**Spanning Tree Protocol (STP IEEE 802.1d)**

Das Spanning Tree Protocol dient zur Vermeidung redundanter Netzpfade (Schleifen) im LAN, speziell in geswitchten Umgebungen. In einem Netzwerk, mit mehreren, untereinander verbundenen Bridges kann es passieren, dass Frames, die zu einer unbekannten MAC geleitet werden sollen, unendlich lange im Kreis laufen.

Funktionsweise:

Zur Kommunikation zwischen den Switches wird das Bridge-Protokoll genutzt. Die Bezeichnung Switch ist abgeleitet von Bridge, da Switches die Weiterentwicklung der Bridge sind (Switches werden auch als Multiport-Bridges bezeichnet).

Die Pakete dieses Protokolls werden Bridge Protocol Data Unit (BPDU) genannt. Sie werden im Datenfeld eines Ethernet-Datenpaketes (Ethernet-Frame) per Broadcast an die benachbarten Switches versendet.

Zunächst wird unter den Spanning Tree fähigen Bridges im Netz eine sog. Root Bridge gewählt, die die „Chef” des Netzes wird. Dies geschieht, indem alle Bridges ihre Bridge-ID (die jede Bridge besitzt) an eine bestimmte Multicast-Gruppe mitteilen. Die Bridge ID ist 8 Byte lang (2 Bytes Bridge Priority und 6 Bytes MAC Adresse). Die Bridge mit der niedrigsten Priorität wird zur Root Bridge. Sollte die Bridge Priority identisch sein, wird als ergänzendes Kriterium die MAC Adresse der Komponenten benutzt (auch hier gewinnt wieder die Bridge mit der niedrigeren Zahl).

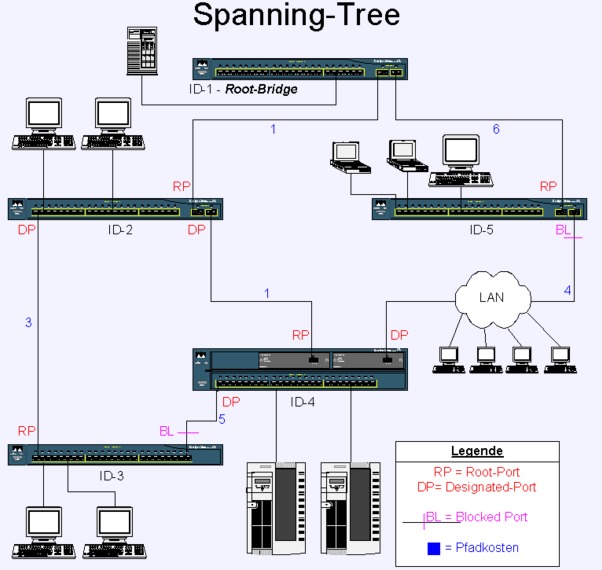
Von der Root Bridge aus werden nun Pfade festgelegt, über die die anderen Bridges im Netz erreichbar sind. Sind redundante Pfade vorhanden, so müssen die dortigen Bridges den entsprechenden Port deaktivieren. Die Pfade, über die kommuniziert werden darf, werden anhand von Pfadkosten bestimmt, die die dortige Bridge übermittelt.

Die Kosten sind abhängig vom Abstand zur Root Bridge und dem zur Verfügung stehenden Uplink zum Ziel. Ein 10 Mbit/s-Uplink hat üblicherweise höhere Pfadkosten als ein 100 Mbit/s-Uplink zum gleichen Ziel, der 10 Mbit Link würde daher als redundanter Pfad geblockt werden.

Die Pfadkosten sind nach IEEE-Vorgaben genormt, können aber manuell abweichend festgelegt werden, beispielsweise um bei gleicher Geschwindigkeit einen bevorzugten Uplink auszuwählen, um so die reellen Kosten von Standleitungen widerzuspiegeln. Auf diese Weise ist jedes Teilnetz im geswitchten LAN nur noch über eine einzige, die Designated Bridge, erreichbar. In der grafischen Darstellung ergibt sich ein Baum aus Netzpfaden, der dem Algorithmus sowie dem Protokoll seinen Namen gab.

Die Root Bridge teilt den in der Hierarchie eine Stufe unterhalb liegenden Designated Bridges im Abstand von zwei Sekunden mit, dass sie noch da ist, woraufhin die empfangende Designated Bridge ebenfalls an nachfolgende Bridges die entsprechende Information senden darf.

Wenn diese Hello-Pakete ausbleiben, hat sich folglich an der Topologie des Netzes etwas geändert, und das Netz muss sich reorganisieren. Diese Neuberechnung des Baumes dauert im schlimmsten Fall bis zu 30 Sekunden. Während dieser Zeit dürfen die Spanning-Tree fähigen Bridges außer Spanning-Tree-Informationen keine Pakete im Netz weiterleiten. Dies ist einer der größten Kritikpunkte am klassischen Spanning Tree Protokoll, da es möglich ist, mit gefälschten Spanning-Tree-Paketen eine Topologieänderung zu signalisieren und das gesamte Netz für bis zu 30 Sekunden lahmzulegen. Um diesen potenziellen Sicherheitsmangel zu beheben, aber auch um bei echten Topologieänderungen das Netz schnell wieder in einen benutzbaren Zustand zu bringen, wurden schon früh von verschiedenen Herstellern Verbesserungen an der Implementierung des Spanning Tree Protokolls bzw. der dazu verwendeten Algorithmen entwickelt. Eine davon, das Rapid Spanning Tree Protocol (RSTP), ist inzwischen zum offiziellen IEEE-Standard 802.1w geworden.

[](http://www.r33net.de/wp-uploads/2010/11/stp.jpg)

**STP Port Modi**  
-Listening – Lauscht auf Hello Nachrichten. Es werden keine MAC gelernt. Zwischending zwischen blocking und forwarding  
-Learning – Lauscht ebenfalls auf BPDUs, lernt MACs, leitet aber nicht weiter.  
-Disabled – Port ist down

**Optionale STP Features**

Etherchannel  
Etherchannel Verbindungen werden als einzelner Link betrachtet und können aus zwei bis 8 Verbindungen zwischen zwei Switches bestehen. Dadurch erhöht sich die Bandbreite und die Anzahl paralleler Verbindungen wird reduziert. Diese Verbindungen werden Trunks genannt. Alle Trunks sind im Etherchannel entweder im forwarding oder im blocking modus

PortFast  
PortFast versetzt einen Port, direkt nach dem aktivieren in den forwarding Modus. Da dies auf Ports, an denen Bridges hängen wenig Sinn macht, wird PortFast nur für die Ports aktiviert, an denen PCs, bzw. andere End-Geräte angeschlossen sind. Sie können eine Sicherung aktivieren, die PortFast deaktiviert, sobald ein BPDU eingeht.

**Spanning-Tree**  
Protokoll zum verhindern von Schleifen in geswitchten Netzwerken  
STP setzt die Ports entweder in einen FORWARD oder in einen BLOCKING Zustand  
FORWARD -> ist Teil des Spanning-Trees -> sendet und empfängt Frames  
BLOCKING -> sendet keine Frames und ignoriert eingehende Frames

[](http://www.r33net.de/wp-uploads/2010/11/stp2.jpg)  
STP verursacht, dass Frames längere Wege zurücklegen müssen  
großer Vorteil ist aber es entstehen keine Schleifen

**Funktionsweise STP**  
-Spanning-Tree-Algorithmus erstellt eine Baumstruktur, in der es immer nur einen Weg zu einem Segment (Kollisionsdomain) gibt  
-Da es nur einen Weg gibt, gibt es keine Schleifen  
-Es werden nur die Ports in den Spanning-Tree aufgenommen, die gebraucht werden (FORWARD), alle Anderen werden auf BLOCKING gesetzt.  
-Es gibt 3 Kriterien, wann ein Port auf FORWARD steht  
-STP wählt eine Root-Bridge (alle Ports auf FORWARD)  
D-er Port an den Non-Root-Bridges mit den geringsten administrativen Kosten zur Root-Bridge wird Root-Port (FORWARD)  
-Der Port zu einem Segment mit den geringsten administrativen Kosten zur Root-Bridge wird Designated-Port genannt (FORWARD)  
-Alle anderen Ports werden auf BLOCKING gesetzt

**Administrative Kosten (IEEE)**

|  |  |  |
| --- | --- | --- |
| Ethernet Speed | Original Kosten | Geänderte Kosten |
| 10 MBit/s | 100 | 100 |
| 100 MBit/s | 10 | 19 |
| 1 GBit/s | 1 | 4 |
| 10 GBit/s | 1 | 2 |

Diese Werte können auch pro Port verändert werden

**Befehle** (Cisco) In *Packet Tracer einige nicht verfügbar*.

|  |  |
| --- | --- |
| **Switch# show spanning-tree** | **zeigt Root-Bridge ID und Eigene-ID**  **zeigt die Timereinstellungen**  **zeigt den derzeitigen Portstatus (FWD;BLK)** |
| **Switch# show spanning-tree detail** | **Zeigt Infos zu Spanning-Tree pro Interface** |
| Switch# terminal monitor | Aktiviert die Ausgabe von Debug-Meldungen |
| Switch# debug spanning-tree events | Gibt Statusmeldungen aus, wenn die STP Topologie geändert wird |
| *Switch(config-if)# spanning-tree cost 2* | *Ändert die Kosten eines Interfaces* |
| **Switch(config)# spanning-tree vlan 1 root primary**  **Spanning-tree vlan 1 root secondary** | **Die Bridge/Switch wird Root-Bridge(die Priorität wird automatisch verringert)**  **Wird Root-Bridge bei Ausfall der Root-Bridge** |

**EtherChannel**

|  |  |
| --- | --- |
| Switch(config-if)#  channel-group 1 mode on | Fügt das Interface dem Port-Channel hinzu  (EtherChannels wird als Po1 dargestellt) |
| Switch# show etherchannel 1 summary | Zeigt den Status über den EtherChannel an.  welche Ports sind in dem EtherChannel |

**PortFast**

|  |  |
| --- | --- |
| Switch(config-if)#  switchport mode access | FastPort kann nur für Access-Link aktiviert werden |
| Switch(config-if)# spanning-tree portfast | Aktiviert PortFast für dieses Interface |

BPDU Guard

|  |  |
| --- | --- |
| Switch(config-if)#  bpduguard | Es werden keine bpdu Pakete angenommen.  Für access ports von Endgeräten |