

Netzwerk Komponenten



<https://iuk.one/1012-1026>

Clemens H. Cap

ORCID: 0000-0003-3958-6136

Department of Computer Science
University of **Rostock**
Rostock, Germany
clemens.cap@uni-rostock.de

Version 1



1. Bridge

Ziele: Wir lernen Netzwerk-Komponenten zur Verbindung auf Layer 1 und 2 kennen.

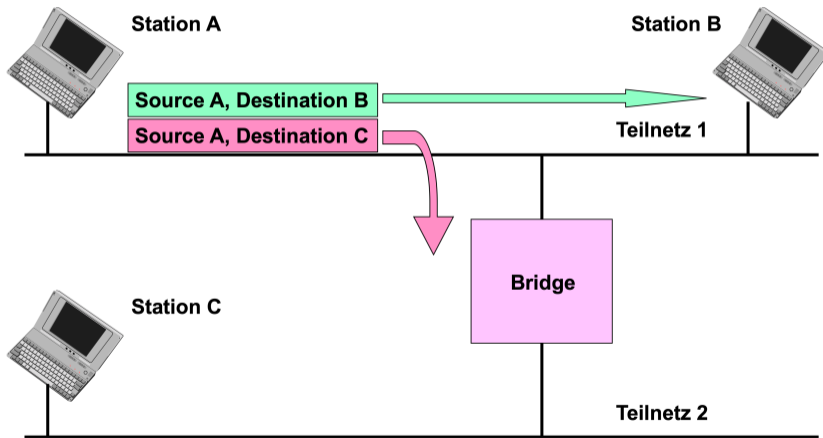
1. Bridge

2. Router

3. Weitere Komponenten

1. Bridge

Aufgabe der Bridge



1. Bridge

Bridge

OSI: Link Layer 2.

Bridge ist für Layer 3 transparent (nicht erkenntlich).

Aufgabe: Selektives Weiterleiten zwischen Netzwerken derselben Layer 2 Technologie.

CSMA/CD: Teilnetze haben eigene Kollisions-Domänen.

Adressen: Müssen über alle Bridge-gekoppelten Teilnetze hinweg eindeutig sein.

Bridge lernt, welche Adressen auf beiden Seiten vorhanden sind.

Bridge kann Pakete nach Layer 2 Adressen filtern.

Lern-Mechanismus:

- Jedes Interface der Bridge hat eine Adreßtabelle.
- Adreßtabelle speichert alle an diesem Interface gesehenen Adressen.

Auslieferungs-Mechanismus:

- Adresse nicht gefunden: An alle Interfaces außer dem Ursprung senden.
- Adresse in Tabelle des Ursprungs: Paket verwerfen, wurde lokal geliefert.
- Adresse in Tabelle eines anderen Interface: Paket an dieses Interface senden.

Spanning Tree Mechanismus:

- **Problem:** Lern-Mechanismus kann bei mehreren Bridges zu Paketschleifen führen.
- Spanning Tree Algorithmus bewirkt Tabellenmodifikation, die das verhindert.

Transceiver, Bridge, Switch, Hub & Co (1)

Auf Layer-1 und Layer-2 finden sich diverse Geräte verschiedener Bezeichnungen.

Präzise Abgrenzung schwierig, Bezeichnungen Technologie- und Hersteller-spezifisch.

Transceiver: Rein physikalische Signalerzeugung.

Repeater: Weiterleitung auf Layer-1 durch Signal-Verstärkung.

Typischerweise Verbindung zweier Netzteile.

Hub: Sternverteiler auf Layer-1.

Empfangenes Paket an alle anderen verbundenen Netzteile weitergeleitet (1:n).

Konzentrator: Sternbündelung auf Layer-1 oder 2.

Bündelt viele Endgeräte an eine Netzanbindung. (n:1).

Bridge: Verbindung zweier Netzteile.

Mehr oder weniger intelligente Auswahlmechanismen.

Switch: Verbindung zu mehreren Netzteilen, typisch sind 8 – 64

Mehr oder weniger intelligente Auswahlmechanismen.

Sehr ähnlich zur Multiport-Bridge, Unterschiede vor allem in Implementierung.

Switch ist typischerweise das "intelligenterere" Gerät.

Weiterleitung bei Fehlern und Kollisionen

Cut Through: Weiterleitung sobald Zieladresse gelesen.

- Geringe Verzögerungszeit (einige [μs]).
- Kollisionen und Fehler nicht erkennbar.
- Auch kollidierte und fehlerhafte Frames werden weitergeleitet.

Store-and-Forward: Weiterleitung erst nach Empfang des ganzen Pakets.

- Höhere Verzögerung, je nach Frame-Länge bis zu einigen [ms].
- Kollisionen und Fehler sind erkennbar.
- Nur fehlerfreie Frames weitergeleitet.

Adaptive: Anpassung an die bessere Strategie.

- Bei geringer Last: Cut-Through (nur wenig Fehler & Kollisionen zu erwarten).
- Bei hoher Last: Store-and-Forward (mehr Fehler & Kollisionen; diese verhindern).

2. Router

Ziel: Router erlauben die netzübergreifende Kommunikation zwischen Geräten, die in verschiedene Netze eingebunden sind.

1. Bridge

2. Router

3. Weitere Komponenten

Aufgabe des Routers

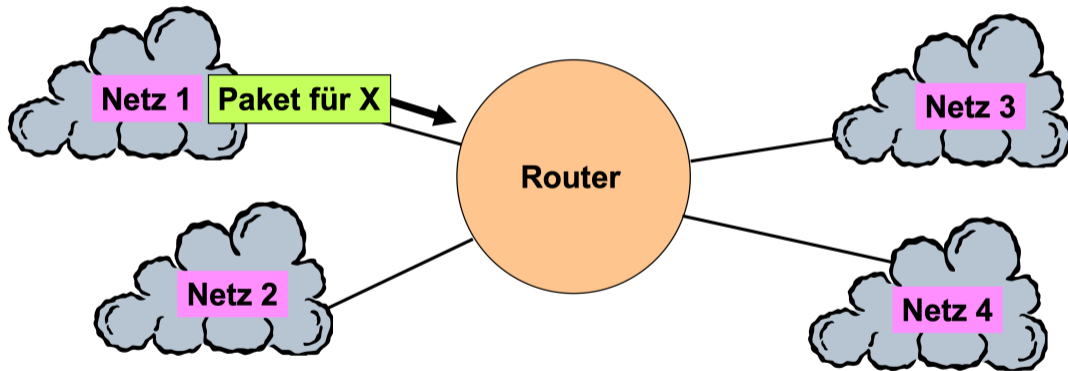


Abb. 1: Ein Router ist mit mehreren Netzen verbunden. Er bekommt von einem Netz ein Datenpaket und muß dann entscheiden, an welches Netz er dieses Datenpaket weiterleitet.

2. Router

Mechanismus des Routing

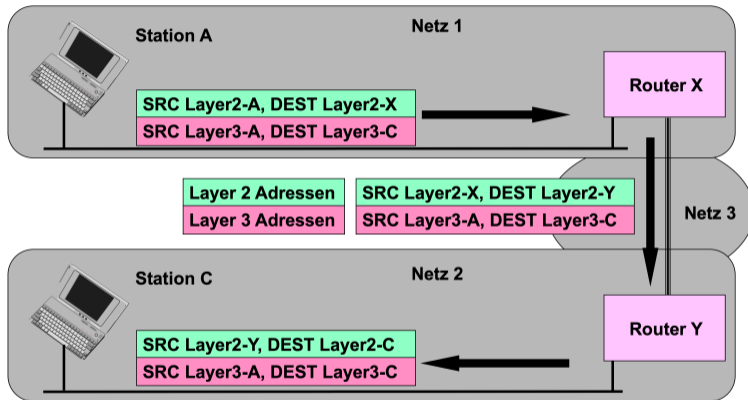


Abb. 2: Router X und Router Y sind durch Netz 3 verbunden. Durch geeignetes Umsetzen von Layer-2 Adressen durch die beiden Router gelangen Pakete von Netz 1 über Netz 3 nach Netz 2. Dazu senden die Stationen Datenpakete, die nicht innerhalb des eigenen Netzes vermittelt werden können, an den zuständigen Router, der dann zu wissen hat, wie er diese an welchen zuständigen Router bzw. welches Zielnetz er sie zu vermitteln hat.

OSI: Network Layer 3

Aufgaben:

- Weiterleiten von Frames zwischen Netzen beliebiger Technologien.
- Bestimmung des konkreten Pfads der Weiterleitung.

Layer-3-Adressen (1)

Layer-2-Adressen: Innerhalb einer Technologie und eines Netzes.

Bsp: Ethernet, WLAN, Bluetooth.

Layer-3-Adressen: Technologie- und netzübergreifende Adressen.

Bsp: Internet IPv4, IPv6.

Nötig: Übersetzung zwischen Layer-2- und Layer-3-Adressen.

Eindeutigkeit der Adressierung:

- Layer 2 benötigt nur lokale Eindeutigkeit.
- Layer 3 benötigt globale Eindeutigkeit für öffentliche Adressen und erlaubt lokale Mehrdeutigkeit für private Adressen (Bsp: 192.168.*.*).
- Auf beiden Layern bestehen Konzepte für Gruppen-Adressen.

Hierarchische Struktur:

- Ziel: Will einzelne Netzwerke identifizieren und darin ggf. noch Subnetze.
- Weg: Splitte Adresse in Netz-, Subnetz- und Host-Anteile.
- Folge: Effizienteres Routing dank hierarchischer Struktur.

Größe des Adreßraums:

- Paradox Ethernet Adreßraum (6 Byte) größer als IPv4 Adreßraum (4 Byte).
- Neu: IPv6 Adreßraum hat 16 Byte.

Routing ist Optimierung unter Randbedingungen

Was wird optimiert?

- Kosten, Latenzen, Datenraten, Fehlerraten usw.
- Für ein Paket, eine Verbindung, für einen Netzbereich oder global.

Was sind **Randbedingungen**?

- Gewährleistung von **Dienstgütern**.
Bsp: Constant bit rate für einen wichtigen Video-Strom.
- Gewährleistung von **Regelsätzen** (sog. policies).
Bsp: Bestimmte Daten nur über einen bestimmten Anbieter routen.

Wie wird optimiert?

- Jeder Router hat zunächst nur lokales Wissen.
- Router informieren sich gegenseitig über **Routing Informations-Protokolle**.

Flußsteuerung im Router

Aufgaben der Flußsteuerung:

- Vermeiden von **Staus** (sog. Congestion)
- Herstellen möglichst guter **Dienstqualität** (sog. QoS - Quality of Service)
- Gewährleistung **angeforderter Dienstgüte**
Bsp: Vorgegebene konstante Bitrate für eine Video-Übertragung.
- **Anpassen** des Paketstroms an vorhandene Leitungen (sog. Traffic Shaping)

Verfügbare Methoden:

- **Source Quenching**: Reduziere Sendegeschwindigkeit an der Quelle.
- **Router Queueing**: Sortiere Pakete in Queues und behandle diese verschieden.
- **Load Shedding**: Bei Überlast gezielt Pakete fallen lassen.
- **Route Adaptation**: Ausnutzen aller verfügbaren Routen.

Staus (Congestion)

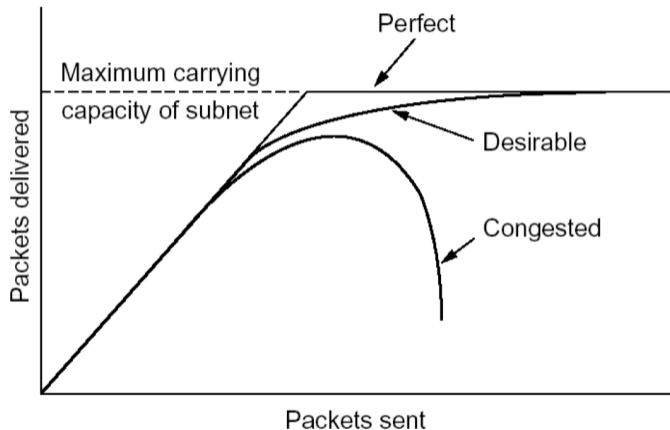


Abb. 3: Viele Punkt-zu-Punkt Verbindungen neigen aufgrund der eingesetzten Protokolle zu **Congestion**. Bsp: Ethernet mit 1-persistent CSMA/CD. Das bedeutet: Bei steigendem Verkehrsaufkommen geht der Durchsatz herunter. Dieses Verhalten können Router versuchen auszugleichen.

Strategien des Router Queueing

FIFO Queueing (First in First Out): Nach Reihenfolge des Eintreffens.

- Vorteil: Einfach zu implementieren & modellieren.
- Nachteil: Keine Priorisierung von Paketen möglich.

Weighted Fair Queueing: Mehrere Queues, mit fairem Multiplexing

- Vorteil: Alle Queues immer wieder bedient, nach vorgegebener Gewichtung.
- Vorteil: Unter hoher Last verhungert keine Queue.

Priority Queueing: Mehrere Queues, nach Prioritäten

- Zuweisung der gesamten Bandbreite an die jeweils wichtigste Queue.
- Vorteil: Wichtiger Verkehr erhält stets hohe Bandbreite.
- Nachteil: Wichtiger Verkehr kann weniger wichtigen (dauerhaft) blockieren.

Custom Queueing: Benutzer regelt Aufteilung nach eigenem Algorithmus.

Auswahl: Pro Interface jeweils eigene Strategien möglich.

3. Weitere Komponenten

Ziele: Was es sonst noch so alles gibt...

1. Bridge
2. Router
3. Weitere Komponenten

OSI: Meist oberhalb Layer 4

Aufgaben: Verbindung unterschiedlicher Protokollwelten.

Oft: Anpassungsaufgaben auf Layer 6 und 7.

Beispiele:

- **H.323 Gateway:** Verbindet VoIP / H.323 und PSTN (klassisches Telefon-Netz).
- **Samba:** Setzt SMB (Windows) und NFS (Linux) Dateiaufrufe um.
- **OSI / SNA Gateway:** Setzt zwei komplette Stacks ineinander um.

NAT (Network Address Translation) Gateway

Situation: Firma oder WG hat einen Internet-Anschluß mit einer IP-Adresse.
Dahinter ein ganzes Netz mit vielen Endgeräten.

Problem 1: Outgoing NAT.

Wenn ein internes Endgerät einen Server außen kontaktiert
dann sieht dieser nur die eine IP-Adresse.

Wie findet die Antwort das anfragende Endgerät im internen Netz?

Problem 2: Incoming NAT.

Firma will dem Internet 3 Dienste auf je 1 Server anbieten.

Wie finden Anfragen aus dem Internet an die eine IP-Adresse
den jeweils dafür zuständigen Server?

Lösung: NAT Gateway beobachtet Pakete und übersetzt die Adressen und Ports.

3. Weitere Komponenten

NAT (Network Address Translation) Gateway

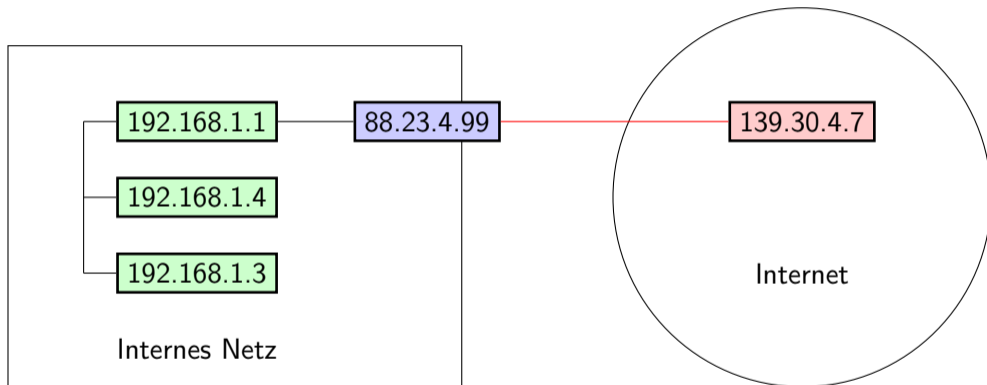


Abb. 4: Die **grünen Knoten** des internen Netzes können auf den **139-er Server** im Internet über das **88-er NAT Gateway** zugreifen. Der **139-er Server** sieht nur die Adresse des **88-er NAT Gateways**. Anfragen aus dem Internet werden an das **88-er NAT Gateway** gerichtet, das an die jeweils Port-weise konfigurierten grünen Knoten weiterleitet.

Firewall

OSI: Layer 2 und höher

Aufgaben: Unterbinden unerwünschter Kommunikation.

- Herausfiltern von Datenpaketen.
- Unterbinden verbindungsorientierter Dienste.
- Anpassen von Dienstqualität-Anforderungen an Regelvorgaben (policies).
- Meist auf Basis von Filterregeln.

Beispiele:

- Layer 2: Nach SRC oder DST Ethernet-Adresse filtern.
- Layer 3: Nach SRC oder DST IP-Adresse filtern.
- Layer 4: Nach SRC oder DST Portnummer filtern.
- Layer 7: Nach Inhalten filtern (zB: Java Applets, ActiveX).
- Layer 7: Nach Protokollheader filtern (zB: PICS Header für "adult" content).
- Layer 7: Nach Applikationsdaten filtern (Bsp: Subject der E-Mail).
- Layer 7: Nach Uhrzeit filtern (zB: Keine E-Mail zwischen 24 und 06 Uhr).

OSI: Meistens Layer 4 und / oder 7

Aufgaben: Stellvertreter für einen Netzdienst.

Beispiele:

- **Web Proxy:** Web Seite vom lokalen Proxy geladen statt vom Web-Server.
Bsp: Cache, Ad Blocking, Content Filter uvm.
- **TCP Wrapper:** Proxy auf Layer 4, protokolliert und filtert.
Bsp: Zusätzliches Paßwort, Zugangslimitierung uvm.

Transparenz von Komponenten

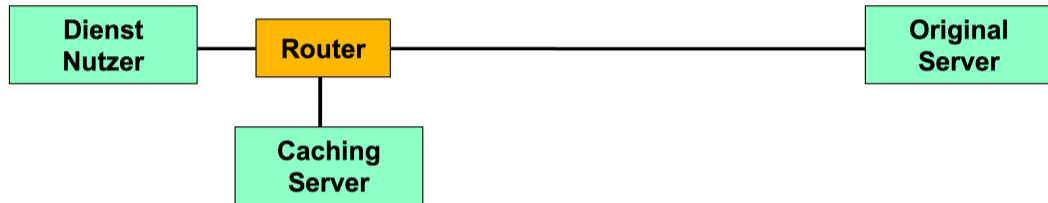


Abb. 5: Caching Server als transparentes Proxy geschaltet.

Transparentes Proxy:

- Anfrage des Dienst-Nutzers wird vom Router an Caching Server weitergeleitet.
- Caching Server kann autonom bei Original Server anfragen.
- Benutzer merkt nicht, daß Antwort von anderem Gerät kommt als vom Server.

Intransparenz von Komponenten



Abb. 6: Intransparentes Proxy.

Intransparentes Proxy:

- Client muß Proxy-Architektur unterstützen.
- Dienst-Nutzer aktiviert im Client einen Proxy-Server.
- Client kontaktiert Proxy-Server.
- Benutzer erkennt, daß Antwort von anderem Gerät kommt als vom Server.

Anhang

Übersicht

Verzeichnis aller Abbildungen

Abb

Rechtliche Hinweise

§

Zitierweise dieses Dokuments

→

Verzeichnis aller Folien



1	Aufgabe des Router	10
2	Router	11
3	Congestion	17
4	Network Address Translation	22
5	Caching Server als transparentes Proxy geschaltet.	25
6	Intransparentes Proxy.	26

Die hier angebotenen Inhalte unterliegen deutschem Urheberrecht. Inhalte Dritter werden unter Nennung der Rechtsgrundlage ihrer Nutzung und der geltenden Lizenzbestimmungen hier angeführt. Auf das Literaturverzeichnis wird verwiesen. Das **Zitatrecht** in dem für wissenschaftliche Werke üblichen Ausmaß wird beansprucht. Wenn Sie eine Urheberrechtsverletzung erkennen, so bitten wir um Hinweis an den auf der Titelseite genannten Autor und werden entsprechende Inhalte sofort entfernen oder fehlende Rechtsnennungen nachholen. Bei Produkt- und Firmennamen können Markenrechte Dritter bestehen. Verweise und Verlinkungen wurden zum Zeitpunkt des Setzens der Verweise überprüft; sie dienen der Information des Lesers. Der Autor macht sich die Inhalte, auch in der Form, wie sie zum Zeitpunkt des Setzens des Verweises vorlagen, nicht zu eigen und kann diese nicht laufend auf Veränderungen überprüfen.

Alle sonstigen, hier nicht angeführten Inhalte unterliegen dem Copyright des Autors, Prof. Dr. Clemens Cap, ©2020. Wenn Sie diese Inhalte nützlich finden, können Sie darauf verlinken oder sie zitieren. Jede weitere Verbreitung, Speicherung, Vervielfältigung oder sonstige Verwertung außerhalb der Grenzen des Urheberrechts bedarf der schriftlichen Zustimmung des Rechteinhabers. Dieses dient der Sicherung der Aktualität der Inhalte und soll dem Autor auch die Einhaltung urheberrechtlicher Einschränkungen wie beispielsweise **Par 60a UrhG** ermöglichen.

Die Bereitstellung der Inhalte erfolgt hier zur persönlichen Information des Lesers. Eine Haftung für mittelbare oder unmittelbare Schäden wird im maximal rechtlich zulässigen Ausmaß ausgeschlossen, mit Ausnahme von Vorsatz und grober Fahrlässigkeit. Eine Garantie für den Fortbestand dieses Informationsangebots wird nicht gegeben.

Die Anfertigung einer persönlichen Sicherungskopie für die private, nicht gewerbliche und nicht öffentliche Nutzung ist zulässig, sofern sie nicht von einer offensichtlich rechtswidrig hergestellten oder zugänglich gemachten Vorlage stammt.

Zitierweise dieses Dokuments

Wenn Sie Inhalte aus diesem Werk nutzen oder darauf verweisen wollen, zitieren Sie es bitte wie folgt:

Clemens H. Cap: Netzwerk Komponenten. Electronic document. <https://iuk.one/1012-1026>
25. 1. 2021.

Bibtex Information: <https://iuk.one/1012-1026.bib>

```
@misc{doc:1012-1026,  
  author      = {Clemens H. Cap},  
  title       = {Netzwerk Komponenten},  
  year        = {2021},  
  month       = {1},  
  howpublished = {Electronic document},  
  url         = {https://iuk.one/1012-1026}  
}
```

Typographic Information:

Typeset on January 25, 2021

This is pdfTeX, Version 3.14159265-2.6-1.40.21 (TeX Live 2020) kpathsea version 6.3.2

This is pgf in version 3.1.5b

This is preamble-slides.tex myFormat©C.H.Cap

1 Titelseite

1. Bridge

3 Aufgabe der Bridge

4 Bridge

5 Mechanismen

6 Transceiver, Bridge, Switch, Hub & Co (1)

7 Transceiver, Bridge, Switch, Hub & Co (2)

8 Weiterleitung bei Fehlern und Kollisionen

2. Router

10 Aufgabe des Routers

11 Mechanismus des Routing

12 Router

13 Layer-3-Adressen (1)

14 Layer-3-Adressen (2)

15 Routing ist Optimierung unter Randbedingungen

16 Flußsteuerung im Router

17 Staus (Congestion)

18 Strategien des Router Queueing

3. Weitere Komponenten

20 Gateways

21 NAT (Network Address Translation) Gateway

22 NAT (Network Address Translation) Gateway

23 Firewall

24 Proxy

25 Transparenz von Komponenten

26 Intransparenz von Komponenten

Legende:

 Fortsetzungsseite

 Seite ohne Überschrift

 Bildseite