openHPI-Kurs: Wie funktioniert das Internet?

Einführung Rechnernetze

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

Rechnernetze (1/2)

Wie können Nachrichten von einem Computer, Smartphone oder Tablet an Freunde oder Bekannte im Nachbarhaus oder ans andere Ende der Welt übertragen werden?

Brauchen zunächst Verständnis der **Funktionsweise von Rechnernetzwerken** – wie können zwei Rechner Daten austauschen?

Jedes Netzwerk ist charakterisiert durch seine

- Infrastruktur – Netzwerkkarte, Kabel, Funk, …
- Adressformate und Adressierungsschemata
- Zugriffssteuerung – wer darf wann senden, damit die Datenübertragung möglichst fehlerfrei funktioniert
- eigene Anforderungen und Mechanismen

Rechnernetze (2/2)

Es gibt sehr viele verschiedene Typen von Rechnernetzwerken und Technologien:

- LAN – Lokale Netzwerke, z.B.
  - Ethernet – wichtigste LAN Technologie
- WLAN – Kabellose Netze
- WAN – Weitverkehrsnetze
- …

Wollen uns die verschiedenen Rechnernetztechnologien in Woche 2 näher anschauen und befassen mit den Grundprinzipien von

- Routing in Weitverkehrsnetzen und wichtigen Routingverfahren

In einem **Exkurs** soll kurz beschrieben werden, wie Texte, Bilder und Videos über Netzwerke transportierbar werden

openHPI-Kurs: Wie funktioniert das Internet?

LAN – Lokale Netze

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

Einführung (1/2)

LAN – **Local Area Networks** – lokale Netze verbinden Rechner in enger räumlicher Nachbarschaft (~ mehrere hundert Meter)

- Im Gegensatz zu Punkt-zu-Punkt-Verbindungen nutzen die an ein LAN angeschlossenen Rechner Netzwerkinfrastruktur und Übertragungsmedium gemeinsam
- Gemeinsame Nutzung der Netzressourcen schafft hohe Wirtschaftlichkeit
- LANs sind die am weitesten verbreitete Form von Rechnernetzen
- LANs sind in der Regel private Netze, die ohne besondere Vorschriften von jedermann auf seinem Grundstück installiert und betrieben werden können

Einführung (2/2)

Gemeinsame Nutzung des Übertragungsmediums erfordert hohen Koordinations- und Verwaltungsaufwand

Grundidee

- Versendete Datenpakete werden zunächst von allen angeschlossenen Rechnern empfangen „**Broadcast Network**"
- Adressfeld im Datenpaket spezifiziert den eigentlichen Empfänger
- Nach Empfang eines Datenpakets überprüft jeder Rechner, ob das Paket für ihn bestimmt ist – wenn
  - nein → Paket wird verworfen
  - ja → Paket wird verarbeitet

Adressierung im LAN (1/3)

Damit ein Rechner im LAN eindeutig angesprochen werden kann, wird ihm eine **Adresse** zugeordnet

- Adressen sind Werte in einem festgelegten Format, die ein Rechnernetz oder einen Rechner (genauer eine Netzwerkschnittstelle) eindeutig identifizieren
- Auf jeder Schicht des Kommunikationsprotokollstapels können eigene Adressformate definiert sein
- Jedes Datenpaket enthält in einem Header die Adressen des Senders (Source) und des Empfängers (Destination) sowie weitere für den korrekten Transport notwendige Zusatzinformationen

Adressierung im LAN (2/3)

LAN-Kommunikationsschnittstelle eines angeschlossenen Rechners filtert ankommende Datenpakete anhand der Empfängeradressen aus und übergibt sie bei Adressübereinstimmung an dessen Betriebssystem

- Zu sendende Daten werden an LAN-Kommunikationsschnittstelle übergeben, dort zu Paketen verpackt, adressiert und versendet (ohne CPU des Rechners in Anspruch zu nehmen)
- Man unterscheidet
  - **Individualadressen** – Adresse für individuellen Rechner
  - **Multicast-Adressen** – gemeinsame Gruppenadresse für Rechnerauswahl
  - **Broadcast-Adressen** – zur Adressierung aller Rechner eines LANs

Adressierung im LAN (3/3)

Von besonderer Bedeutung sind sogenannte **MAC-Adressen** – **Media Access Control Address** – die Hardwareadressen der LAN-Kommunikationsschnittstellen

Eine MAC-Adresse darf innerhalb eines LANs nur einmal vorkommen, sie muss eindeutig sein. Man unterscheidet:

- **statische Adresse** – weltweit eindeutige, vom Hersteller einer LAN-Schnittstellenkarte vergebene Hardwareadresse
- **konfigurierbare Adresse** – werden durch Netzbetreiber frei festgelegt, lediglich Eindeutigkeit im LAN muss gewährleistet sein
- **dynamische Adresse** – LAN-Schnittstellenkarte initiiert bei Neustart des Rechners automatische Zuordnung einer Hardwareadresse (evtl. Fehlversuche)

MAC-Adressen folgen IEEE-802-Adressierungsschema - 16 oder 48 Bit

Paketformat im LAN

Jede LAN-Technologie definiert ihr eigenes **Paketformat**

- Pakete bestehen aus **Nutzdaten** und **Paketheader**
- Paketheader enthält neben Adressdaten zusätzliche Verwaltungsinformationen, z.B. Art der Nutzdaten, …
- Jede Schicht im Protokollstapel einer Netzwerktechnologie fügt dem Datenpaket einen eigenen Paketheader hinzu, zusammen mit diesem bildet es dann die Nutzdaten der darunterliegenden Schicht

Spezielle LAN-Hardware (1/2)

LAN-Schnittstellenkarten (auch Netzwerkadapter, Netzwerkkarte, LAN-Kommunikationsschnittstellenkarte, Network Interface Card (NIC), …):

- Hardware zum Anschluss eines Rechners an ein LAN
- LAN-Schnittstellenkarten sind jeweils für eine LAN-Technologie ausgelegt
- Funktionieren wie Ein-/Ausgabegeräte und übernehmen Einzelheiten der Paketübertragung ohne auf CPU des Rechners zuzugreifen
- Können im LAN benutzte physikalische Signale richtig interpretieren
- Filtern nicht relevante Datenpakete aus

Spezielle LAN-Hardware (2/2)

Network-Analyzer (auch Network-Sniffer, Packet-Sniffer, **Sniffer**):

- (Tragbares) Gerät bzw. spezielle Software zur Ermittlung der Leistungsfähigkeit eines LANs und zur Fehlererkennung
- „Hört" alle über das Netzwerk verschickte Daten ab – im „Promiscuous Mode" kann jedes empfangene Paket an Analyse-Software des Network-Analyzers zur weiteren Untersuchung weitergeleitet werden
- Network-Analyzer sind auch einsetzbar zur Überwachung bestimmter Rechner

Wichtige LAN-Technologien

Ethernet

- wichtigste LAN-Technologie

Token-Ring-Technologie

- lange Zeit Hauptkonkurrent von Ethernet

FDDI – Fiber Distributed Data Interface

- ähnlich zu Token-Ring aber mit Glasfaser und anderem Zugriffsmechanismus

ATM – Asynchronous Transfer Mode

- Basistechnologie für B-ISDN

...

LAN-Erweiterungen (1/2)

Zur Erweiterung der begrenzten Reichweite eines LANs und zur Kopplung verschiedener LANs stehen spezielle Hardware-Komponenten bereit, wie z.B.

Optisches Modem (Fiber Modem) – zur Ausdehnung von LANs

- machen Erweiterung von kupferkabelbasierten LANs durch Lichtwellenleiterstrecken möglich

LAN-Repeater – zur Ausdehnung von LANs

- können Signale (elektrische oder optische) verstärken

Bridge – zur Ausdehnung und Kopplung von LANs

- vollständige Rechner, die unterschiedliche LAN-Technologien verknüpfen können

…

LAN-Erweiterungen (2/2)

...

Switch – zur Kopplung von Computern und LAN-Segmenten

- Für jedes eingehende Paket wird das jeweilige Ziel festgestellt und das Paket wird nur an dieses Ziel gesendet

Hub – zur Kopplung von Computern und LAN-Segmenten

- Geräte, die gleichartige LAN-Technologien verknüpfen können. Alle eingehenden Pakete werden an alle angeschlossenen Geräte gesendet

openHPI-Kurs Wie funktioniert das Internet?

Ethernet – Wichtigste LAN Technologie

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

Allgemeines

Ethernet ist die wichtigste LAN-Technologie, ursprünglich basierend auf Bus-Topologie

Anfänge:

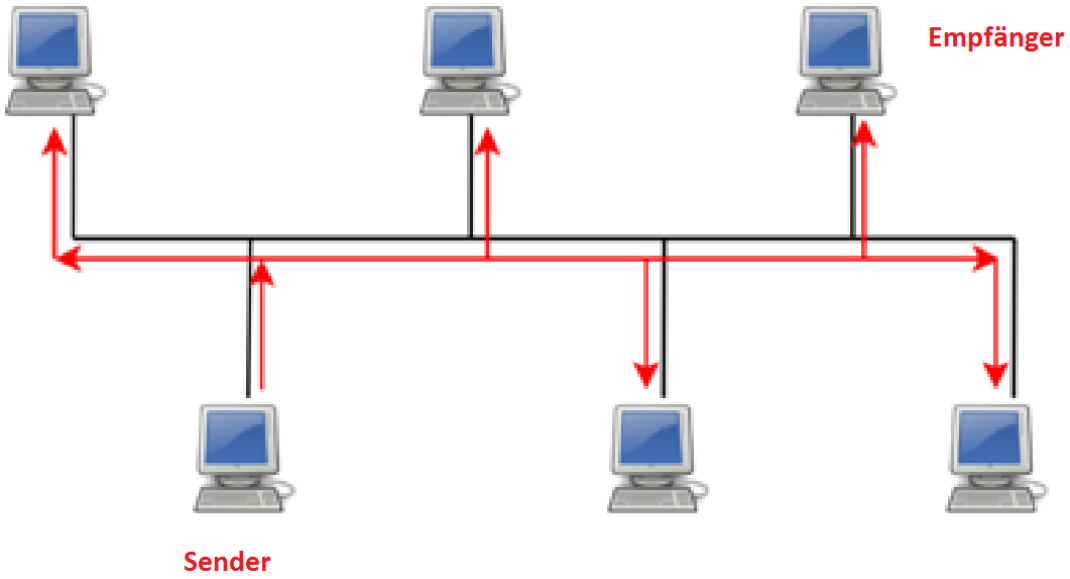
- Konzipiert am XEROX PARC (R. Metcalfe, D. Boggs) Anfang der 70er Jahre
- Erstes Ethernet konnte bis zu 256 Rechner bei max. Kabellänge von 1.000m mit Bandbreite 2,94 Mbps vernetzen
- IEEE ratifizierte 10Mbps-Ethernet-Spezifikation der Allianz aus Xerox, Digital, Intel

Basiskomponenten:

- Ethernet-Kabel – physikalisches Medium
- CSMA/CD – Regelwerk für konkurrierenden Zugriff auf das Übertragungsmedium
- Ethernet-Datenpakete (Frame, Rahmen) – Struktur der zu sendenden Datensätze

Ethernet - Grundprinzip

Datenpakete werden über den Bus versendet



Alle angeschlossenen Rechner empfangen jedes Datenpaket, doch nur der Zielrechner verarbeitet es

Ethernet-Vielfachzugriffsalgorithmus CSMA/CD (1/3)

Ethernet-Vielfachzugriffsalgorithmus:
Carrier **S**ense **M**ultiple **A**ccess / **C**ollision **D**etection

- Sobald ein Rechner ein Paket sendet, wird es von allen angeschlossenen Rechnern – **Broadcast** – empfangen
- Zu jedem Zeitpunkt kann höchstens ein Paket übertragen werden; werden zwei Pakete gleichzeitig übertragen, kommt es zur Kollision
- **CSMA/CD** regelt
  - konkurrierenden Sendezugriff der Rechner und
  - Auflösung von Kollisionen

Ethernet-Vielfachzugriffsalgorithmus CSMA/CD (2/3)

Grundregeln:

- **Carrier Sensing**:
  - Rechner „horcht“ auf Ether, bevor er sendet
  - Ist Ether besetzt, wartet er eine zufällige Zeitspanne „Back Off-Time“ ab
- **Collision Detection**:
  - Rechner horchen, ob eine Kollision stattgefunden hat
  - Wenn ja, wird Übertragung abgebrochen „JAM Signal“

Ethernet-Vielfachzugriffsalgorithmus CSMA/CD (3/3)

- Ethernet bietet **verbindungslosen** (connectionless) Dienst
- Ethernet bietet **unzuverlässigen** (non-reliable) Dienst
  - Paket beinhaltet zwar Prüfsumme, nach Empfang wird jedoch kein explizites Acknowledgement zurückgeschickt (weder bei Erfolg, noch bei Misserfolg) – um Fehlerbehebung muss sich ein Protokoll einer höheren Schicht kümmern

Ethernet-Datenpaketformat

Grundstruktur der Datenpakete ist bei allen Ethernet-Technologien gleich

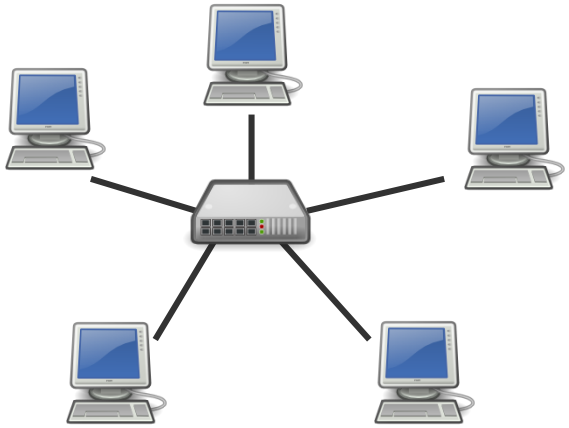
- Präambel – 7 bzw. 8 Byte
  - 7 Bytes beginnen mit „10101010“ – wecken Empfänger und dienen zur Synchronisation
  - letztes Byte endet mit „10101011“ – zeigt Beginn des eigentlichen Pakets an
- Zieladresse und Ursprungsadresse – jeweils 6 Byte
- Typfeld – weist Paket als Paket des Ethernet-Protokolls (also des Data-Link-Layer) aus
- Nutzdaten – 46 bis 1500 Byte - mit abschließender Prüfsumme – 4 Byte

Ethernet-Topologien (Beispiele)

Bus

Alle Computer empfangen das Datenpaket, doch nur der Zielrechner verarbeitet es

Stern



Datenpakete werden über die zentrale Station (Hub/Switch) an den Zielrechner gesendet

Ethernet-Hardwarekomponenten (1/5)

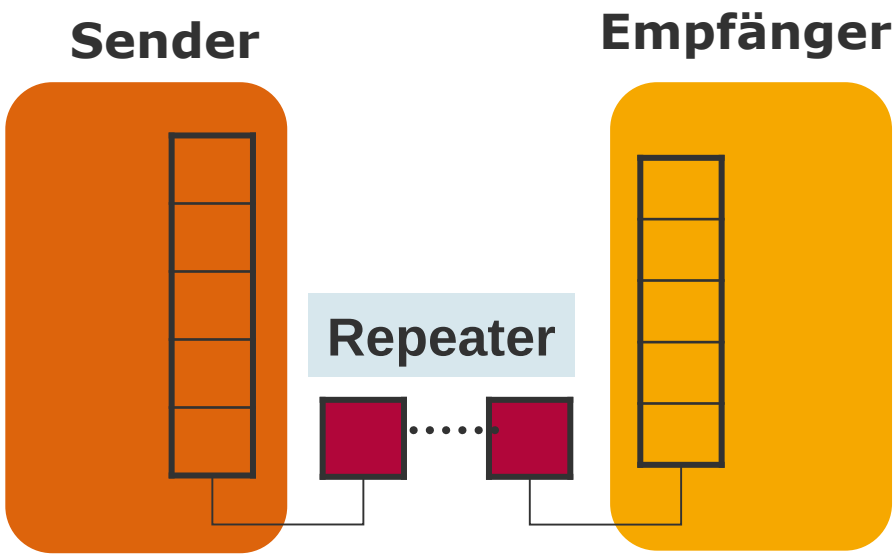
- Ein Ethernet-Segment besteht aus einer Rechnergruppe an einem Bus
- Jedes Ethernet-Segment bildet eine **Collision Domain**
- Ethernet-Segmente können über verschiedene Zwischensysteme verbunden werden
  - **Repeater** – verbinden einzelne Segmente zu größerem Verbund, der sich wie eine einzige Collision Domain verhält
  - **Bridges** – verbinden verschiedene, physikalisch getrennte Collision Domains, in denen jeweils parallel kommuniziert werden kann
  - **Switches** – leiten Pakete nur über den jeweiligen Port an das Ziel-Segment des LANs weiter
  - **Router** – können verschiedene Ethernet-LANs miteinander verbinden

Ethernet-Hardwarekomponenten (2/5)

Repeater arbeiten auf unterster Schicht (physikalische Schicht), sind daher für höhere Schichten „unsichtbar“

- Dienen zur reinen Signalverstärkung bei der Überwindung größerer Distanzen
- Verfügen über keinerlei „Eigenintelligenz“

4	Anwendung
3	TCP (Transport)
2	IP (Internet)
1	Sicherung (LAN)
0	**Hardware**



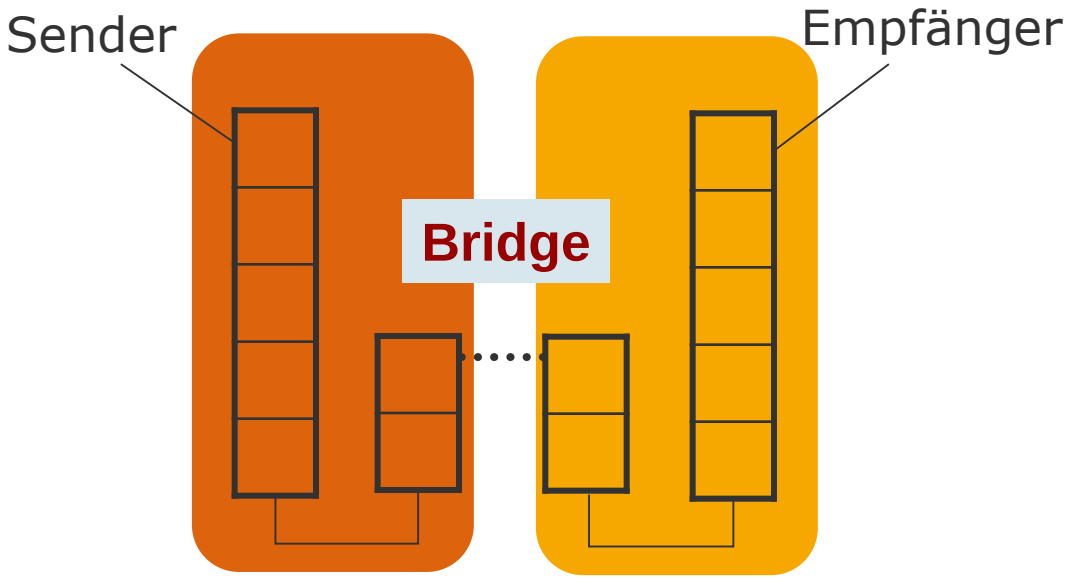
Ethernet-Hardwarekomponenten (3/5)

Bridge verbindet zwei LAN-Segmente

Switch verbindet einzelne Rechner im LAN (oder mehrere Segmente)

- LAN-Erweiterung mit **intelligentem Verkehrsmanagement**
- Lokaler Verkehr bleibt lokal, wird nicht über Bridge weitergeleitet

4	Anwendung
3	TCP (Transport)
2	IP (Internet)
1	**Sicherung (LAN)**
0	Hardware

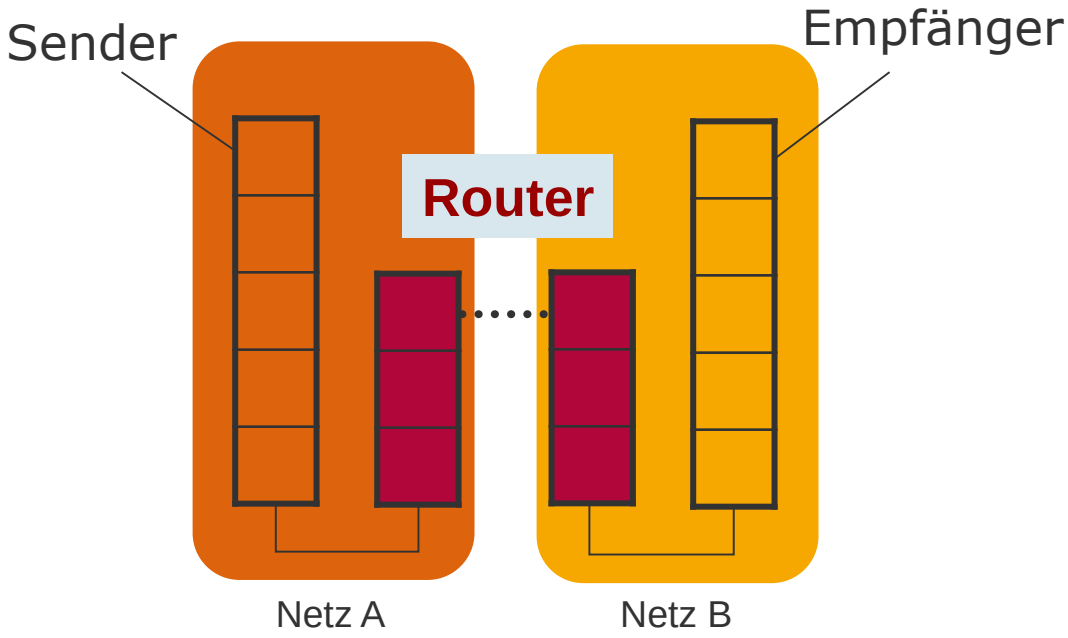


Ethernet-Hardwarekomponenten (4/5)

Router verbinden zwei autarke Netze zu einem Internet

- Subnetze werden logisch auf Schicht 2 getrennt
- Netzwerktopologie muss dem Router bekannt sein, um Datenpakete effizient weiterleiten zu können

4	Anwendung
3	TCP (Transport)
2	**IP (Internet)**
1	Sicherung (LAN)
0	Hardware

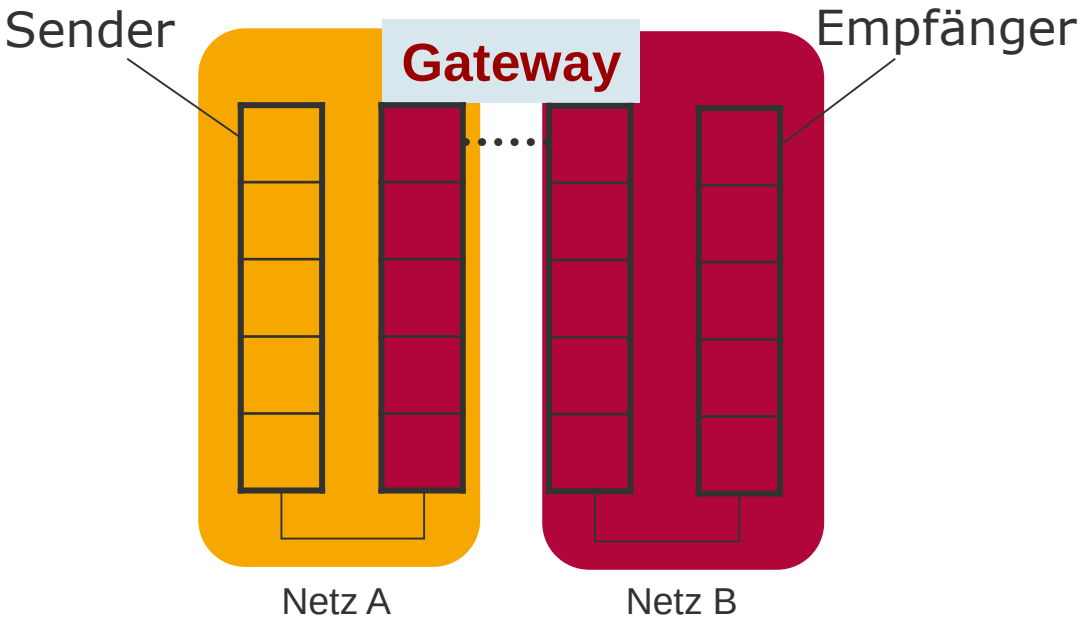


Ethernet-Hardwarekomponenten (5/5)

Gateway verbindet Netzwerke zu einem neuen System

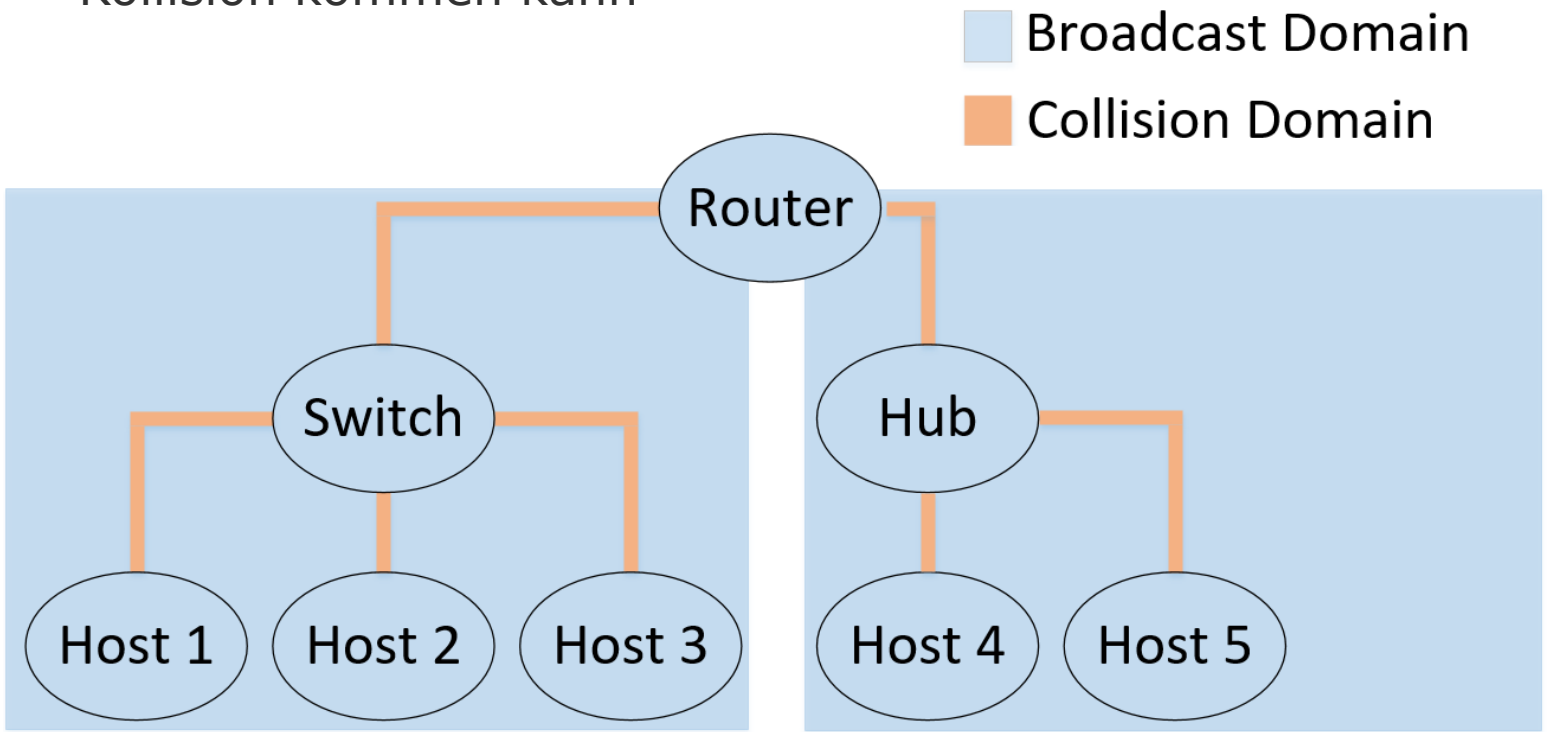
- Ermöglicht Kommunikation zwischen Anwendungsprogrammen bzw. Komponenten einer verteilten Anwendung auf unterschiedlichen Endsystemen
- Übersetzt unterschiedliche Anwendungsprotokolle ineinander

4	Anwendung
3	TCP (Transport)
2	IP (Internet)
1	Sicherung (LAN)
0	Hardware



Broadcast / Collision Domains

- **Broadcast Domain** – alle Rechner im Netz, die Broadcast-Pakete empfangen können
- **Collision Domain** – alle Rechner, zwischen denen es zu einer Kollision kommen kann



Ethernet-Varianten (1/3)

- Ethernet-Varianten unterscheiden sich in Bezug auf
  - Übertragungsmedien – Koaxialkabel, Twisted-Pair, Glasfaserkabel, …
  - Begrenzungsparameter, Anzahl anschließbarer Rechner, Bandbreiten, Topologie, …
- **10 Mbps – Varianten**
  - 10BASE5 – ursprünglicher Standard, nutzt teure Kabel (Thick Ethernet)
  - 10BASE2 – nutzt preiswerteres Kabel (Thin Ethernet)
  - 10BASE-T – nutzt einfaches Telefonkabel (Twisted Pair) als Übertragungsmedium, sternförmige Verkabelung mit zentralem Hub
  - 10BASE-F – nutzt weniger fehleranfälliges Glasfaserkabel

Ethernet-Varianten (2/3)

100 Mbps Ethernet – Fast Ethernet

- Bandbreite von 100 Mbps kann Bursts auch bei Multimediaanwendungen verkraften
- Folgt Entwicklungslinien von 10BASE-T
- Nutzt verschiedene Leitungsmaterialien, z.B. Doppeladerkabel, abgeschirmte Doppeladerkabel oder Lichtwellenleiterkabel
- Alle Fast-Ethernet-Varianten nutzen Sterntopologie

Ethernet-Varianten (3/3)

1 Gbps Ethernet – Gigabit-Ethernet

- Backbone-Technologie zur Verbindung von Subnetzen unterschiedlicher Bandbreite, heute auch in lokalen Netzen

10 Gbps Ethernet

- Weiterentwicklung der Backbone-Technologie, Einsatz in MAN und WAN

Broadband Ethernet

- Überträgt keine digitalen Basisbandsignale, sondern moduliert diese auf Träger bestimmter Frequenzen (analoge Übertragung) – über Frequenzmultiplexverfahren können so mehrere Ethernet-Systeme über ein einziges Koaxialkabel betrieben werden

Auf einen Blick

- Ethernet kann mehrere hundert Rechner im Umkreis von ca. 1 km vernetzen
- Relativ hohe Datenrate
- Geringe Verzögerung durch Verzicht auf Speicher und Transportlogik
- Sehr einfache Algorithmen für Zugriff auf Übertragungsmedium und Adressierung
- Effiziente Nutzung und faire Zugriffsverteilung für alle Teilnehmer
- Hohe Zuverlässigkeit, keine zentrale Steuerung
- Hohe Stabilität auch unter Last

openHPI-Kurs Wie funktioniert das Internet?

WLAN – Kabellose Netze

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

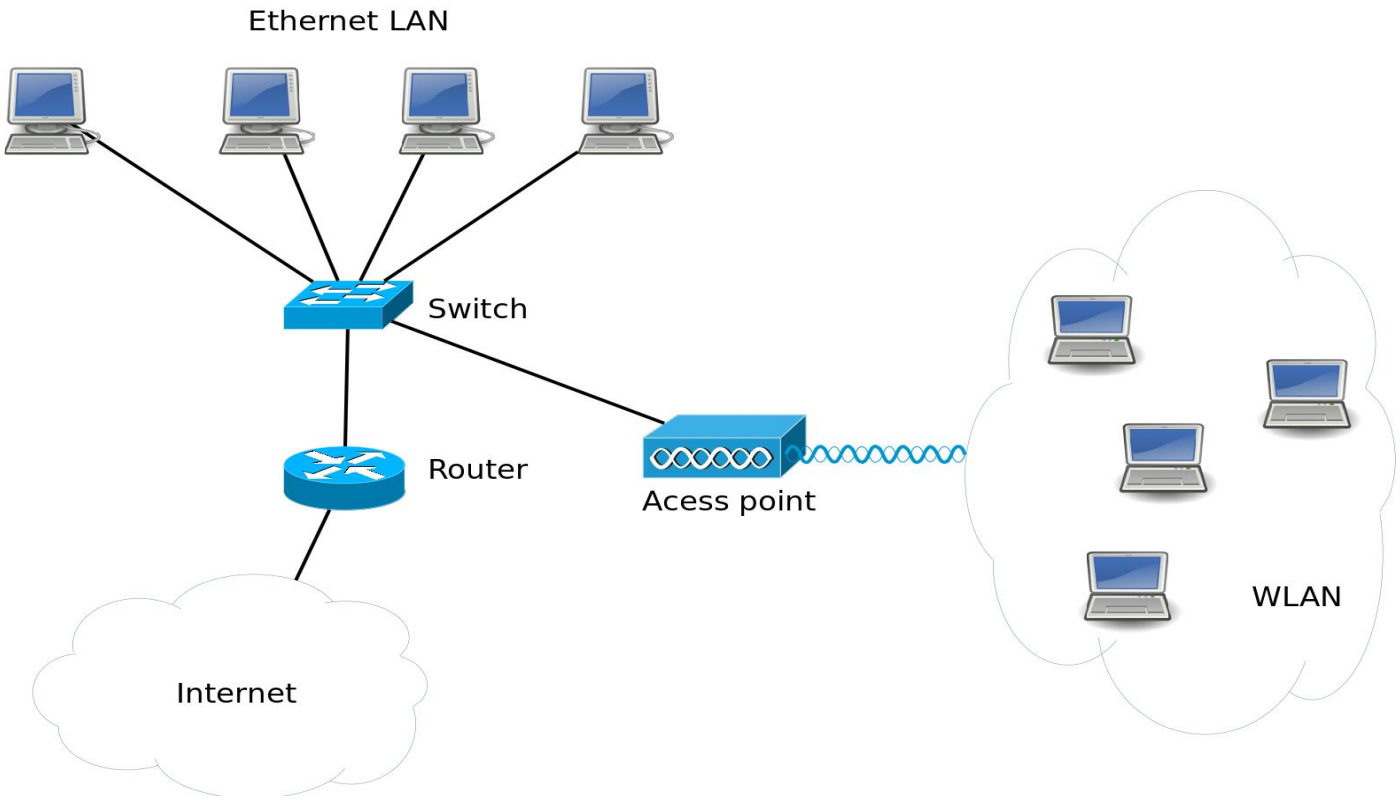
WLAN – Kabelloses Netz (1/3)

Funkbasierte Netzwerke – **Wireless LAN** – WLAN – werden immer beliebter

- WLANs erlauben ubiquitäres Computing – „jederzeit an jedem Ort"
- Geschichtlicher Ursprung: ALOHAnet (1971) – Funknetz zur Vernetzung der Hawaiianischen Hauptinseln mit einem Zentralrechner (9.600 bps)
- WLANs besitzen Sterntopologie – zentrale Basisstationen – **Access Points** – sorgen für Weiterleitung der Datenpakete an erreichbare Rechner
- IEEE 802.11 spezifiziert WLAN-Standard, z.B.
  - 802.11a – 54 Mbps im 5 GHz Frequenzband
  - 802.11b – 11 Mbps im 2,4 GHz Frequenzband
  - 802.11i – Verbesserung der Sicherheit

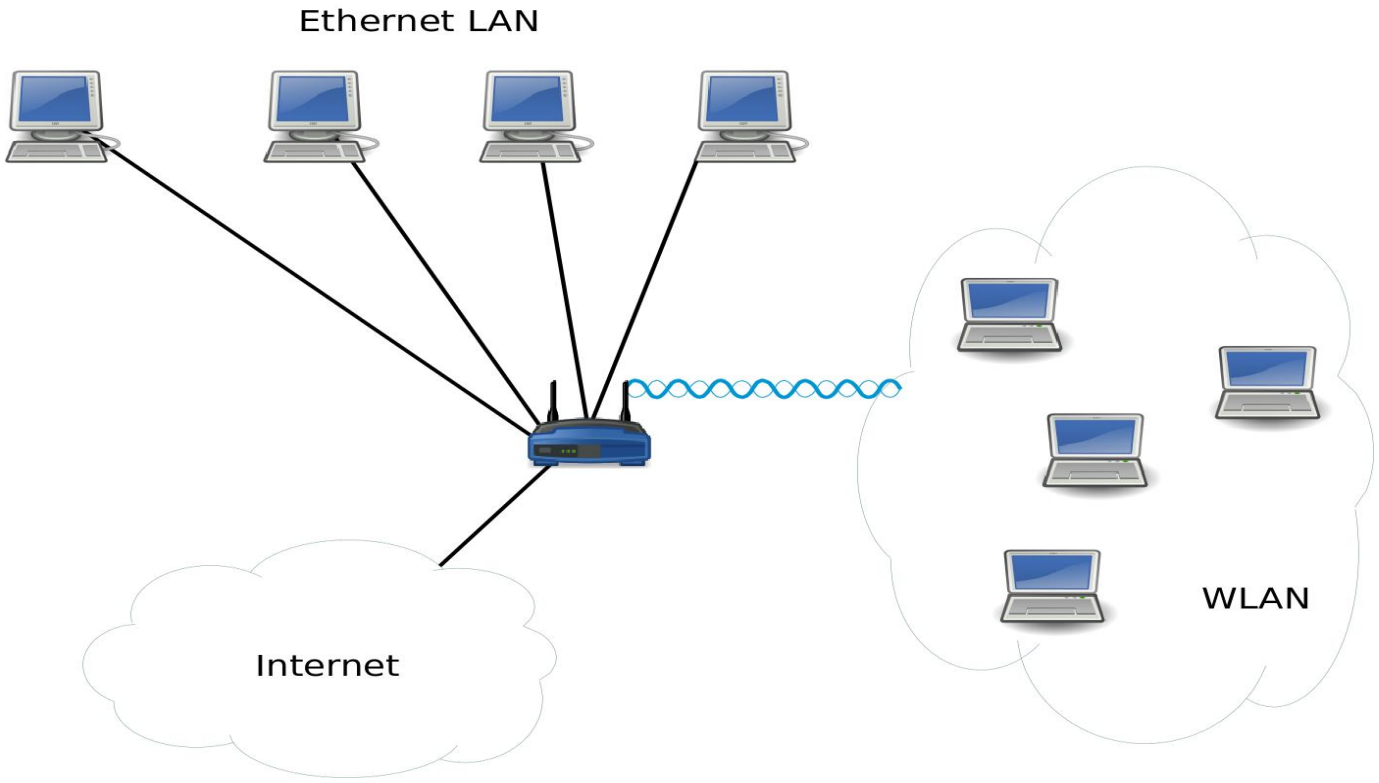
WLAN – Kabelloses Netz (2/3)

Anbindung eines WLAN an ein sternenförmiges Ethernet-Netzwerk und das Internet über dedizierte Zwischensysteme – **Switch** / **Router** / **Access Point**:



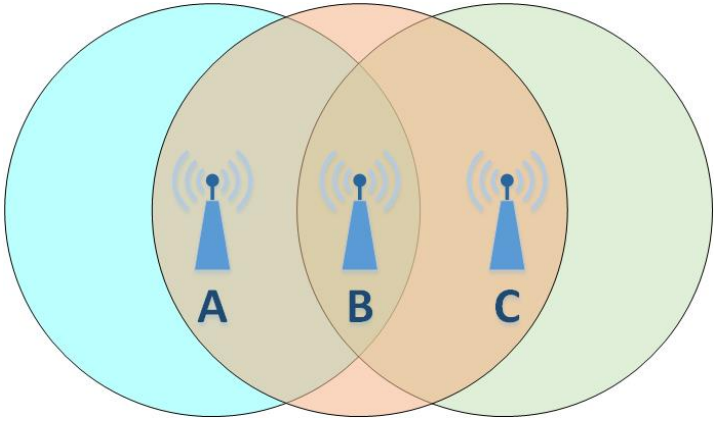
WLAN – Kabelloses Netz (3/3)

Heute werden die einzelnen, dedizierten Geräte in „All-in-One"-Geräten zusammengefasst:



Vielfachzugriffsregelung im kabellosen Netz (1/3)

- Vielfachzugriffsregelung erfolgt ähnlich wie mit *CSMA/CD* im Ethernet. Dennoch können Kollisionen auftreten, zum Beispiel beim *Hidden-Station*-Problem
  - Die Knoten A und C können Knoten B erreichen, sind jedoch voreinander verdeckt
  - Bei Knoten B kollidieren die gleichzeitig eintreffenden Signale der Knoten A und C

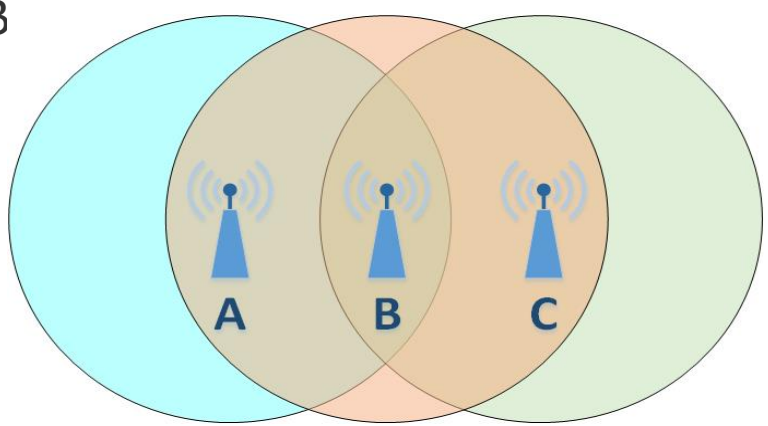


- Zur Vermeidung von **Kollisionen** wird „***Carrier Sense Multiple Access/Collision Avoidance***" *(*CSMA/CA*)* angewendet

Vielfachzugriffsregelung im kabellosen Netz (2/3)

Carrier Sense Multiple Access/Collision Avoidance:

- A sendet "*Request To Send*" (RTS) an B
- B sendet "*Clear To Send*" (CTS) an A
- A sendet "*Data Sending*" (DS) an B
- A sendet Datenpaket an B und
- B sendet "*Acknowledgement*" (ACK) an



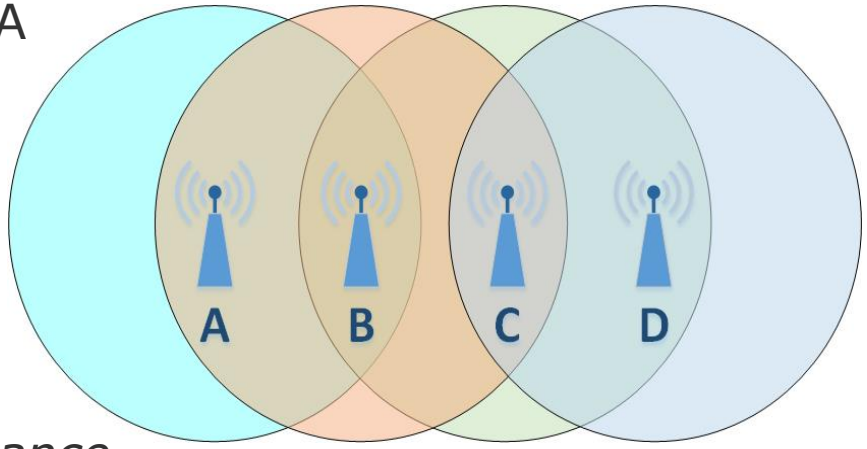
Alle Knoten, die ein RTS/CTS hören, warten

- Kollisionen können nur noch bei RTS/CTS auftreten, jedoch nicht bei der Übertragung von Nutzdaten
- Im Fall einer Kollision warten beide Sender eine **zufällige** Zeitspanne, bevor sie ein neues RTS senden

Vielfachzugriffsregelung
Exposed-Station-Problem (3/3)

Das ***Exposed-Station*-Problem** sorgt für weitere Komplikationen

- D kann nicht mit Knoten C kommunizieren, obwohl D außerhalb der Sende-/Empfangsbereiche von A und B liegt und keine Kollisionen auftreten
- C hatte das CTS von Knoten B an Knoten A gehört und antwortet deshalb D nicht



- *„Multiple Access with Collision Avoidance for Wireless"* (MACAW) Verfahren kann hier angewendet werden:
  - Knoten D sendet ein *„Request to Send"* an C
  - C antwortet diesmal nach einer kurzen Pause mit einem *„Request for Request To Send"* (RRTS) an D
  - Es folgt das bereits vorgestellte Protokoll von CSMA/CA

Sicherheit in kabellosen Netzen (1/2)

- Aufgrund der Natur des Übertragungsmediums ist das Sicherheitsniveau in funkbasierten Netzen wesentlich geringer als in kabelgebundenen
- Zum Abhören und zur nichtautorisierten Benutzung ist kein physikalischer Zugang notwendig
- Auch Entdeckung eines WLANs ist nicht schwierig
  → „Parkplatz-Attacke“
- Angriffe auf WLANs
  - Passive Angriffe zur Entschlüsselung des Datenverkehrs durch statistische Analyse
  - Aktive Angriffe…

Sicherheit in kabellosen Netzen (2/2)

- Zum Schutz von WLANs wurde ursprünglich in IEEE 802.11b das Verschlüsselungsprotokoll **WEP** – Wired Equivalent Privacy – definiert
- WEP-Protokoll basiert auf geheimem symmetrischen Schlüssel, der zwischen AP und teilnehmenden Rechnern vereinbart wird
  - Aber **Achtung**: WEP basiert auf unsicherem Verschlüsselungsalgorithmus RC4 und kann leicht geknackt werden

Sicherheit in kabellosen Netzen (2/2)

- Heute sollen in WLANs deshalb statt WEP sicherere Verschlüsselungsprotokolle eingesetzt werden
  - WPA bzw.
  - **besser** noch **WPA2**
    - **WPA2** nutzt **AES** (Advanced Encryption Standard) als sicheres Verschlüsselungsverfahren
- **Achtung**: Wird das sogenannte Wi-Fi Protected Setup (WPS) genutzt, dann kann Angreifer **Brute-Force-Attacke** durchführen, um an die WPS PIN zu gelangen und damit dann WPA/WPA2 umgehen …

openHPI-Kurs Wie funktioniert das Internet?

WAN – Weitverkehrsnetze

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

WANs – Weitverkehrsnetze

- **WANs** – **Wide Area Networks** – Weitverkehrsnetze ermöglichen den Zusammenschluss mehrerer LANs zu einem Netzwerkverbund
- Anzahl der angeschlossenen Rechner bzw. LANs und räumliche Ausdehnung kann Erfordernissen angepasst werden
- Ziel der Kopplung in einem WAN ist Schaffung eines scheinbar einheitlichen Netzwerkes – **Internet** oder **virtuelles Netz** –, in dem alle Endsysteme der verschiedenen angeschlossenen LANs ungehindert miteinander kommunizieren können

→ **Internetworking**

Paketvermittlung im WAN

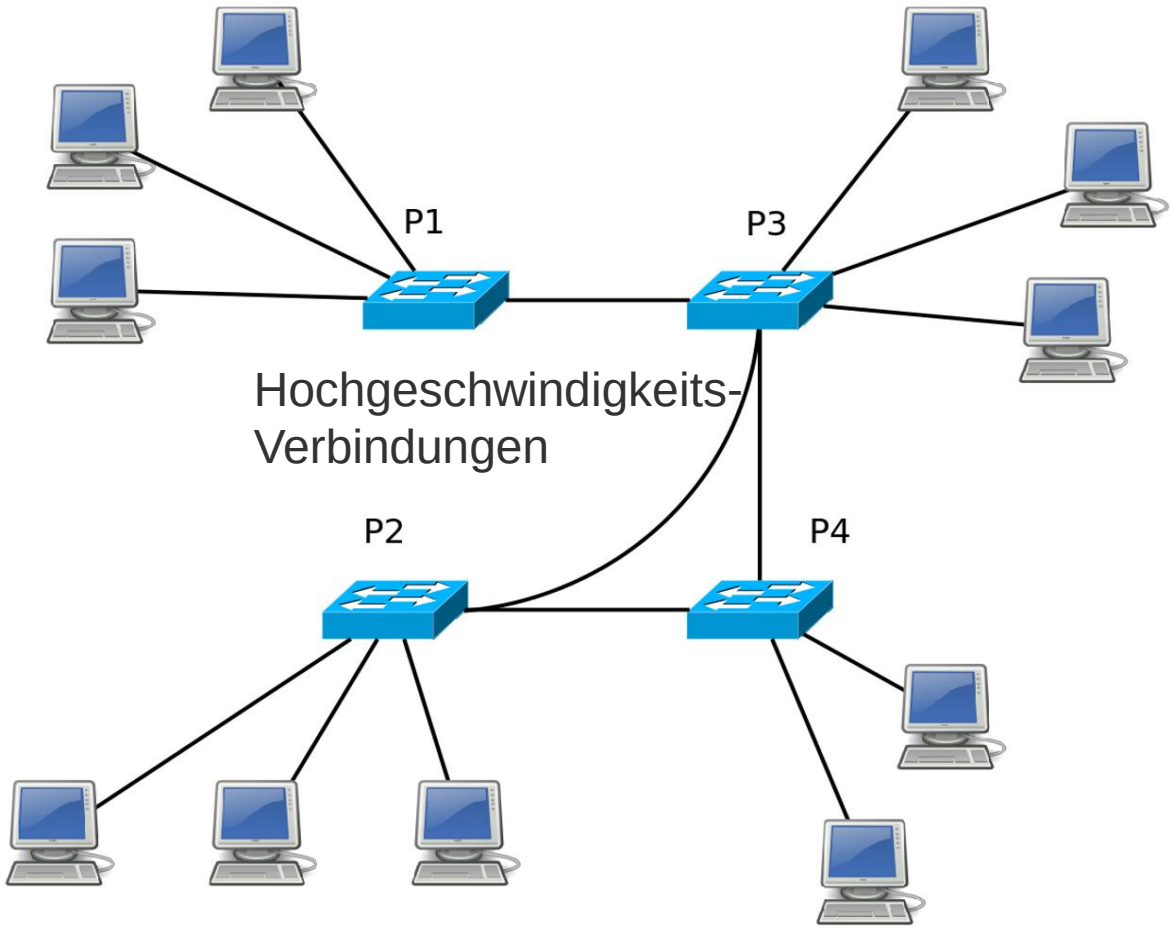
Paketvermittlung – **Packet Switching** – Grundprinzip der Datenübertragung im WAN: zu übertragende Daten werden in einzelne Pakete zerlegt und unabhängig voneinander zugestellt

Zum Anschluss eines LANs an ein WAN wird dieses über ein Zwischensystem – **Paketvermittler** – mit dem WAN verbunden

- Paketvermittler sind spezielle Rechner, die sehr schnell Datenpakete empfangen, zwischenspeichern, auswerten und weiterleiten können
- Um eine hohe Datenübertragungsrate zu erreichen, sind die **Routing-Algorithmen** zur Weiterleitung der Datenpakete meist in Hardware realisiert

Aufbau eines WAN

Paketvermittler:



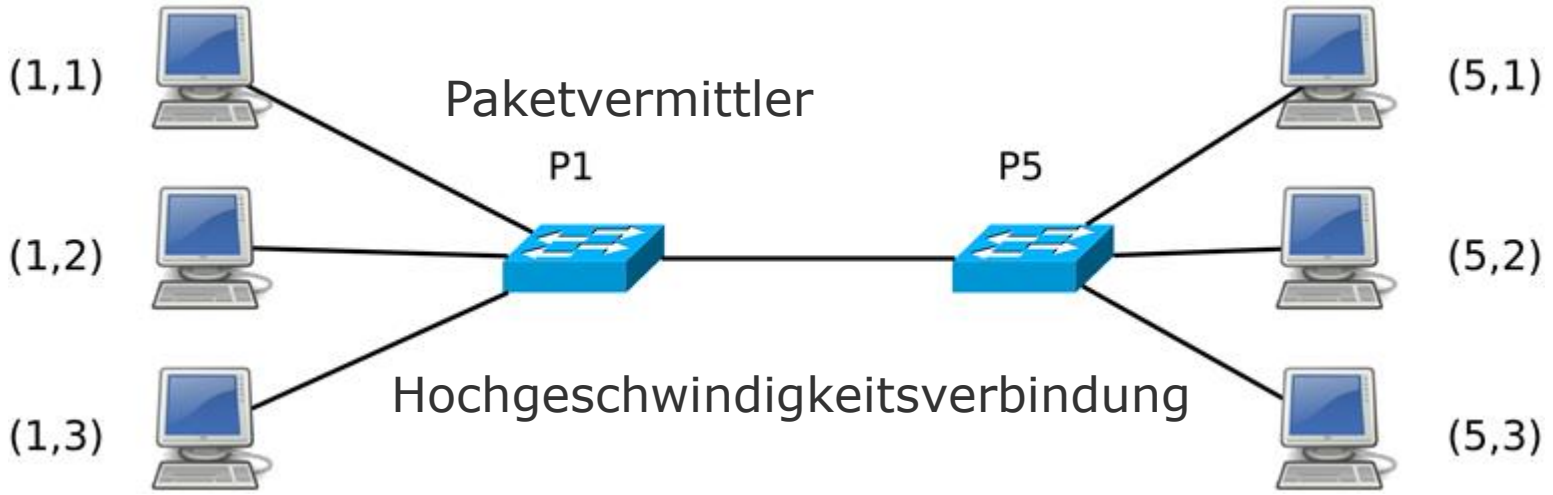
angeschlossene
Endsysteme

Adressierung im WAN (1/4)

Damit Paketvermittler entscheiden können, über welchen Ausgang ein Paket weiterzuleiten ist, braucht jedes Endsystem eine eigene Adresse in einem einheitlichen Format

In WANs werden **hierarchische Adressierungsschemata** verwendet:

- **Adress-Präfix** – Adresse des Netzwerks
- **Adress-Suffix** – Adresse des angeschlossenen Endsystems

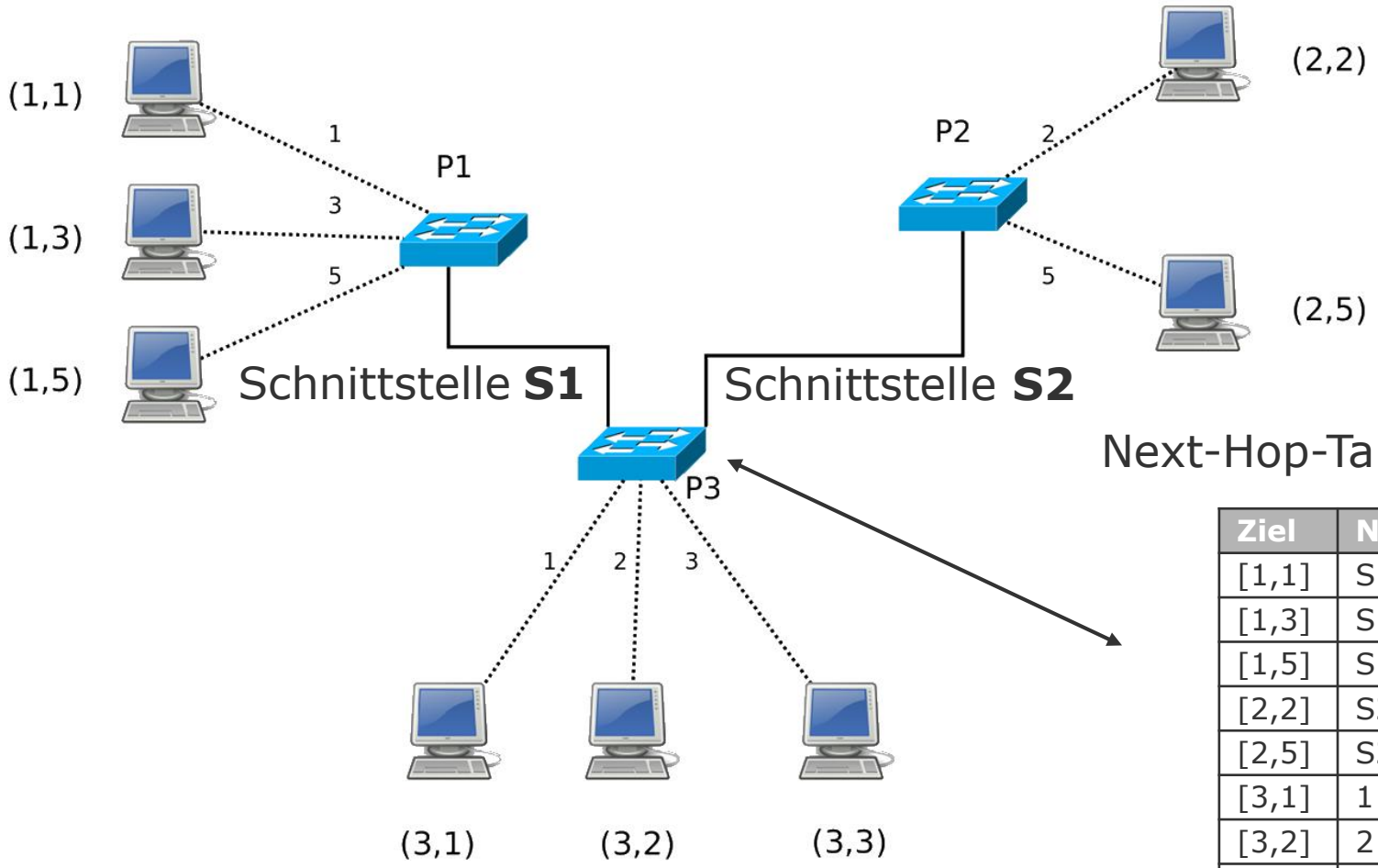


Adressierung im WAN (2/4)

Gehört Zieladresse eines Rechners zu einem direkt benachbarten Paketvermittler, wird das Paket dorthin weitergeleitet, ansonsten wird es zu einem Paketvermittler gesandt, der auf dem Weg zur Zieladresse liegt – dessen Auswahl hängt von Zieladresse und gewählter Route ab

- Paketvermittler hat keine Information über vollständige Wegstrecken, sondern nur über mögliche nächste Teilstrecken → Teilstreckenvermittlung oder → **Next-Hop-Forwarding** – Weiterleitung erfolgt unabhängig von Herkunft
- Um für ein Datenpaket den Next Hop bestimmen zu können, verwaltet jeder Paketvermittler eine → **Routing-Tabelle** oder → **Next-Hop-Tabelle**

Adressierung im WAN (3/4)



Next-Hop-Tabelle von P3

Ziel	Next Hop
[1,1]	S1
[1,3]	S1
[1,5]	S1
[2,2]	S2
[2,5]	S2
[3,1]	1
[3,2]	2
[3,3]	3

Adressierung im WAN (4/4)

Weiterleitungsalgorithmus:

- Zieladresse auswerten
- Eintrag in Routing-Tabelle suchen
- Paket über den verzeichneten Ausgang weiterleiten

Weiterleitungsalgorithmen können sehr effizient in Hardware implementiert werden

Zugang zum WAN

Leitungsgebundener Zugang über

- analoges Telefon (Modem), ISDN
- DSL, z.B. ADSL, ADSL2+, UADSL, HDSL, SDSL, VDSL, VDSL2
- Kabel-TV

Kabelloser Zugang

- Richtfunk, z.B. WiMAX
- Satellit
- Mobiles Internet, z.B. GSM, GPRS, UMTS, HSDPA, LTE, LTE-Advanced…

openHPI-Kurs: Wie funktioniert das Internet?

Wichtige Routingverfahren

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

Isoliertes Routing (1/3)

Beim **isolierten Routing** werden nur die lokal verfügbaren Informationen, z.B. Länge der Warteschlange vor einem Ausgang, oder Zustand eines Nachbarn ausgewertet

Wichtige Beispiele:

- Fluten, selektives Fluten oder Hot-Potato

Fluten oder **Flooding**:

- **Idee**: Jedes eintreffende Paket wird über alle anderen Anschlüsse des Routers weitergeleitet
  - Vervielfachung der Pakete erzeugt sehr hohe Netzlast
  - Zur Eindämmung werden den Paketen Hop-Counter oder Zeitstempel mitgegeben und es wird sichergestellt, dass ein Router ein Paket nie zweimal ausliefert

Isoliertes Routing (2/3)

Selektives Fluten oder **Selective Flooding**:

- **Idee**: Jedes eintreffende Paket wird über alle Anschlüsse des Routers weitergeleitet, die in etwa in die richtige Richtung weisen
  - Router brauchen dazu Informationen über den Aufbau des Netzwerks

Fluten und selektives Fluten sind wegen Erzeugung hoher Netzlast meist nicht praktikabel

Anwendungen sind jedoch sinnvoll bei

- Verteilung von Updates für verteilte Datenbanken (Synchronizität)
- militärischen Anwendungen mit hoher Störanfälligkeit

Aber **Evaluation**: Fluten findet stets die kürzeste Route

Isoliertes Routing (3/3)

Hot-Potato-Routing:

- **Idee**: Router versucht, eintreffendes Paket auf dem schnellsten Weg loszuwerden, also über den Ausgang mit der aktuell kürzesten Warteschlange
- **Probleme**:
  - Pakete finden selten kürzesten Weg, sondern machen Umwege
  - Verstärkung von Netzwerküberlastung – Pakete werden abgesendet, auch wenn sich Pakete auf dem Weg zum Empfänger stauen

Distanzvektor-Routing (1/2)

Distanzvektor-Routing (oder Bellman-Ford- oder Ford-Fulkerson Algorithmus) ist dezentrales dynamisches Routing-Verfahren

- Jeder Router berechnet seine Routing-Tabelle lokal und weiht Nachbar-Router ein in seinen Kenntnisstand von der Netzwerktopologie
- Routing-Informationen werden periodisch ausgetauscht, sodass nach einer gewissen Zeit jeder Router die kürzesten Wege zu allen Zielen im Netzwerk kennt
- Durch den periodischen Informationsaustausch können sich Router an Veränderungen im Netzwerk anpassen, z.B. bei Ausfall einer Verbindung
- Jeder Router speichert (in einem Vektor) neben Next-Hop-Eintrag auch die Distanz zum Ziel ➔ **Distanzvektor**

Distanzvektor-Routing (2/2)

- Distanzberechnung erfolgt auf Basis einer vorgegebenen Routing-Metrik, z.B. Anzahl der Hops, Warteschlangenlänge, Übertragungszeit, …
- Distanzvektor (DV) wird durch Austausch von Routing-Informationen mit den Nachbar-Routern ständig aktualisiert
  - Router prüfen Dreiecksungleichung:

    Distanz zum Ziel Z in DV von Nachbar A + …

    … + Distanz zu A **<** Distanz zu Z in eigenem DV?

    → eigenen DV updaten
- Distanzvektor-Routing war das erste Routing-Verfahren im ARPANET, es wurde in RFC 1058 als **Routing Information Protocol** – **RIP** standardisiert

OSPF – Link-State-Routing

Distanzvektor-Routing-Verfahren wurde im Internet wegen seiner langsamen Konvergenz durch **OSPF** – **Link-State-Routing** – abgelöst

Link-State-Routing ist dezentrales dynamisches Routing-Verfahren

- Router tauschen Informationen über Status der Verbindungen zu Nachbarn aus und keine vollständige Tabellen
- Routing-Informationen werden per Broadcast gleichzeitig an alle Router im Netzwerk gesendet
- Verfahren erlaubt sehr schnelle Anpassung an sich verändernde Netzwerksituationen
- Standardisiert in RFC 2328
- **OSPF** („Open Shortest Paths First“) basiert auf „Shortest Paths First“-Algorithmus aka. **Dijkstra-Algorithmus**