# Einführung zu

# Bridging, Routing, Spanning Trees, Cisco IOS

Diese Folien orientieren sich an den Lecture-Slides von
Panwar, Mao, Ryoo und Li
(http://catt.poly.edu/CATT/TCPIPEssentials.html)

Jörn Stuphorn
stuphorn@rvs.uni-bielefeld.de

# Stand der Veranstaltung



| | |
|---|---|
| 13. April 2005 | Unix-Umgebung |
| 20. April 2005 | Unix-Umgebung |
| 27. April 2005 | Unix-Umgebung |
| 4. Mai 2005 | ARP, ICMP, ping |
| 11. Mai 2005 | IP-Adressen & Subnetzmasken |
| ***18. Mai 2005*** | ***Einführung in Bridging, Routing, ...*** |
| *25. Mai 2005* | *IOS, Spanning-Tree* |
| *1. Juni 2005* | *Statisches Routing* |
| *8. Juni 2005* | *UDP-, MTU- und IP-Fragmentierung* |
| *15. Juni 2005* | *TCP-Verbindungen und -Datenfluss* |
| *22. Juni 2005* | *DHCP und NTP* |
| *29. Juni 2005* | *NAT und Firewalls* |
| *6. Juli 2005* | *Verschlüsselung, Vertraulichkeit, Authentisierung* |
| *13. Juli 2005* | *Sichere Anwendungen* |
| *20. Juli 2005* | *Wireless LAN* |

# Inhalt



**Bisher:**

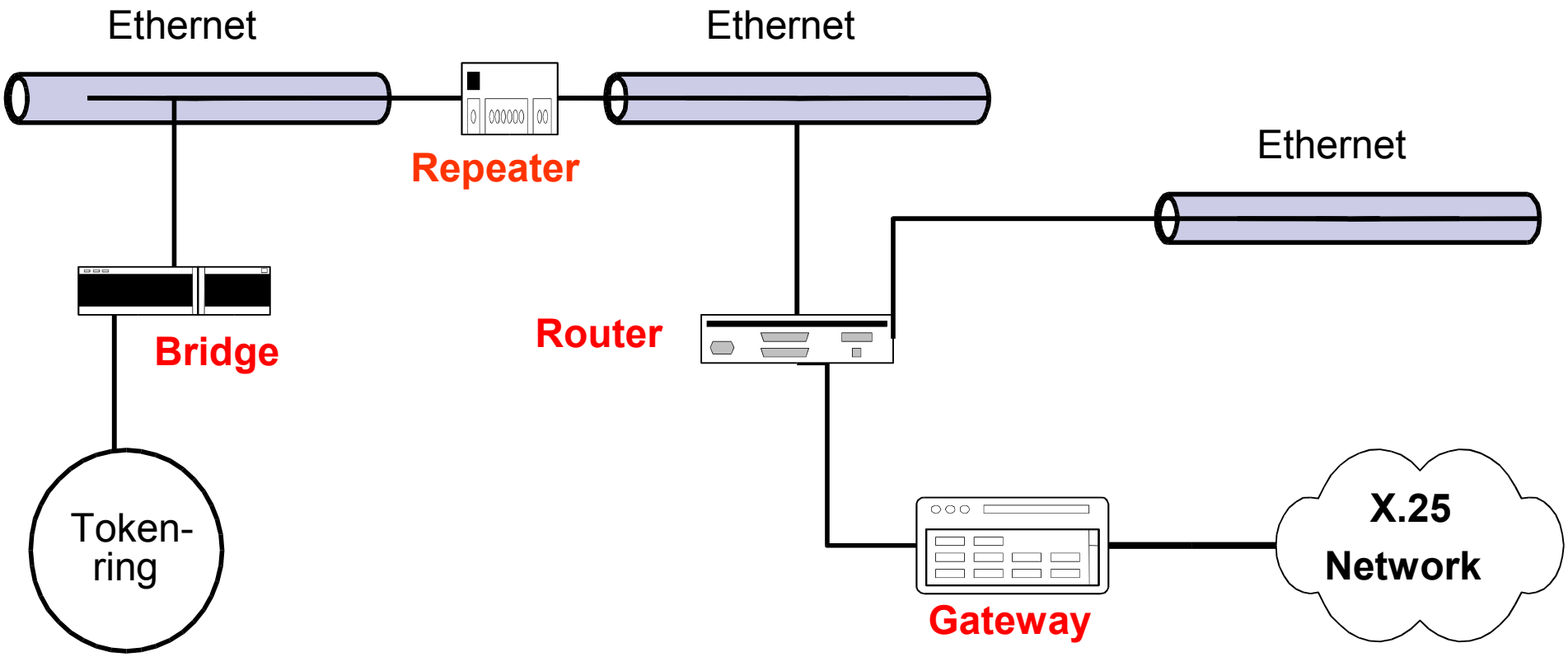
- Betriebssystem
- Netzwerk Interface am Compuer

**Jetzt:**

- Geräte zur Verbindung von Netzwerken
  - gleichen Typs
  - unterschiedlichen Typs
- Bridges

# Verbindung von Netzwerken

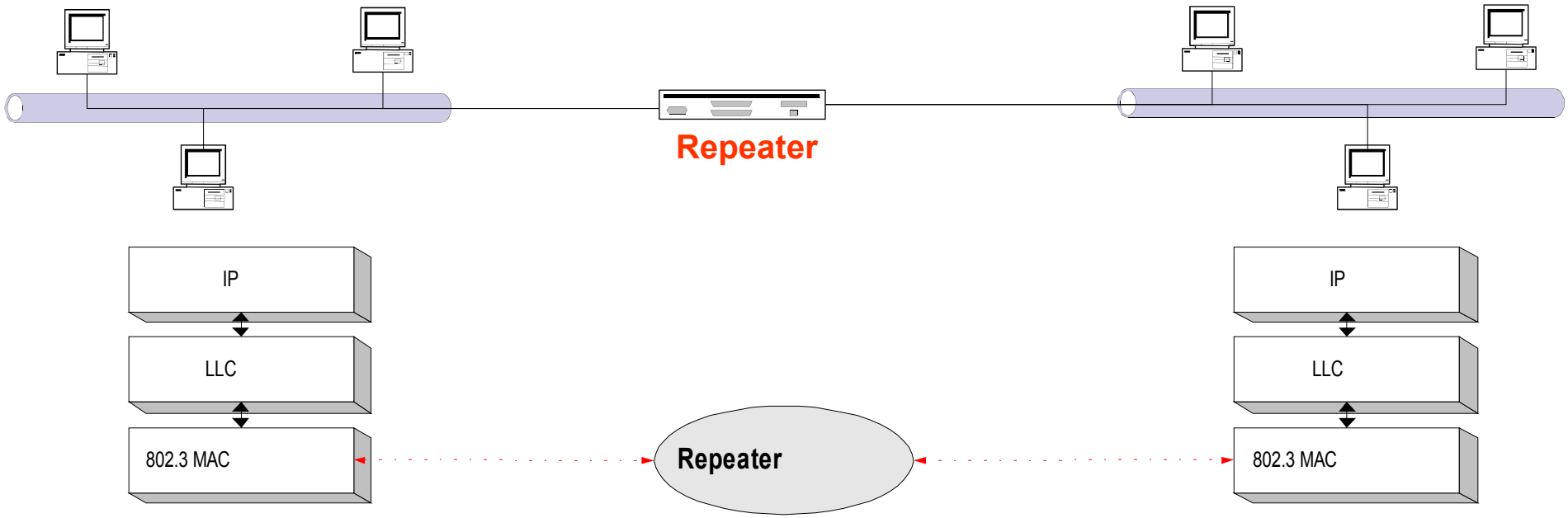





- Repeater
- Bridge
- Router
- Gateway

# Repeater

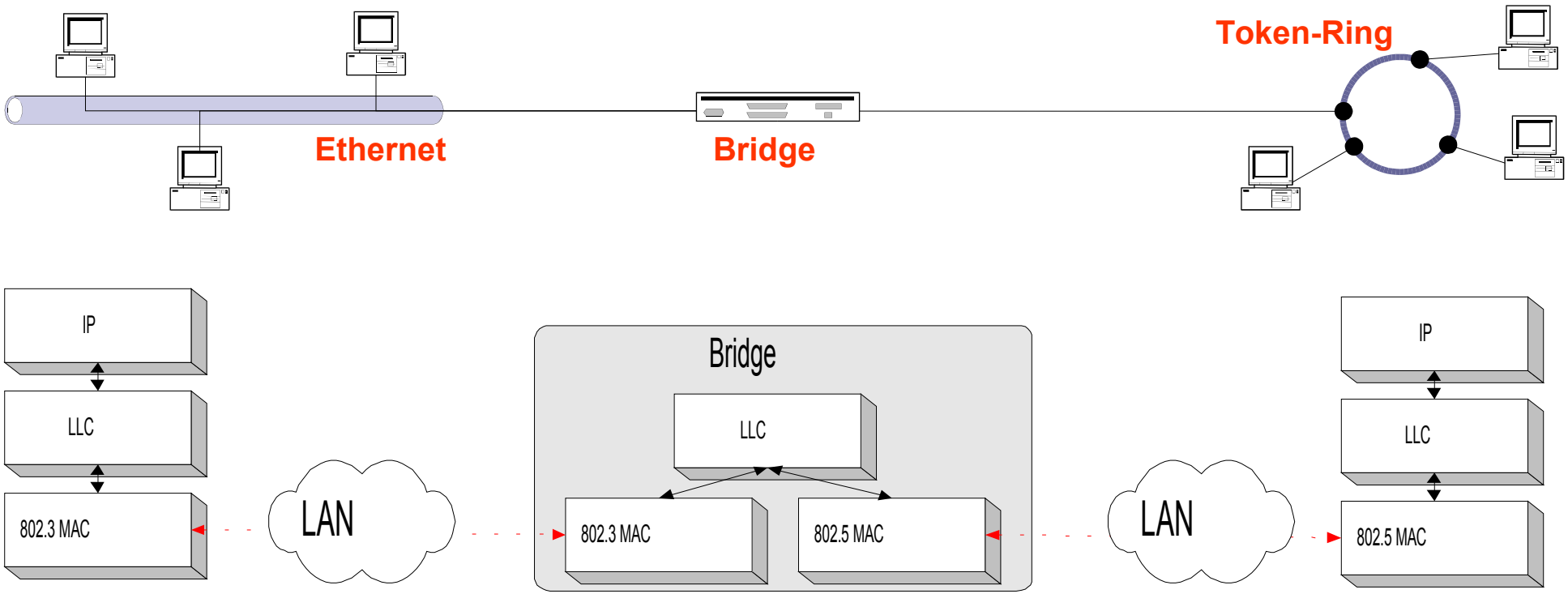





- verbinden mehrere Ethernet-Segmente miteinander
- nur Verlängerung des Netzstranges
- Arbeitsweise:
  - empfängt Signale
  - verstärkt diese
  - sendet verstärkte Signale auf nächsten Abschnitt.
- Auch Kollisionen werden verstärkt.

# Bridge

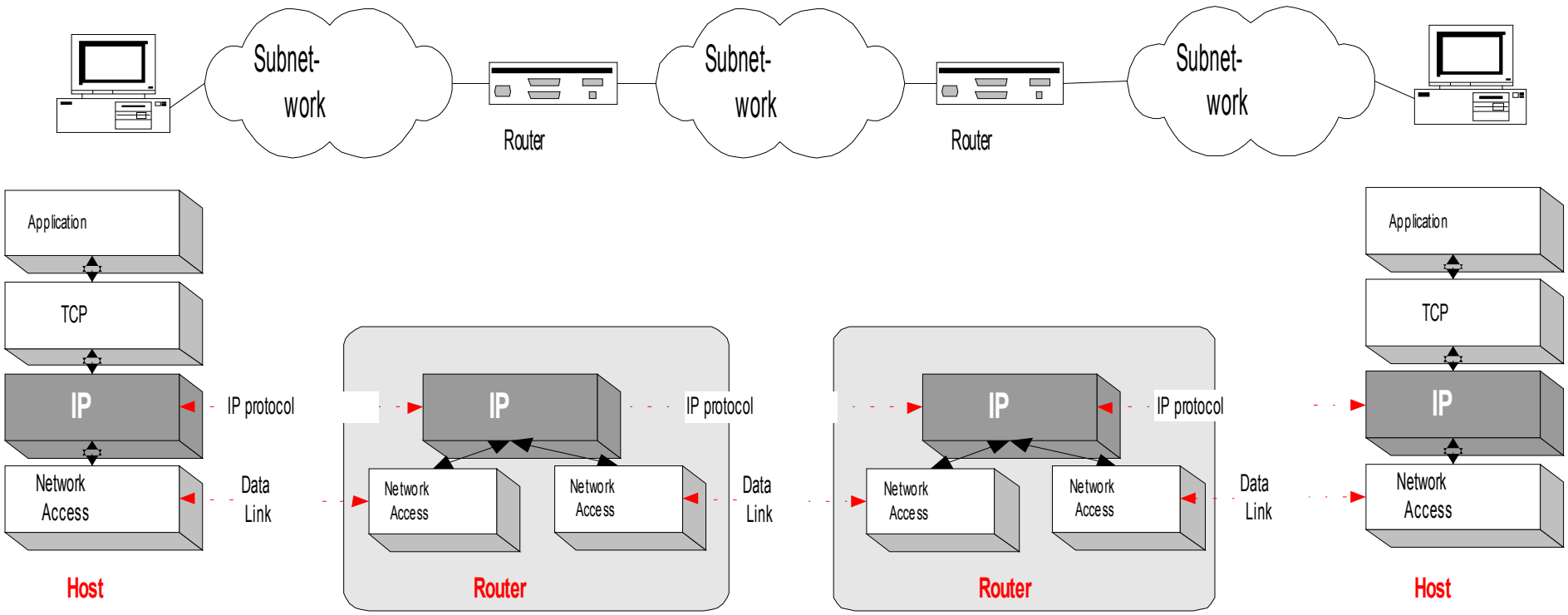





- verbinden mehrere LANs, auch unterschiedlichen Typs
- Bridge operiert auf der Ebene des DataLink Layers
- Wenn kein eindeutiger Pfad zu den Zielen besteht wird Routing erforderlich.

# Router

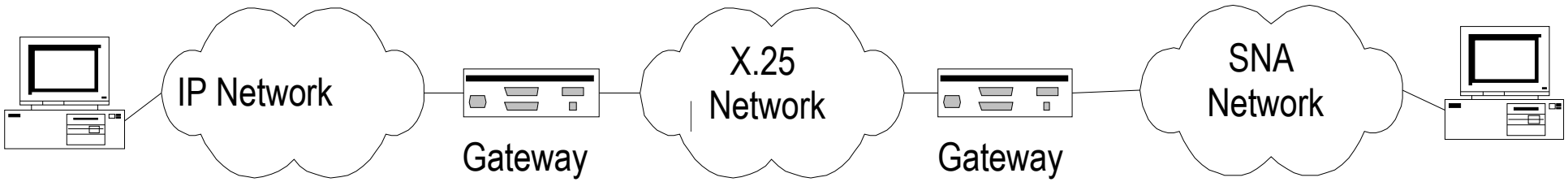





- Router operieren auf der Ebene des Network Layers
- Verbinden unterschiediche Subnetworks untereinander

# Gateway






SNA: System Network Architecture

- Gateway wird in unterschiedlichen Zusammenhängen unterschiedliche Bedeutungen benutzt:

- „Gateway“ wird als allgemeine Bezeichnung für Router (Level 3) benutzt
- „Gateway“ wird auch ein Gerät genannt, das
  - Verschiedene Level 3 Netzwerke untereinander verbindet und
  - Protokollumwandlung leistet („Multi-protocol router“)

# Bridges

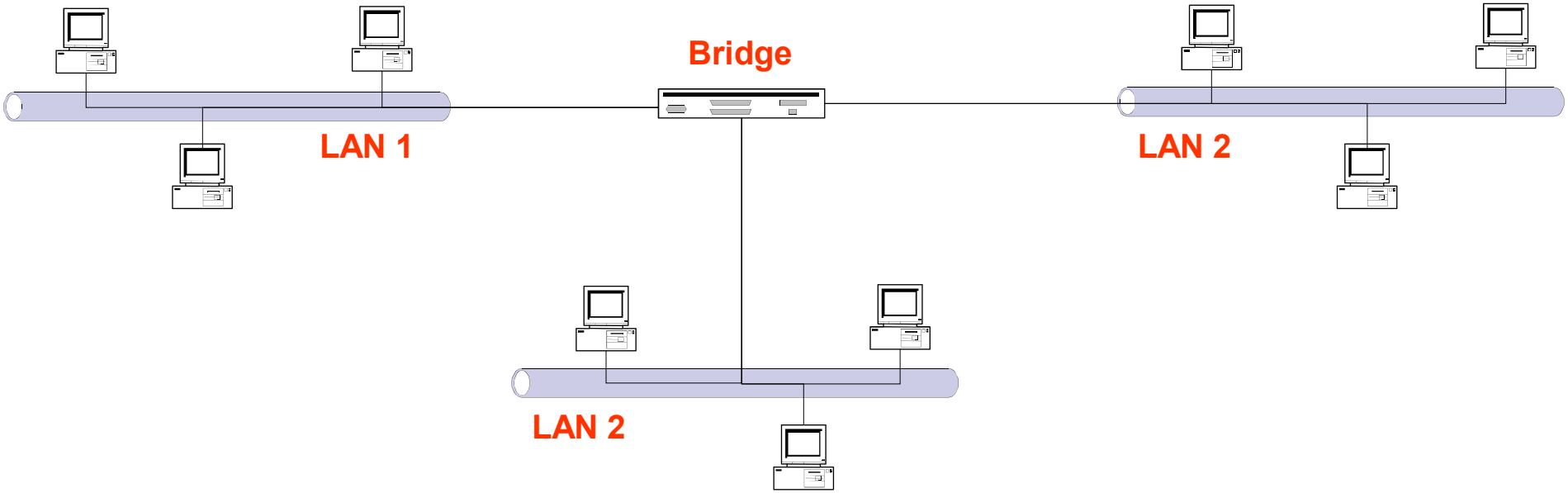


- Was sind Bridges?
- Wofür werden Bridges benötigt?
- Wie funktioniert eine Bridge?
- Adressauflösung einer Bridge

# Was sind Bridges?



- Verbinden mehrere LANs
- Leitet Frames an ein anderes LAN weiter, wenn der Empfänger nicht zum lokalen LAN gehört
- Eine einzelne Bridge kann mehr als zwei LANs miteinander verbinden.



# Wofür Bridges?



- Bridges ermöglichen den Aufbau von vielen kleinen LANs anstatt einem großen LAN

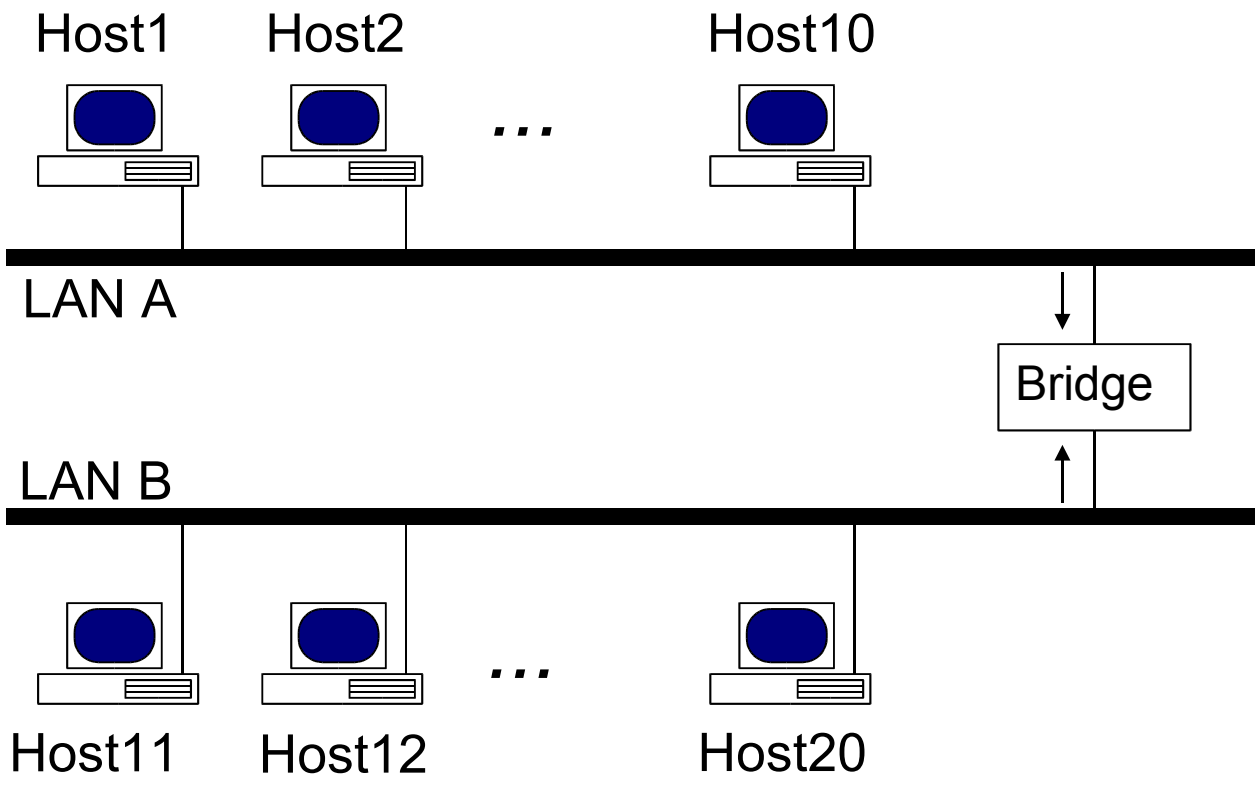
  dadurch erfolgt Verbesserung von
  - Ausfallsicherheit
  - Durchsatz
  - Sicherheit
  - geographische Strukturierung

- *Transparente Bridges* (transparent bridges) werden von den Hosts nicht bemerkt
  - Ein Frame wird einfach von einem Netzwerk in das nächste übertragen/kopiert
  - Header- und Daten-Bereich werden dabei nicht verändert

# Wie funktioniert eine Bridge?



- Beispiel:
  - Frames von *Host1* bis *Host10* werden auf *LAN A* angenommen
  - Frames von *Host11* bis *Host20* werden auf *LAN B* angenommen



# Filtering Database

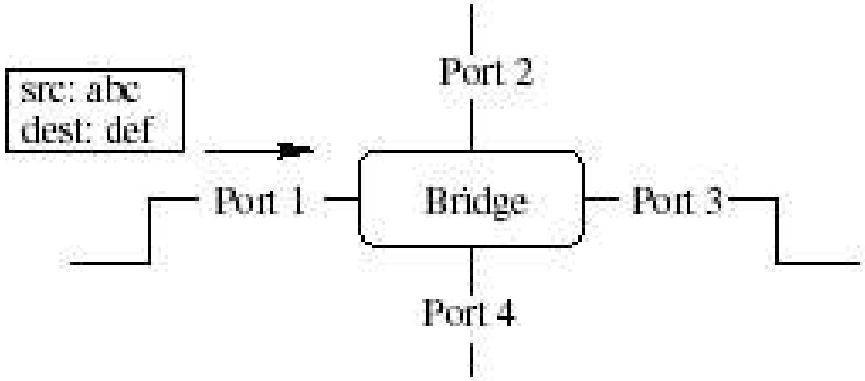


- Die MAC Adressen eines Host werden in einer Filter-Datenbank (filtering Database) in der Brigde gespeichert.
- Elemente der Einträge:
  - Die MAC Adresse des Ziels
  - Der Port der Brigde, an den Pakete an diese MAC Adresse weitergeleitet werden sollen
  - Das Alter des Eintrags
- Die Filter-Datenbank könnte auch statisch gesetzt werden
- In einer IEEE 802.1d bridge wird die Datenbank automatisch mittels eines Adress-Lernprozesses gefüllt

# Adress-Lern-Prozess



- Empfängt die Bridge einen Frame, werden folgende Informationen in die Filter-Datenbank übernommen
  - MAC Adresse der Quelle und
  - der Port auf dem die Nachricht empfangen wurde
- Standard-Alter eines neuen Eintrags ist 300 sec.




The original filtering database:

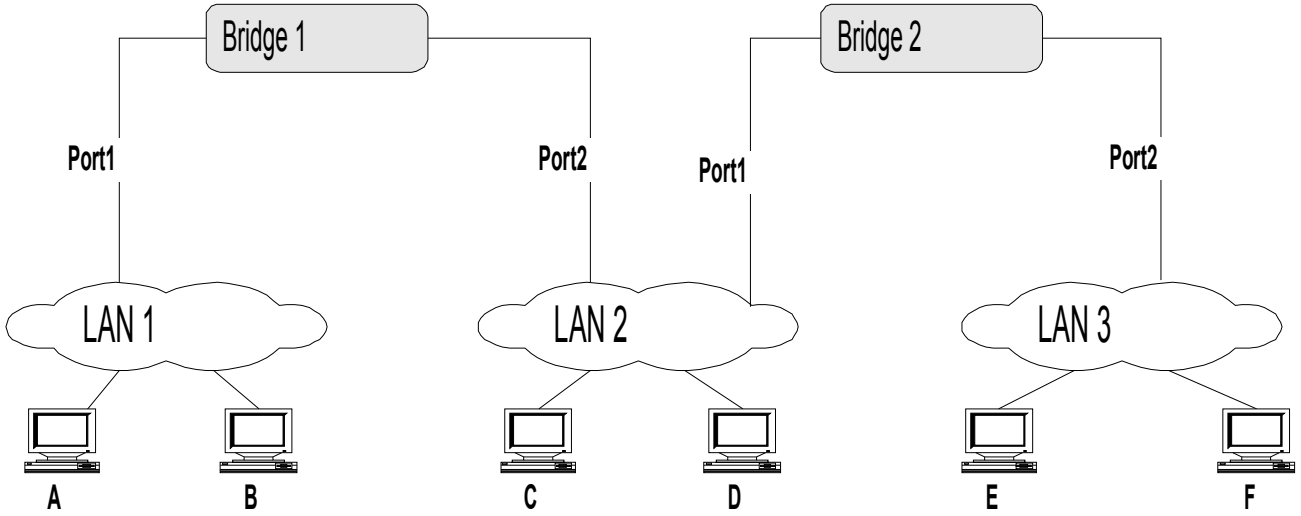
| Dest. | Port | Age |
|---|---|---|
| | | |

The new filtering database:

| Dest. | Port | Age |
|---|---|---|
| abc | 1 | 300s |

# „Adress-Lerning“ - Beispiel






- Folgende Pakete werden übertragen:
  - <SRC=A, Dest=F>
  - <SRC=C, Dest=A>
  - <SRC=E, Dest=C>

- Was haben die jeweiligen Bridges gelernt?

# Operationen der Bridge



- Entscheidungen über die Weiterleitung (***Forwarding***) von Frames werden in der Bridge mittels Nachschlags in der Filter-Datenbank gemacht
- Wenn ein Eintrag gefunden wird, wird der Frame an das Netzsegment weitergeleitet, dass im Eintrag angegeben ist
- Wird kein Eintrag in der Filter-Datenbank gefunden, wird ***Flooding*** benutzt
  - Der Frame wird an alle aktiven Ports der Bridge weitergeleitet.
  - Ausnahme: Der Frame wird nicht an den Port weitergeleitet, über den er von der Bridge empfangen wurde.

# Forwarding-Bedingungen

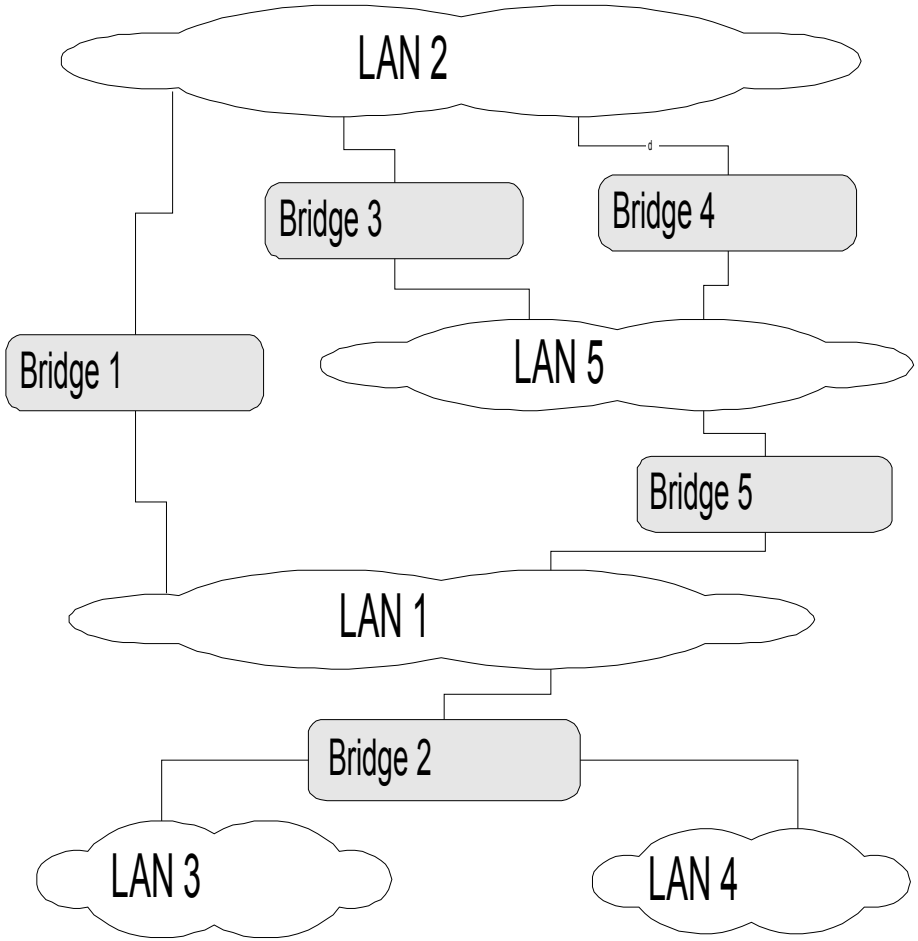


- Ein Rahmen wird nur dann weitergeleitet, wenn ...
  - der *empfangende Port (receiving port)* in einem „Forwarding state“ ist, d.h. es eingestellt ist, dass Frames von dem verbundenen Netzsegment an andere Segmente weitergeleitet werden sollen,
  - der *übertragende Port (transmitting port)* in einem „Forwarding state“ ist, es also eingestellt ist, dass dieses Netzsegment Frames weiterleiten wird,
  - entweder ein entsprechender Eintrag in der Filter-Datenbank gemacht ist, oder das Ziel nicht in der Filter-Datenbank vorhanden ist (*flooding),*
  - der transmitting Port nicht gleichzeitig der receiving Port ist
  - die maximale Größe der service data unit des transmitting Ports nicht erschöpft wird.

# Bedarf von Routing



- wenn einige LANs nur durch mehrfache *hops* erreicht werden können
- Wenn der Pfad zwischen zwei LANs nicht eindeutig ist.



# Routing



- Welche Verfahren exisiteren?
- Welche Gefahr stellen Loops dar?

# Routing mit Bridges

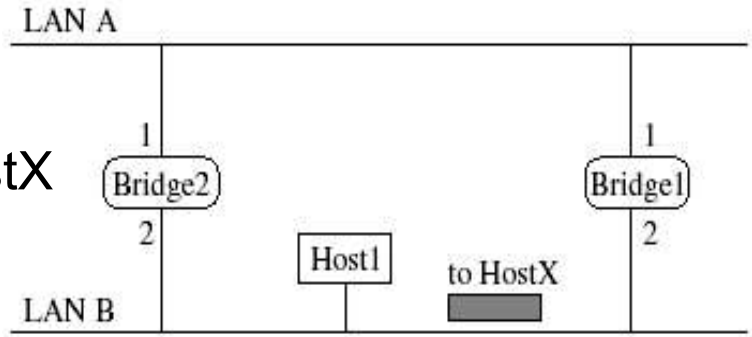


- Für Routing existieren drei wesentliche Ansätze:
  - Fixed Routing
  - Source Routing
  - Spanning Tree Routing (transparente Bridges)
- Fixed Routing wird in vielen kommerziellen Produkten benutzt
- Source- und Spanning Tree Routing sind von der IEEE 802 Arbeitsgruppe standardisiert worden
  - Source Routing vom Token Ring Komitee (IEEE 802.5)
  - Spanning Tree vom IEEE 802.1 Komitee (Internetworking)
- Nur Spanning Tree wird eingehender besprochen

# Gefahr von Loops



- Das bisher besprochene Address-Learning und Forwarding Schema kann ernsthafte Probleme auslösen, wenn Schleifen (*Loops*) existieren
- Annahme
  - Host1 sendet an HostX
  - B1 und B2 haben keinen Eintrag zu HostX
  - Bridge1 und Bridge2 empfangen beide den Frame auf LAN B und lernen, dass Host1 zu LAN B gehört




  - B1 und B2 nehmen beide Host1 in ihre Filter-DB auf
  - B1 und B2 leiten den Frame an LAN A weiter
  - B1 und B2 empfangen den Frame des jeweils anderen und lernen, dass Host1 zu LAN A gehört.
  - B1 und B2 ändern ihre Filter-DB entsprechend
  - B1 und B2 leiten den Frame an LAN A weiter
  - ... ad infinitum ...
- Ergebnis: Broadcast Sturm (broadcast storm)

# Spanning Trees



- Lösung des Loop Problems:
  Loops entfernen

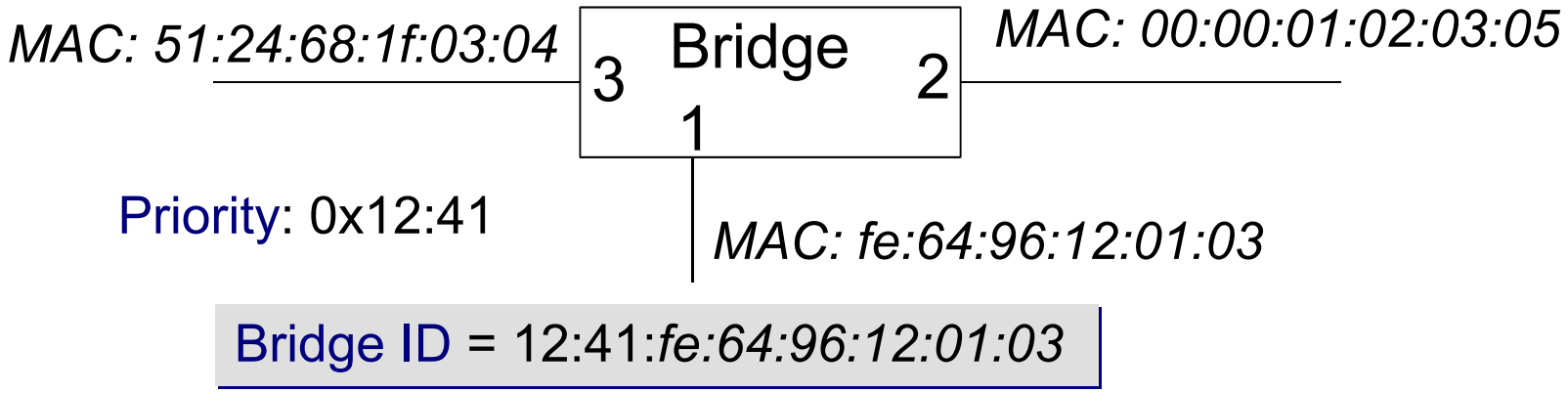
- IEEE 802.1 hat einen Algorithmus entwickelt, der einen Spanning Tree (aufspannenden Baum) in einem dynamischen Umfeld wartet.

- Methode:
  - Bridges tauschen Nachrichten aus *Configuration Bridge Protocol Data Unit (Configuration BPDUs)* um
  - Bridges konfigurieren und
  - Baum zu erzeugen

# Bridge ID



- Um Spanning Tree aufbauen zu können, müssen die Bridges eindeutig identifiziert werden.
  - Brigde ID bildet sich aus
    *priority-level* + *MAC Adresse*
  - Priority-Level = 2 Bytes,
    MAC Adresse = 6 Bytes
  - Eine Bridge hat mehrere MAC Adressen (für jeden Port eine) aber nur ***eine*** Bridge ID.
    Die Bridge ID benutzt die MAC Adresse des niedrigst nummerierten Bridge Ports (port 1)

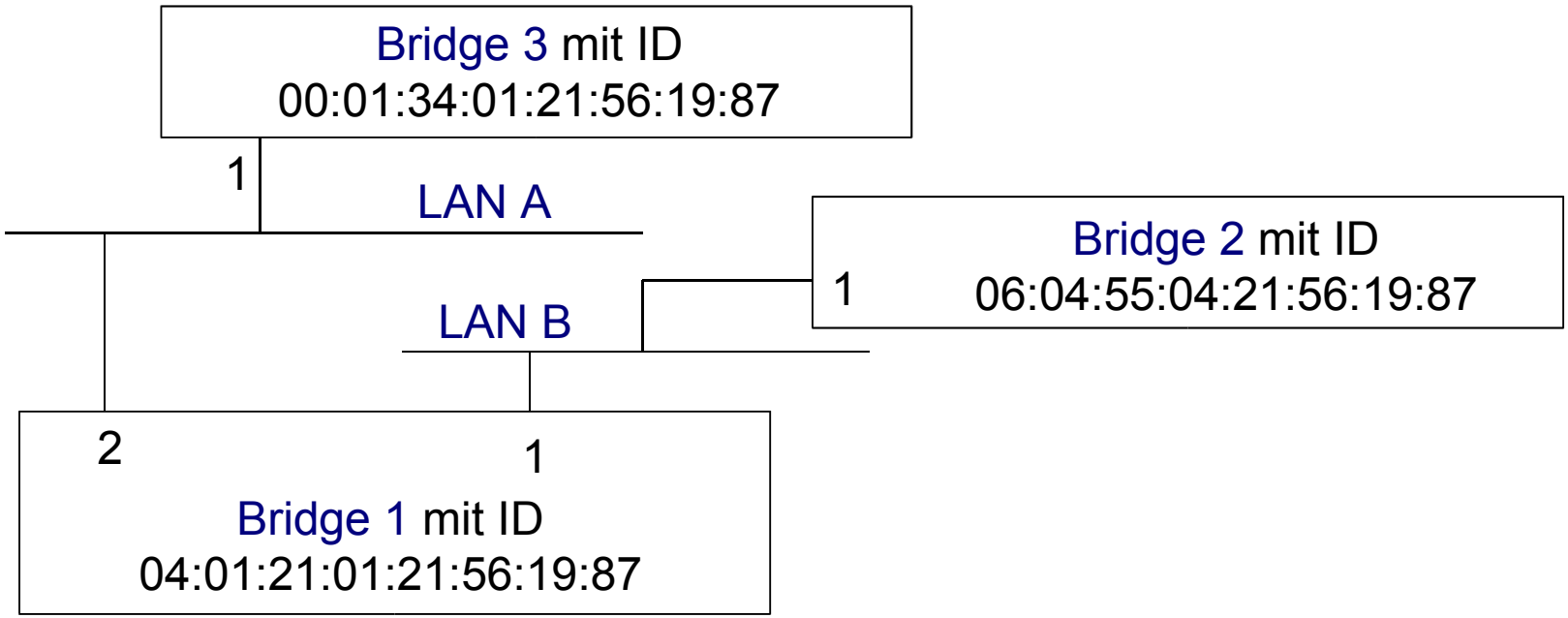


# Root Bridge eines Netzwerks



- Baum braucht Wurzel.
- Wurzel durch Root Brigde festgelegt.

- Root Bridge ist immer die Bridge, mit der niedrigsten Bridge ID




Root bridge ist Bridge 3, weil es die niedrigste ID besitzt

# Informationen jeder Bridge



- Root Port
  - der Port, über den die Root Bridge mit den wenigsten hops erreicht werden kann
- Root Path Cost
  - die Kosten des Pfades zur Root Bridge mit den niedrigsten Kosten

- Beispiel (vorhergehendes Schema)
  - Bridge 1:
  - Root Port: port 2
    - Root Bridge (Bridge 3) ist über Port 2 verbunden
  - Root Path Cost: 1
    - Bridge 3 ist nur einen Hop entfernt

- Wir gehen davon aus, dass die Kosten gleich der Anzahl an Hops ist. Die Kosten können aber auch anders festgelegt werden.

# Informationen jedes LANs



- vorgesehene Bridge (designated bridge)
- vorgesehener Port (designated port)
  - Die eine Bridge im LAN, die den minimal cost Pfad zur Root Bridge stellt und der Port auf diesem Pfad
  - Wenn zwei Bridges identische Kosten anbieten, wird die mit der niedrigsten ID (höchste Priorität) gewählt
  - Wenn die min-cost Bridge zwei oder mehr Ports zum LAN hat, wähle den Port mit der niedrigsten ID

- Beispiel (vorhergehendes Schema)
  - Für LAN A:
    - designated Bridge: Bridge 3 (Root Bridge)
    - designated Port: Port 1
  - Für LAN B:
    - designated Bridge: Bridge 1 (näher an Root Bridge als Bridge 2)
    - designated Port: Port 2

# Bemerkungen



- Ein LAN ist das Gebilde, das eine designierte Bridge und einen designierten Port besitzt
- Es existiert keine zentrale Kontrollinstanz in einem LAN (das LAN ist eine Gruppe von Hosts)
- Nur die Bridge kann entscheiden, ob Sie designierte Bridge und was der designierte Port für ein LAN ist.

- Beispiel zum vorhergehenden Schema:
  - Bridge 1 muss feststellen, ob sie die designierte Bridge von LAN A (über Port 2 verbunden) und
  - ob sie die designierte Bridge von LAN B (über Port 1 verbunden) ist.

# Spanning Tree Algorithmus



- Schritt 1: Identifiziere die Root Bridge des Netzwerks
- Schritt 2: Identifiziere die Root Ports aller Bridges des Netzwerks
- Schritt 3: Identifiziere für alle Brigdes, welche Ports designierte Ports für die angeschlossenen LANs sind.

- Der Spanning Tree baut sich aus allen Root Ports und allen designated Ports der Bridges auf.
- Diese Ports werden alle in den *forwarding state* versetzt
- Alle übrigen Ports werden in den *blocked state* versetzt

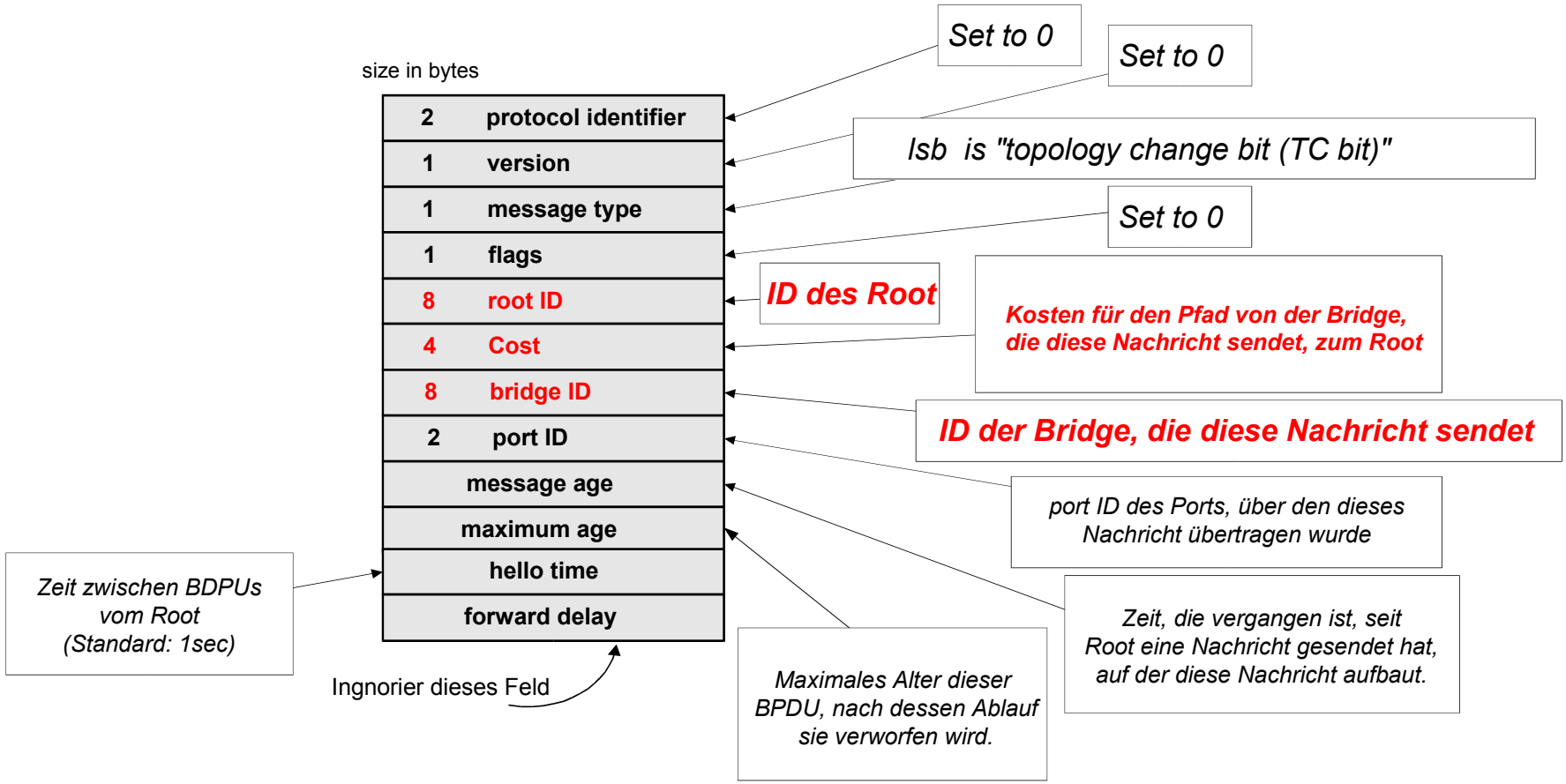
# Ermitteln des Spanning Trees



- Die Bridges ermitteln den Spanning Tree unter Verwendung eines verteilten (distributed) Ansatzes
- Dafür werden BPDUs (*bridge protocol data unit)* benutzt
  - Wahl einer Bridge als Root Bridge
  - Jede Bridge legt fest:
    - einen Root Port
    - die verbundenen Root Pfad Kosten
  - Jede Bridge legt fest, ob sie die designated Bridge für die mit ihr verbundenen LANs ist.
  - Wähle die Ports aus, die im Spanning Tree enthalten sein sollen.
    - Root Ports und designierte Ports
  - Es dauert eine Weile, bis das Netzwerk konvergiert ist.

# Configuration BDPUs

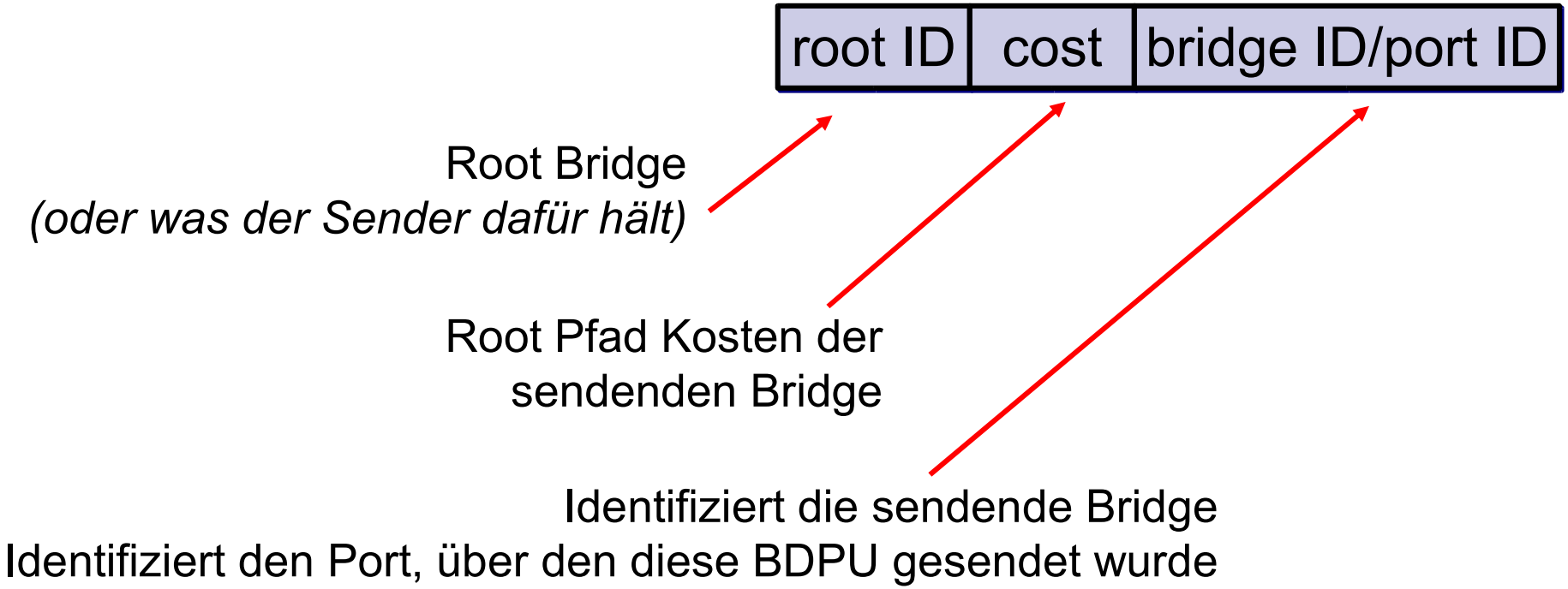




# BDPUs in Kurzfassung



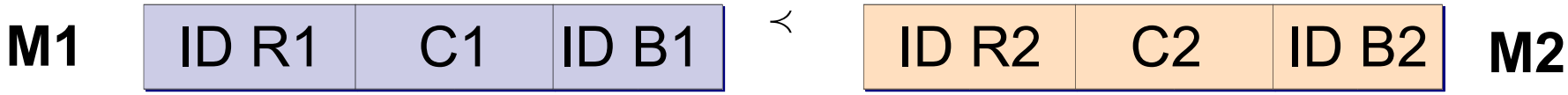
- Jede Brigde sendet BDPUs, die die folgenden Informationen enthalten:



# Ordnen von Nachrichten



- Über die Ordnungsrelation "$\prec$" können BPDUs geordnet werden




- Ordnungskriterien:
  - Wenn (R1 < R2)
    M1 $\prec$ M2
  - Sonst, wenn ((R1 == R2) $\wedge$ (C1 < C2))
    M1 $\prec$ M2
  - Sonst, wenn ((R1 == R2) $\wedge$ (C1 == C2) $\wedge$ (B1 < B2))
    M1 $\prec$ M2

# Identifikation der Root Bridge



- Initialzustand: Jede Bridge nimmt sich selber als Root Bridge an
- Jede Bridge sendet BDPUs in folgender Form über das LAN


- Jede Bridge vergleicht die BPDUs, die auf ihren Ports ankommen gegen die BDPU, die sie selber aussendet
- Als Root Bridge wird die root ID genommen, die bisher empfangen wurde.
- Wird eine kleinere ID empfangen, wird die Root Information aktualisiert

# Root Pfad Kosten, Root Port



- Zum aktuellen Zeitpunkt:
  - Bridge B glaubt zu wissen, dass z.B. Bridge R Root Bridge ist
  - Bridge B bestimmt die Root Pfad Kosten wie folgt:
    - Wenn B=R: Kosten = 0
    - Sonst: Kosten = {niedrigste Kosten in einer BDPU empfangen} + 1
  - Root Port von Bridge B ist der Port, über den die Root Bridge mit den geringsten Kosten erreicht werden kann (In Bezug auf die Relation "$\prec$").
  - Sind R und Kosten bekannt, kann B seine BDPU generieren (die aber nicht zwangsläufig gesendet werden muss)

| R | Cost | B |
|---|---|---|

# Designated Bridge & Port

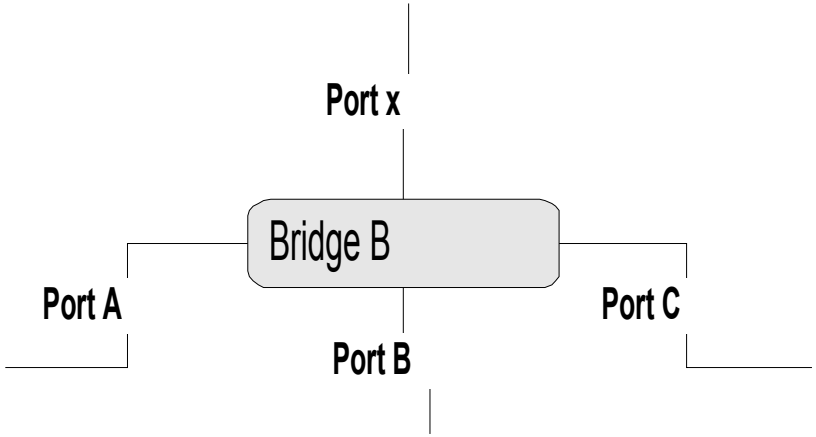


- B hat seine BDPU generiert

| R | Cost | B |
|---|---|---|

- B sendet diese BDPU an einen seiner Ports, z.B. Port x, nur, wenn seine BDPU kleiner (“$\prec$“) als jede über Port x empfangene BDPU ist.

- In diesem Fall nimmt B auch an, dass es die designierte Bridge für das an Port x angeschlossene LAN ist.



# Auswahl der Ports für Tree

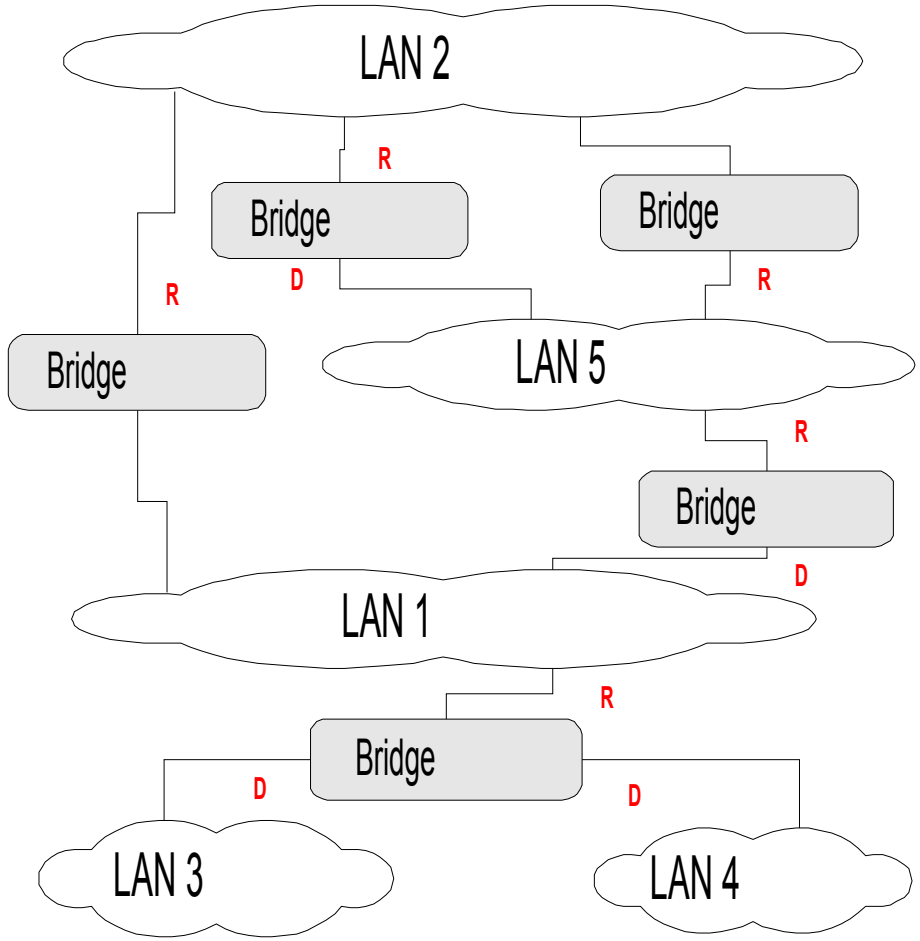


- Bridge B hat die Root Bridge des Netzwerks berechnet, den Root Port, die Root Pfad Kosten und ob sie die designierte Bridge für die angeschlossenen LANs ist.
- B kann nun entscheiden, welche Ports im Spanning Tree sind:
  - B's Root Port ist Teil des Spanning Trees
  - Alle Ports, für die B die designierte Bridge ist, sind Teil des Spanning Tree
- B's Ports, die zum Spanning Tree gehören, werden Pakete weiterleiten *(forwarding state)*
- B's Ports die nicht zum Spanning Tree gehören, werden Pakete blockiert *(blocking state)*

# Aufbau des Spanning Tree



- Die Abbildung rechts stelle das Netzwerk dar.
- Angenommen, dass die Bridges designated Ports (D) und Root Ports (R) wie angegeben bestimmt haben.
- Wie sieht der Spanning Tree des Netzwerks aus?



# Anpassen an Veränderungen

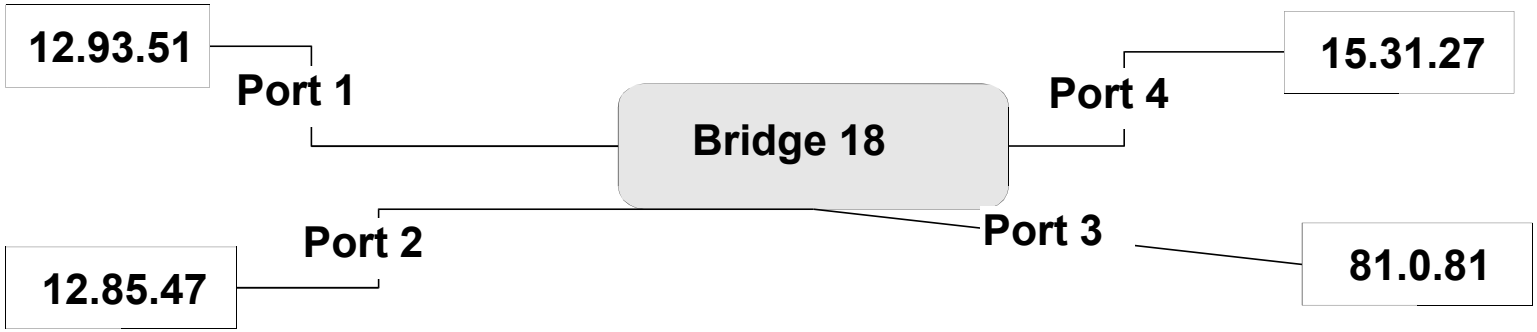


- Bridges tauschen kontinuierlich BDPUs aus (unter Befolgung der besprochenen Regeln)
- Die Bridges können sich dadurch an veränderte Gegebenheiten in der Topologie anpassen.
- Immer, wenn eine BDPU auf einem Port, z.B. Port x, empfangen wird, entscheidet die Bridge, z.B. B,
  - Kann B die designierte Bridge für das an Port x angeschlossene LAN werden?
  - Kann Port x der Root Port werden?

# Beispiel 1



- Eine Bridge hat die ID 18
- Die niedrigsten Nachrichten, die über ihre 4 Ports empfangen wurden, sind in der Grafik angegeben.

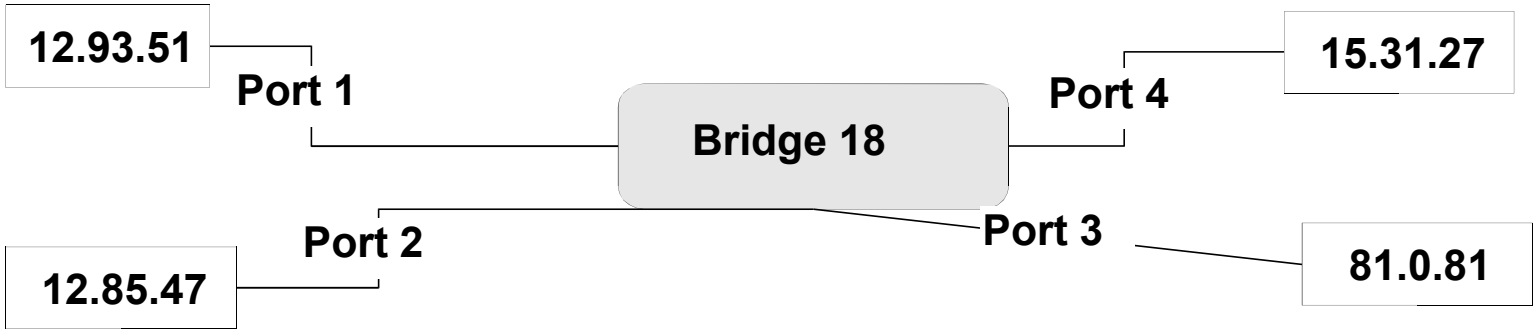



- Was ist die Root Bridge?
- Wie hoch sind die Root Pfad Kosten für Bridge 18?
- Welches ist der Root Port?
- Wie sieht BPDU von Bridge 18 aus?
- Für welche LANs ist Bridge 18 designated Bridge?

# Beispiel 1



- Eine Bridge hat die ID 18
- Die niedrigsten Nachrichten, die über ihre 4 Ports empfangen wurden, sind in der Grafik angegeben.

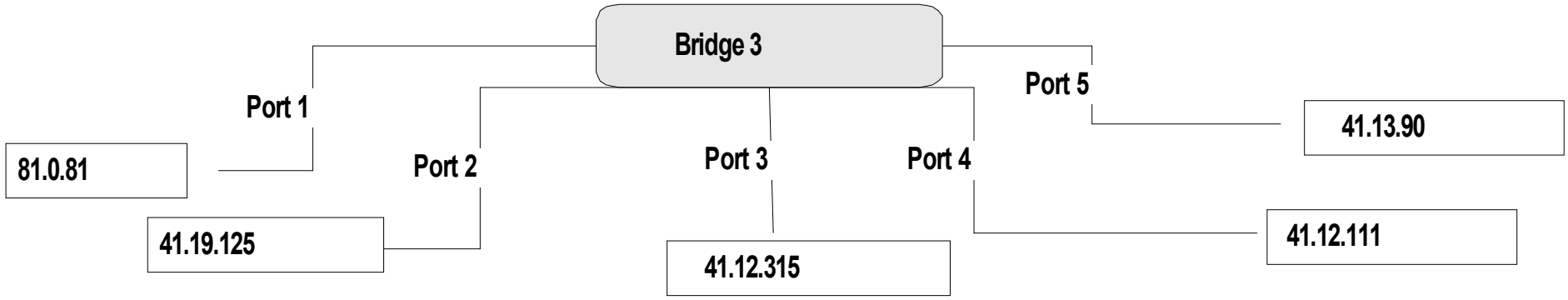



- Was ist die Root Bridge? 12
- Wie hoch sind die Root Pfad Kosten für Bridge 18? 86
- Welches ist der Root Port? 2
- Wie sieht BPDU von Bridge 18 aus? 12.86.18
- Für welche LANs ist Bridge 18 designated Bridge? 1,3,4

# Beispiel 2



- Eine Bridge hat die ID 18
- Die niedrigsten Nachrichten, die über ihre 4 Ports empfangen wurden, sind in der Grafik angegeben.

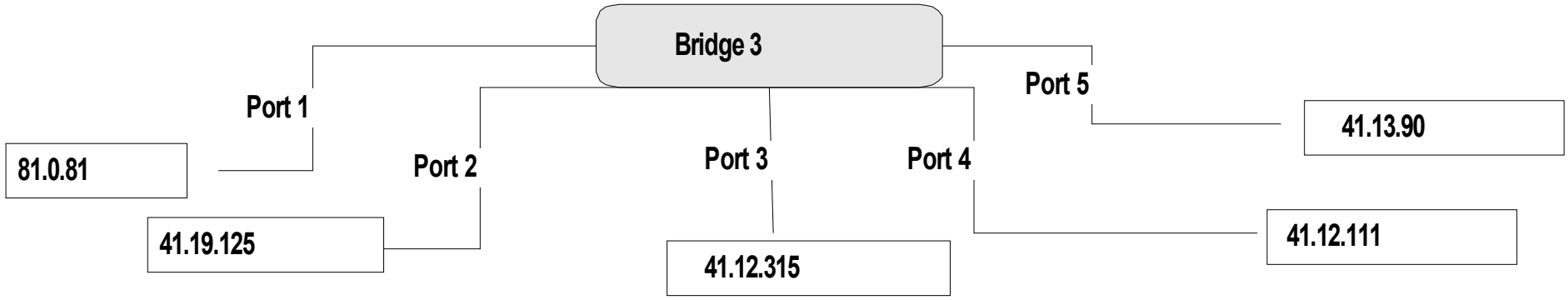



- Was ist die Root Bridge?
- Wie hoch sind die Root Pfad Kosten für Bridge 3?
- Welches ist der Root Port?
- Wie sieht BPDU von Bridge 3 aus?
- Für welche LANs ist Bridge 3 designated Bridge?

# Beispiel 2



- Eine Bridge hat die ID 18
- Die niedrigsten Nachrichten, die über ihre 4 Ports empfangen wurden, sind in der Grafik angegeben.

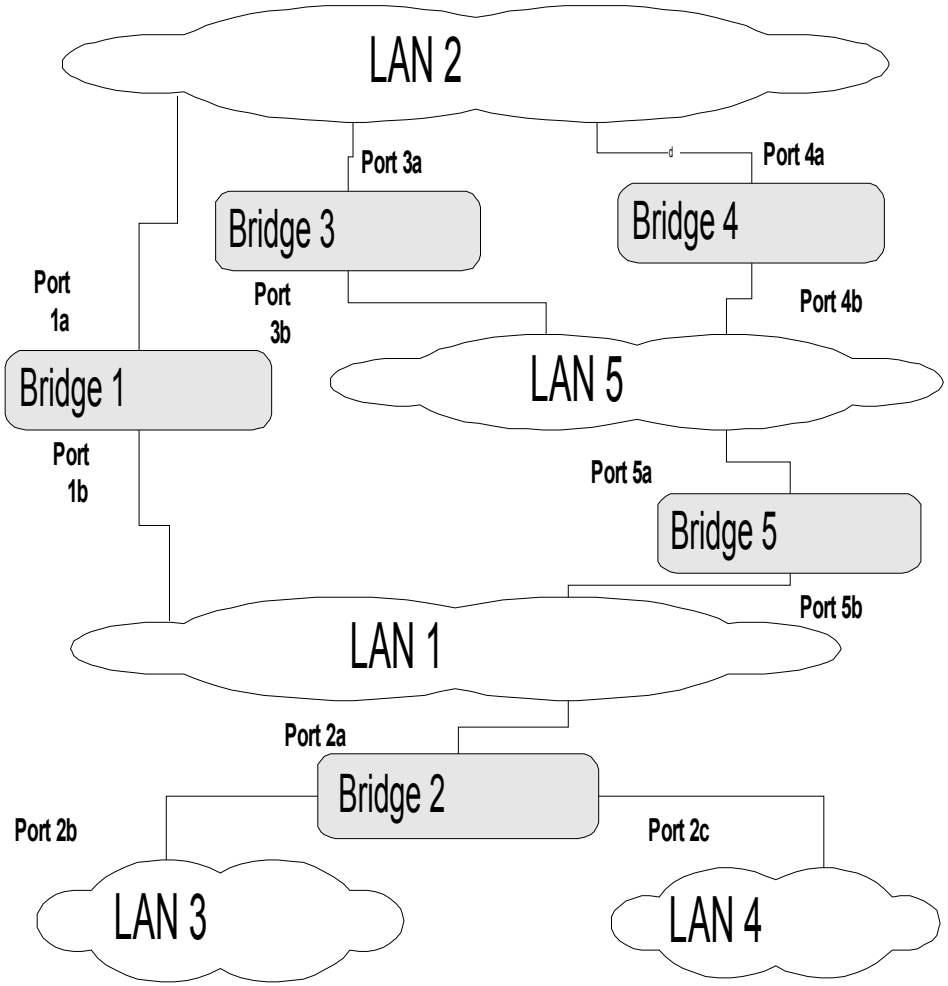



- Was ist die Root Bridge? 41
- Wie hoch sind die Root Pfad Kosten für Bridge 3? 13
- Welches ist der Root Port? 4
- Wie sieht BPDU von Bridge 3 aus? 41.13.3
- Für welche LANs ist Bridge 3 designated Bridge? 1,2,5

# Netzwerkbeispiel



- Die IDs der Bridges sind 1,2,3,4,5 und die Port IDs sind in der Abbildung angegeben.
- Die Bridges wenden den Spanning Tree Alg. an
- Annahme, dass Kosten gleich Anzahl der Hops zum Root sind
- Zeige, welche Nachrichten übermittelt werden, bis Tree geformt wurde.



# Interessanter Fall 1

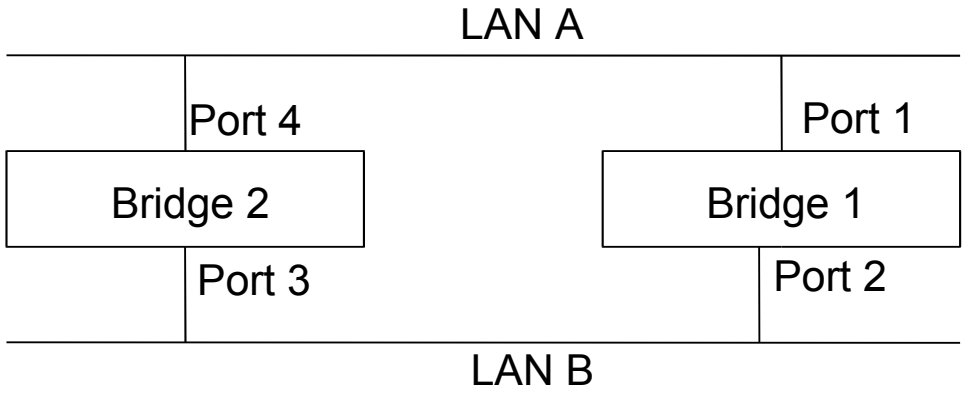


- Wenn zwei min-cost BPDUs an einer Bridge auf zwei verschiedenen Ports empfangen werden, die
  - identisch in der Root ID, Root Pfad Kosten und ID der sendenden Bridge sind und
  - die root ID die niedrigste aller bisher empfangenen root IDs ist

- dann werden die designierten Ports für die LANs verglichen, die den Ports entsprechen, über die die BPDUs empfangen wurden.
  - Die niedrigere von diesen beiden wird gewählt
  - Der Port auf der Bridge,
    der diese BDPUs empfängt und
    zum LAN der designierten Ports gehört,
    ist der Root Port der Bridge

# Beispiel






- Bridge 2 empfängt 2 BDPUs [1,0,1] an Ports 3 und 4
- Der designierte Port für LAN A ist Port 1 auf Bridge 1
- Der designierte Port für LAN B ist Port 2 auf Bridge 1
- Da Port 1 niedriger als Port 2 ist, hat er höhere Priorität
- Also wird Port 4 Root Port der Bridge 2

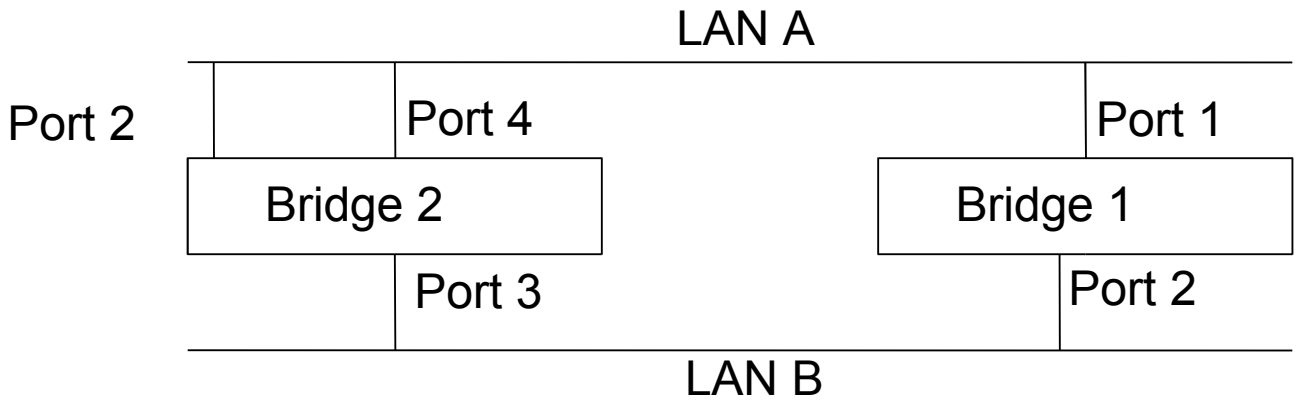
# Interessanter Fall 2



- Noch weiter:
  - Wenn auch die designierten Ports des LANs identisch sind,
  - die mit den Ports auf der Bridge korrespondieren,
  - die die gleichen BDPUs empfangen,
- Dann überprüf die Port Nummern der empfangenden Bridge, auf denen diese BDPUs empfangen werden
- Wähle den niedrigeren als Root Port aus.

# Beispiel






- Ports 2 und 4 von Bridge 2 gehören zu LAN A
- Beide empfangen die BDPUs [1,0,1] von Bridge 1

- Der designierte Port für LAN A ist Port 1 auf Bridge 1
- Also sind sogar die designierten Ports identisch

- Es wird also zwischen Port 2 und Port 4 der Root Port ausgewählt
- Also wird Port 2 Root Port der Bridge 2

# Priorität



- Werden zwei Bridge Identifier numerisch verglichen,
- wird die niedrigere Nummer die Bridge der höheren Priorität kennzeichnen.

- Ist es möglich, dass zwei Bridges die gleiche Priorität haben?

- Ist es möglich, dass zwei Bridges die gleiche Bridge ID haben?

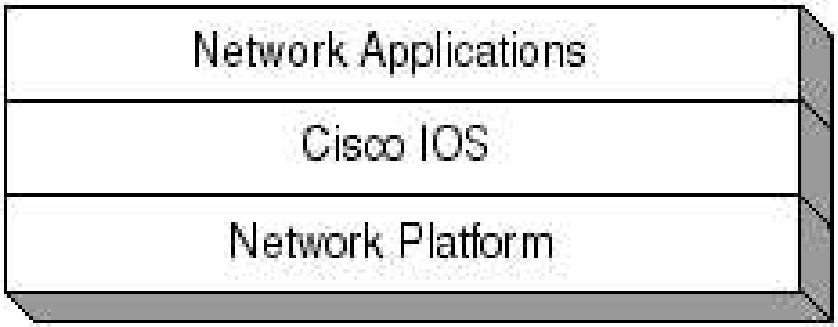
# Cisco IOS



- Zur Konfiguration eines Routers oder einer Bridge werden also Funktionen von höheren Schichten benötigt.
- Auch Management Aufgaben müssen erfüllt werden
- Cisco Internet Operating Sysetm (IOS) ist die am weitesten verbreitete Netzwerk System Software.

# Cisco IOS






- Ermöglicht Netzwerk Services für
  - Administration,
  - Wartung und
  - Betrieb
- Unterstützt eine breite Auswahl an Plattformen und viele Netzwerk Protokolle
- Ermöglicht Einrichtung von Netzwerk Anwendungen auf den Netzwerk Plattformen

# Cisco IOS Configuration



- Unterschiedliche Wege zur Konfiguration eines Cisco Geräts existieren
- Das Cisco Command Line Interface CLI ist das grundlegendste Benutzer Interface
- Es existieren sechs verschiedene Konfigurationsmodi im CLI:
  - User EXEC
  - Privileged EXEC
  - Global Configuration
  - Interface Configuration
  - Subinterface Configuration
  - ROM Monitor