“ quasi die Netzwerkkarte, die die Informationen als einen „Bitstrom“ mittels physikalischer Signale (Spannungssignale, optische Signale oder Funk-Signale) überträgt.

Jede TCP/IP-Netzwerkkarte hat „fest eingebaut“ eine sogenannte MAC-Adresse. Eine solche MAC-Adresse besteht aus einer 48 Bit-Integerzahl, die (ähnlich wie eine IPv6 Adresse) in hexadezimaler Form geschrieben wird. Zur besseren Lesbarkeit werden jeweils zwei Hex-Ziffern zusammen gefasst und mittels Bindestrich oder Doppelpunkt optisch voneinander getrennt.

Beispiel: **d7:1e:f3:80:74:38** oder **d7-1e-f3-80-74-38**

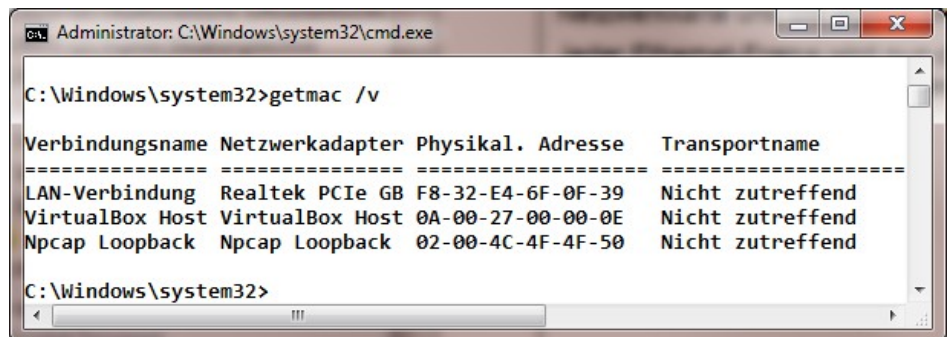
Die Netzzugangsschicht erzeugt ihrerseits einen sogenannten Ethernet-Rahmen (Ethernet-Frame) mit einem eigenen Header. In diesem Header werden u.a. die MAC-Adresse der Ziel-Netzwerkkarte und die eigene MAC-Adresse (Quell-Netzwerkkarte) eingetragen. Nutzlast des Ethernet-Frames sind die von der Internetschicht erhaltenen Daten.

Jeder Ethernet-Frame wird nun durch die Netzwerkkarte in das betreffende Signal des Transportmediums (elektrisches, optisches oder Funk-Signal) umgeformt und „auf die Reise geschickt“.

Mit dem Befehl **getmac /v** lässt sich für jeden Netzwerkadaper dessen MAC-Adresse anzeigen.

Da diese „fest eingebaut“ ist, bezeichnet man sie auch als **physikalische Adresse**.

Innerhalb eines Netzwerks darf diese Adresse keinesfalls zweimal vorkommen!



```

Administrator: C:\Windows\system32\cmd.exe
C:\Windows\system32>getmac /v

Verbindungsname Netzwerkadapter Physikal. Adresse Transportname
-----
LAN-Verbindung Realtek PCIe GB F8-32-E4-6F-0F-39 Nicht zutreffend
VirtualBox Host VirtualBox Host 0A-00-27-00-00-0E Nicht zutreffend
Npcap Loopback Npcap Loopback 02-00-4C-4F-4F-50 Nicht zutreffend

C:\Windows\system32>

```

Und wie geht's nach dem Versand weiter?

Die physikalischen Signale gelangen (irgendwann nach einigen Bruchteilen von Sekunden) zum Zielrechner. Die Netzwerkkarte des Zielrechners wandelt die physikalischen Signale in einen Bitstrom um und überprüft anhand der eigenen MAC-Adresse und der in den Daten angegebenen Ziel-MAC-Adresse, ob die Daten für ihn bestimmt sind. Die im Ethernet-Frame enthaltenen Daten werden nun an die Internetschicht weitergereicht. Dort wird der IP-Header ausgewertet und entfernt. Die verbleibenden Nutzdaten (TCP-Header + Anwendungsdaten) gelangen zur Transportschicht. Die Transportschicht wertet ebenfalls deren Header aus und reicht die Anwendungsdaten an die betreffende Server-Anwendung. Welche dies ist, gibt die Ziel-Portnummer (z.B. 80) an,

Die betreffende Anwendung erzeugt die Antwortdaten und übermittelt diese auf dem umgekehrten Weg.

Befinden sich Client und Server in verschiedenen Netzen, passieren die Daten auf ihrem Weg vom Client zum Server (und umgekehrt) weitere Rechnersysteme, die man „**Router**“ nennt.

Diese Router sorgen anhand der Ziel-IP im IP-Header, dass die Signale ihr Ziel erreichen. Wie dies erfolgt...davon später ;-)