

Kommunikationstechnik Teil 3 Webservices

DI (FH) Andreas Pötscher

HTL Litec

*Die **Client-Server-Architektur** ist das fundamentale Konzept der modernen Netzwerkkommunikation und basiert auf einer klaren Rollenverteilung zwischen zwei Partnern. Der Server ist dabei der passive Teil der auf eine Verbindung vom Client wartet. Während der Client aktiv die Verbindung zum Server aufbaut.*

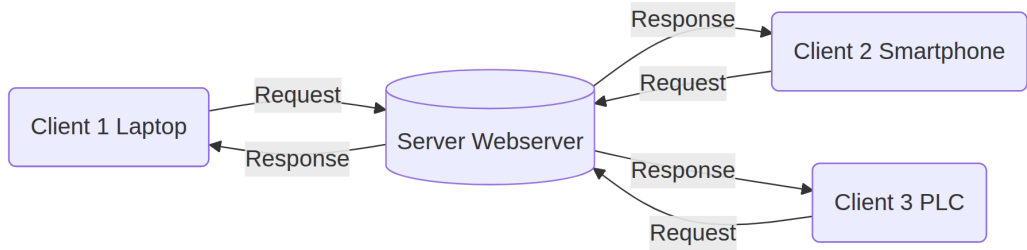


Figure 1: Ein Server mit mehreren verbundenen Clients

Beispiel Öffnen einer Website

1. Der Benutzer tippt in seinem Browser die Adresse *www.litec.ac.at* in die Adressleiste.

Beispiel Öffnen einer Website

1. Der Benutzer tippt in seinem Browser die Adresse *www.litec.ac.at* in die Adressleiste.
2. Der Browser baut eine Verbindung zum Webserver auf (meistens mit TCP/IP) und sendet einen Request.

Beispiel Öffnen einer Website

1. Der Benutzer tippt in seinem Browser die Adresse *www.litec.ac.at* in die Adressleiste.
2. Der Browser baut eine Verbindung zum Webserver auf (meistens mit TCP/IP) und sendet einen Request.
3. Der Server sendet einen Response, der die Website enthält, zurück da den Browser.

Beispiel Öffnen einer Website

1. Der Benutzer tippt in seinem Browser die Adresse *www.litec.ac.at* in die Adressleiste.
2. Der Browser baut eine Verbindung zum Webserver auf (meistens mit TCP/IP) und sendet einen Request.
3. Der Server sendet einen Response, der die Website enthält, zurück da den Browser.
4. Der Browser zeigt die Website an.

Beispiel Abfragen eines Webservice

1. Eine Dashboard-Software aktualisiert Wetterdaten einmal in der Stunde.

Beispiel Abfragen eines Webservice

1. Eine Dashboard-Software aktualisiert Wetterdaten einmal in der Stunde.
2. Die Software baut eine Verbindung zum Server auf (meistens mit TCP/IP) und sendet einen Request.

Beispiel Abfragen eines Webservice

1. Eine Dashboard-Software aktualisiert Wetterdaten einmal in der Stunde.
2. Die Software baut eine Verbindung zum Server auf (meistens mit TCP/IP) und sendet einen Request.
3. Der Server sendet einen Response, der die Wetterdaten als json String enthält, zurück an die Software.

Beispiel Abfragen eines Webservice

1. Eine Dashboard-Software aktualisiert Wetterdaten einmal in der Stunde.
2. Die Software baut eine Verbindung zum Server auf (meistens mit TCP/IP) und sendet einen Request.
3. Der Server sendet einen Response, der die Wetterdaten als json String enthält, zurück an die Software.
4. Die Wetterdaten werden am Dashboard angezeigt.

Für die Kommunikation von Geräten in einem Netzwerk wird sehr häufig das HTTP Protokoll verwendet. Eine HTTP-Nachricht ist das formale Paket, das zwischen Client und Server geschnürt wird. Da HTTP ein textbasiertes Protokoll ist, folgt der Aufbau einer strengen, für Menschen lesbaren Struktur, die in Request (Anfrage) und Response (Antwort) unterteilt wird.

1. Mit Node-Red einen HTTP Server aufbauen und Website mit dem Browser ansehen.
2. Daten aus dem Request auf der Website anzeigen.
3. Mit Node-Red einen HTTP Client aufbauen.
4. Mit Node-Red einen TCP Server aufbauen und mit dem Browser darauf verbinden.

Ein HTTP Request wird vom Client an den Server in einem lesbaren Format (als Text) gesendet. Beispielsweise:

```
> GET /news HTTP/1.1  
> Host: www.litec.ac.at  
> User-Agent: curl/8.5.0  
> Accept: */*
```

Der Request besteht dabei aus drei Teilen:

Request start line: GET /news HTTP/1.1

- ▶ Die Methode die Verwendet wird z.B. GET
- ▶ Den Pfad zur gewünschten Unter-Seite z.B. /news. Wenn die Hauptseite aufgerufen werden soll dann muss / verwendet werden.
- ▶ Die Protokollversion z.B. HTTP/1.1

Request Headers:

- ▶ Enthält Parameter in der Form Name: Wert
- ▶ Die Adresse die aufgerufen werden soll Host: `www.litec.ac.at`
- ▶ Software den Request absetzt. User-Agent: `curl/8.5.0`
- ▶ Dateien die im Response akzeptiert werden. Accept: `*/*`
- ▶ Daneben gibt es noch mehr optionale Parameter

Request Body:

- ▶ Optional für bestimmte Methoden (z.B. POST).
- ▶ Enthält die Daten die übertragen werden.

- ▶ **GET:** Holt ein Dokument vom Server. *Beispiel:* Laden einer Website.

- ▶ **GET:** Holt ein Dokument vom Server. *Beispiel:* Laden einer Website.
- ▶ **HEAD:** Holt den Header eines Dokuments vom Server. *Beispiel:* Vorladen einer Website

- ▶ **GET:** Holt ein Dokument vom Server. *Beispiel:* Laden einer Website.
- ▶ **HEAD:** Holt den Header eines Dokuments vom Server. *Beispiel:* Vorladen einer Website
- ▶ **POST:** Sendet Daten zum Server. *Beispiel:* Daten werden auf einer Website eingegeben und zum Server gesendet.

- ▶ **GET:** Holt ein Dokument vom Server. *Beispiel:* Laden einer Website.
- ▶ **HEAD:** Holt den Header eines Dokuments vom Server. *Beispiel:* Vorladen einer Website
- ▶ **POST:** Sendet Daten zum Server. *Beispiel:* Daten werden auf einer Website eingegeben und zum Server gesendet.
- ▶ **PUT:** Sendet eine Datei zum Server. *Beispiel:* Hochladen von neuem Content einer Website.

- ▶ **GET:** Holt ein Dokument vom Server. *Beispiel:* Laden einer Website.
- ▶ **HEAD:** Holt den Header eines Dokuments vom Server. *Beispiel:* Vorladen einer Website
- ▶ **POST:** Sendet Daten zum Server. *Beispiel:* Daten werden auf einer Website eingegeben und zum Server gesendet.
- ▶ **PUT:** Sendet eine Datei zum Server. *Beispiel:* Hochladen von neuem Content einer Website.
- ▶ **TRACE** Verfolgt eine Message zum Server. *Beispiel:* Testen einer Verbindung.

- ▶ **GET:** Holt ein Dokument vom Server. *Beispiel:* Laden einer Website.
- ▶ **HEAD:** Holt den Header eines Dokuments vom Server. *Beispiel:* Vorladen einer Website
- ▶ **POST:** Sendet Daten zum Server. *Beispiel:* Daten werden auf einer Website eingegeben und zum Server gesendet.
- ▶ **PUT:** Sendet eine Datei zum Server. *Beispiel:* Hochladen von neuem Content einer Website.
- ▶ **TRACE** Verfolgt eine Message zum Server. *Beispiel:* Testen einer Verbindung.
- ▶ **OPTIONS** Anfrage nach den Options eines Servers. *Beispiel:* Anfragen welche Methoden der Server anbietet.

- ▶ **GET:** Holt ein Dokument vom Server. *Beispiel:* Laden einer Website.
- ▶ **HEAD:** Holt den Header eines Dokuments vom Server. *Beispiel:* Vorladen einer Website
- ▶ **POST:** Sendet Daten zum Server. *Beispiel:* Daten werden auf einer Website eingegeben und zum Server gesendet.
- ▶ **PUT:** Sendet eine Datei zum Server. *Beispiel:* Hochladen von neuem Content einer Website.
- ▶ **TRACE** Verfolgt eine Message zum Server. *Beispiel:* Testen einer Verbindung.
- ▶ **OPTIONS** Anfrage nach den Options eines Servers. *Beispiel:* Anfragen welche Methoden der Server anbietet.
- ▶ **DELETE** Löscht ein Dokument vom Server. *Beispiel:* Löschen einer Artikels aus einem Online Shop.

1. Mit Node-Red einen HTTP Server mit einen html Textinput aufbauen und Website mit dem Browser ansehen.
2. Mit Node-Red den HTTP POST abfragen.

Die Antwort (Response) wird vom Server an den Client zurückgesendet. Sie bestätigt den Erhalt der Anfrage und liefert die gewünschten Daten oder eine Fehlermeldung.

Beispielsweise:

```
< HTTP/1.1 200 OK
< Content-Type: text/html; charset=UTF-8
< Content-Length: 1542
< Server: Apache/2.4.58
<
< <!DOCTYPE html><html>... (Daten)
```

Der Response besteht ebenfalls aus drei Teilen:

Status line: HTTP/1.1 200 OK

- ▶ Die verwendete Protokollversion, z. B. HTTP/1.1.
- ▶ Der Status-Code, eine dreistellige Zahl, die das Ergebnis angibt, z. B. 200.
- ▶ Die Status-Message, eine kurze Textbeschreibung zum Code, z. B. OK.

Response Headers:

- ▶ Enthält Metadaten zur Antwort in der Form `Name: Wert`.
- ▶ Der Datentyp der Antwort: `Content-Type: text/html` (zeigt an, dass eine Webseite folgt).
- ▶ Die Größe der Daten im Body: `Content-Length: 1542` (in Bytes).
- ▶ Informationen über die Server-Software: `Server: Apache/2.4.58`.
- ▶ Weitere optionale Parameter (z. B. Datum, Cache-Einstellungen).

Response Body

- ▶ Enthält die eigentliche Nutzlast (Payload).
- ▶ Das kann der HTML-Code einer Webseite, ein Bild oder ein Datensatz im JSON-Format (z. B. Sensorwerte der SPS) sein.
- ▶ Der Body ist durch eine Leerzeile von den Headern getrennt.

Der Server teilt dem Client über einen dreistelligen Code mit, wie die Anfrage verarbeitet wurde. Man unterscheidet fünf Kategorien:

- ▶ **1xx Information:** Die Anfrage wurde empfangen, die Bearbeitung dauert an.
Beispiel: 100.

Der Server teilt dem Client über einen dreistelligen Code mit, wie die Anfrage verarbeitet wurde. Man unterscheidet fünf Kategorien:

- ▶ **1xx Information:** Die Anfrage wurde empfangen, die Bearbeitung dauert an.
Beispiel: 100.
- ▶ **2xx: Erfolg:** Die Anfrage wurde erfolgreich bearbeitet. *Beispiel:* 200 OK Die Standardantwort für erfolgreiche GET-Anfragen, 201 Created Die Anfrage war erfolgreich und eine neue Ressource wurde erstellt (oft nach POST/PUT).

Der Server teilt dem Client über einen dreistelligen Code mit, wie die Anfrage verarbeitet wurde. Man unterscheidet fünf Kategorien:

- ▶ **1xx Information:** Die Anfrage wurde empfangen, die Bearbeitung dauert an.
Beispiel: 100.
- ▶ **2xx: Erfolg:** Die Anfrage wurde erfolgreich bearbeitet. *Beispiel:* 200 OK Die Standardantwort für erfolgreiche GET-Anfragen, 201 Created Die Anfrage war erfolgreich und eine neue Ressource wurde erstellt (oft nach POST/PUT).
- ▶ **3xx Umleitung:** Weitere Schritte sind erforderlich, um die Anfrage abzuschließen. *Beispiel:* 301 Moved Permanently Die angeforderte Seite/Datei befindet sich nun dauerhaft unter einer anderen Adresse.

Der Server teilt dem Client über einen dreistelligen Code mit, wie die Anfrage verarbeitet wurde. Man unterscheidet fünf Kategorien:

- ▶ **4xx Client Fehler:** Die Anfrage war fehlerhaft oder kann nicht ausgeführt werden.
Beispiel: 400 Bad Request Die Anfrage war syntaktisch falsch (z. B. Fehler im JSON-Body). 401 Unauthorized Der Zugriff erfordert eine Authentifizierung (z. B. Login fehlt).

Der Server teilt dem Client über einen dreistelligen Code mit, wie die Anfrage verarbeitet wurde. Man unterscheidet fünf Kategorien:

- ▶ **4xx Client Fehler:** Die Anfrage war fehlerhaft oder kann nicht ausgeführt werden. *Beispiel:* 400 Bad Request Die Anfrage war syntaktisch falsch (z. B. Fehler im JSON-Body). 401 Unauthorized Der Zugriff erfordert eine Authentifizierung (z. B. Login fehlt).
- ▶ **5xx** Der Server hat die Anfrage eigentlich verstanden, konnte sie aber nicht verarbeiten. *Beispiel:* 500 Internal Server Error Ein allgemeiner Fehler im Server (z. B. Absturz des SPS-Webservice-Skripts). 503 Service Unavailable Der Server ist überlastet oder wird gerade gewartet.

URL (Uniform Resource Locator)

Eine URL (Uniform Resource Locator) ist die eindeutige Webadresse, die als Adresse einer Ressource (Webseite, Bild, Datei) im Internet dient. Z.B.

`http://www.litec.ac.at/fileadmin/user_upload/00_TS_Anmeldeformular.dotx`

Die Adresse besteht aus 3 Teilen.

- ▶ **Scheme:** Das Protokoll das verwendet wird. `http://`
- ▶ **Host:** Ort an dem der Server liegt. `www.litec.ac.at` Kann auch nur eine IP-Adresse sein. Z.B. `192.168.88.1`
- ▶ **Path:** Pfad zur gewünschten Resource.
`/fileadmin/user_upload/00_TS_Anmeldeformular.dotx`

Parameter können direkt an die URL (Uniform resource locator) angehängt werden. Das wird oft für Filter oder IDs genutzt. Diese werden mit einem Fragezeichen getrennt an die URL angehängt und bestehen aus Key-Value Pairs

URL?key1=value1&key2=value2. Der Server kann diese dann als Parameter weiter verwenden und dementsprechend für die Antwort nutzen.

Beispiel, es soll über ein Webservice die Temperatur von Sensor 42 in der Einheit celsius abgefragt werden:

```
/api/sensor?id=42&unit=celsius
```

Um die Sicherheit der Datenübertragung zu gewährleisten, wird HTTP heute fast ausschließlich mit TLS (Transport Layer Security) kombiniert, was als HTTPS bezeichnet wird.

- ▶ Das Problem bei HTTP: Daten werden im Klartext übertragen. In einem Netzwerk könnte jeder Teilnehmer (z. B. im Firmen-WLAN) Passwörter oder sensible Sensordaten mitlesen (Sniffing).

Um die Sicherheit der Datenübertragung zu gewährleisten, wird HTTP heute fast ausschließlich mit TLS (Transport Layer Security) kombiniert, was als HTTPS bezeichnet wird.

- ▶ Das Problem bei HTTP: Daten werden im Klartext übertragen. In einem Netzwerk könnte jeder Teilnehmer (z. B. im Firmen-WLAN) Passwörter oder sensible Sensordaten mitlesen (Sniffing).
- ▶ Die Lösung HTTPS: Bevor die eigentlichen HTTP-Daten fließen, bauen Client und Server einen verschlüsselten Tunnel auf. Dabei authentifiziert sich der Server mit einem Zertifikat, um sicherzustellen, dass der Client wirklich mit der echten SPS oder dem echten Server spricht (Schutz vor Man-in-the-Middle-Angriffen).

Um die Sicherheit der Datenübertragung zu gewährleisten, wird HTTP heute fast ausschließlich mit TLS (Transport Layer Security) kombiniert, was als HTTPS bezeichnet wird.

- ▶ Das Problem bei HTTP: Daten werden im Klartext übertragen. In einem Netzwerk könnte jeder Teilnehmer (z. B. im Firmen-WLAN) Passwörter oder sensible Sensordaten mitlesen (Sniffing).
- ▶ Die Lösung HTTPS: Bevor die eigentlichen HTTP-Daten fließen, bauen Client und Server einen verschlüsselten Tunnel auf. Dabei authentifiziert sich der Server mit einem Zertifikat, um sicherzustellen, dass der Client wirklich mit der echten SPS oder dem echten Server spricht (Schutz vor Man-in-the-Middle-Angriffen).
- ▶ Auswirkung auf die Nachricht: Die Anatomie der Nachricht (Request/Response) bleibt identisch, aber der gesamte Inhalt wird für Außenstehende unlesbar chiffriert.