Internetworking
→ Netzkoppelelemente

Prof. Dr. Norbert Pohlmann
Fachbereich Informatik
Verteilte Systeme und Informationssicherheit

Fachhochschule Gelsenkirchen

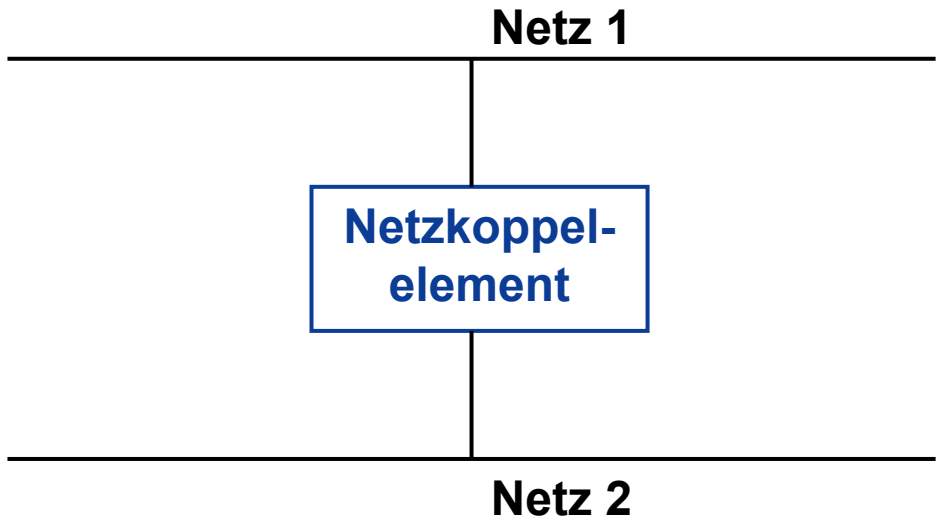
Inhalt

- Netzkoppelelemente: Einführung und Aufgaben
- Prinzipielle Realisierungsmöglichkeit der Netzkopplung
- Repeater (Hubs)
- Bridges (Switches)
- Router
- Gateways
- Zusammenfassung

Inhalt

- **Netzkoppelelemente: Einführung und Aufgaben**
- Prinzipielle Realisierungsmöglichkeit der Netzkopplung
- Repeater (Hubs)
- Bridges (Switches)
- Router
- Gateways
- Zusammenfassung

Netzkoppelelemente
→ Einführung (1/3)



- Um die **Verbindung zwischen zwei Netzen** herzustellen, die aufgrund technischer oder geographischer Gegebenheiten nicht direkt (also durch ein Kabel) gekoppelt werden können, werden **Netzkoppelelemente** (auch Netzkoppeleinheiten genannt) verwendet.
- Diese sind im allgemeinsten Fall **Stationen an zwei Netzen** und stellen **durch ihre Funktion die Verbindung zwischen diesen Netzen** her.

Netzkoppelelemente
→ Einführung (2/3)

Durch Netzkoppelelemente ist es möglich

- die **physikalische Begrenzung** der Ausdehnung eines lokalen Netzes (durch Kopplung mehrerer solcher Teilnetze) zu umgehen
- lokales Datenaufkommen durch **Bildung von logischen Teilnetzen** vom restlichen Netzwerk zu entkoppeln
- Teilnetze mittels Netzkoppeleinheiten zu einem Netz für den **bereichsübergreifenden Verkehr** zu koppeln, damit nur noch bereichsübergreifender Datenverkehr das gesamte Netz belastet (Lastkopplung).
- Netze mit **unterschiedlichen Protokollarchitekturen miteinander zu koppeln** (z.B. Netze mit herstellerspezifischen Protokollen wie IBM-SNA oder DECnet)

Netzkoppelelemente
→ Einführung (3/3)

Teilnetz

- Rechnersysteme, die über eine gemeinsame Verbindungsschicht (Sicherungsschicht - Schicht 2 des OSI-Referenzmodells) erreicht werden, formen aus Sicht der Netzwerkschicht (Schicht 3 des OSI-Referenzmodells) ein Teilnetz.
- Der Einsatz der Netzwerkschicht (Vermittlungsebene) ist in der Regel nur dann sinnvoll, wenn Rechnersysteme in verschiedenen Teilnetzen miteinander kommunizieren.

Heterogenes Netz

- Unter einem heterogenen Netz versteht man ein Rechnernetz, das aus heterogenen Komponenten aufgebaut ist.
  - Verschiedene Zugriffsverfahren: (z.B. Ethernet, Token Ring)
  - Verschiedene Protokoll-Familien: (z.B. DECnet, TCP/IP)
  - Verschiedene Rechnersysteme: (z.B. PC, Mainframe)

Netzkoppelelemente
→ Aufgaben

- Zu koppelnde Netze können sich in vielen Merkmalen unterscheiden.
- Es ist Aufgabe der Netzkoppeleinheiten, diese **Unterschiede zu überwinden** und eine Kommunikation zu ermöglichen.
- In einer Netzkoppeleinheit werden die **Protokolle** der beteiligten Netze **aufeinander abgebildet**.
- Handelt es sich bei den beteiligten Netzen um Netze mit gleicher Protokollarchitektur, so kann die Information direkt weitergegeben werden.
- Handelt es sich allerdings um Netze unterschiedlicher Protokollarchitektur, so müssen bei einem Informationsaustausch von einem zum anderen Netz die Steuerinformationen des einen Netzes entfernt und die Steuerinformationen des anderen Netzes eingeführt bzw. eingepackt werden.

Netzkoppelelemente
→ Aufgaben: Abbildung der PDU-Parameter

- Die Sequenz von Protokolldaten (PDU, Protocol Data Units) des einen Netzes müssen auf Sequenzen von PDUs des anderen Netzes abgebildet werden.
- Dabei werden die Parameter von PDUs wie folgt unterschieden:
  - **Parameter, die in beiden Netzen die selbe Bedeutung haben** und somit nicht umgesetzt werden müssen.
  - **Parameter, die umgesetzt werden müssen, da sie in beiden Netzen unterschiedliche Bedeutung haben.**
  - **Parameter, die nur im sendenden Netz definiert sind** und somit von der Netzkoppeleinheit entfernt werden müssen.
  - **Parameter, die nur im empfangenden Netz definiert sind** und somit von der Netzkoppeleinheit erzeugt werden müssen.

Netzkoppelelemente
→ Aufgaben: Wegsuche (Routing) und Adressierung

- Mittels Routing sollen Pakete effizient vom Absender zum Ziel zugestellt werden.
- Üblicherweise werden mit diesem Begriff zwei separate Funktionen zusammengefasst:
  - Beschaffung und Unterhaltung von ***Zustellinformationen***
  - Ausnutzung der Zustellinformationen für die ***Zustellung***
- Unter Zustellinformationen versteht man z.B. Weglängen, Adressen, usw.
- Die Routing-Entscheidung („Welchen Weg wähle ich?“) kann auf zwei Kriterienklassen beruhen.

Wegsuche (Routing) und Adressierung
→ Routing-Entscheidung: Fixe Kriterien

- Die erste Klasse beinhaltet fixe Kriterien, wie zum Beispiel Wege oder Teilwege zu Zielen.
- Diese werden manuell in statische Routing-Tabellen eingetragen.
- Die Nachführung dieser Tabellen ist lästig, allerdings hat diese Variante Sicherheitsvorteile, da nur die bekannten eingetragenen Adressen transportiert werden und andere Stationen keine Möglichkeit haben, in die Kommunikation über die Netzkoppeleinheiten hinweg eingebunden zu werden.
- Man spricht bei diesem Verfahren deshalb auch vom sogenannten **Protected Mode**.
- Dynamische Änderungen im Netz, wie z.B. das Ein- und Ausschalten eines Systems werden nicht berücksichtigt.

Wegsuche (Routing) und Adressierung
→ Routing-Entscheidung: Dynamische Kriterien

- Die zweite Klasse beinhaltet dynamische Kriterien, die teilweise berechnet werden und in einer dynamischen Tabelle stehen.
- Hier werden Änderungen im Netz erkannt und entsprechend vermerkt.
- Zu den Kriterien zählen z.B.:
  - momentan arbeitende Knoten
  - minimale Anzahl von passierten Knoten
  - minimale Weglänge zu einem Knoten
  - Gesamtlast
  - gleichmäßige Auslastung der Ressourcen
  - Verfügbarkeit der Verbindung

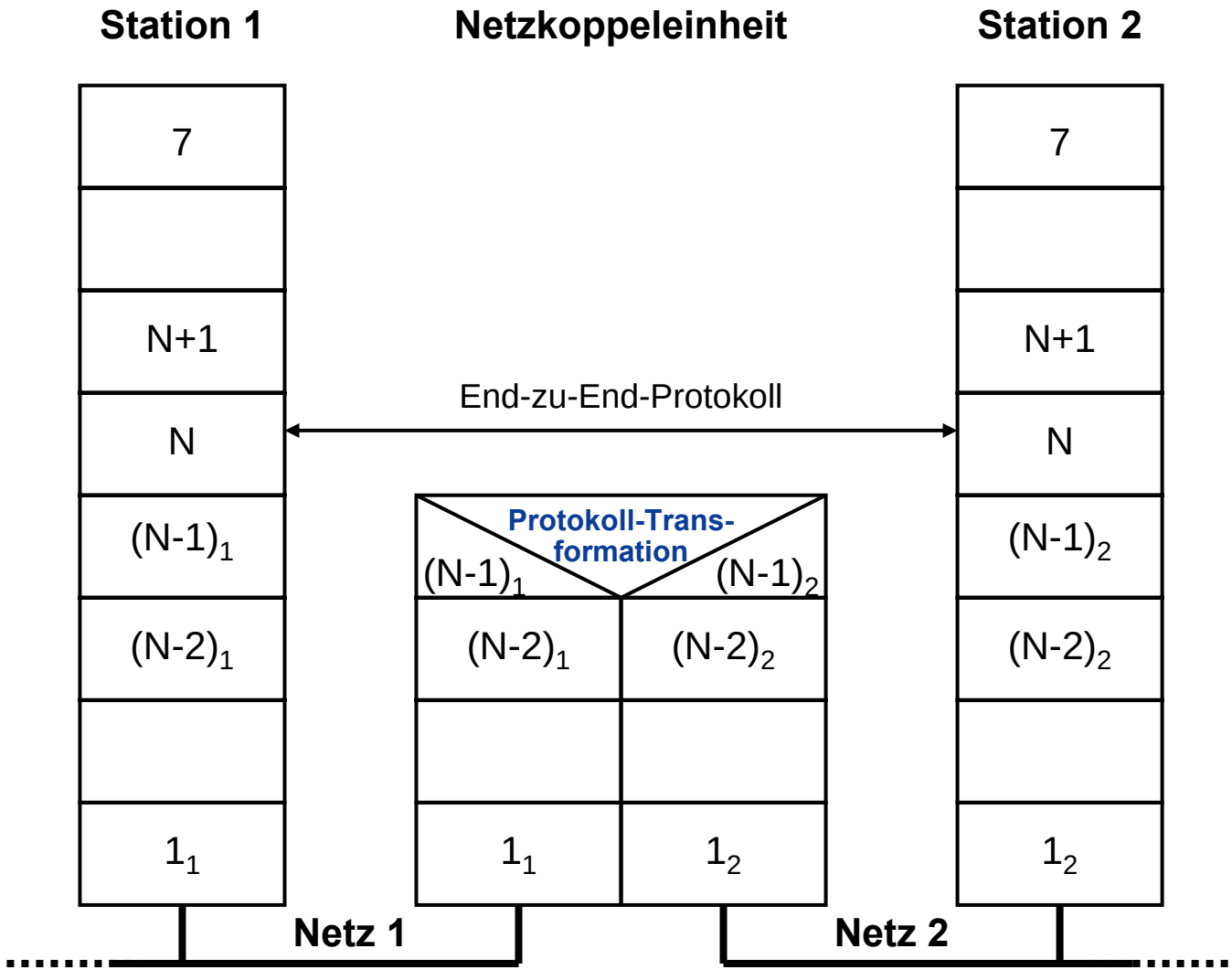
Inhalt

- Netzkoppelelemente: Einführung und Aufgaben
- **Prinzipielle Realisierungsmöglichkeit der Netzkopplung**
- Repeater (Hubs)
- Bridges (Switches)
- Router
- Gateways
- Zusammenfassung

Prinzipielle Realisierungsmöglichkeit
der Netzkopplung

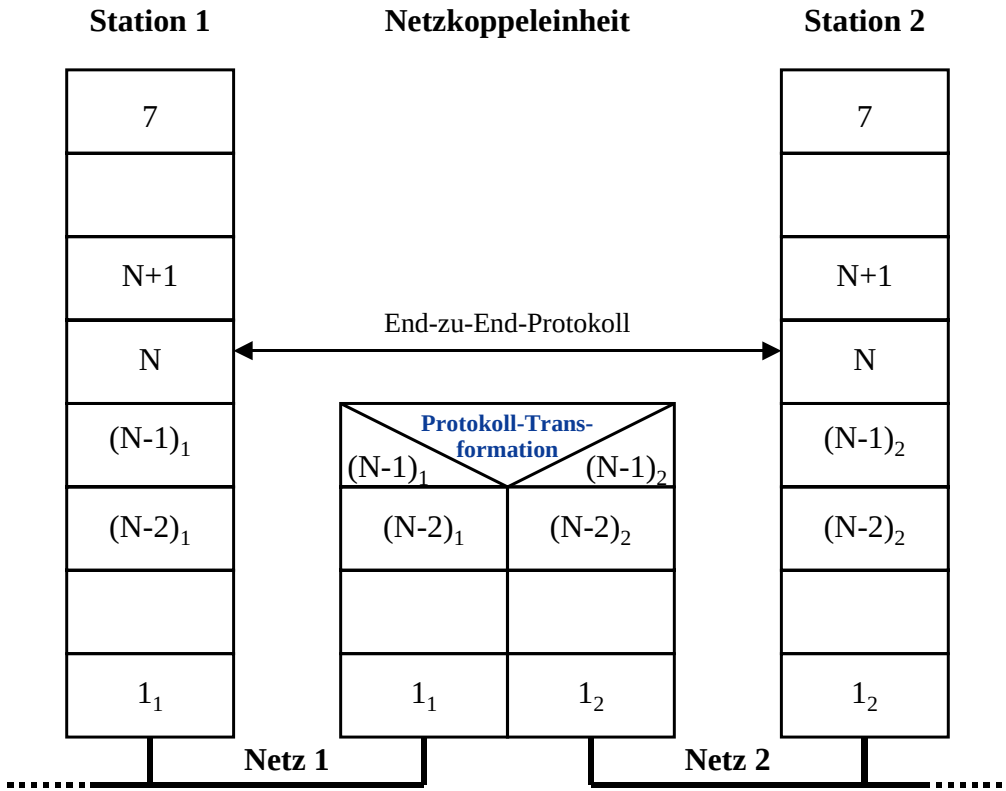
- Geht man bei der Kopplung zweier Netze davon aus, dass auf der Schicht N-1 die Protokolle der zu koppelnden Netze verschieden und von Schicht N an aufwärts identisch sind (die Schichten 1 bis N-2 können, soweit vorhanden, identisch oder verschieden sein), so gibt es folgende Möglichkeiten der Kopplung:
  - Netzkopplung durch **Protokolltransformation**
  - Netzkopplung durch **Einführung eines globalen Protokolls**
  - Netzkopplung auf der **ersten gemeinsamen Schicht**

Netzkopplung
→ durch Protokolltransformation (1/2)

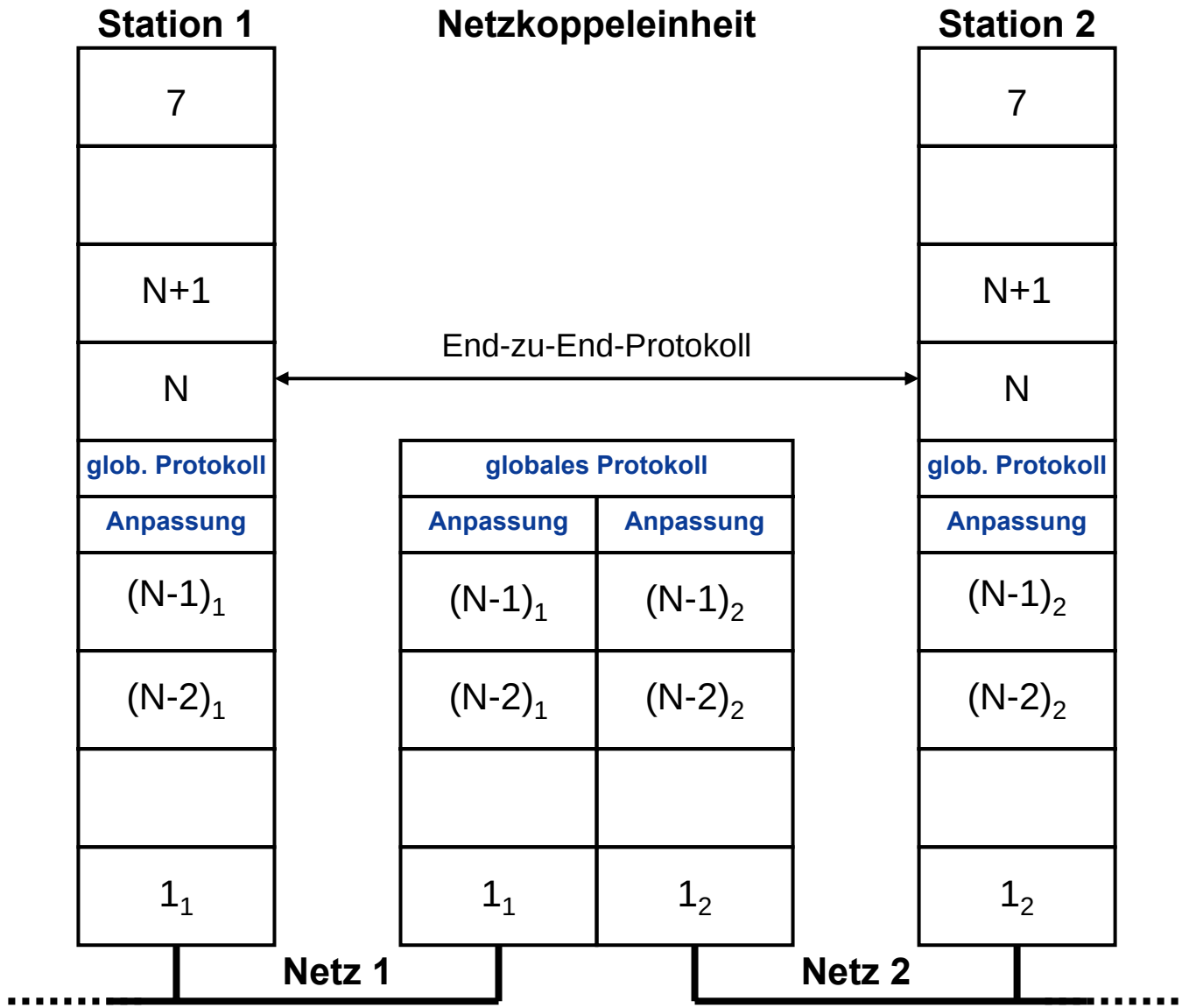


Netzkopplung
→ durch Protokolltransformation (2/2)

- Die Kopplung durch Protokolltransformation wird auf der letzten unterschiedlichen Schicht (N-1) realisiert.
- Sie hat oft einen Verlust der Funktionalitäten zur Folge, da zu Funktionen des einen Netzes nicht immer eine entsprechende Funktion auf dem anderen Netz existiert.
- Ein Vorteil der Protokoll-transformation sind die End-zu-End-Protokolle von der Schicht N an aufwärts, wodurch z.B. eine End-zu-End-Flusskontrolle realisiert werden kann!

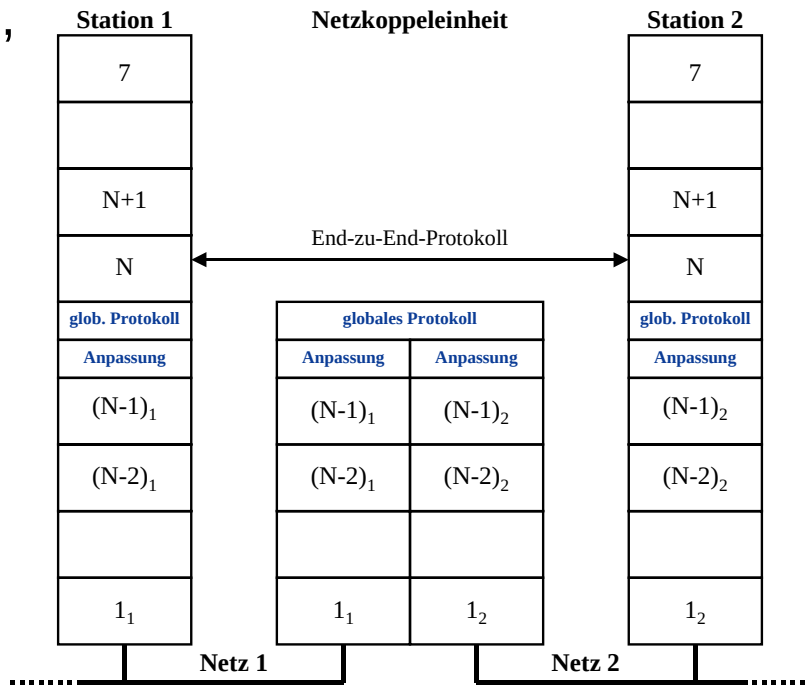


Netzkopplung
→ durch Einführung eines globalen Protokolls (1/2)

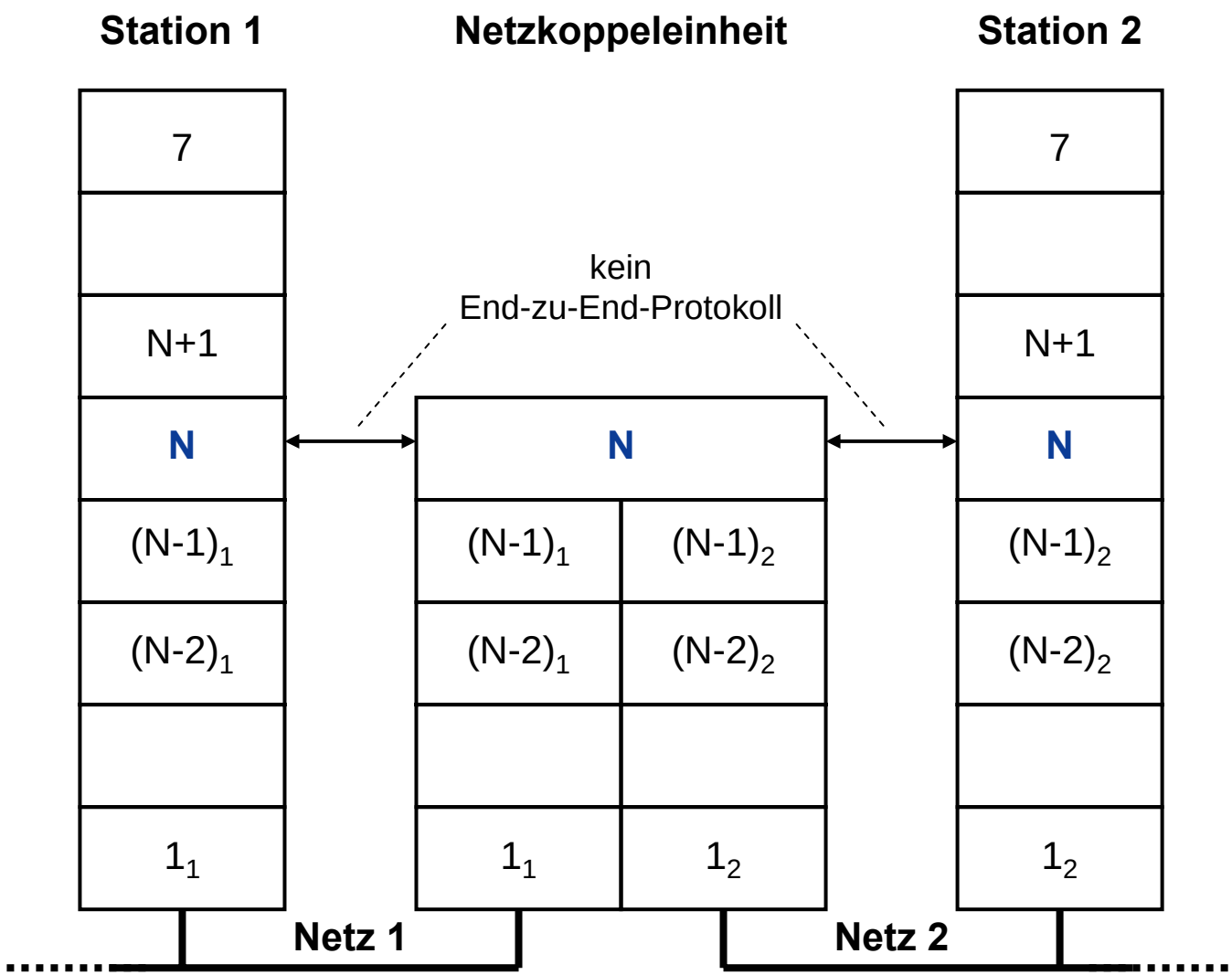


Netzkopplung
→ durch Einführung eines globalen Protokolls (2/2)

- Auch die Kopplung durch Einführung eines globalen Protokolls wird in der letzten verschiedenen Schicht (N-1) realisiert.
- In dieser Schicht wird ein globales Protokoll sowohl in Netz 1 als auch in Netz 2 eingeführt, in welches die netzspezifischen Protokolle dieser Schicht mittels einer Anpassungsschicht angepasst werden.
- Diese Koppelungsart hat den **Nachteil**, dass die Protokolle der Schicht N-1 in allen Stationen der beteiligten Netze erweitert werden müssen.
- Der **Vorteil** eines globalen Protokolls sind die End-zu-End-Protokolle von der Schicht N an aufwärts, wodurch z.B. eine End-zu-End-Flusskontrolle realisiert werden kann (wie bei der Protokolltransformation).

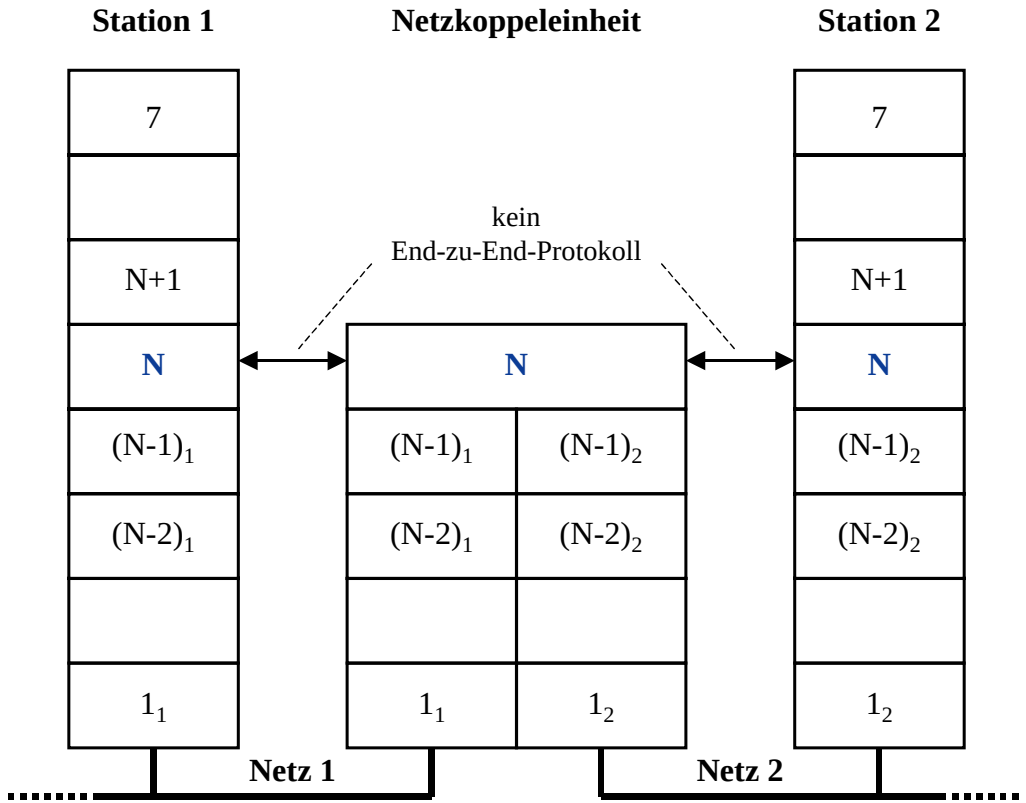


Netzkopplung
→ auf der ersten gemeinsamen Schicht (1/2)



Netzkopplung
→ auf der ersten gemeinsamen Schicht (2/2)

- Bei der Kopplung auf der ersten gemeinsamen Schicht ist keine Protokolltransformation notwendig.
- PDUs werden von der einen Seite der Netzkoppeleinheit in der Schicht N auf die andere Seite weitergegeben.
- Ein Erweitern der Protokolle ist nicht notwendig, dafür geht das End-zu-End-Protokoll auf der Schicht N verloren (z.B. Problem beim Transport-Protokoll).

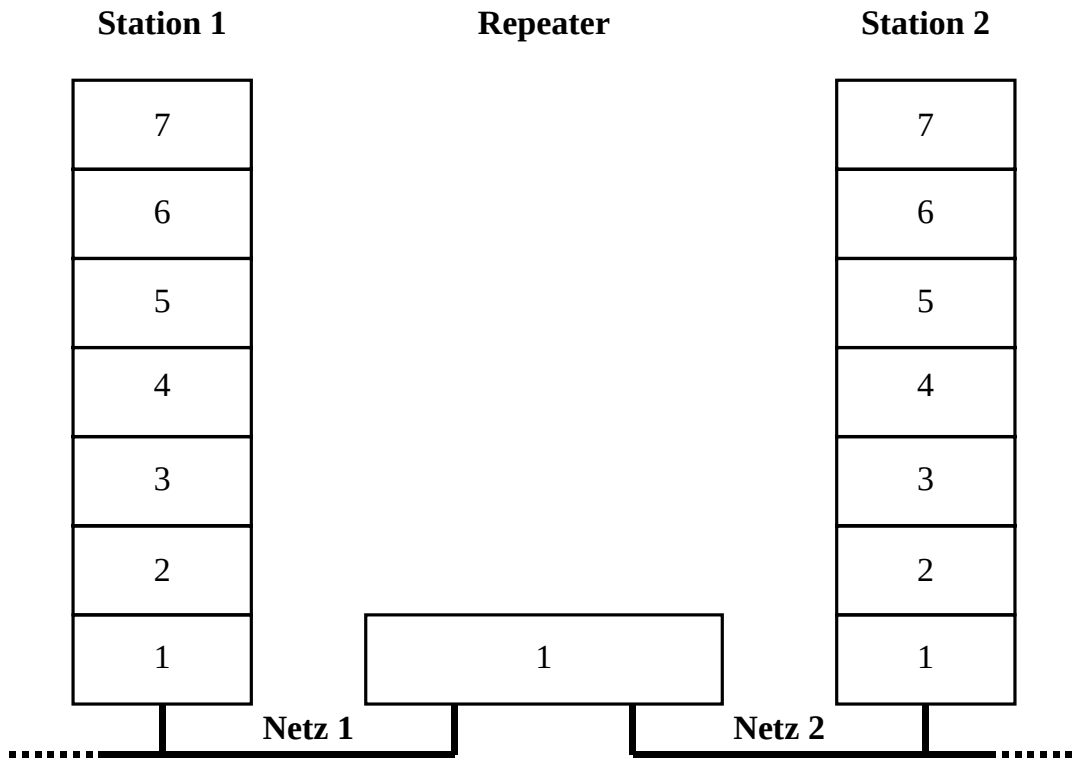


Inhalt

- Netzkoppelelemente: Einführung und Aufgaben
- Prinzipielle Realisierungsmöglichkeit der Netzkopplung
- **Repeater (Hubs)**
- Bridges (Switches)
- Router
- Gateways
- Zusammenfassung

Repeater

→ Hubs



Repeater (1/4)

- **Repeater** stellen die **einfachste Art der Netzkopplung** dar.
- Sie verbinden zwei Netze gleichen Typs (im allgemeinen zwei Ethernet-Segmente) auf der Bitübertragungsschicht (Schicht 1).
- Der Repeater ist ein **elektrischer Signalverstärker** und dient dazu, Netze, deren räumliche Ausdehnung aus physikalischen Gründen (Signaldämpfung und Signalverformung begrenzt sind, zu erweitern.
- Die Anzahl der zu koppelnden Netze ist dabei begrenzt, da es bei den einzelnen lokalen Netzen Einschränkungen der Ausdehnung durch das Übertragungsprotokoll gibt.
- Das bei **Ethernet** verwendete Zuteilungsverfahren CSMA/CD (Carrier Sense Multiple Access / Collision Detection) beispielsweise schreibt eine **maximale erlaubte Laufzeit der Daten** vor, um die sichere Erkennung von Kollisionen zu gewährleisten.
- Zu einer Kollision kommt es, wenn zwei Stationen gleichzeitig auf das Übertragungsmedium zugreifen, um eine Nachricht zu versenden.

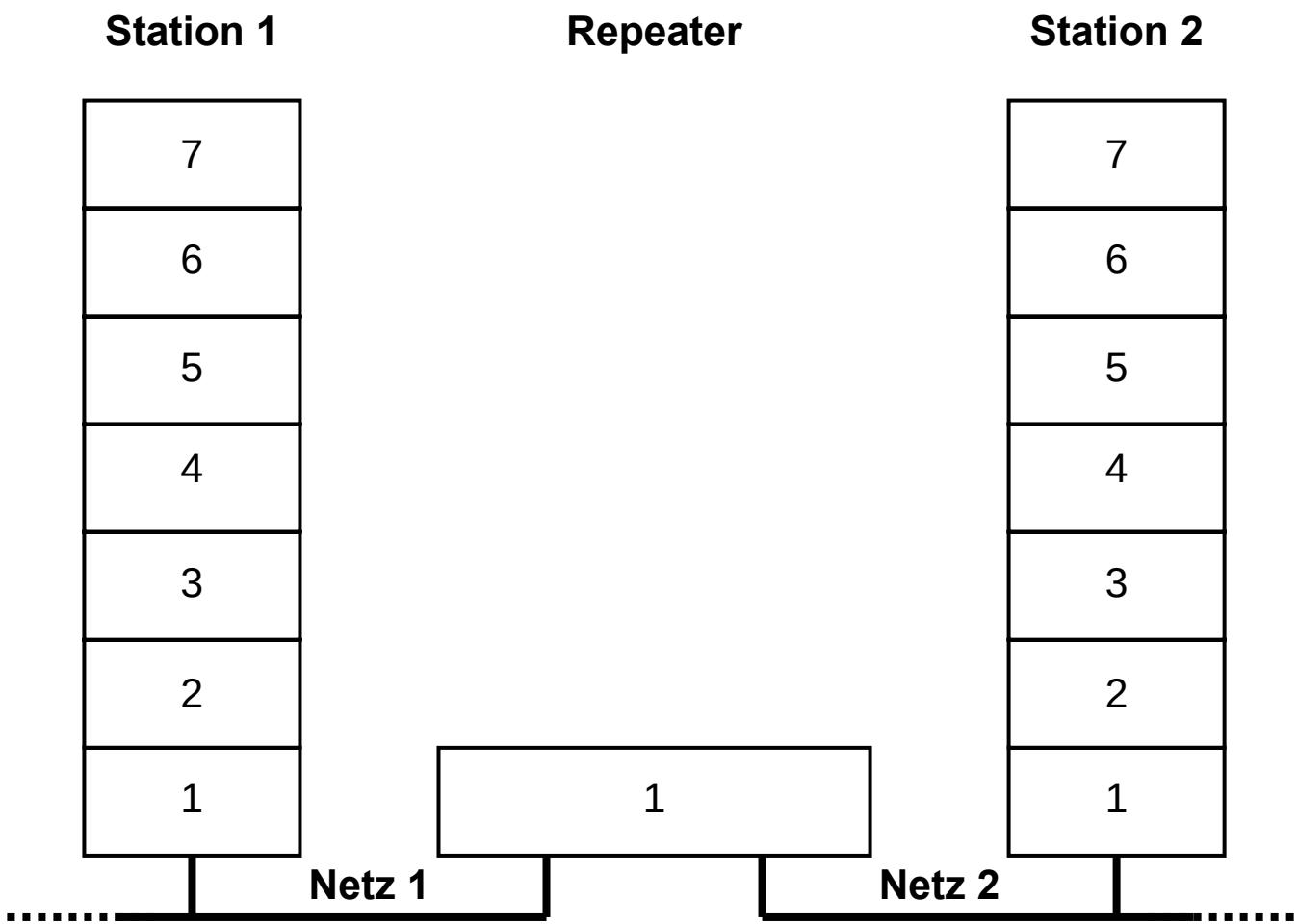
Repeater (2/4)

- Durch den **Kollisionserkennungsmechanismus** wird die Kollision von beiden sendenden Stationen erkannt, worauf diese ihren Sendebetrieb einstellen und ihn nach kurzer Pause zeitlich versetzt wieder aufnehmen.
- Die sendenden Stationen hören das Medium nur solange ab, solange sie sich im Sendebetrieb befinden.
- Wird in dieser Zeit keine Kollision erkannt, so wird dies von der sendenden Station als Ankunftsbestätigung aufgefasst.
- Das Signal muss also innerhalb der kürzesten möglichen Paketdauer bis an das Ende des Netzes und wieder zurück gelangen, damit der Mechanismus funktioniert.
- Aus diesem Grund dürfen sich bei Ethernet zwischen zwei beliebigen Endstationen max. 4 Repeater befinden.
- Bei der Kooplung mittels Repeater müssen beide miteinander zu verbindende Netzwerke auf allen sieben Schichten des OSI-Referenzmodells identisch sein.

Repeater (3/4)

- Ein Repeater kopiert blindlings jedes Bit von einem Kabelsegment zum anderen, durch ihn erhält man praktisch ein Netz, das aus mehreren Netzsegmenten aufgebaut ist.
- Durch den Einsatz von Repeatern erfolgt keine Aufsplittung des Netzes in logische Teilnetze, wie es z.B. bei Bridges der Fall ist.
- **Multiport-Repeater** haben mehrere LAN-Ports und können so mehrere Segmente miteinander verbinden.
- **Sternkoppler (Hubsysteme - Hub)**
  - Wie Multiport-Repeater, sie können jedoch weitaus mehr Segmente konzentrieren und darüber hinaus verschiedene Medien von KOAX oder Glasfaser integrieren.
  - Bei Ethernet-Netzwerken, die mit ***Twisted Pair-Verkabelung*** aufgebaut werden, ist an jedem Port des Sternkopplers (in diesem Fall meist **Hub** genannt) nur eine Station (oder ein weiterer **Hub**) angeschlossen.
  - Der **Hub** übernimmt dann die Weiterleitung der auf einem Port ankommenden Pakete an alle anderen Ports.

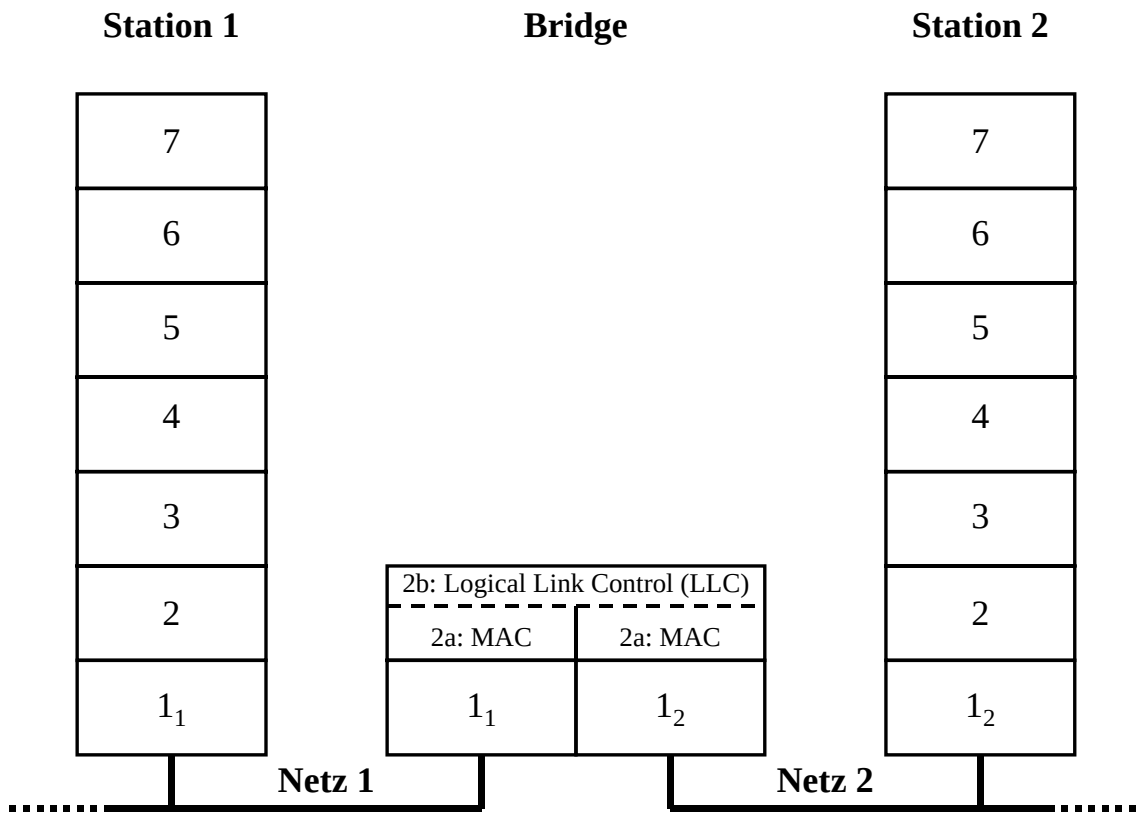
Repeater (4/4)
→ Netzkopplung mit einem Repeater



Inhalt

- Netzkoppelelemente: Einführung und Aufgaben
- Prinzipielle Realisierungsmöglichkeit der Netzkopplung
- Repeater (Hubs)
- **Bridges (Switches)**
- Router
- Gateways
- Zusammenfassung

Bridges
→ Switches



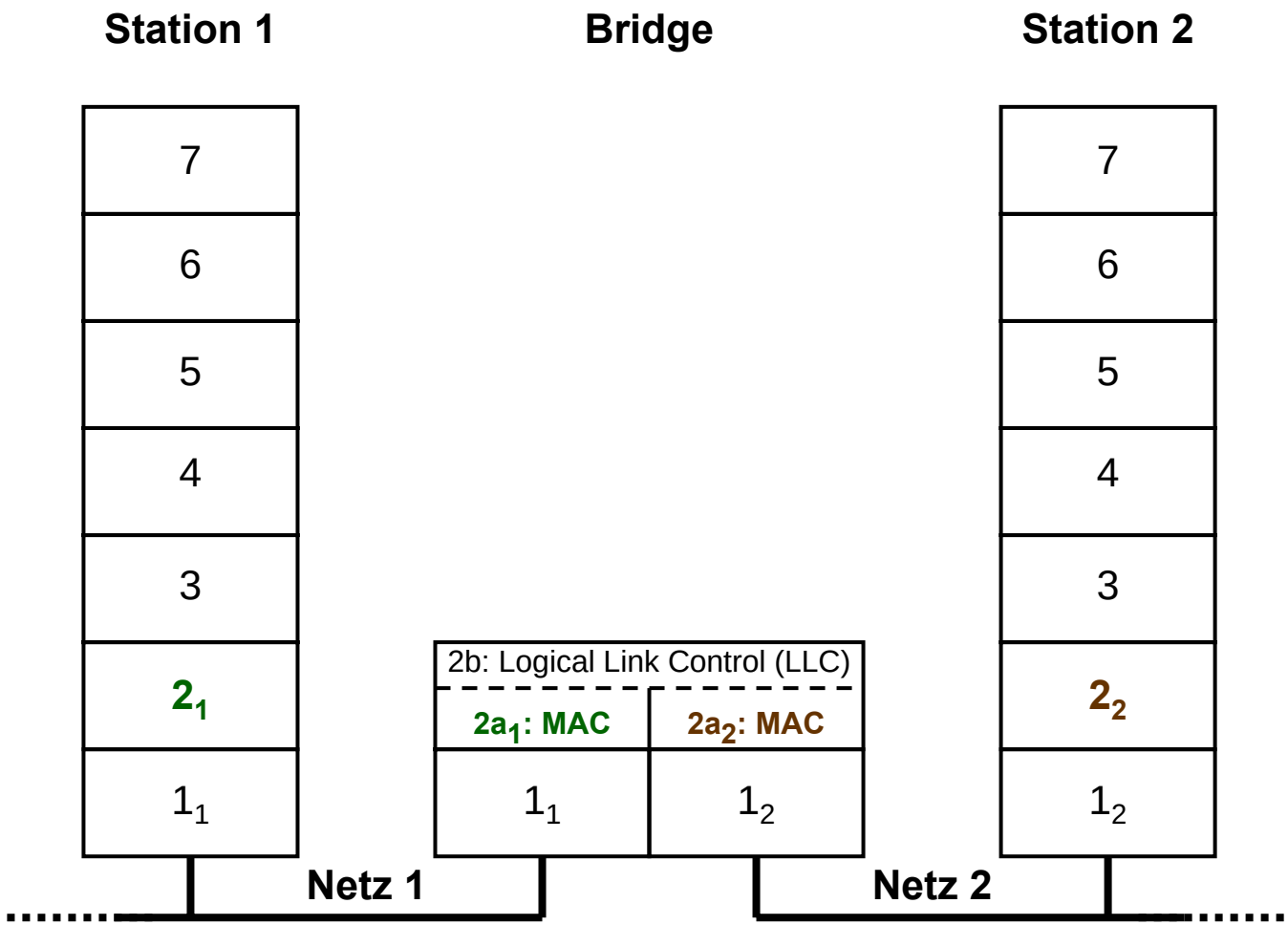
Bridges (1/6)

- Bridges sind Netzkoppeleinheiten, die **verschiedene Segmente eines Netzes zu einem Gesamtnetz verbinden**.
- Eine Bridge kann zur Erweiterung der räumlichen Ausdehnung eines Netzes verschiedene Netzsegmente auch dann noch miteinander verbinden, wenn aufgrund einer beschränkten erlaubten Anzahl kein Repeater mehr eingesetzt werden darf.
- Dies rührt daher, dass bei einer Kopplung mittels **Bridge eine logische Trennung der beiden Netzsegmente** vorgenommen wird.
- Bridges übernehmen die **Zwischenspeicherung** der Datenpakete und sorgen für einen **kollisionsfreien Weitertransport**.
- Fehlerhafte Frames (z.B. durch Übertragungsfehler oder Kollision) werden nicht weitergeleitet.
- Man spricht hier auch davon, dass eine Bridge das Netzwerk in mehrere Kollisionsdomänen (Collision Domains) aufteilt, da die Auswirkung einer Kollision auf ein Segment begrenzt bleibt.
- Meist arbeiten Bridges auf der Ebene 2a (Medium Access Control MAC) des OSI-Modells, so dass mittels einer solchen Bridge eine Kopplung nur zwischen Netzen gleichen Typs möglich sind.

Bridges (2/6)

- Grundsätzlich sind Bridges in der Lage, sowohl gleichartige, als auch, bezüglich ihrer physikalischen Eigenschaften und des Zugangsverfahrens, unterschiedliche Netzwerke miteinander zu verbinden.
- **Mixed Media Bridges** arbeiten auf Ebene 2b (Logical Link Control LLC) des OSI-Modells und können somit auch Netzwerke mit unterschiedlichen MAC-Protokollen koppeln (z.B. Ethernet und Token Ring).
- Da bei einer solchen Umsetzung aber viele Probleme auftreten (z.B. unterschiedliche Paketgrößen und Übertragungsraten) und die Art und Weise, wie die Umsetzung zwischen unterschiedlichen Netzwerktypen erfolgen soll, nicht standardisiert ist, gibt es auch keine **„richtige“ Art** der Umsetzung.
- Die in den Datenpaketen enthaltenen Informationen werden, außer der MAC-Layer-Source- und Destination-Adressen, von einer Bridge nicht ausgewertet.
- Daher können Bridges mit jedem Kommunikationsprotokoll der Schicht 3 zusammenarbeiten, sind also protokollunabhängig.

Bridges (3/6)
→ Netzkopplung über eine (Mixed Media-)Bridge



Bridges (4/6)
→ Filternde Bridge

- Um Datenverkehr in Teilnetzen, deren Stationen häufig miteinander kommunizieren, vom Gesamtverkehr zu isolieren, werden filternde Bridges eingesetzt.
- Eine **filternde Bridge** ist ein **intelligentes System** im Netz, welches nur Pakete von einem Teilnetz zum anderen übergibt, die von einer Station des einen Teilnetzes für eine Station in einem anderen Teilnetz bestimmt sind.
- Dadurch wird das übrige Netz nur dann belastet, wenn Daten erzeugt werden, die für andere Stationen in einem anderen Teilnetz bestimmt sind.
- Der interne Datenverkehr der einzelnen Teilnetze wird also lokal begrenzt, lediglich der zu anderen Teilnetzen übergreifende Verkehr wird über die Bridge weitergeleitet.
- Auch im punkto Sicherheit bietet die Technik des Filtering einige Vorteile.
- Durch das logische Trennen der Netze wird durch die filternde Bridge ein Weg geschaffen, den übergreifenden Verkehr zu kontrollieren.

Bridges (5/6)
→ Filternde Bridge

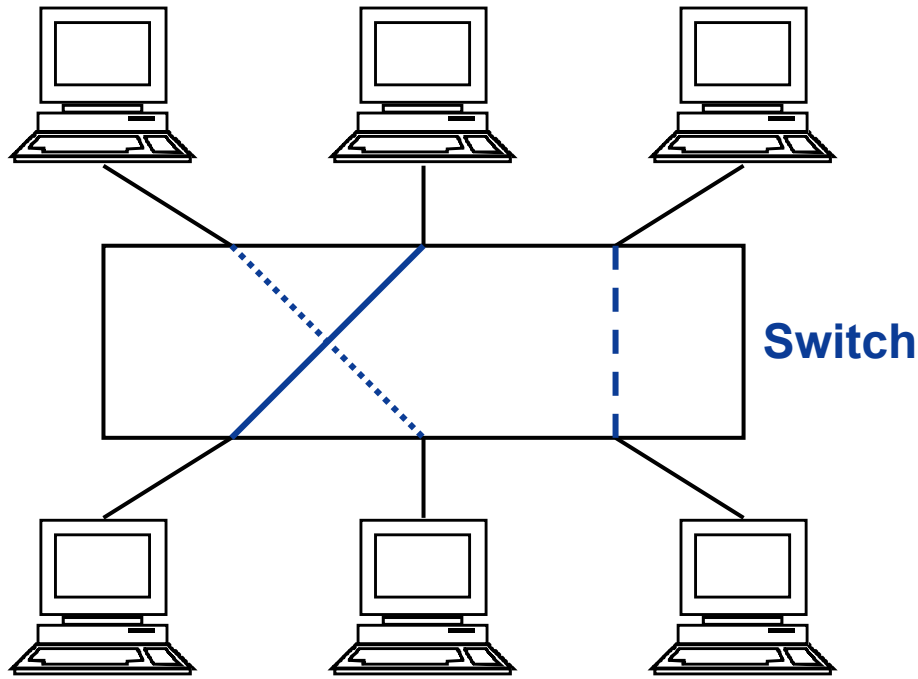
- Datenpakete können gezielt vom Zugang ins übrige Netz ausgeschlossen werden.
- Die meisten Bridges werten die im Datenpaket enthaltenen Empfänger- oder Absenderadressen aus.
- Manche Bridges verwenden zusätzlich einen sogenannten Protocol-Type-Filter.
- Protocol-Type-Filter werden eingesetzt, um Datenpakete eines bestimmten Protocols nicht in andere Teilnetze zu übertragen.
- Eine andere Variante dieses Filters gibt bestimmten Protokollen bei der Übertragung eine höhere Priorität.

Bridges (6/6)
→ Multiport Bridge

- Nachdem lange Zeit 2-Port-Bridges den Markt dominierten, die genau zwei Teilnetze miteinander verbinden, werden heute aufgrund des Bedarfs vieler Teilnetze immer häufiger sogenannten Multiport-Bridges eingesetzt, die mehrere Teilnetze miteinander verbinden können.
- Sie verbinden in der Regel vier oder acht Teilnetze.
- Multiport-Bridges erleichtern den Aufbau von Baumstrukturen (Mehrfachverzweigungen), außerdem wird die Konzentration mehrerer Ports in einer Bridge die Anzahl der notwendigen Brücken und die Lastverteilung auf verschiedene Verbindungen erleichtert.

Switches
→ Übersicht (1/3)

- Switches stellen eine Sonderform von Multiport-Bridges dar, die vor allem in Ethernet Netzwerken mit Twisted Pair Verkabelung von großer Bedeutung sind.
- Ein Switch kann gleichzeitig mehrere interne Verbindungen mit voller Geschwindigkeit bereitstellen.



Switches
→ Übersicht (2/3)

- Die Anzahl der gleichzeitigen Verbindungen entspricht überlicherweise der halben Portanzahl.
- So wären z.B. bei einem Switch mit 8 Ports **vier** gleichzeitige Verbindungen zwischen jeweils 2 Stationen mit maximaler Geschwindigkeit möglich.
- Der Switch ordnet dabei anhand der MAC-Zieladresse dem ankommenden Rahmen den passenden Ausgangsport zu.
- Ein wichtiger Begriff im Zusammenhang mit Switches ist die aggregierte Bandbreite.
- Damit wird die maximale Übertragungsrate, die der Switch zur Verfügung stellen kann, bezeichnet.
- Diese Größe ist abhängig von der Anzahl der Ports und der Übertragungsgeschwindigkeit.

$$\text{aggregierte Bandbreite} = \frac{\text{Portzahl}}{2} * \text{Übertragungsgeschwindigkeit}$$

Switches
→ Übersicht (3/3)

- Die interne Verbindung der Ports, die sogenannte Backplane, muss natürlich in der Lage sein, die hohen Übertragungsgeschwindigkeiten innerhalb des Gerätes zu bewältigen.
- Verwendet man einen 12-Port Switch mit 10 Mbit/s, ergibt sich nach der Formel eine aggregierte Bandbreite von 60 Mbit/s.
- Switche, bei denen alle Ports mit derselben Übertragungsrate arbeiten, sind vor allem für Peer-to-Peer-Netze geeignet, bei denen alle Geräte auf die Dienste der anderen Geräte zugreifen.
- Da aber in den meisten Netzen eine serverbasierte Struktur verwendet wird und dabei der größte Teil des Verkehrs zwischen einem Server und den Arbeitsstationen stattfindet, werden Switches oftmals mit einem Uplink-Port angeboten.
- Dieser bietet dann z.B. eine 100 MBit-Verbindung zum Server und mehrere 10 Mbit-Verbindungen zu den Arbeitsstationen.

Switches
→ Strategien (1/2)

- Für das Switching bestehen zwei unterschiedliche Strategien:
  - das **sichere** Store-and-Forward und
  - das **schnelle** Cut-Through-Verfahren

- **Store-and-Forward-Switching**
  - Bei diesem Verfahren wird zunächst, wie bei einer normalen Bridge, das ankommende Datenpaket komplett gespeichert und überprüft.
  - Ist das Paket, z.B. aufgrund einer Kollision, beschädigt, wird es verworfen.
  - Dadurch werden nur korrekte Pakete weitergeleitet.
  - Durch die Zwischenspeicherung der Daten kommt es jedoch zu einer erheblichen Verzögerung der Datenübertragung.
  - Die **Lese- und Verarbeitungszeit** (Latency-Zeit) liegt je nach Paketgröße bei **100 bis 1300µs**.
  - Ein Switch, der mehrere langsamere Ports auf einen schnelleren Port umsetzt, arbeitet immer im Store-and-Forward!

Switches
→ Strategien (2/2)

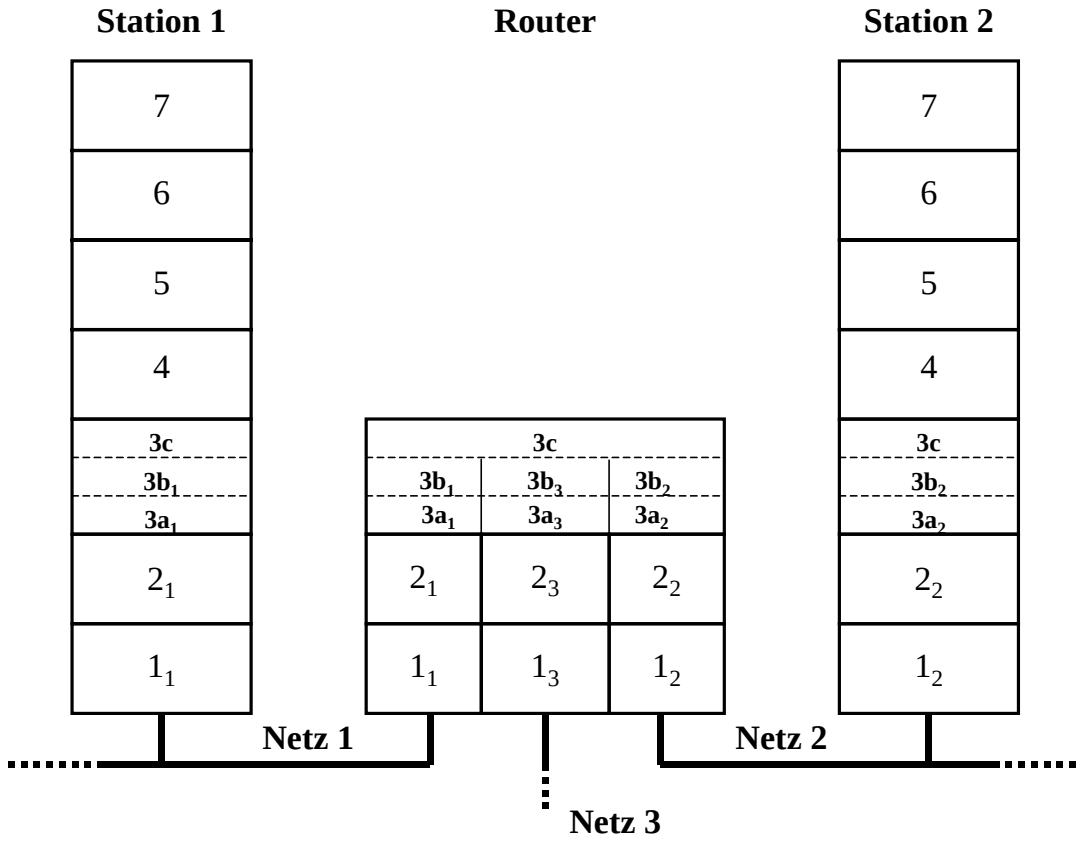
- **Cut-Through-Switching**
  - Die Weiterleitung der Datenpakete beginnt beim Cut-Through-Switching sobald die 6 Byte lange Zieladresse gelesen wurde.
  - Dadurch kann der Switch nach den ersten 20 bis 30 Byte die Verbindung zwischen dem Eingangs- und Ausgangsport herstellen.
  - Die Verzögerungszeit pro Datenpaket liegt dadurch nur bei etwa **30 bis 60µs**, es werden jedoch eventuell auch **beschädigte Pakete weitergeleitet**.

- **Hybrid-Switching**
  - Das Hybrid-Switching-Verfahren, auch adaptives Switching genannt, versucht die Vorteile von Store-and-Forward und Cut-Through zu vereinen.
  - Ein Hybrid-Switch arbeitet normalerweise als Cut-Through-Switch, beobachtet dabei aber ständig die Anzahl der beschädigten Pakete.
  - Übersteigt diese Anzahl einen Grenzwert, schaltet der Swtich auf Store-and-Forward Betriebsart um und verhindert damit, dass beschädigte Pakete in die anderen Netzsegmente weitergeleitet werden.
  - Geht die Fehlerrate wieder zurück, arbeitet er wieder mit der schnelleren Cut-Through-Betriebsart.

Inhalt

- Netzkoppelelemente: Einführung und Aufgaben
- Prinzipielle Realisierungsmöglichkeit der Netzkopplung
- Repeater (Hubs)
- Bridges (Switches)
- **Router**
- Gateways
- Zusammenfassung

Router


Station 1
Router
Station 2
7
6
5
4
3c
3b1
3a1
21
11
3c
3b1
3b3
3b2
3a1
3a3
3a2
21
23
22
11
13
12
3c
3b2
3a2
22
12
Netz 1
Netz 2
Netz 3

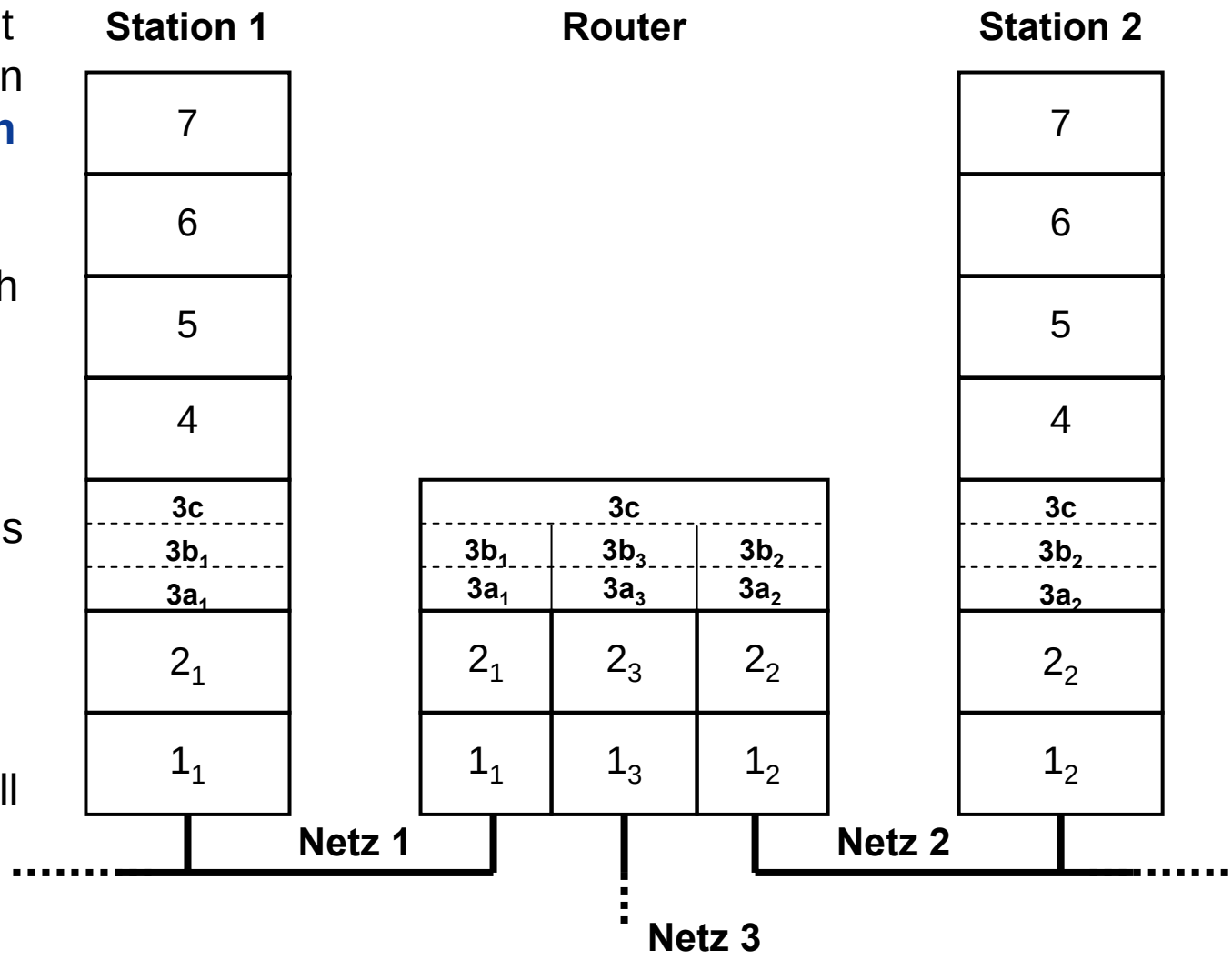
Router (1/4)

- Ein Router koppelt das Netz mit unterschiedlichen Netzadressen auf der Vermittlungsschicht (Sicht 3), dies bedeutet, dass die zu koppelnden Netze in den Schichten 1 und 2 unterschiedlich sein dürfen.
- Router können protokollabhängig sein und werden dann als Single Protocol Router bezeichnet (TCP/IP-Router, DECnet-Router).
- Es gibt aber auch sogenannte Multiple Protocol Router, die mehrere Protokolle verstehen und transportieren können.
- Ein Router ist nicht transparent, d.h. der Absender der Datenpakete muss von der Existenz des Router wissen und diesen direkt adressieren, damit die Datenpakete weitergeleitet werden können.
- Dies macht die Arbeitsweise eines Routers im Vergleich zu einer Bridge wesentlich effizienter, da er nur die Datenpakete aufnehmen muss, die für ihn bestimmt sind.

Router (2/4)
→ Netzkopplung über einen Router (3 zu koppelnde Netze)

- Die Vermittungsschicht kann bei Routern in **drei Teilschichten** aufgeteilt werden, wobei die Teilschicht 3a noch teilnetzspezifisch ist.

- Die Anpassung des Protokolls der Teilschicht 3a an das Protokoll der Teilschicht 3c wird durch das Protokoll der Teilschicht 3b vorgenommen.



Router (3/4)

- Da Router in der Lage sind, sich gegenseitig Informationen zu übermitteln und mit Endgeräten zu kommunizieren, können Router mit anderen Routern oder Rechnersystemen die Routing-Informationen austauschen und aktualisieren.
- Ein Router ist deshalb in der Lage, genau zu wissen, wo eine Adresse im Netz zu finden ist.
- Als Protokoll wird meist ein globales Internetprotokoll (IP) verwendet, das insbesondere die Wegesuche im globalen Netz vornimmt.
- Ein Router arbeitet nicht mit der MAC Source- und Destination-Adresse, sondern direkt mit der IP-, DECnet- usw. Adresse.
- Mit Hilfe dieser Adressen und den dazugehörigen Routing-Protokollen baut ein Router die dazugehörigen Routing-Tabellen auf.
- Bei den meisten Routern geschieht dieser Aufbau automatisch nach dem Einschalten des Routers.
- In Ausnahmefällen, wenn genau feststeht, dass Router sich nicht ändern, können Router mit statischen Routing-Tabellen verwendet werden.

Router (4/4)

- Grundsätzlich unterscheidet man zwei Arten von Routing-Protokollen:

Interior Gateway Protocol (IGP)

- Ein Interior Gateway Protocol (IGP) wird innerhalb eines Netzes eingesetzt.
- Das bekannteste IGP ist das ***Router Information Protocol (RIP)***, welches aufgrund seiner Einschränkungen und Probleme durch das ***Open Shortest Path First (OSPF)*** abgelöst wird.

Exterior Gateway Protocol (EGP)

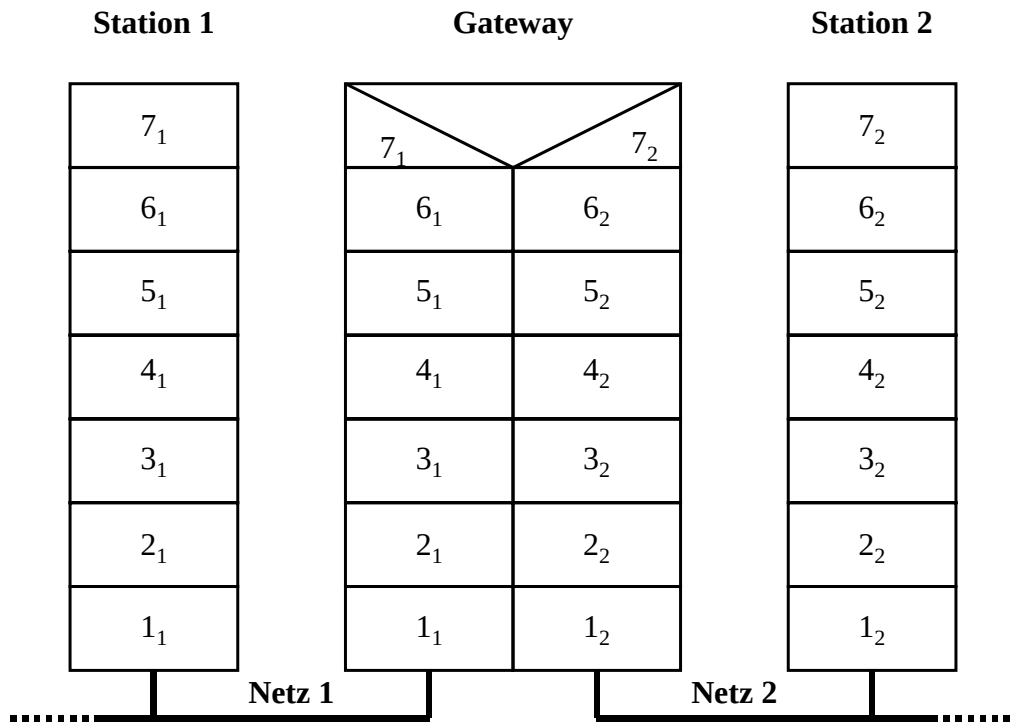
- Zur Kommunikation zwischen Routern in autonomen Systemen (AS) wird ein Exterior Gateway Protocol (EGP) eingesetzt.
- Das seit 1984 bestehende Protokoll EGP wurde mittlerweile weitgehend durch das ***Border Gateway Protocol (BGP)*** abgelöst.

Siehe Netzwerkmanagement Vorlesung: „Routing-Protokolle“

Inhalt

- Netzkoppelelemente: Einführung und Aufgaben
- Prinzipielle Realisierungsmöglichkeit der Netzkopplung
- Repeater (Hubs)
- Bridges (Switches)
- Router
- **Gateways**
- Zusammenfassung

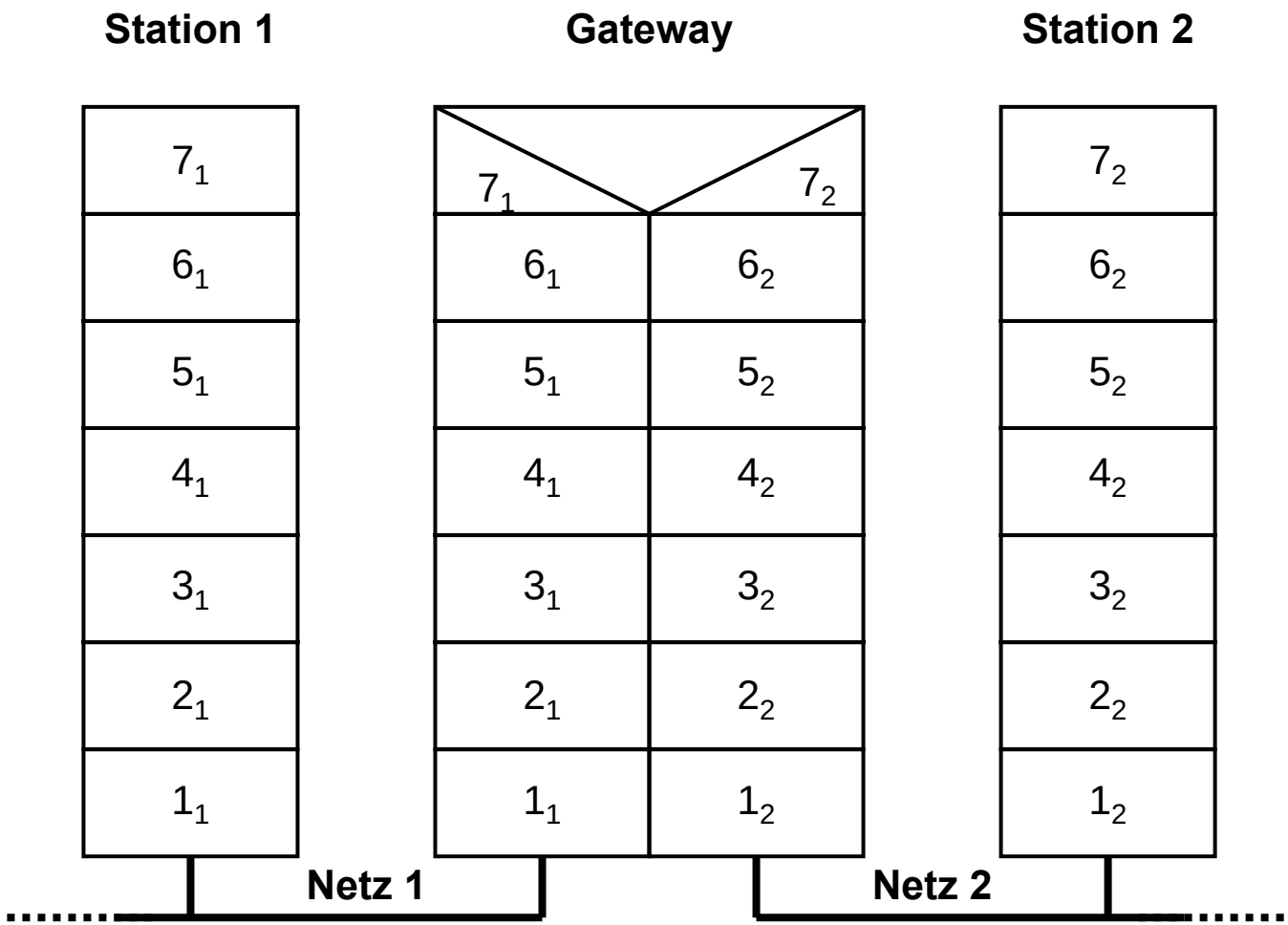
Gateways


Station 1
Gateway
Station 2
7_1
6_1
5_1
4_1
3_1
2_1
1_1
7_1
7_2
6_1
6_2
5_1
5_2
4_1
4_2
3_1
3_2
2_1
2_2
1_1
1_2
7_2
6_2
5_2
4_2
3_2
2_2
1_2
Netz 1
Netz 2

Gateway (1/2)

- Durch ein Gateway werden Netzwerke ab der Transportschicht (Schicht 4) oder höher miteinander gekoppelt.
- In der Regel werden Netzwerke miteinander verbunden, die überhaupt nichts mehr gemeinsam haben.
- Aus diesem Grund erstrecken sich die Aufgaben eines Gateways in den meisten Fällen über alle sieben Ebenen des OSI-Referenzmodells.
- Gateways verbinden also Netze mit unterschiedlichen Protokollfamilien wie z.B. TCP/IP-Netze mit einem DECnet (oder SNA).
- Sie müssen softwaremäßig den Übergang zwischen den verschiedenen Protokollen bewerkstelligen.

Gateway (2/2)
→ Netzkopplung über Gateway



Inhalt

- Netzkoppelelemente: Einführung und Aufgaben
- Prinzipielle Realisierungsmöglichkeit der Netzkopplung
- Repeater (Hubs)
- Bridges (Switches)
- Router
- Gateways
- **Zusammenfassung**

Zusammenfassung
→ Netzkoppelelemente

- Um die **Verbindung zwischen zwei Netzen** herzustellen, die aufgrund technischer oder geographischer Gegebenheiten nicht direkt gekoppelt werden können, werden **Netzkoppelelemente** verwendet.

Durch Netzkoppelelemente ist es möglich

- die physikalische Begrenzung der Ausdehnung eines lokalen Netzes zu umgehen **(Repeater/Hubs)**
- lokales Datenaufkommen durch Bildung von logischen Teilnetzen vom restlichen Netzwerk zu entkoppeln **(Bridges/Switches)**
- Teilnetze mittels Netzkoppeleinheiten zu einem Netz für den bereichsübergreifenden Verkehr zu koppeln **(Router)**
- Netze mit unterschiedlichen Protokollarchitekturen miteinander zu koppeln **(Gateways)**

Internetworking
→ Netzkoppelelemente

Vielen Dank für Ihre Aufmerksamkeit

Fragen ?

norbert.pohlmann@informatik.fh-gelsenkirchen.de

Fachhochschule Gelsenkirchen