05 Switching

1 Thema des Praktikums

In diesem Praktikum werden funktionale Eigenschaften von Store-and-Forward-Switches untersucht.

Die Schwerpunkte des Praktikums sind:

- Self-Learning-Mechanismus
- Verhalten mit Spanning-Tree-Algorithmus

Mittels Filtering-Database kann ein Switch Frames gezielt an ein Netz-Segment weiterleiten. Mit Hilfe eines Self-Learning-Algorithmus ist er in der Lage, die bestehende Netztopologie zu erfassen und die Filtering-Database selbständig anzupassen. Im ersten Teil wird durch den Versand von vorbereiteten Frames die Filtering-Database eines Switches gezielt beeinflusst. Der Vorgang des Self-Learning-Mechanismus und die Auswirkungen werden theoretisch analysiert und praktisch überprüft.

Das Spanning-Tree-Protocol (STP) ist zentraler Teil von Switch-Infrastrukturen, um Frames eindeutig weiterleiten zu können. Es stellt sicher, dass zwischen zwei Netzpunkten jeweils nur ein Datenpfad existiert. Eine Netztopologie kann redundante Datenpfade enthalten. Der Spanning Tree Algorithmus sieht vor, dass redundante Datenpfade gesperrt werden und ein Frame somit nicht mehrfach im Netz verkehrt. Im zweiten Teil soll ein Netz aufgebaut werden, das mittels Spanning Tree konfiguriert wird. Danach sollen die Auswirkungen von Verbindungsausfällen auf den Spanning Tree ermittelt werden.

2 Vorbereitung

2.1 Self-Learning-Mechanismus

- Lesen Sie den Abschnitt «8.1 Gezielte Paketvermittlung» im Anwenderhandbuch zum Industrial ETHERNET Switch RS20 (siehe Anhang A) und beantworten Sie folgenden Fragen:

Wozu dient die Filtering-Database (deutsch Filtertabelle, Adresstabelle)

In die Filtertabelle kommen die Adressen, welcher das Gerät gelernt hat

Wie viele Adressen kann die Filtering-Database dieses Switches enthalten?

8'000

Was ist die Aging Time?

Ist das Alter, wie lang es sich bereits in der Tabelle befindet, wenn eine Adresse dieses Alter übersteigt, wird es gelöscht

Was ist die Standardeinstellung für die Aging Time?

300 Sekunden

- Gegeben sei die Netzkonfiguration gemäss Abbildung 1. Überlegen Sie sich, auf welchen Segmenten die Frames vom Switch weitergeleitet werden, wenn ein Datenverkehr gemäss Tabelle 2 (Nodes) vorliegt.

  A→C bedeutet z.B., dass ein Frame vom Rechner A an die Zieladresse C verschickt wird.

  In Tabelle 2 tragen Sie in den Spalten unter „Theoretische Lösung“ ein O ein, falls ein Frame vom Switch empfangen wurde und ein X falls es vom Switch dort ausgegeben wird.

2.2 Spanning-Tree-Protocol

Lesen Sie den Abschnitt «5.1 Das Spanning Tree Protokoll» im Anwenderhandbuch Redundanz-Konfiguration Industrial RS20 (siehe Anhang B) und beantworten Sie folgenden Fragen:

Wie ist der Bridge Identifier aufgebaut?

Ein Bridge Identifier besteht aus 8 Bytes. Die zwei höchstwertigen Bytes sind die Prioritätszahl. Die sechs niederwertigen Bytes sind die MAX-Adresse der Brücke

Wie kann man als Administrator die Root-Bridge festlegen?

Die Brücke mit dem kleinsten Zahlenwert für die Brückenidentifikation wird zur Wurzelbrücke (root Bridge).

Falls es von einer Bridge mehrere Pfade zu Root gibt, welches ist das primäre Kriterium zur Pfadauswahl.

Brückenidentifikation

Welche Eigenschaft einer Verbindung bestimmt massgeblich die Pfadkosten?

Portidentifikation

3 Versuchsdurchführung zur Filtering-Database

- Bauen Sie die Versuchskonfiguration gemäss Abbildung 1 auf.

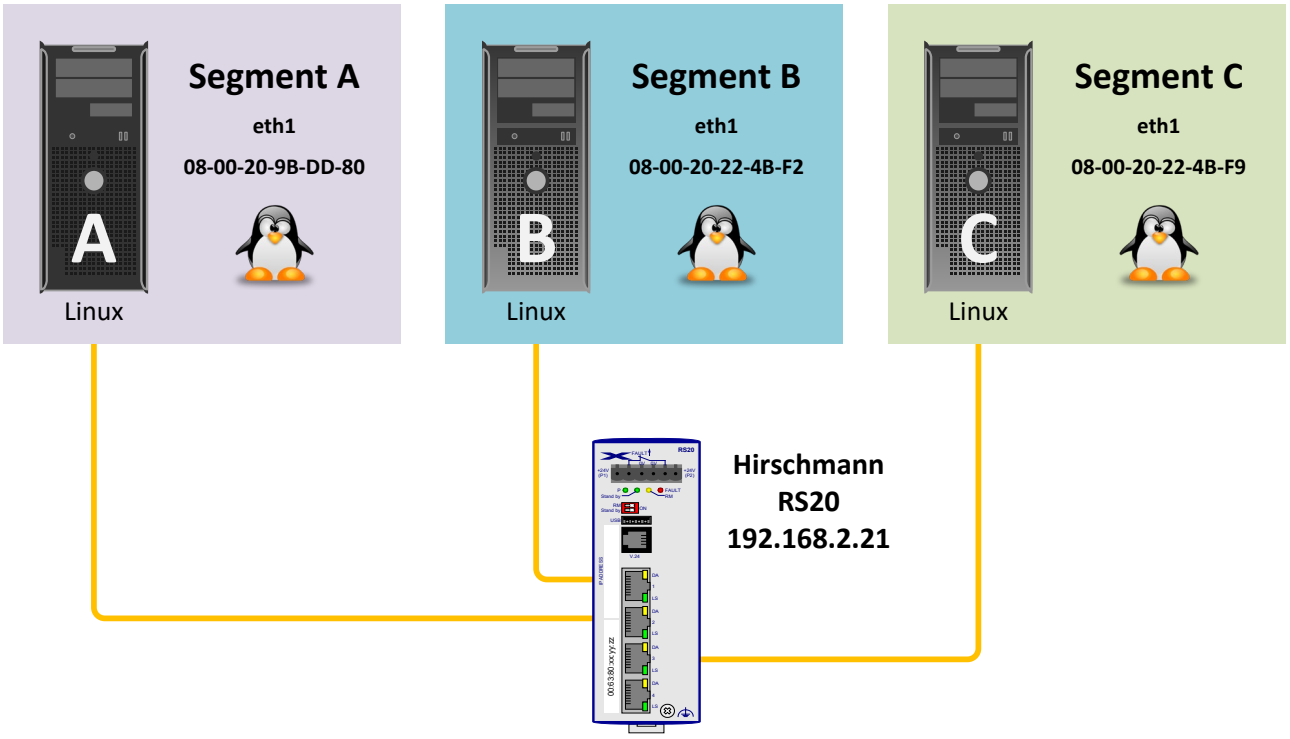

Abbildung 1

- Starten Sie alle Rechner mit Linux, öffnen Sie auf jedem ein Terminal und setzen Sie die Dateien zurück. Wechseln Sie dazu ins Verzeichnis des Praktikum 5 und starten Sie das Script:
  `cd /home/ktlabor/praktika/05_prakt/`
  `./download-kt`

Der verwendete Switch Hirschmann RS20 besitzen vier Fast Ethernet Ports 10/100 BASE-T und einen V.24-Port, wobei letzterer im Praktikum nicht verwendet wird.

- Setzten Sie die Konfiguration des Switches zurück. Dazu wird er ausgeschaltet und mit eingestecktem USB-Stick gebootet. Er konfiguriert dann selbständig unter anderem die IP-Adresse.
  Wichtig: Es muss zwingend der zum Switch gehörige USB-Stick verwendet werden!
  Entfernen Sie nach dem Booten (nach ca. 1 Minute) die USB-Sticks wieder.
- Starten Sie auf einem der Rechner einen Browser und öffnen Sie das Webinterface des Switches. Hierfür muss im Adressfeld die IP-Adresse des Switches (http://192.168.2.21 bis http://192.168.2.24) eingegeben werden.

  Hinweis: Wenn ein Java-Update verlangt wird, ignorieren Sie diese Aufforderung.
- Logen Sie auf dem Switch ein:
  User: **`admin`**
  Passwort: **`private`**

Im Folgenden sollen zwischen den Rechnern Ethernet-Frames mit definierten Absender- und Empfänger-adresse verschickt werden. Dazu führen Sie auf dem jeweiligen Rechner das passende Script aus:

Beispiel: **`./AtoC`** Prozedur zum Senden eines Frames von Rechner A zum Rechner C

- Starten Sie auf allen PCs Wireshark (eth1) und setzen Sie einen Filter für die MAC-Adressen der Test-Frames, damit nur diese angezeigt werden:
  Filter: **`eth.addr contains 08:00:20`**
- Löschen Sie über das Webinterface die Filtering-Database des Switches:
  Menüpunkt: **`Neustart → MAC-Adresstabelle zurücksetzen`**
- Überprüfen Sie mit Wireshark, auf welchen Segmenten A, B oder C die Frames von Tabelle 2 auftreten. Die Buchstaben A, B, C und F stehen symbolisch für die Mac-Adressen der Rechner-Ports. Die Zuordnung ist in Tabelle 1 dargestellt. F bezeichnet eine Mac-Adresse, die keinem der Rechner-Ports zugeordnet ist.

Rechner	Mac Adresse
A	08-00-20-9B-DD-80
B	08-00-20-22-4B-F2
C	08-00-20-22-4B-F9
F	08-00-20-9B-DD-82

Tabelle 1

- Arbeiten Sie die Tabelle 2 zügig durch und tragen Sie die Resultate in der Spalte Messung ein.

Step	Nodes S → E	Versuchsdurchführung: PC / Script		Theoretische Lösung			Messung		
				A	B	C	A	B	C
1	A→F	PC A:	AtoF						
2	A→B	PC A:	AtoB						
3	A→C	PC A:	AtoC						
4	B→A	PC B:	BtoA						
5	B→C	PC B:	BtoC						
6	C→A	PC C:	CtoA						
7	C→B	PC C:	CtoB						
8	A→F	PC A:	AtoF						
9	A→B	PC A:	AtoB						
10	A→C	PC A:	AtoC						

Tabelle 2

Wie erklären Sie allfällige Abweichungen zwischen der theoretischen Lösung und der Messung?

Wird die Absender- oder Empfängeradresse eines Frames für die Filterung verwendet?

Auf welchen Ethernet-Ports werden die Frames versendet, wenn der Switch die Empfängeradresse noch nicht in der Filtering-Database gespeichert hat?

Welche die Frames werden immer an alle Ports versendet?

Wie gross ist die eingestellte Aging Time (Menüpunkt: **`Switching:Global`** *)?*

- Setzen Sie die Aging-Time auf 30 Sekunden (oder 60 Sekunden, wenn Sie bei der Eingabe langsam sind).
- Löschen Sie erneut die Filtering-Database des Switches

  Menüpunkt: **`Neustart → MAC-Adresstabelle zurücksetzen`**
- Führen Sie die Sendefolge von Tabelle 2 nochmals durch und notieren Sie jeweils nach dem Versenden, wann (Zeit und Step) und wie sich die Filtering-Database des Switches verändert hat.

Zeit	Step	S → E	MAC-Adresse	Port 1.1	Port 1.2	Port 1.3	Port 1.4

Tabelle 3

Welche Adresse ist für das Self-Learning des Switches massgebend (Absender- oder Empfängeradresse)?

Wann genau (zeitlich) verschwinden die Einträge wieder aus der Filtering-Database?

Warum wäre eine unendlich grosse Aging Time keine gute Wahl?

Was ist das Problem, wenn die Aging-Time zu kurz gewählt wird?

Zeigen Sie die Resultate dem Laborbetreuer.

4 Messungen zum Spanning Tree Protocol

Für diesen Versuch werden die Rechner A und B mit Linux betrieben.

- Bauen Sie die Versuchskonfiguration gemäss Abbildung 1 auf.

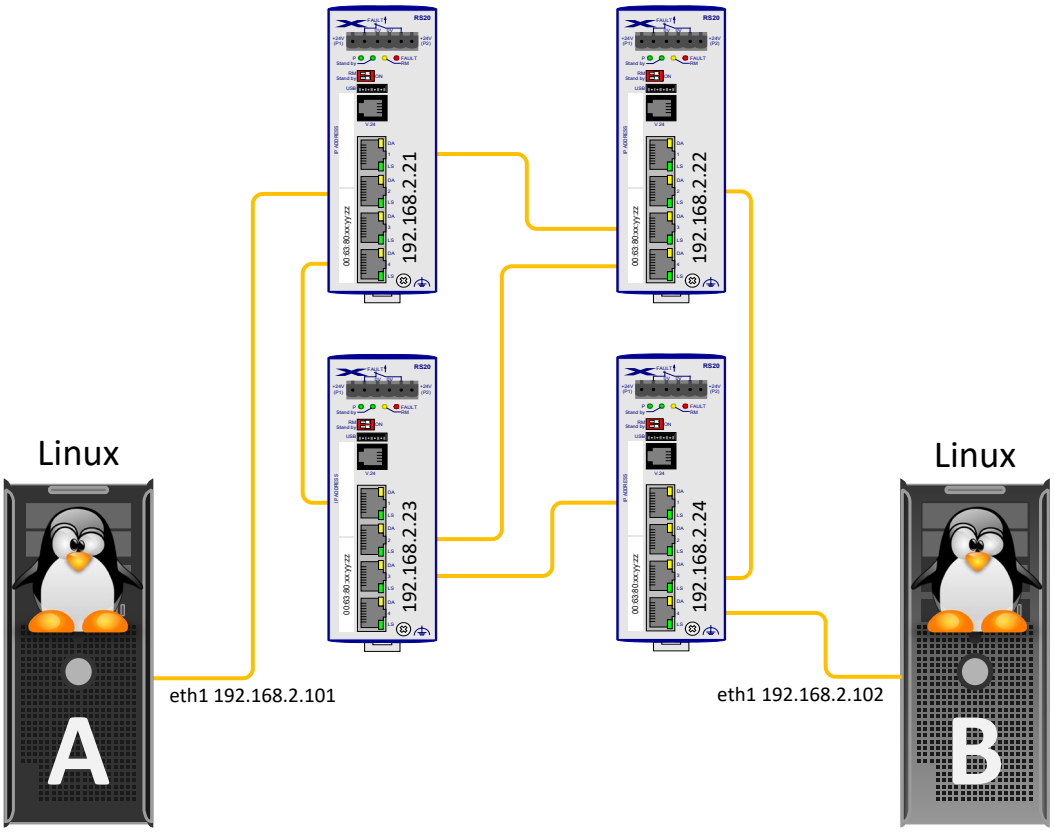

Abbildung 2

- Starten Sie Wireshark auf Rechner B (entfernen Sie die Filter falls noch gesetzt von vorher). Untersuchen Sie die BPDU-Frames (Bridge Protocol Data Unit).

Welcher Switch ist für den Aufbau des Spanning Tree verantwortlich?

Wie heisst das Protokoll-Feld, indem die Root zu finden ist?

Was lässt sich über die MAC-Adresse des Root-Switches sagen?

Die BPDU-Frames werden in einem bestimmten Intervall von dem Root-Switch (Root-Bridge) abgesetzt. Dieses Intervall ist die so genannte Hello-Time. Diese kann beim Switch verändert werden.

Wie gross ist die Hello-Time?

Was sind die Vor-/Nachteile einer kurzen Hello-Time?

- Zeichnen Sie die physikalischen Verbindungen Ihres Aufbaus in Abbildung 3 ein und kennzeichnen Sie aktive Leitungen zwischen den Switches farblich (erkennbar an der orange blinkenden LED).
  Die Anzeige von Daten-Traffic auf den Switch-Ports (orange blinkende LEDs) können Sie forcieren, indem Sie wie folgt Broadcast-Frames senden (auf Rechner A oder B):
  `sendframes eth1 -d ff:ff:ff:ff:ff:ff`

Was passiert, wenn Sie eine oder mehrere aktive Leitungen unterbrechen?

- Zeichnen Sie die beobachtete Veränderung andersfarbig in Abbildung 3 ein!

Abbildung 3

- Stecken Sie die Kabel wieder ein gemäss Ausgangslage in Abbildung 2.
- Machen Sie den Switch unten links (192.168.2.23) zur Root, indem Sie seine Parameter ändern.

Welche(n) Parameter mussten Sie anpassen?

Was für ein Prozess ist abgelaufen?

Was hat sich in den BPDU-Frames verändert?

Zeigen Sie die Resultate dem Laborbetreuer.

5 Zusatzaufgaben

- Untersuchen Sie, was geschieht, wenn Sie in der aktiven, redundanten Verbindung einen Hub dazwischenschalten; z.B. zwischen Switch 3 und 2.

- Was ändert sich an den Pfadkosten und aus welchem Grund?

- Versuchen Sie, die Nutzung der Verbindung über den Hub zu erzwingen, indem Sie an den Switches gezielt die Switch-Prioritäten und/oder die Pfadkosten verändern.

- Entfernen Sie den Hub wieder und verbinden Sie zwei Switches über parallele Leitungen und erklären Sie, wie die Auswahl der aktiven Verbindung erfolgt.

- Schalten Sie an den beiden Switches das Spanning Tree Protokoll aus und untersuchen Sie das Verhalten, wenn ein Loop gesteckt wird.

8.1 Gezielte Paketvermittlung

Durch gezielte Paketvermittlung hilft Ihnen das Gerät, Sie vor unnötiger Netzbelastung zu bewahren. Folgende Funktionen bietet Ihnen das Gerät zur gezielten Paketvermittlung:

- Store and Forward
- Multiadress-Fähigkeit
- Altern gelernter Adressen
- Statische Adresseinträge
- Ausschalten der gezielten Paketvermittlung

8.1.1 Store and Forward

Alle Daten, die das Gerät empfängt, werden gespeichert und auf ihre Gültigkeit geprüft. Ungültige und fehlerhafte Datenpakete (> 1.536 Bytes oder CRC-Fehler) sowie Fragmente (< 64 Bytes) werden verworfen. Gültige Datenpakete leitet das Gerät weiter.

8.1.2 Multiadress-Fähigkeit

Das Gerät lernt alle Quelladressen je Port. Nur Pakete mit

- unbekannten Ziel-Adressen
- diesen Ziel-Adressen oder
- einer Multi-/Broadcast-Ziel-Adresse

im Zieladressfeld werden an diesen Port gesendet. Gelernte Quelladressen trägt das Gerät in seine Filtertabelle ein (siehe auf Seite 118 „Statische Adresseinträge eingeben“).
Das Gerät kann bis zu 8.000 Adressen lernen. Dies wird notwendig, wenn an einem oder mehreren Ports mehr als ein Endgerät angeschlossen ist. So können mehrere eigenständige Subnetze an das Gerät angeschlossen werden.

8.1.3 Altern gelernter Adressen

Das Gerät überwacht das Alter der gelernten Adressen. Adresseinträge, die ein bestimmtes Alter, die Aging Time, überschreiten, löscht das Gerät aus seiner Adresstabelle.
Datenpakete mit einer unbekannten Zieladresse flutet das Gerät.
Datenpakete mit bekannter Zieladresse vermittelt das Gerät gezielt.

Hinweis: Ein Neustart löscht die gelernten Adresseinträge.

- ☐ Wählen Sie den Dialog `Switching:Global`.
- ☐ Geben Sie die Aging Time für alle dynamischen Einträge im Bereich von 10 bis 630 Sekunden (Einheit: 1 Sekunde, Voreinstellung: 30). Im Zusammenhang mit der Router-Redundanz wählen Sie die Zeit ≥ 30 Sekunden.

8.1.4 Statische Adresseinträge eingeben

Eine wichtige Funktion des Gerätes ist unter anderem die Filterfunktion. Sie selektiert Datenpakete nach definierten Mustern, den Filtern. Diesen Mustern sind Vermittlungsvorschriften zugeordnet. Das heißt, ein Datenpaket, das ein Gerät an einem Port empfängt, wird mit den Mustern verglichen. Besteht ein Muster, mit dem das Datenpaket übereinstimmt, dann sendet oder blockiert ein Gerät dieses Datenpaket entsprechend den Vermittlungsvorschriften an den betroffenen Ports.

Als Filterkriterium können gelten:

- Zieladresse (Destination Address),
- Broadcast-Adresse,
- Gruppenadresse (Multicast),
- VLAN-Zugehörigkeit.

Zur Speicherung der einzelnen Filter dient die Filtertabelle (Forwarding Database, FDB). Sie enthält 3 Teile: einen statischen und zwei dynamische Teile.

- Der Management-Administrator beschreibt den statischen Teil der Filtertabelle (`dot1qStaticTable`).
- Das Gerät besitzt die Fähigkeit, während des Betriebes zu lernen, an welchem Port es Datenpakete mit welchen Quelladressen empfängt (siehe auf Seite 116 „Multiadress-Fähigkeit“). Diese Information wird in einen dynamischen Teil (`dot1qTpFdbTable`) geschrieben.
- Von Nachbar-Agenten dynamisch gelernte und die per GMRP gelernten Adressen werden in den anderen dynamischen Teil geschrieben.

Adressen, die schon in der statischen Filtertabelle stehen, übernimmt das Gerät automatisch in den dynamischen Teil.
Eine statisch eingetragene Adresse kann nicht durch Lernen überschrieben werden.

Hinweis: Bei aktivem Ring-Manager sind keine permanenten Unicast-Einträge möglich.

5 Rapid Spanning Tree

Hinweis: Das Spanning Tree Protokoll und das Rapid Spanning Tree Protokoll sind Protokolle für MAC Brücken und im Standard IEEE 802.1D-2004 bzw. IEEE 802.1w beschrieben. Daher wird in der folgenden Beschreibung dieser Protokolle meist der Begriff Brücke statt Switch verwendet.

Lokale Netze werden immer größer. Dies gilt sowohl für die geographische Ausdehnung, als auch für die Anzahl der Netzteilnehmer. So ist es oft sinnvoll gleich mehrere Brücken einzusetzen, um z. B.:

- die Netzlast in Teilbereichen zu verringern,
- redundante Verbindungen aufzubauen und
- Entfernungseinschränkungen zu überwinden.

Der Einsatz mehrerer Brücken mit mehrfachen, redundanten Verbindungen zwischen den Teilnetzen kann jedoch zu Schleifen/Loops und damit zum Totalausfall des Netzes führen. Um dies zu verhindern, wurde der (Rapid) Spanning Tree Algorithmus entwickelt. Das Rapid Spanning Tree Protokoll (RSTP) ermöglicht Redundanz durch Unterbrechung von Schleifen.

RSTP ist eine Weiterentwicklung des Spanning Tree Protokolls (STP) und ist zu diesem kompatibel. Das STP benötigt beim Ausfall einer Verbindung oder einer Brücke eine Rekonfigurationszeit von bis zu 30 s. Dies war in zeitkritischen Anwendungen nicht mehr akzeptabel. Daher wurde das STP zum RSTP weiterentwickelt was zu Rekonfigurationszeiten von unter einer Sekunde führte.

Hinweis: Der Standard schreibt vor, dass alle Brücken innerhalb eines Netzes mit dem (Rapid) Spanning Tree Algorithmus arbeiten. Beim gleichzeitigen Einsatz von STP und RSTP gehen jedoch die Vorteile der schnelleren Rekonfiguration beim RSTP verloren.

5.1 Das Spanning Tree Protokoll

Da RSTP eine Weiterentwicklung des STP ist, gelten alle folgenden Beschreibungen des STP auch für das RSTP.

5.1.1 Die Aufgaben des STP

Der Spanning Tree Algorithmus reduziert Netztopologien, die mit Brücken aufgebaut sind und Ringstrukturen durch redundante Verbindungen aufweisen, auf eine Baumstruktur. Dabei trennt STP die Ringstrukturen nach vorgegebenen Regeln auf, indem es redundante Pfade deaktiviert. Wird im Fehlerfall ein Pfad unterbrochen, aktiviert das STP den zuvor deaktivierten Pfad wieder. Dies erlaubt redundante Verbindungen zur Erhöhung der Datensicherheit.
Das STP ermittelt bei der Bildung der Baumstruktur eine sogenannte Wurzelbrücke. Sie bildet die Basis der STP-Baumstruktur.

Merkmale des STP-Algorithmus:

- automatische Rekonfiguration der Baumstruktur bei Brückenfehler oder Unterbrechung eines Datenpfades,
- Stabilisierung der Baumstruktur bis zur maximalen Netzgröße (bis zu 39 Hops, abhängig von der Einstellung für „Max. Age“)
- Stabilisierung innerhalb einer kurzen bekannten Zeit,
- durch das Management vorbestimmbare und reproduzierbare Topologie,
- Transparenz für die Endgeräte,
- geringe Netzlast gegenüber der verfügbaren Übertragungskapazität durch die Einrichtung der Baumstruktur.

5.1.2 Die Brückenparameter

Jede Brücke wird eindeutig durch Parameter beschrieben:

- Brückenidentifikation (Bridge Identifier),
- Wurzelpfadkosten der Brückenports,
- Portidentifikation (Port Identifier).

5.1.3 Brückenidentifikation (Bridge Identifier)

Die Brückenidentifikation besteht aus acht Byte. Die zwei höchstwertigen Bytes sind die Prioritätszahl. Die Voreinstellung für die Prioritätszahl ist 32 768, jedoch kann der Management-Administrator diese zur Konfiguration des Netzes verändern. Die sechs niederwertigen Bytes der Brückenidentifikation sind die MAC-Adresse der Brücke. Die MAC-Adresse garantiert, dass jede Brücke eine andere Brückenidentifikation besitzt.
Die Brücke mit dem kleinsten Zahlenwert für die Brückenidentifikation besitzt die höchste Priorität.

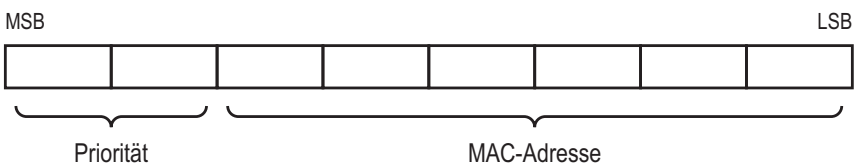

Abb. 39: Brückenidentifikation

5.1.4 Wurzelpfadkosten

Jedem Pfad, der zwei Brücken miteinander verbindet, sind Kosten für die Übertragung (Pfadkosten) zugeordnet. Der Switch legt diesen Wert in Abhängigkeit von der Übertragungsgeschwindigkeit fest (siehe Tab. 12). Dabei ordnet er Pfaden mit niedrigerer Übertragungsgeschwindigkeit die höheren Pfadkosten zu.

Alternativ dazu kann auch der Management-Administrator die Pfadkosten festlegen. Dabei ordnet er - wie der Switch - Pfaden mit niedrigerer Übertragungsgeschwindigkeit die höheren Pfadkosten zu. Da er aber diesen Wert letztendlich frei wählen kann, verfügt er hiermit über ein Werkzeug, bei redundanten Pfaden einem bestimmten Pfad den Vorzug zu geben.

Die Wurzelpfadkosten sind die Summe aller Einzelpfadkosten der Pfade, die ein Datenpaket zwischen dem angeschlossenen Port einer Brücke und der Wurzelbrücke passiert.

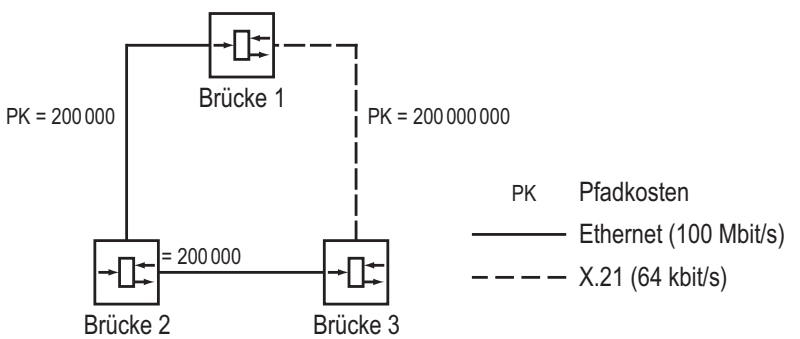

Abb. 40: Pfadkosten

Datenrate	Empfohlener Wert	Empfohlener Bereich	Möglicher Bereich
<=100 KBit/s	200 000 000*	20 000 000-200 000 000	1-200 000 000
1 MBit/s	20 000 000*	2 000 000-200 000 000	1-200 000 000
10 MBit/s	2 000 000*	200 000-20 000 000	1-200 000 000
100 MBit/s	200 000*	20 000-2 000 000	1-200 000 000
1 GBit/s	20 000	2 000-200 000	1-200 000 000
10 GBit/s	2 000	200-20 000	1-200 000 000
100 GBit/s	200	20-2 000	1-200 000 000
1 TBit/s	20	2-200	1-200 000 000
10 TBit/s	2	1-20	1-200 000 000

Tab. 12: Empfohlene Pfadkosten beim RSTP in Abhängigkeit von der Datenrate
** Brücken, die zu IEEE 802.1D, 1998 Edition konform sind, und nur 16 Bit-Werte für die Pfadkosten unterstützen, sollten als Pfadkosten den Wert 65 535 anwenden, wenn Sie im Zusammenhang mit Brücken benutzt werden, die 32 Bit-Werte für die Pfadkosten unterstützen.*

Hinweis: Sind mit Link-Aggregation (siehe auf Seite 11 „Link Aggregation“) Verbindungsleitungen zwischen Switches zu einem Trunk zusammengefasst, so reduzieren sich die Pfadkosten entprechend der Anzahl der Verbindungen, die zu einem Trunk zusammengefasst sind.

5.1.5 Portidentifikation

Die Portidentifikation besteht aus zwei Byte. Ein Teil, das niederwertigere Byte, gibt die feste Beziehung zur physikalischen Portnummer wieder. Dieser Teil gewährleistet, dass kein Port einer Brücke die gleiche Bezeichnung wie ein anderer Port dieser Brücke trägt. Der zweite Teil ist die Portprioritätszahl, die der Management-Administrator festlegt (Voreinstellung: 128). Auch hier gilt: der Port mit dem kleinsten Zahlenwert für die Portidentifikation besitzt die höchste Priorität.

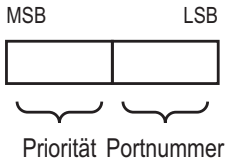

Abb. 41: Portidentifikation

5.2 Regeln für die Erstellung der Baumstruktur

5.2.1 Brückeninformation

Zur Berechnung der Baumstruktur benötigen die Brücken nähere Informationen über die anderen Brücken, die sich im Netz befinden.
Um diese Informationen zu erhalten, sendet jede Brücke eine BPDU (Bridge Protocol Data Unit) an andere Brücken.

Bestandteil einer BPDU ist unter anderem die

- Brückenidentifikation,
- Wurzelpfadkosten und
- Portidentifikation

(siehe IEEE 802.1D).

5.2.2 Aufbauen der Baumstruktur

- Die Brücke mit dem kleinsten Zahlenwert für die Brückenidentifikation wird zur Wurzelbrücke (Root Bridge). Sie ist die Wurzel der Baumstruktur
- Der Aufbau des Baumes hängt von den Wurzelpfadkosten ab. STP wählt die Struktur so, dass die minimalen Pfadkosten zwischen jeder einzelnen Brücke zur Wurzelbrücke entstehen.
- Bei mehreren Pfaden mit gleichen Wurzelpfadkosten entscheidet die Priorität der Brückenidentifikation der Brücken, die an einen dieser Pfade angeschlossen ist, welche Brücke blockiert.

- Wenn von einer Brücke zwei Pfade mit den gleichen Wurzelpfadkosten wegführen, wird als letztes Kriterium die Portidentifikation herangezogen (siehe Abb. 41). Sie entscheidet, welcher Port gewählt wird.

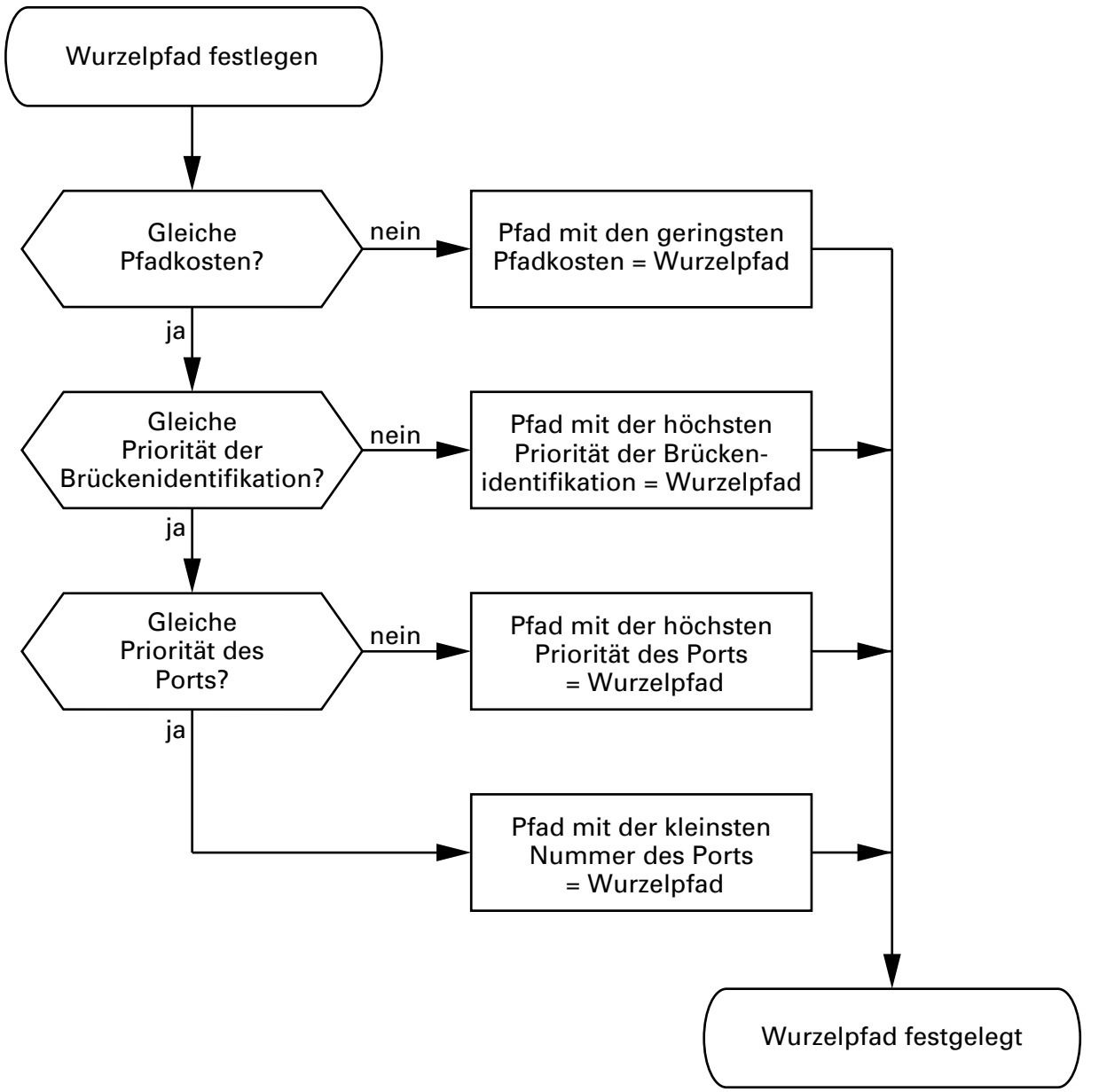

Abb. 42: Flußdiagramm Wurzelpfad festlegen

5.3 Beispiel zum Festlegen der Wurzelpfade

Anhand des Netzplanes (siehe Abb. 43) kann man das Flußdiagramm (siehe Abb. 42) zur Festlegung des Wurzelpfades (Root Path) nachvollziehen. Der Administrator hat für jede Brücke eine andere Priorität in der Brückenidentifikation festgelegt. Die Brücke mit dem kleinsten Zahlenwert für die Brückenidentifikation wird zur Wurzelbrücke, in diesem Fall die Brücke 1. Im Beispiel belasten alle Teilpfade die gleichen Pfadkosten. Der Pfad zwischen Brücke 2 und Brücke 3 wird unterbrochen, da eine Verbindung von Brücke 3 über Brücke 2 zur Wurzelbrücke die doppelten Pfadkosten verursachen würden.

Interessant ist der Pfad von der Brücke 6 zur Wurzelbrücke:

- Der Pfad über Brücke 5 und Brücke 3 verursacht die gleichen Wurzelpfadkosten wie der Pfad über Brücke 4 und Brücke 2.
- Gewählt wird der Pfad über Brücke 4, da der Zahlenwert 28 672 für die Priorität in der Brückenidentifikation kleiner ist als der Zahlenwert 32 768.
- Zwischen Brücke 6 und Brücke 4 gibt es aber zwei Pfade. Hier entscheidet die Portidentifikation.

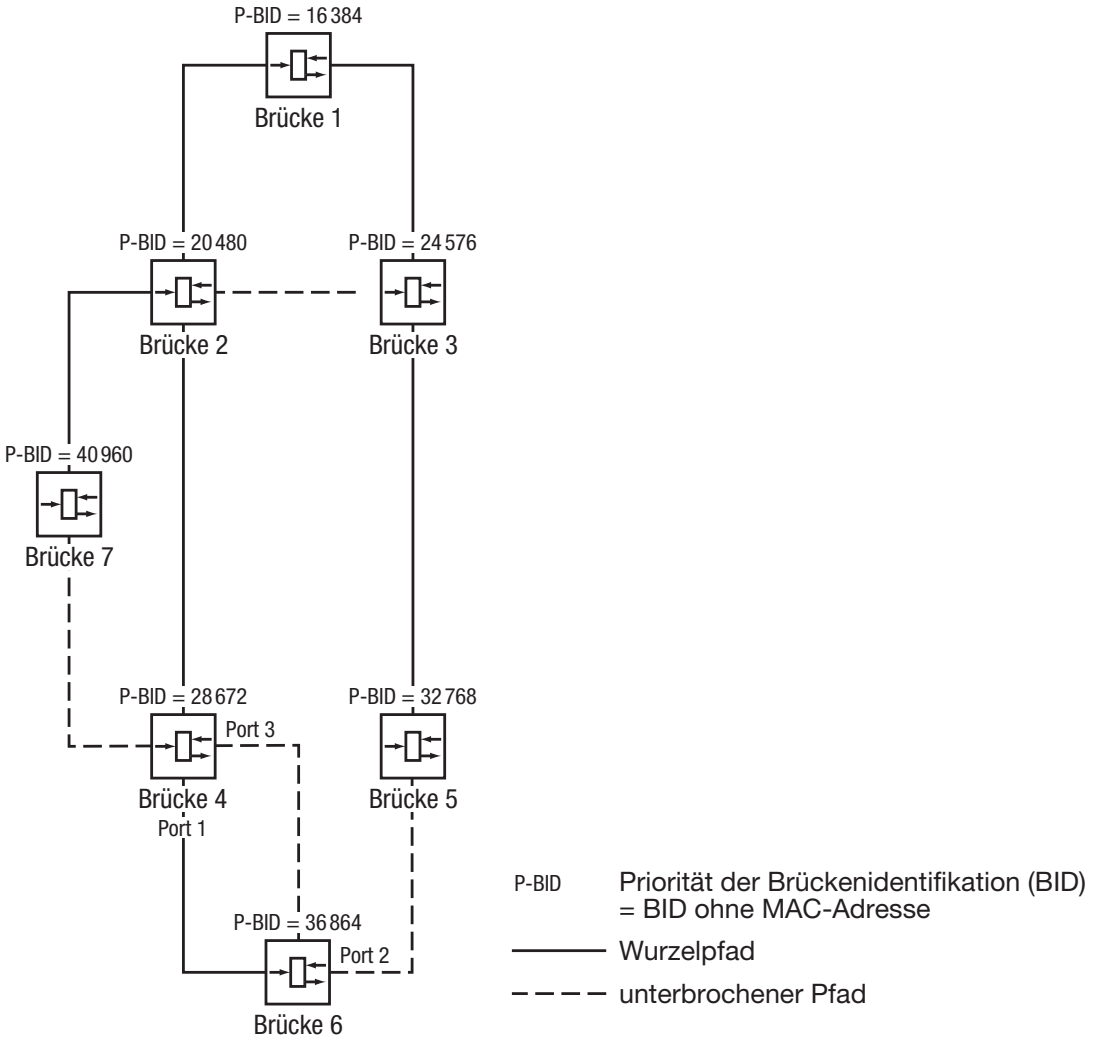

Abb. 43: Beispiel Wurzelpfade festlegen

5.4 Beispiel zur Manipulation der Wurzelpfade

Anhand des Netzplanes (siehe Abb. 44) kann man das Flußdiagramm (siehe Abb. 42) zur Festlegung des Wurzelpfades (Root Path) nachvollziehen. Der Administrator hat
– für jede Brücke außer der Brücke 1 den im Lieferzustand voreingestellten Wert von 32 768 belassen und
– der Brücke 1 den Wert 16 384 gegeben und damit zur Wurzelbrücke erhoben.
Im Beispiel belasten alle Teilpfade die gleichen Pfadkosten. Der Pfad zwischen Brücke 2 und Brücke 3 wird unterbrochen, da eine Verbindung von Brücke 3 über Brücke 2 zur Wurzelbrücke die doppelten Pfadkosten verursachen würden.

Interessant ist der Pfad von der Brücke 6 zur Wurzelbrücke:

- Der Pfad über Brücke 5 und Brücke 3 verursacht die gleichen Wurzelpfadkosten wie der Pfad über Brücke 4 und Brücke 2.
- STP wählt den Pfad über die Brücke, die in der Brückenidentifikation die niedrigere MAC-Adresse hat (im Bild dargestellt Brücke 4).
- Zwischen Brücke 6 und Brücke 4 gibt es aber zwei Pfade. Hier entscheidet die Portidentifikation.

Hinweis: Indem der Administrator für jede Brücke außer der Wurzelbrücke den im Lieferzustand voreingestellten Wert der Priorität in der Brückenidentifikation beläßt, bestimmt allein die MAC-Adresse in der Brückenidentifikation welche Brücke bei Ausfall der Wurzelbrücke zur neuen Wurzelbrücke wird

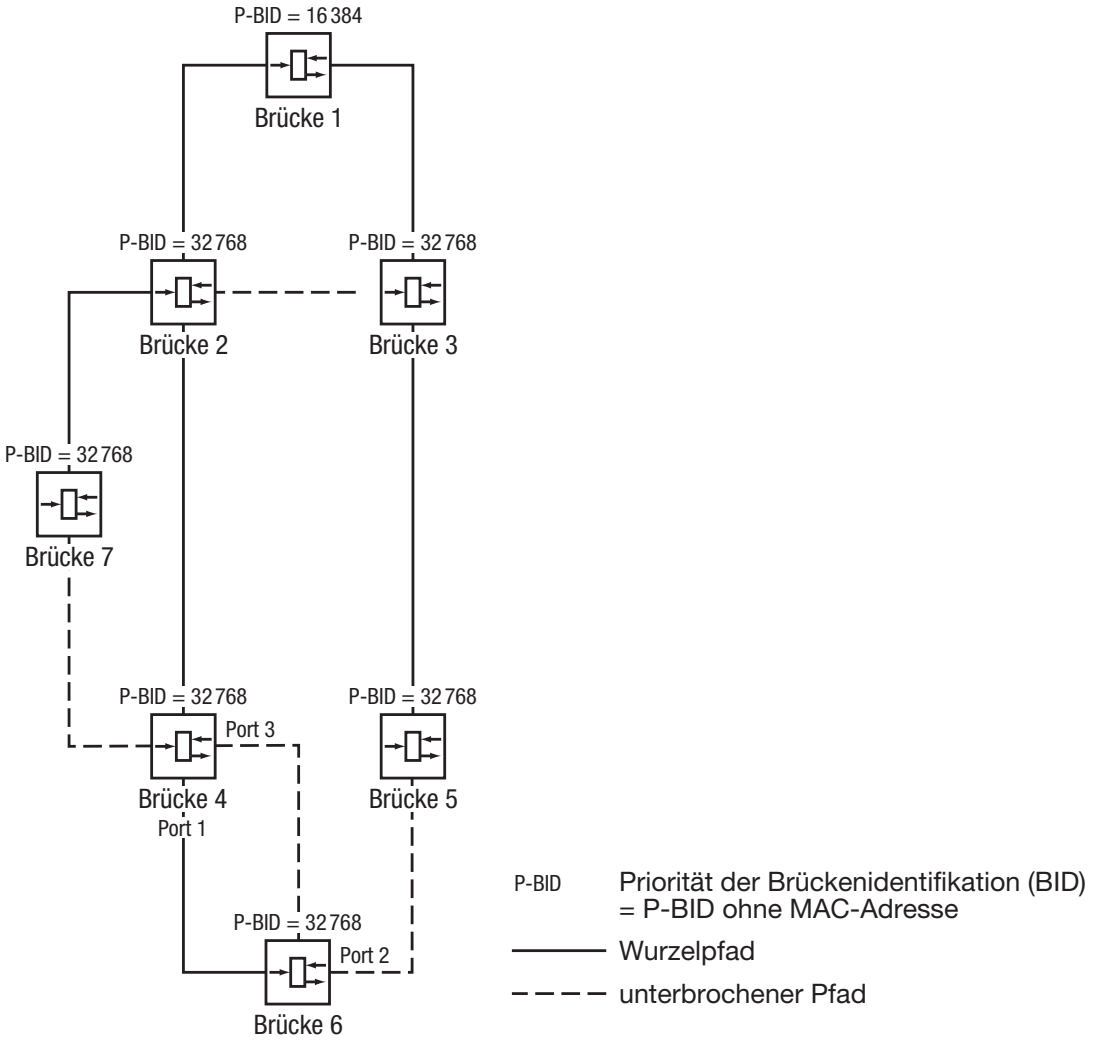

Abb. 44: Beispiel Wurzelpfade manipulieren

5.5 Beispiel zur Manipulation der Baumstruktur

Der Management-Administrator des Netzes stellt bald fest, dass diese Konfiguration mit Brücke 1 als Wurzelbrücke (siehe auf Seite 75 „Beispiel zum Festlegen der Wurzelpfade“) ungünstig ist. Auf den Pfaden zwischen Brücke 1 zu Brücke 2 und Brücke 1 zu Brücke 3 summieren sich die Kontrollpakete, die die Wurzelbrücke zu allen anderen Brücken sendet.
Erhebt der Management-Administrator die Brücke 2 zur Wurzelbrücke, dann verteilt sich die Belastung der Teilnetze durch Kontrollpakete wesentlich besser. Hieraus entsteht die dargestellte Konfiguration (siehe Abb. 45). Die Wege zwischen den einzelnen Brücken zur Wurzelbrücke sind kürzer geworden.

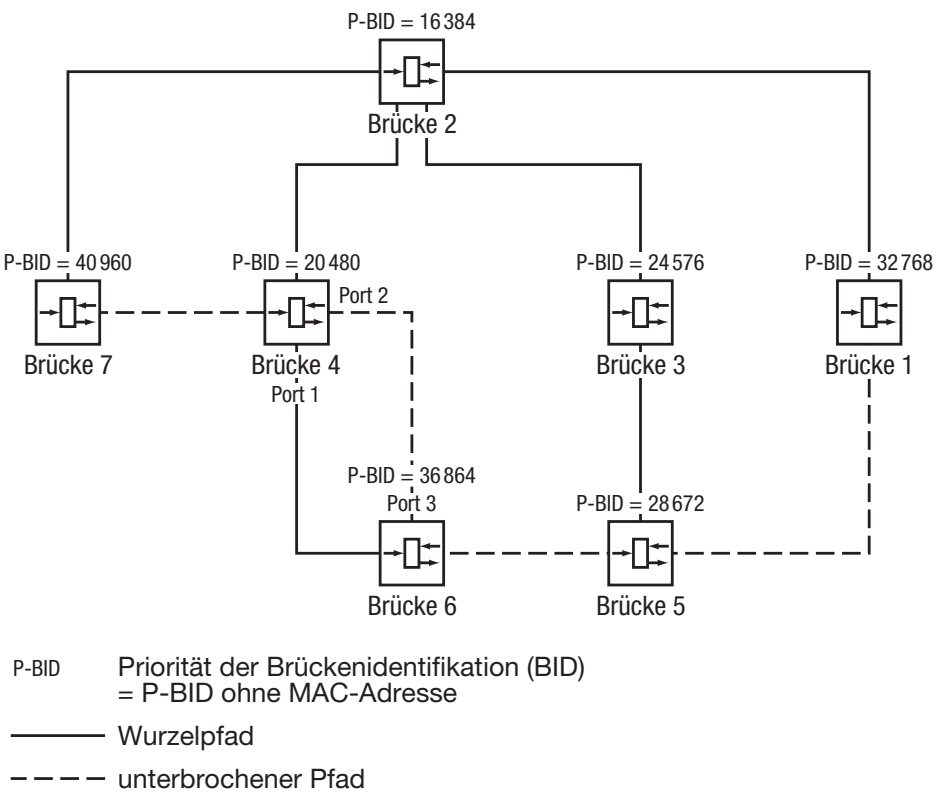

Abb. 45: Beispiel Baumstruktur manipulieren

Hinweis: Die Filtertabelle bietet Ihnen für Multicast-Adressen die Möglichkeit, bis zu 100 Filter-Einträge zu erzeugen.

☐ Wählen Sie den Dialog `Switching:Filter für MAC-Adressen`.

Jede Zeile der Filtertabelle stellt einen Filter dar. Filter legen die Vermittlungsweise von Datenpaketen fest. Sie werden entweder automatisch vom Gerät (Status learned) oder manuell angelegt. Datenpakete, deren Zieladresse in der Tabelle eingetragen ist, werden vom Empfangsport an die in der Tabelle markierten Ports vermittelt. Datenpakete, deren Zieladresse nicht in der Tabelle enthalten ist, werden vom Empfangsport an alle anderen Ports vermittelt. Im Dialog „Filter anlegen“ (siehe Bedientaste unten) haben Sie die Möglichkeit, neue Filter zu erzeugen. Folgende Zustände sind möglich:

- `learned`: Das Filter wurde vom Gerät automatisch angelegt.
- `permanent`: Das Filter wird im Gerät oder auf dem URL dauerhaft gespeichert (siehe auf Seite 62 „Einstellungen speichern“).
- `invalid`: Mit diesem Status löschen Sie ein manuell angelegtes Filter.
- `igmp`: Das Filter wurde durch IGMP-Snooping angelegt.

Um Einträge mit dem Status „learned“ aus der Filtertabelle zu löschen, wählen Sie den Dialog `Grundeinstellungen:Neustart` und klicken Sie auf „MAC-Adresstabelle zurücksetzen“.

8.1.5 Gezielte Paketvermittlung ausschalten

Um die Daten aller Ports beobachten zu können, bietet Ihnen das Gerät die Möglichkeit, das Lernen der Adressen auszuschalten. Ist das Lernen der Adressen ausgeschaltet, dann überträgt das Gerät alle Daten von allen Ports an alle Ports.

☐ Wählen Sie den Dialog `Switching:global`.

Heben Sie die Markierung „Adressen lernen“ auf, um die Daten aller Ports beobachten zu können.