



android



IOS

Internet

Datenübertragung

**TCP/IP Überblick
sowie weitere Protokolle
und Netzwerktechnologien**

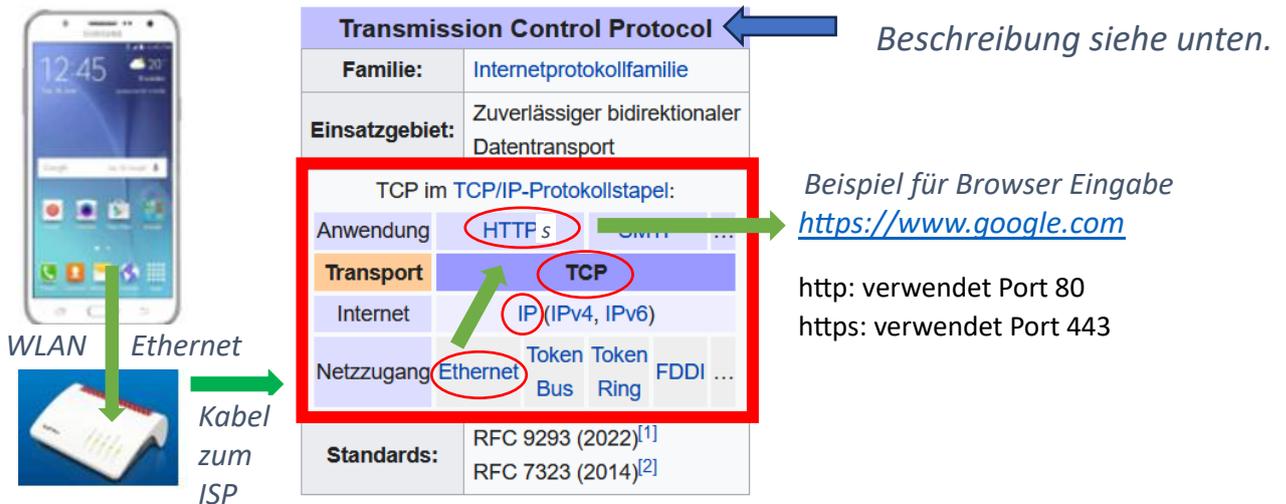


Digital Mobil Handy & Tablet Treff

Das Netz und seine Komponenten

Das Transmission Control Protocol, TCP (Übertragungssteuerungsprotokoll) ist ein Netzwerkprotokoll, das definiert, auf welche Art und Weise Daten zwischen Netzwerkkomponenten ausgetauscht werden sollen. Nahezu sämtliche aktuelle Betriebssysteme moderner Computer beherrschen TCP und nutzen es für den Datenaustausch mit anderen Rechnern. Das Protokoll ist ein zuverlässiges, verbindungsorientiertes, Transportprotokoll in Computernetzwerken. Es ist Teil der Internetprotokollfamilie, der Grundlage des Internets.

TCP ist im Prinzip eine Ende-zu-Ende-Verbindung in Vollduplex, die die Übertragung der Informationen in beide Richtungen zulässt, vergleichbar zu einem Telefongespräch.



Vereinfacht erklärt:

- Anwendung:** Empfänger öffnet Paket und nutzt es.
- Transport:** Zustellung ist vollständig und in richtiger Reihenfolge.
- Internet:** Navigation zeigt Weg durch verschiedene Netze.
- Netzzugang:** Straße auf der das Paket transportiert wird.

Ein vereinfachter Überblick der Abläufe im WorldWideWeb, wenn Daten übertragen werden.

Die Verbindung von z.B. Handy, Tablet, Alexa, TV, Laptop usw. im lokalen Heimnetzwerk erfolgt entweder über eine WLAN- (drahtlose Funkverbindung) oder LAN-Verbindung (mit Kabel) zum Heimrouter (Fritz Box). Diese Verbindungen im lokalen Netzwerk nutzen das Ethernet Protokoll und mittels der MAC-Adresse, die jedem Gerät vom Hersteller fest zugeordnet ist, werden die Daten dem jeweiligen Gerät eindeutig zugeordnet. Die vom Router für das lokale Heimnetzwerk zugewiesenen IP-Adressen werden zur Netzwerkkommunikation und das Routing verwendet.



Digital Mobil Handy & Tablet Treff

Die NAT (Netzwerk Adresse Translation) im Router ‚verbindet‘ die interne IP-Adresse mit der öffentlichen, externen IP-Adresse die der Router vom ISP (Internet Service Provider, Vertragspartner für Festanschluss z.B. Deutsche Telekom, Vodafone u.a.), dynamisch zugewiesen bekommt. Nach Router-Neustart und Verbindungsaufbau ins Internet bekommt der Router eine IP-Adresse zugewiesen, die dann auch im Internet sichtbar ist. An diese IP-Adresse werden dann z.B. auch die Werbeflyer von Unternehmen geschickt.

Das TCP-Protokoll stellt die Verbindung zur Anwendung her und nutzt dazu Ports. Die Kombination von IP-Adresse und Port wird Socket genannt und stellt eine bidirektionale Softwareschnittstelle da. Im Beispiel zu https, über Port 443, genau zu der Anwendung, die uns für Eingaben im Browser-Eingabe-Feld zur Verfügung steht. Zum Weitertransport der Daten wird durch das TCP-Protokoll verwendet das zuverlässige, geordnete Übertragung der Daten zwischen Absender und Empfänger und wieder zurück sicherstellt. *Die Daten, egal ob Dokumente, Bilder, Videos, Sprache (Video und Sprache verwenden hauptsächlich das UDP-Protokoll), werden in kleine Pakete aufgeteilt, diese werden fortlaufend nummeriert und es wird sichergestellt, dass sie am Ziel in der richtigen Reihenfolge und ohne Fehler beim Empfänger ankommen.* Sollten Pakete verloren gehen, weil z.B. die Verbindung zwischendurch schlecht wurde oder Umleitungen im Netzwerk notwendig waren, kümmert sich TCP um erneute Übertragung dieser verlorenen Pakete und reiht sie wieder in der richtigen Reihenfolge ein. TCP kann Paketen auch Priorität einräumen, sodass diese vorrangig übertragen wird.

HTTPS (Hypertext Transfer Protocol Secure) ist die sichere Version von **HTTP**, dem primären Protokoll für die Übertragung von Daten zwischen *Webbrowsern und Websites*. **HTTPS** ist verschlüsselt, um die Sicherheit der Datenübertragung zu verbessern.

Zur Veranschaulichung:

TCP/IP Datenpaket-Größe (MTU- Maximum Transmission Unit)

Typischerweise ist ein TCP-Paket 1500 Bytes groß. Davon werden einige Bytes für Header (Steuerungsbefehle) genutzt, somit bleiben etwas 1460 Bytes für die Nutzdaten.

Ein Bild mit der Größe 1 Megabyte (MB) entspricht ca. 1 Millionen Bytes.

1.000.000 Bytes: 1460 Bytes/Paket ~ **685 Pakete**

Das bedeutet, ein Bild in der gängigen Größe von 1 Megabyte wird in 685 Pakete aufgeteilt und über das Internet versendet. Am Empfangs-Server wird auf richtige Reihenfolge und Vollständigkeit geprüft damit das Bild korrekt dargestellt werden kann. Dann zum Empfänger-Netzwerk und Endgerät weitergeleitet. Wir sehen das komplette Bild.

Latenz ist ein weiteres Schlüsselwort für Datenübertragung im Internet. Es ist die Zeit, die Daten benötigen, um durch ein Netzwerk zu Reisen. Latenzwerte unter 50ms (Millisekunden) sind gut für Echtzeitanwendungen wie VoIP oder Online-Spiele. Akzeptable Werte für die meisten Anwendungen liegen bei bis zu 100ms. Liegen die Werte darüber kann es zu spürbaren Verzögerungen (z.B. bei Videoanrufen) kommen. Messbar mit PING oder <https://www.wieistmeineip.de> .



Digital Mobil Handy & Tablet Treff

Im lokalen Netzwerk (WLAN, LAN) werden die Daten als Ethernet-Frames mit dem Ethernet-Protokoll übertragen. Wenn die Daten das lokale Netzwerk über den Router (Fritz Box) verlassen, werden sie in Form von IP-Paketen mit dem TCP/IP Protokoll übertragen.

Der Vollständigkeit halber hier etwas mehr im Detail. Ein Standard Benutzer muss das aber nicht unbedingt verstehen. Zeigt aber ansatzweise wie komplex die Abläufe sind. Um im Beispiel zu bleiben werden, für das 1MB Bild, 685 so aufgebauter Pakete verschickt. Alles in rasender Geschwindigkeit. Wenn nötig um die ganze Welt!

Aufbau des TCP/IP Headers und Datenfeld. Jedes Datenpaket ist so aufgebaut.

TCP-Pseudo-Header (IPv4)				
Bit offset	Bits 0-3	4-7	8-15	16-31
0	IP-Absenderadresse			
32	IP-Empfängeradresse			
64	00000000		6 (=TCP)	TCP-Länge
96	Quellport			Zielport
128	Sequenznummer			
160	ACK-Nummer			
192	Datenoffset	Reserviert	Flags	Window
224	Prüfsumme			Urgent pointer
256	Options (optional)			
256/288+	Daten			

Jedem Datenpaket, das TCP verschickt, wird ein Header vorangestellt, der die folgenden Daten enthält:

- Sender-Port
- Empfänger-Port
- Paket-Reihenfolge (Nummer)
- Prüfsumme
- Quittierungsnummer
- Flags

TCP-Pakete setzen sich aus dem Header-Bereich und dem Daten-Bereich zusammen. Im Header sind alle Informationen enthalten, die für eine gesicherte TCP-Verbindung wichtig sind. Der TCP-Header ist in mehrere 32-Bit-Blöcke aufgeteilt. Mindestens enthält der Header 5 solcher Blöcke. Somit hat ein TCP-Header eine Länge von mindestens 20 Byte.



Digital Mobil Handy & Tablet Treff

Bedeutung der Felder im TCP-Header

Feldinhalt	Bit	Beschreibung
Quell-Port (Source-Port)	16	Hier steht der Quell-Port, von der die Anwendung das TCP-Paket verschickt. Bei einer Stellenanzahl von 16 Bit beträgt der höchste Port 65.535.
Ziel-Port (Destination-Port)	16	Hier steht der Ziel-Port, über welchen das TCP-Paket der Anwendung zugestellt wird. Bei einer Stellenanzahl von 16 Bit beträgt der höchste Port 65.535.
Sequenz-Nummer	32	Bei jeder TCP-Verbindung werden Nummern zwischen den Kommunikationspartner ausgehandelt. Während der Verbindung werden diese Nummern verwendet um die TCP-Pakete eindeutig zu identifizieren.
Acknowledgement-Nummer	32	Alle Datenpakete werden bestätigt. Dazu dient das ACK-Flag und die Acknowledgement-Nummer, die sich aus der Sequenz-Nummer und der Anzahl von empfangenen Bytes errechnet. Damit kann der Sender feststellen, ob die Daten beim Empfänger vollständig angekommen sind.
Data Offset	4	Hier steht die Anzahl der 32-Bit-Blöcke des TCP-Headers. Die Mindestmenge beträgt 5.
Reserviert	6	Dieser Bereich ist auf 000000 gesetzt und für Erweiterungen des TCP-Headers gedacht.
Flags	6	Kennzeichnung bestimmter für die Kommunikation und Weiterverarbeitung der Daten wichtiger Zustände (URG, ACK, PSH, RST, SYN, FIN).
Window-Größe	16	Der Empfänger sendet dem Sender in diesem Feld die Anzahl an Daten, die der Sender senden darf. Dadurch wird das Überlaufen des Empfangspuffers beim Empfänger verhindert. Den Vorgang nennt man Windowing und dient der Datenflusssteuerung.
Check-Summe	16	Dieses Feld dient der Kontrolle von Header- und Datenbereich.
Urgent-Pointer	16	Zusammen mit der Sequenz-Nummer gibt dieser Wert die genaue Position der Daten im Datenstrom an. Der Wert ist nur gültig, wenn das URG-Flag gesetzt ist.
Optionen/Füllbits (Options/Padding), jeweils 32 Bit lang		Dieses Feld beinhaltet optionale Informationen. Um die 32-Bit-Grenze einzuhalten wird das Options-Feld mit Nullen aufgefüllt.



Digital Mobil Handy & Tablet Treff

Um den Datentransport im Internet zu gewährleisten werden eine Reihe von Protokollen und Netzwerktechnologien verwendet.

Jedes Protokoll hat eine spezifische Rolle um das Netzwerk effizient und sicher zu machen. Hier eine vereinfachte Erklärung des Prozesses und den beteiligten Protokollen.

Daten im (W)LAN (Local Area Network)

Im LAN werden Daten typischerweise über das **Ethernet Protokoll** oder **Wi-Fi** übertragen. Geräte im LAN verwenden das IP-Protokoll (Internet-Protocol) um Datenpakete zu adressieren und weiterzuleiten.

Das **ARP-Protokoll** (Address Resolution Protocol) hilft dabei, *IP-Adressen in MAC-Adressen zu übersetzen*, damit die Datenpakete im LAN korrekt weitergeleitet werden

Datenübertragung ins Internet (WAN)

Um Daten aus dem LAN ins Internet zu senden, wird ein Router verwendet. Der Router verbindet das LAN mit dem **Wide Area Network** (WAN) also dem **WWW**, dem Internet. Der Router verwendet das **IP-Protokoll (IPv4 oder IPv6)** um Datenpakete zu adressieren und weiterzuleiten. Das **NAT-Protokoll** (Network Address Translation) wird verwendet um private IP-Adressen im LAN in öffentliche IP-Adressen umzuwandeln, die im Internet verwendet werden.

Datenübertragung im Internet

Im Internet werden Datenpakete über verschiedene Netzwerke und Router weitergeleitet. Dies geschieht mit **Routing-Protokollen** wie **BGP** (Border Gateway Protocol) oder **OSPF** (Open Shortest Path First). Das **TCP-Protokoll** (Transmission Control Program) wird verwendet um Datenpakete zuverlässig und schnell zu übertragen, das **UDP-Protokoll** (User Datagram Protocol) ist schneller, bietet aber keine Garantie für die Zustellung oder Reihenfolge der Datenpakete. Typische Verwendung für VoIP, Online-Spiele oder Live-Streams.

Datenübertragung zum Empfänger

Die Datenpakete erreichen schließlich den Zielserver oder den Empfänger. Dieser Prozess wird durch das **DNS-Protokoll** (Domain Name System) unterstützt indem Domainnamen in IP-Adressen oder umgekehrt übersetzt werden. Aus z.B. *www.google.com* wird *64.233.191.255* (die genaue Übersetzung variiert je nach Region und Server).

Auf der Anwendungsebene werden u.a. folgende Protokolle verwendet:

HTTP/HTTPS für Webseiten

FTP für Dateiübertragungen

SMTP für E-Mails

VoIP für Sprache

um die Daten zu interpretieren und zu verarbeiten.