



openHPI – Sicherheit im Internet
Offenes Internet

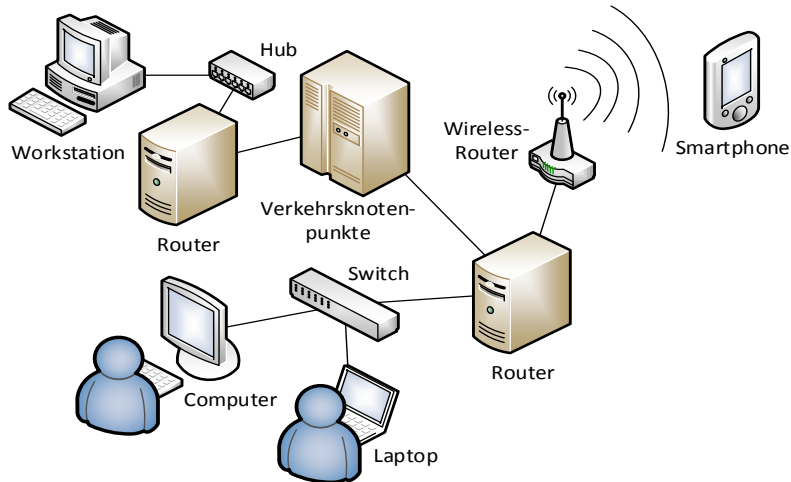
Prof. Dr. Christoph Meinel
Hasso-Plattner-Institut, Potsdam

Komponenten eines Netzwerks

Netzwerke bestehen aus den folgenden Komponenten:

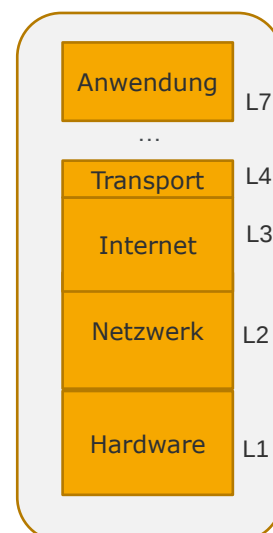
- **Endgeräte** – „Hosts“, z.B.
 - Computer, Laptops, Smartphones, Tablets, Drucker, ...
- **Infrastrukturkomponenten** und **Zwischensysteme** zur
 - Ankopplung von Endgeräten
 - Gewährleistung des Netzwerkbetriebs, z.B.
 - Router, Switches, Gateways
- **Physikalisches Verbindungsmedium**
 - Verkabelung, WLAN-Verbindung, ...

Komponenten eines Netzwerks

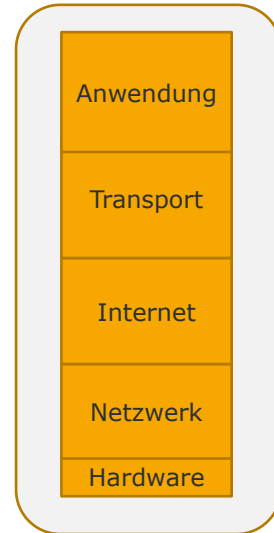


Infrastrukturkomponenten

- **Gateway**
 - Kommunikation zwischen Anwendungen
 - Übersetzung von Anwendungsprotokollen
- **Router**
 - Verbindung von eigenständigen Netzwerken
- **Switches**
 - Verbindung von Endgeräten in einem Netzwerk
- **Repeater**
 - Verstärkung von Signalen bei höheren Distanzen



- **DNS-Adresse** (z.B. www.internet.de)
 - Textuelle Adresse (Hostname) für ein Endgerät (Computer, Smartphone, ...)
- **Port** (z.B. 80 für WWW)
 - Kommunikation zwischen Anwendungen auf Endgeräten
- **IP-Adresse** (z.B. 192.168.0.1)
 - Kommunikation zwischen Endgeräten über Netzwerkgrenzen hinweg
- **Hardwareadresse** (z.B. 00:11:22:33:44:55)
 - Identifiziert Endgeräte in einem Netzwerk



- Nachrichten werden im Internet aufgeteilt in Datenpaketen übertragen. Dieses Prinzip der Datenübertragung heißt **Paketvermittlung**
 - **Route** – Transportweg vom Sender zum Empfänger –, auf dem die einzelnen Datenpakete gesendet werden, verläuft über verschiedene Zwischenstationen (**Router**)
 - Route ist **nicht** von vornherein festgelegt. Jede Zwischenstation entscheidet nur über Weiterleitung an „die richtige“ nächste Vermittlungsstation- „**Next Hop**“
 - Spezielle **Routing-Verfahren** sorgen für Ermittlung einer optimalen Route zum Ziel
- Große Pakete werden vor Übertragung in kleinere Pakete **fragmentiert** und im Endsystem zu ursprünglichen Paketen zusammengesetzt (**defragmentiert**)

Paketvermittlungstechnik heißt „**Store-and-Forward Switching**“ (dt.: Speichern-und-Weiterleiten)

- Weitergabe von Paketen von Zwischenstation zu Zwischenstation
- Daten werden auf Zwischensystem (Switch/Router) zwischengespeichert und dann weitergereicht



Viele der Sicherheitsrisiken des Internets und der Internetworking-Technik **erklären sich aus der Entstehungsgeschichte** des Internet

- Internetprotokolle und Internetworking-Technik wurden in einem Forschungsprojekt entwickelt
 - War nicht gedacht für weltweiten Einsatz als globale Netzwerktechnik für Millionen von Nutzer
 - Ursprungsannahmen:
 - kleine Anzahl von Nutzern
 - vertrauenswürdige Nutzer
- **Sicherheit spielte bei der Entwicklung keine bzw. nur eine untergeordnete Rolle ...**

Es fehlen Mechanismen zur verlässlichen Authentifizierung und Autorisierung

- Es ist leicht, sich im Internet als jemand anderes auszugeben, sowohl
 - bei Internet- und Transportprotokollen (IP, ICMP, TCP, UDP)
 - als auch bei Anwendungsprotokollen (HTTP, SMTP, POP3, ...)

Das begünstigt die folgenden **Angriffe**:

- Fälschung von Adressen – „**Spoofing**“
- Zwischenschalten in Verbindungen – „**Man-in-the-Middle**“
- Umgehen der Authentifizierung – „**Privilege Escalation**“

Verbindungen sind nicht abgesichert

- Aufgrund der ursprünglichen Annahme, dass Internet nur von vertrauenswürdigen Nutzern benutzt wird
 - Nachrichten / Datenpakete werden im Klartext gesendet und können von anderen gelesen und modifiziert werden

Das begünstigt die folgenden **Angriffe**

- Zwischenschalten in Verbindungen – „**Man-in-the-Middle**“
- Abhören – „**Eavesdropping**“ / „**Sniffing**“