

Publikation: HP Procurve Best Practice Spanning Tree
Dokumentenname: procure_best_practice_spanning_tree.pdf
Autor: Ingentive Networks GmbH
Version: 1.0

Nutzungsbedingungen

Die Nutzung, Vervielfältigung und Verbreitung dieser Publikation und von verbundenen Grafiken wird hiermit unter der Bedingung gestattet, dass der Urheberrechtshinweis auf allen Kopien erscheint und dass sowohl der Urheberrechtshinweis als auch dieser Zustimmungshinweis erscheinen. Alle sonstigen Rechte bleiben vorbehalten.

Der Name der Ingentive Networks GmbH darf im Zusammenhang mit der Verbreitung dieser Publikation durch Werbung oder sonstige Veröffentlichung, nur mit ausdrücklicher vorheriger schriftlicher Zustimmung verwendet werden.

Ingentive Networks GmbH übernimmt keine Gewähr für die Verwendbarkeit dieser Information zu irgendwelchen Zwecken. Diese Publikation wird so wie hier bestehend zugänglich gemacht, ohne jegliche Gewähr oder sonstige Verpflichtung. Jegliche Gewährleistung im Zusammenhang mit dieser Information und deren Verwendung, ausdrücklich oder stillschweigend, gesetzlich oder aus sonstigem Rechtsgrund (einschließlich der Gewährleistung für bestimmte Eigenschaften oder der Verwendbarkeit für einen bestimmten Zweck) ist ausgeschlossen.

Ingentive Networks GmbH haftet nicht für Bearbeitungsfehler oder Nutzungsausfall, entgangenen Gewinn oder erwartete ersparte Aufwendungen, Verlust des Firmenwerts (goodwill) oder Verlust von Daten oder Verträgen sowie für jegliche Art von indirekten Vermögens- oder Folgeschäden (einschließlich Schäden aufgrund von Ansprüchen Dritter), welche im Zusammenhang mit der Verwendung dieser Publikation entstehen.

Die Nutzung dieser Publikation ist unter den Bedingungen erlaubt, dass (1) der unten angeführte Copyright-Vermerk auf allen Kopien erscheint, und dass der Copyright-Vermerk und dieser Genehmigungsvermerk erscheinen, (2) die Dokumente dieser Web-Site nur zu informativischen, nichtkommerziellen oder privaten Zwecken genutzt und nicht über Computernetze oder sonstigen Medien veröffentlicht werden, und (3) die Dokumente nicht verändert werden. Die Nutzung zu anderen Zwecken erfordert eine explizite Genehmigung seitens Ingentive Networks GmbH

Diese Publikation kann technische Ungenauigkeiten oder typographische Fehler enthalten. Die darin enthaltenen Informationen werden regelmäßig verändert oder ergänzt. Die Ingentive Networks GmbH behält sich vor, jederzeit Änderungen und/oder Verbesserungen an einem oder mehreren der darin beschriebenen Produkte und/oder einem oder mehreren der Programme vorzunehmen.

„HP“, „Procurve“ und „Ingentive Networks“ sind eingetragene Warenzeichen.

Inhalt

1	Einleitung	3
2	Terminologie	3
2.1	IEEE Standard 802.1D-1998	4
2.2	IEEE 802.1w Rapid Spanning Tree	4
2.3	IEEE 802.1s Multiple Spanning Tree.....	4
3	Design.....	5
4	Implementierung bei HP	6
4.1	Konfiguration von 802.1D-1998.....	6
4.2	Konfiguration von Rapid Spanning Tree (RSTP)	7
4.3	Konfiguration von Multiple Instance Spanning Tree (MSTP)	8
4.4	Erweiterte Spanning Tree Konfiguration	11

1 Einleitung

Diese Publikation soll Netzwerkadministratoren bei der Planung und Implementierung des Spanning Tree Protokolls von HP ProCurve basierenden Netzwerkinfrastrukturen unterstützen. Die verwendeten Kommandos beziehen sich auf Geräte mit ProVision ASIC und K.14.xx Firmware Version. Die Kommandos und Ausgaben auf anderen Switches können geringfügig abweichen.

2 Terminologie

Beim Aufbau von redundanten Netzwerkinfrastrukturen, die auf Ethernet Technologie basieren ist es wichtig, dass ein geeigneter Mechanismus existiert, der die redundanten Pfade kontrolliert, für Nutzdaten blockiert und nur im Fehlerfall aktiviert. Zu diesem Zweck kommt das Spanning Tree Protokoll zum Einsatz. Dieses Protokoll wurde bereits in mehreren Version von der internationalen Standardisierungsbehörde IEEE als Standard verabschiedet und ist somit von vielen Herstellern implementiert worden.

Die Kommunikation basiert auf einem OSI Schicht 2 Protokoll Datenpaketen, den sog. **Bridge PDU**.

Grundlage für alle Spanning Tree Protokolle ist ein Algorithmus, der als Resultat hat, dass eine eindeutige Netzwerkstruktur erzeugt wird. Eindeutig bedeutet in diesem Zusammenhang, dass zwischen zwei beliebigen Punkten im Netzwerk genau ein Pfad existiert. Die resultierende Netzwerkstruktur hat die Ähnlichkeit mit einem Baum, da die Topologie von einem zentralen Punkt im Netzwerk aus errechnet wird. Dieser zentrale Punkt wird als **Root Bridge** bezeichnet und kann per Konfiguration festgelegt werden.

Bild 1 zeigt eine von Spanning Tree kontrollierte Infrastruktur, in der Switch 1 als Root Bridge festgelegt wurde und den zentralen Ausgangspunkt für die Topologie darstellt.

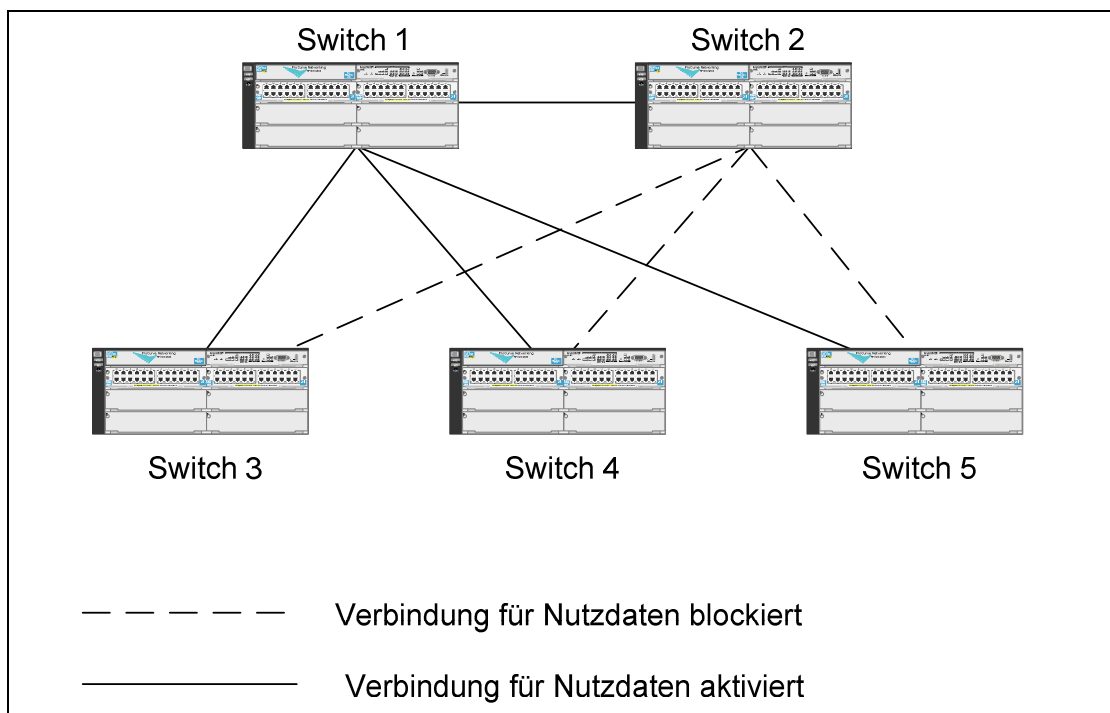


Abbildung 1

Die Entscheidung des Algorithmusses welche Pfade für Daten offen und welche blockiert werden, erfolgt anhand eines Prioritätenmodells, bei dem auch die Bandbreiten der Verbindungen in Betracht gezogen werden. Primäre Entscheidungsgrundlage für die Bevorzugung eines Ports vor einem anderen, sind die sog. **Port Kosten**. Diese werden anhand einer voreingestellten Tabelle von der Bandbreite abgeleitet, kann aber auch pro Port konfiguriert werden. Abhängig von den Port Kosten und Prioritäten werden innerhalb des Algorithmusses sog. **Port Rollen** vergeben. Je nach Port Rolle wird dann entschieden, in welchem Status ein Port geführt wird. Mögliche Port Status kann **Blocking** oder **Forwarding** sein

Weitere Eigenschaft des Spanning Tree Protokolls ist die Aktivierung von blockierten Ports. Dies ist notwendig, wenn beispielsweise ein Fehler bei einer Verbindung auftritt und eine vormal aktive Verbindung nicht mehr zur Verfügung steht. Die Zeit, die benötigt wird, um nach einem eingetretenen Fehlerfall wieder eine stabile Topologie herzustellen nennt man **Konvergenzzeit**.

2.1 IEEE Standard 802.1D-1998

Dieser Standard aus dem Jahre 1998 ist die erstmalig standardisierte Spanning Tree Version. Dieser Standard ist auf den meisten Hersteller noch implementiert besitzt aber aus heutiger Sicht einige Nachteile. Größtes Manko ist die relative hohe Konvergenzzeit von mindestens 40 Sekunden. Weiterhin ist eine Skalierung zwischen höheren Bandbreiten (1 und 10 Gigabit) nur schlecht möglich, da nur 16 Bit zur Darstellung der Port Kosten zur Verfügung stehen.

2.2 IEEE 802.1w Rapid Spanning Tree

Dieser Standard adressiert die im 802.1D bekannten Probleme und verkürzt die Konvergenzzeit auf wenige Sekunden. Durch die Implementierung neuer Port Rollen ist es auch möglich Konvergenzzeiten von weniger als einer Sekunde zu erreichen. Eine weitere Verbesserung ist die bessere Unterscheidbarkeit zwischen den Bandbreiten, da das Feld für die Port Kosten auf 32 Bit erhöht wurde. Die Kosten und veränderten Timer sind in einem separaten Standard definiert (802.1t). Alle relevanten Rapid Spanning Tree Standards wurden im Jahre 2004 wieder dem 802.1D-2004 Standard zugeführt.

2.3 IEEE 802.1s Multiple Spanning Tree

Dieser Standard ist eine Weiterentwicklung des Spanning Tree Standards und ist dem IEEE 802.1Q Standard angelehnt. Es adressiert die Problematik, dass beim herkömmlichen Spanning Tree bzw. RSTP redundante immer für Nutzdaten blockiert werden und diese Verbindungen nur im Fehlerfall aktiv sind. Multiple Spanning Tree kann diese Restriktion auflösen, da sich mehrere Topologien errechnen lassen und somit der Datenverkehr auf die redundanten Pfade aufgeteilt werden kann. Voraussetzung für eine derartige Konfiguration ist der Einsatz von VLANs. Diese VLAN werden in einer geeigneten Form zu sog. **Instanzen** zusammengefasst. Dieser Instanz kann dann eine Topologie zugeordnet werden. Neben der Zuordnung der Instanzen zu den jeweiligen VLANs müssen noch weitere Konfigurationsparameter festgelegt werden. Dazu gehört die sog. **MST Region Name** und die **Revision Nummer**. Diese Parameter lassen miteinander kommunizierende Switches erkennen, ob ein Nachbar zu einen gemeinsamen Konfigurationssatz besitzt und zu einer sog. **Region** gehört, denn nur dann lässt sich für jede Instanz eine eindeutige Topologie errechnen.

Um Abwärtskompatibilität zu Nicht-MSTP fähigen Switches zu gewährleisten gibt es immer eine nicht abschaltbare Instanz 0, die sog. **Internal Spanning Tree (IST)**

3 Design

Beim Design von redundanten Netzwerken ist die Wahl der Spanning Tree Protokoll Version ein wichtiger Parameter, da nachträgliche Änderungen der Protokoll Versionen nur mit Wartungsfenstern verbunden sind und erheblichen Aufwand nach sich ziehen. Daher ist es wichtig die Planung für die Wahl der Protokoll Version und auch die entsprechenden Parameter im Vorfeld durchzuführen.

Generelle Empfehlung bezüglich der Protokoll Versionen gibt es nicht. Es lassen sich nur die Vor und Nachteile der einzelnen Versionen herausstellen. Aufgrund der beschriebenen Nachteile des alten 802.1D Spanning Tree Protokolls und der Tatsache, dass RSTP abwärtskompatibel zu dieser Version ist, kann man in jedem Fall RSTP einsetzen. Diese Version kommt auch immer dann zum Einsatz, wenn das Netzwerk möglichst einfach gestaltet werden soll. Weiterhin macht es Sinn wenn die Anzahl der VLANs gering ist, so dass sich eine gleichmäßige Aufteilung in mehrere Instanzen nicht ergibt.

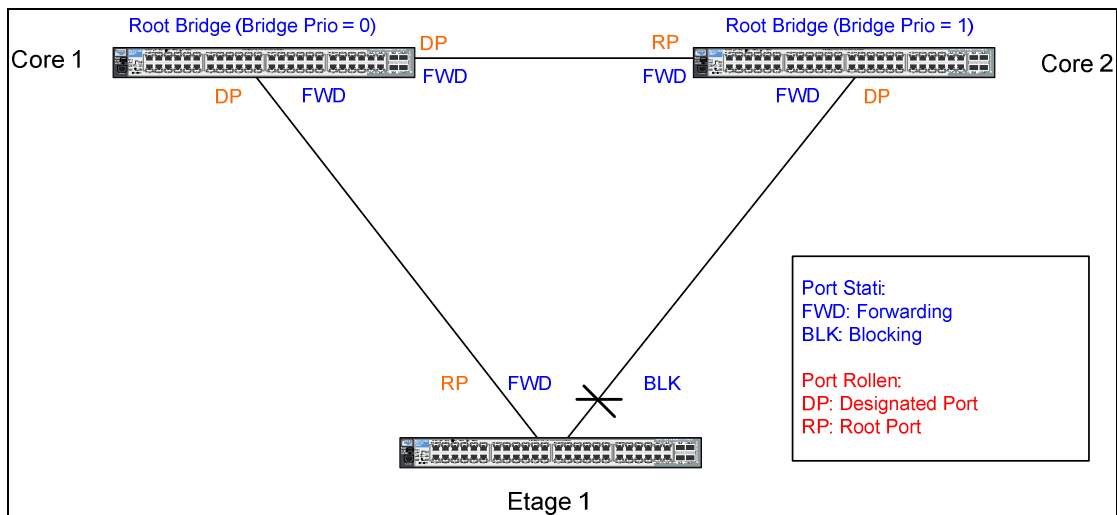
Dahingegen macht sich in größeren Umgebungen der Einsatz von MSTP bezahlt, da wie beschrieben die VLANs auf Instanzen aufgeteilt werden können und die Infrastruktur besser ausgenutzt werden kann. Es muss allerdings eine hinreichend große Anzahl an VLANs existieren, so dass der zusätzliche Aufwand sich lohnt. Weiterhin darf nicht unerwähnt bleiben, dass der Einsatz von MSTP eine zusätzliche Komplexität in der Netzwerk Konfiguration verursacht und diese auch vom Betriebspersonal beherrscht werden muss.

Bei der Auswahl der Root Bridge ist zu erwähnen, dass diese immer eine möglichst zentrale Komponente im Netzwerk sein soll und die Root Bridge in jedem Fall per Konfiguration der Bridge Priorität festgelegt werden sollte. Wird dies versäumt, so wird der Switch mit der geringsten MAC Adresse als Root Bridge festgelegt - also eine zufällige Wahl. Um der Situation Rechnung zu tragen, dass die Root Bridge auch ausfallen kann, ist es empfehlenswert immer eine zweite Root Bridge festzulegen, die diese Rolle übernehmen kann. Für die Auswahl der zweiten Root Bridge gelten die gleichen Kriterien.

4 Implementierung bei HP

4.1 Konfiguration von 802.1D-1998

In der Praxis spielt diese Version nur noch selten eine Rolle, wird aber der Vollständigkeit wegen erwähnt. In der folgenden Beispielkonfiguration soll die Topologie gemäß Abbildung 2 konfiguriert werden. Alle Querverbindungen sind Gigabit Verbindungen.



Auf Core 1 wird die Bridge Priorität auf 0 gesetzt, um sicherzustellen, dass dieser die Root Bridge wird:

```
Core1(config)# spanning-tree force-version stp-compatible
Core1(config)# spanning-tree priority 0
Core1(config)# spanning-tree legacy-path-cost
Core1(config)# spanning-tree
```

Auf Core 2 wird die Bridge Priorität auf 1 gesetzt, um sicherzustellen, dass dieser Root Bridge wird im Falle eines Ausfalls von Core 1

```
Core2(config)# spanning-tree force-version stp-compatible
Core2(config)# spanning-tree priority 1
Core2(config)# spanning-tree legacy-path-cost
Core2(config)# spanning-tree
```

Die Bridge Priorität auf allen anderen Switches muss nicht geändert werden. Sie beträgt 8.

```
Etage1(config)# spanning-tree force-version stp-compatible
Etage1(config)# spanning-tree legacy-path-cost
Etage1(config)# spanning-tree
```

4.2 Konfiguration von Rapid Spanning Tree (RSTP)

Bei der Konfiguration des RSTP kommen die gleichen Kommandos zum Einsatz. Es muss lediglich die Protokoll Version verändert werden:

```
Core1(config)# spanning-tree force-version rstp-operation
Core1(config)# spanning-tree priority 0
Core1(config)# spanning-tree
```

```
Core2(config)# spanning-tree force-version rstp-operation
Core2(config)# spanning-tree priority 1
Core2(config)# spanning-tree
```

```
Etage1(config)# spanning-tree force-version rstp-operation
Etage1(config)# spanning-tree
```

Die Überprüfung der Konfiguration kann mit folgenden Kommandos durchgeführt werden:

```
Core1(config)# sh spanning-tree | ex Disa
```

Multiple Spanning Tree (MST) Information

STP Enabled : Yes
Force Version : RSTP-operation
IST Mapped VLANs : 1-4094
Switch MAC Address : 0017a4-88dd80
Switch Priority : 0
Max Age : 20
Max Hops : 20
Forward Delay : 15

Topology Change Count : 36
Time Since Last Change : 2 mins

CST Root MAC Address : 0017a4-88dd80
CST Root Priority : 0
CST Root Path Cost : 0
CST Root Port : This switch is root

Annotations:
= „Exclude Disabled“ zeigt nur aktive Ports an
Switch arbeitet im RSTP Modus
Bridge Priority
Zeigt an, dass dieser Switch die Root Bridge ist

Port	Type	Cost	Prio rity	State	Designated Bridge	Hello Time	PtP	Edge
21	100/1000T	200000	128	Forwarding	0017a4-88dd80	2	Yes	Yes
Trk1		20000	64	Forwarding	0017a4-88dd80	2	Yes	No
Trk10		10000	64	Forwarding	0017a4-88dd80	2	Yes	No

```

Etage1# sh spanning-tree | ex Disa
Multiple Spanning Tree (MST) Information

STP Enabled      : Yes
Force Version    : RSTP-operation
IST Mapped VLANs : 1-4094
Switch MAC Address : 001635-b3ac40
Switch Priority   : 32768
Max Age          : 20
Max Hops         : 20
Forward Delay    : 15

Topology Change Count : 49
Time Since Last Change : 4 mins

CST Root MAC Address : 0017a4-88dd80
CST Root Priority     : 0
CST Root Path Cost   : 20000
CST Root Port        : Trk1

IST Regional Root MAC Address : 001635-b3ac40
IST Regional Root Priority     : 32768
IST Regional Root Path Cost    : 0
IST Remaining Hops             : 20

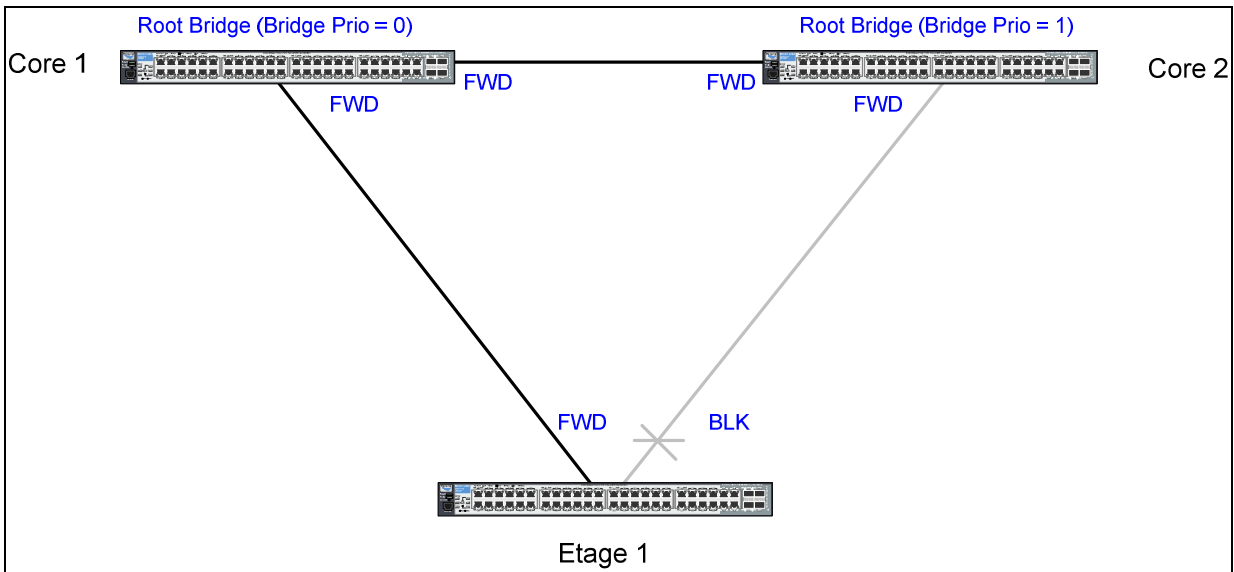
```

= „Exclude Disabled“ zeigt nur aktive Ports an
 Switch arbeitet im RSTP Modus
 Anzahl der Topologieänderungen
 Nächster Port zur Root Bridge
 Switch Ports (Edge = No)
 Endgeräteports (Edge = Yes)

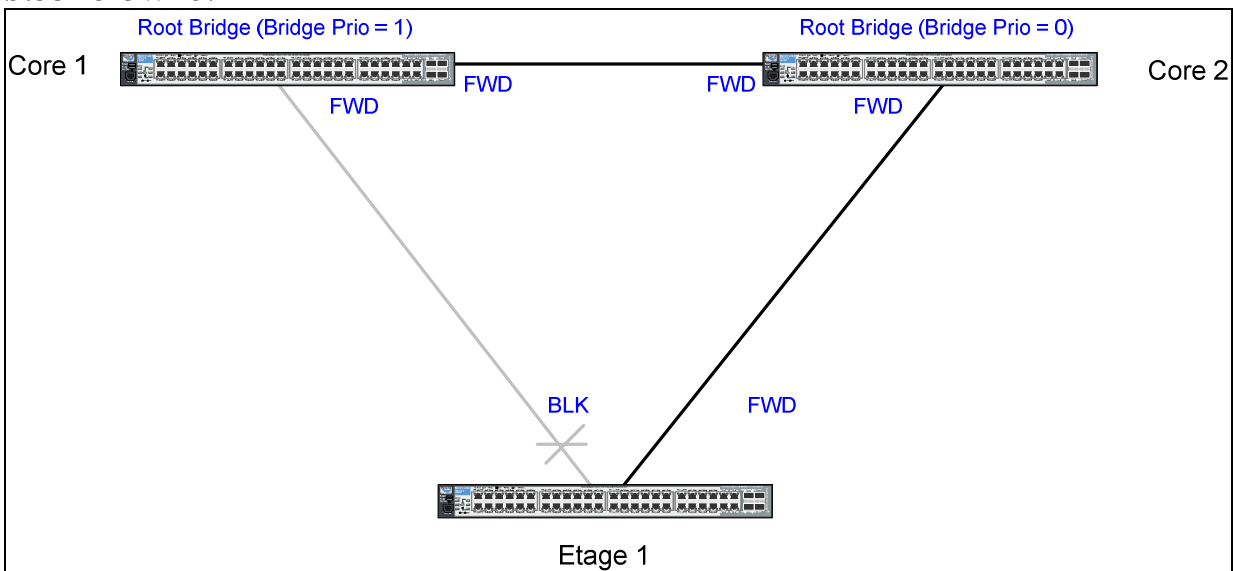
Port	Type	Cost	Priority	State	Designated Bridge	Hello Time	PtP	Edge
1	100/1000T	200000	128	Forwarding	001635-b3ac40	2	Yes	Yes
13	100/1000T	20000	128	Forwarding	001635-b3ac40	2	Yes	Yes
15	100/1000T	20000	128	Forwarding	001635-b3ac40	2	Yes	Yes
Trk1		20000	64	Forwarding	0017a4-88dd80	2	Yes	No
Trk2		20000	64	Blocking	0016b9-6d3b40	2	Yes	No

4.3 Konfiguration von Multiple Instance Spanning Tree (MSTP)

In folgendem Beispiel wird für alle ungeraden VLANs eine Instanz 1 erstellt, für die die Topologie folgendermaßen aussieht:



Der Instanz 2 werden alle geraden VLANs zugeordnet und durch Verlegung der Root Bridge von Core1 auf Core2 wird erreicht, dass der Pfad zwischen Core1 und Etage1 blockiert wird:



Konfiguration auf ALLEN Switches, die am MSTP teilnehmen wollen (Region):

```
spanning-tree force-version mstp-operation
```

StandardEinstellung bei allen neuen ProCurve Switches und taucht daher nicht in der Konfiguration auf

```
spanning-tree config-name "INGENTIVE"
spanning-tree config-revision 1
spanning-tree instance 1 vlan 11 13 15
spanning-tree instance 2 vlan 10 12 14
```

Config-Name, Revision und Instanzen müssen auf allen MST Switches identisch sein!

```
Core1(config)# spanning-tree priority 0
Core1(config)# spanning-tree instance 1 priority 0
Core1(config)# spanning-tree instance 2 priority 1
Core1(config)# spanning-tree
```

```
Core2(config)# spanning-tree priority 1
Core2(config)# spanning-tree instance 1 priority 1
Core2(config)# spanning-tree instance 2 priority 0
Core2(config)# spanning-tree
```

```
Etagel# sh spanning-tree mst-config
```

MST Configuration Identifier Information

```
MST Configuration Name : INGENTIVE
MST Configuration Revision : 1
MST Configuration Digest : 0x16B221B577C2197D1BD49C3A72DEF82B
```

```
IST Mapped VLANs : 1-9,16-4094
```

Instance ID Mapped VLANs

```
-----
1          11,13,15
2          10,12,14
```

Hashwert muss auf allen MST Switches identisch sein. Wird aus folgenden Parametern gebildet:

- Configuration Name,
- Revision Nummer
- Instanz - VLAN Zuordnung

```
Etagel# sh spanning-tree instance 1 | ex Disa
```

MST Instance Information

```
Instance ID : 1
Mapped VLANs : 11,13,15
Switch Priority : 32768
```

```
Topology Change Count : 14
Time Since Last Change : 5 mins
```

```
Regional Root MAC Address : 0017a4-88dd80
Regional Root Priority : 0
Regional Root Path Cost : 20000
Regional Root Port : Trk1
Remaining Hops : 19
```

Port	Type	Cost	Priority	Role	State	Designated Bridge
1	100/1000T	200000	0	Designated	Forwarding	001635-b3ac40
13	100/1000T	20000	0	Designated	Forwarding	001635-b3ac40
15	100/1000T	20000	0	Designated	Forwarding	001635-b3ac40
Trk1		20000	0	Root	Forwarding	0017a4-88dd80
Trk2		20000	0	Alternate	Blocking	0016b9-6d3b40

Ausgabe der Spanning Tree Information erfolgt hier für jede Instanz separat. Zur Instanz 1 sind die VLANs 11, 13 und 15 zugeordnet.

4.4 Erweiterte Spanning Tree Konfiguration

BPDU Protection

Das Spanning Tree Protokoll beinhaltet keine Überprüfung ob ein benachbarter Spanning Tree Switch auch berechtigt ist Spanning Tree Informationen zu schicken. Um Fehlkonfigurationen oder mutwilligen Angriffen vorzubeugen, sollte man auf den Ports, an denen man keine Spanning Tree Geräte angeschlossen hat, eine Absicherung einbauen. Diese Funktionalität nennt man BPDU Protection und dient dazu einen Port abzuschalten, sobald eine Spanning Tree PDU entdeckt wird.

```
spanning-tree 1-20 bpdu-protection
spanning-tree bpdu-protection-timeout 300
```

Versehentlich wird ein Kabel auf 3 und 5 gesteckt:

```
I 08/10/09 16:13:42 00435 ports: port 3 is Blocked by STP
I 08/10/09 16:13:42 00435 ports: port 5 is Blocked by STP
I 08/10/09 16:13:42 00840 stp: port 5 disabled - BPDU received on protected
port.
I 08/10/09 16:13:42 00840 stp: port 3 disabled - BPDU received on protected
port.
I 08/10/09 16:13:42 00898 ports: BPDU protect(5) has disabled port 5 for 0
seconds
I 08/10/09 16:13:42 00898 ports: BPDU protect(5) has disabled port 3 for 0
seconds
I 08/10/09 16:13:43 00077 ports: port 5 is now off-line
I 08/10/09 16:13:43 00077 ports: port 3 is now off-line
```

```
Etagel(config)# sh spanning-tree
```

...

Port	Type	Cost	Prio rity	State	Designated Bridge	Hello Time	PtP	Edge
1	100/1000T	200000	128	Forwarding	001635-b3ac40	2	Yes	Yes
2	100/1000T	Auto	128	Disabled				
3	100/1000T	20000	128	BpduError		2	Yes	No
4	100/1000T	Auto	128	Disabled				
5	100/1000T	20000	128	BpduError		2	Yes	No

Best Practice: Konfigurieren Sie BPDU Protection auf allen Endgeräte Ports. Somit verhindern Sie, dass versehentlich STP fähige Switches kaskadiert werden und das Netzwerk stören.

Admin Edge Port

In der Standardeinstellung ist jeder Port in der sog. „Auto Edge“ Modus eingestellt. Das bedeutet, dass der Switch versucht zu erkennen um was für einen Port es sich handelt:

Edge Port: An diesem Port ist kein Spanning Tree fähiges Gerät angeschlossen

Non Edge Port: An diesem Port ist ein Spanning Tree fähiges Geräte angeschlossen

Zur Erkennung wartet der Switch in der Regel 3 Sekunden auf eingehende BPDUs. Werden innerhalb dieser Zeit keine empfangen, wird der Port auf „Edge“ Port

eingestellt. Innerhalb dieser 3 Sekunden ist der Port für Nutzdaten blockiert. Um diese 3 Sekunden zu umgehen, kann man den Port fest auf Admin Edge einstellen:

```
spanning-tree 1-20 admin-edge-port
```

Best Practice: Konfigurieren Sie das Admin Edge Feature auf allen Endgeräte Ports wo Sie keine Spanning Tree fähigen Switches erwarten. Dies beschleunigt das Zustandekommen einer Netzwerkverbindung jedes Ports um ca. 3 Sekunden.