5.6 STP, Schleifen und Broadcast-Stürme

Auf OSI-Schicht 2 können Schleifen besonders gefährlich sein.

Eine Schleife entsteht, wenn es in einem Switch-Netz mehrere aktive Wege gibt, über die Frames endlos im Kreis laufen können.

Das kann dazu führen, dass ein Netzwerk sehr schnell überlastet wird.

Merksatz:

```
Layer-2-Schleifen können ein Netzwerk lahmlegen.
```

Warum sind Schleifen auf Schicht 2 gefährlich?

Auf Schicht 3 gibt es bei IP-Paketen ein Feld, das die Lebensdauer begrenzt.

Dieses Feld heißt:

```
TTL
```

TTL steht für:

```
Time To Live
```

Bei Ethernet-Frames auf Schicht 2 gibt es so eine Begrenzung nicht in gleicher Weise.

Das bedeutet:

```
Ein Frame kann bei einer Schleife immer wieder weitergeleitet werden.
```

Dadurch kann ein Netzwerk überlastet werden.

Merksatz:

```
Ethernet-Frames haben keine TTL wie IP-Pakete.
```

Begriff: Schleife

Eine Schleife im Netzwerk bedeutet:

```
Es gibt einen Kreisweg,
über den Frames immer wieder weitergeleitet werden können.
```

Beispiel:

```
Switch A
→ Switch B
→ Switch C
→ zurück zu Switch A
```

Wenn alle Verbindungen aktiv sind und keine Schutzmechanismen greifen, können Frames im Kreis laufen.

Merksatz:

```
Schleife = Frames können im Kreis laufen.
```

Wie entsteht eine Layer-2-Schleife?

Eine Schleife kann entstehen durch:

```
- doppelte Switch-Verbindungen
- falsch gesteckte Kabel
- redundante Leitungen ohne STP
- falsch konfigurierte Switches
- falsche Trunk-Konfiguration
- versehentlich verbundenes Patchkabel
- mehrere Wege zwischen denselben Switches
```

Beispiel:

```
Ein Mitarbeiter steckt versehentlich zwei Netzwerkdosen mit einem Patchkabel zusammen.
```

Oder:

Zwei Switches werden mehrfach verbunden,
ohne dass STP aktiv ist.

Merksatz:

Schleifen entstehen oft durch redundante oder falsch gesteckte Verbindungen.

Warum baut man überhaupt redundante Verbindungen?

Redundanz bedeutet:

Es gibt einen zusätzlichen Ersatzweg.

Das ist grundsätzlich sinnvoll.

Wenn eine Verbindung ausfällt, kann eine andere Verbindung übernehmen.

Beispiel:

Switch A ist über zwei Wege mit Switch B verbunden.

Vorteil:

höhere Ausfallsicherheit

Problem:

Ohne Schutzmechanismus kann daraus eine Schleife entstehen.

Merksatz:

Redundanz ist gut,
aber auf Schicht 2 muss sie kontrolliert werden.

Folgen einer Layer-2-Schleife

Eine Layer-2-Schleife kann schwere Folgen haben.

Typische Auswirkungen:

- Broadcast-Sturm
- sehr hohe Switch-Last
- volle Netzwerkbandbreite
- instabile MAC-Adresstabelle
- Paketverluste
- hohe Latenz
- Verbindungsabbrüche
- Netzwerk kaum noch nutzbar
- Dienste nicht erreichbar

Merksatz:

Eine kleine Schleife kann ein ganzes LAN stören.

Broadcast-Sturm

Ein Broadcast-Sturm entsteht, wenn sehr viele Broadcast-Frames im Netzwerk unterwegs sind.

Bei einer Schleife können Broadcasts immer wieder weitergeleitet werden.

Da Broadcasts an alle Ports im VLAN gesendet werden, vervielfachen sie sich sehr schnell.

Typische Broadcasts sind zum Beispiel:

- ARP-Anfragen
- DHCP-Anfragen
- bestimmte lokale Suchdienste

Merksatz:

Broadcast-Sturm = zu viele Broadcasts im lokalen Netz.

Warum vervielfachen sich Broadcasts?

Ein Switch leitet Broadcasts innerhalb eines VLANs an alle passenden Ports weiter.

Wenn eine Schleife vorhanden ist, kann derselbe Broadcast über mehrere Wege zurückkommen.

Dann wird er erneut verteilt.

Das kann sich schnell aufschaukeln.

Vereinfacht:

```
Broadcast kommt rein.
Switch verteilt ihn.
Broadcast kommt über anderen Weg zurück.
Switch verteilt ihn wieder.
```

Merksatz:

```
In einer Schleife können Broadcasts immer wieder neu verteilt werden.
```

Unicast-Flooding durch Schleifen

Nicht nur Broadcasts können problematisch sein.

Auch unbekannte Unicast-Frames können geflutet werden.

Unbekannter Unicast bedeutet:

```
Ziel-MAC ist dem Switch nicht bekannt.
```

Dann sendet der Switch den Frame an mehrere Ports.

Wenn zusätzlich eine Schleife besteht, kann auch dieser Verkehr stark zunehmen.

Merksatz:

```
Schleifen verstärken Broadcasts und unbekannten Unicast-Verkehr.
```

MAC-Adresstabelle wird instabil

Switches lernen MAC-Adressen über die Quell-MAC-Adresse eingehender Frames.

Bei einer Schleife kann derselbe Frame über verschiedene Ports wieder auftauchen.

Dadurch kann der Switch glauben:

```
dieselbe MAC-Adresse ist plötzlich an einem anderen Port erreichbar.
```

Die MAC-Adresse „wandert“ dann ständig in der Tabelle.

Das nennt man häufig:

```
MAC Flapping
```

Merksatz:

```
MAC Flapping = dieselbe MAC-Adresse erscheint ständig an wechselnden Ports.
```

Begriff: MAC Flapping

MAC Flapping bedeutet:

```
Eine MAC-Adresse wird vom Switch immer wieder an unterschiedlichen Ports gelernt.
```

Mögliche Ursachen:

```
- Layer-2-Schleife
- falsch verkabelte Switches
- fehlerhafte Redundanz
- falsch konfigurierte Link Aggregation
- virtuelle Systeme mit wechselnden Pfaden
```

In vielen Fällen ist MAC Flapping ein ernstes Warnsignal.

Merksatz:

```
MAC Flapping kann auf eine Schleife hinweisen.
```

STP

STP steht für:

```
Spanning Tree Protocol
```

STP ist ein Protokoll, das Schleifen in Layer-2-Netzen verhindern soll.

Die Grundidee:

```
Es darf nur ein schleifenfreier aktiver Pfad bestehen.
```

Redundante Pfade werden nicht entfernt, sondern blockiert.

Wenn eine aktive Verbindung ausfällt, kann ein blockierter Ersatzweg freigeschaltet werden.

Merksatz:

```
STP verhindert Layer-2-Schleifen.
```

Warum heißt es Spanning Tree?

Spanning Tree bedeutet sinngemäß:

```
aufspannender Baum
```

Ein Baum hat in der Netzwerktopologie keine Schleifen.

STP berechnet aus einem vermaschten Switch-Netz eine schleifenfreie Baumstruktur.

Vereinfacht:

```
Viele mögliche Wege
werden auf
einen schleifenfreien aktiven Weg reduziert.
```

Merksatz:

```
STP macht aus einem vermaschten Netz einen schleifenfreien Baum.
```

Grundprinzip von STP

STP arbeitet vereinfacht so:

1. Switches tauschen STP-Informationen aus.
2. Eine Root Bridge wird bestimmt.
3. Jeder Switch berechnet seinen besten Weg zur Root Bridge.
4. Bestimmte Ports bleiben aktiv.
5. Andere Ports werden blockiert, um Schleifen zu verhindern.

Merksatz:

STP entscheidet,
welche Ports weiterleiten und welche blockieren.

Root Bridge

Die Root Bridge ist der zentrale Bezugspunkt im STP-Netz.

Alle Switches berechnen ihre Wege zur Root Bridge.

Die Root Bridge wird anhand einer Priorität und der Bridge-ID bestimmt.

In der Praxis sollte man die Root Bridge gezielt planen.

Warum?

Sonst kann ein ungeeigneter Switch Root Bridge werden.

Merksatz:

Root Bridge = zentraler Bezugspunkt für STP.

Bridge-ID

Die Bridge-ID dient zur Auswahl der Root Bridge.

Sie besteht vereinfacht aus:

- Bridge-Priorität
- MAC-Adresse des Switches

Der Switch mit der niedrigsten Bridge-ID wird Root Bridge.

Wenn die Priorität gleich ist, entscheidet die MAC-Adresse.

Merksatz:

```
Niedrigste Bridge-ID gewinnt die Root-Bridge-Wahl.
```

STP-Priorität

Die STP-Priorität beeinflusst, welcher Switch Root Bridge wird.

Ein niedrigerer Prioritätswert ist besser.

Beispiel:

```
Switch A Priorität 4096
Switch B Priorität 32768
```

Switch A hat die bessere Priorität und wird eher Root Bridge.

Merksatz:

```
Niedrigere STP-Priorität = bevorzugte Root Bridge.
```

BPDU

BPDU steht für:

```
Bridge Protocol Data Unit
```

BPDUs sind STP-Nachrichten zwischen Switches.

Über BPDUs tauschen Switches Informationen aus, zum Beispiel:

```
- Bridge-ID
- Root-Bridge-Information
- Pfadkosten
- Portinformationen
```

Merksatz:

```
BPDU = STP-Nachricht zwischen Switches.
```

Root Port

Ein Root Port ist der Port eines Switches mit dem besten Weg zur Root Bridge.

Jeder Nicht-Root-Switch hat normalerweise genau einen Root Port.

Dieser Port zeigt aus Sicht des Switches in Richtung Root Bridge.

Merksatz:

```
Root Port = bester Weg zur Root Bridge.
```

Designated Port

Ein Designated Port ist ein Port, der in einem Netzwerksegment Frames weiterleiten darf.

Für jedes Segment wird ein Port ausgewählt, der den Verkehr Richtung Root Bridge beziehungsweise in das Segment weiterleitet.

Merksatz:

```
Designated Port = aktiver Weiterleitungsport für ein Segment.
```

Blocked Port

Ein Blocked Port ist ein Port, der durch STP blockiert wird, um eine Schleife zu verhindern.

Ein blockierter Port leitet keine normalen Datenframes weiter.

Er kann aber weiterhin STP-Informationen empfangen.

Wenn eine aktive Verbindung ausfällt, kann ein blockierter Port später aktiv werden.

Merksatz:

```
Blocked Port = verhindert Schleifen.
```

STP-Portrollen kurz zusammengefasst

Rolle	Bedeutung
Root Port	bester Weg zur Root Bridge
Designated Port	aktiver Port für ein Segment
Blocked Port	blockierter Port zur Schleifenvermeidung

Merksatz:

> Root und Designated leiten weiter.
> Blocked verhindert Schleifen.

STP-Portzustände

Klassisches STP kennt verschiedene Portzustände.

Wichtige Zustände sind:

Zustand	Bedeutung
Blocking	keine Nutzdatenweiterleitung
Listening	hört STP-Informationen
Learning	lernt MAC-Adressen
Forwarding	leitet Frames weiter
Disabled	administrativ oder technisch deaktiviert

Für die Prüfung reicht oft:

> Forwarding = leitet Frames.
> Blocking = blockiert zur Schleifenvermeidung.

Merksatz:

> STP-Ports leiten nicht sofort weiter,
> sondern durchlaufen Zustände.

RSTP

RSTP steht für:

```
Rapid Spanning Tree Protocol
```

RSTP ist eine schnellere Weiterentwicklung von STP.

Es reagiert schneller auf Änderungen im Netzwerk.

Technische Bezeichnung:

```
IEEE 802.1w
```

Vorteil:

```
schnellere Umschaltung bei Ausfall einer Verbindung
```

Merksatz:

```
RSTP = schnelleres STP.
```

MSTP

MSTP steht für:

```
Multiple Spanning Tree Protocol
```

MSTP ermöglicht mehrere Spanning-Tree-Instanzen.

Das ist besonders nützlich bei VLANs.

Technische Bezeichnung:

```
IEEE 802.1s
```

Für AP1/AP2 reicht meistens:

```
MSTP ist eine Erweiterung für mehrere VLAN- oder Instanz-Bereiche.
```

Merksatz:

MSTP = mehrere Spanning Trees für größere VLAN-Umgebungen.

STP, RSTP und MSTP im Vergleich

Protokoll	Bedeutung	Grundidee
STP	Spanning Tree Protocol	Schleifen verhindern
RSTP	Rapid Spanning Tree Protocol	schneller reagieren
MSTP	Multiple Spanning Tree Protocol	mehrere Instanzen unterstützen

Merksatz:

STP verhindert Schleifen.
RSTP ist schneller.
MSTP ist flexibler für VLAN-Umgebungen.

STP und Redundanz

STP ermöglicht Redundanz ohne Schleifen.

Beispiel:

Switch A ist über zwei Wege mit Switch B verbunden.

STP blockiert einen Weg.

Wenn der aktive Weg ausfällt, kann STP den blockierten Weg aktivieren.

Vorteil:

Ausfallsicherheit

Nachteil:

nicht alle redundanten Wege werden gleichzeitig genutzt

Merksatz:

STP blockiert Reservewege,
bis sie gebraucht werden.

STP und Link Aggregation unterscheiden

STP und Link Aggregation werden manchmal verwechselt.

Link Aggregation bündelt mehrere physische Verbindungen zu einer logischen Verbindung.

STP blockiert dagegen redundante Schleifenwege.

Technik	Aufgabe
STP	Schleifen verhindern
Link Aggregation	mehrere Links logisch bündeln

Wichtig:

Werden mehrere Kabel zwischen zwei Switches genutzt,
sollte klar sein,
ob sie als Link Aggregation konfiguriert sind
oder ob STP eingreifen muss.

Merksatz:

Link Aggregation bündelt.
STP blockiert Schleifen.

Link Aggregation kurz erklärt

Link Aggregation bedeutet:

mehrere physische Verbindungen werden zu einer logischen Verbindung zusammengefasst.

Vorteile:

- mehr Gesamtkapazität
- Redundanz

```
- weniger STP-Blockierung zwischen denselben Geräten
```

Häufige Begriffe:

```
- LAG
- Port Channel
- EtherChannel
- Bündelung
```

Merksatz:

```
Link Aggregation = mehrere Kabel als ein logischer Link.
```

LACP

LACP steht für:

```
Link Aggregation Control Protocol
```

LACP ist ein Protokoll zur automatischen Aushandlung von Link Aggregation.

Technische Bezeichnung:

```
IEEE 802.3ad
```

Für AP1/AP2 reicht:

```
LACP hilft,
mehrere physische Links zu einem logischen Link zusammenzufassen.
```

Merksatz:

```
LACP = Protokoll für Link Aggregation.
```

STP und VLANs

STP wirkt in Layer-2-Netzen und hängt oft mit VLANs zusammen.

Je nach Switch-System gibt es verschiedene Varianten:

```
ein Spanning Tree für alle VLANs
oder mehrere Instanzen für verschiedene VLANs
```

Wichtig für die Prüfung:

```
VLANs trennen Broadcast-Domänen.
STP verhindert Schleifen innerhalb der Layer-2-Struktur.
```

Merksatz:

```
VLAN trennt logisch.
STP verhindert Schleifen.
```

Broadcast-Sturm erkennen

Typische Hinweise auf einen Broadcast-Sturm:

```
- Netzwerk extrem langsam
- Switch-LEDs blinken ungewöhnlich stark
- hohe Auslastung auf vielen Ports
- Geräte verlieren Verbindung
- viele Broadcasts im Mitschnitt
- CPU-Last auf Switches steigt
- MAC-Adressen wechseln ständig Ports
- DHCP oder ARP funktioniert unzuverlässig
```

Merksatz:

```
Broadcast-Sturm zeigt sich oft als plötzliches Netzwerkausfall-Problem.
```

Layer-2-Schleife erkennen

Hinweise auf eine Layer-2-Schleife:

- MAC Flapping
- Broadcast-Sturm
- hohe Switch-Auslastung
- Ports laufen voll
- Netzwerk bricht plötzlich ein
- STP-Logs zeigen Änderungen
- gleiche MAC-Adresse an mehreren Ports
- nach Entfernen eines Kabels stabilisiert sich das Netz

Merksatz:

MAC Flapping und Broadcast-Sturm sind starke Schleifen-Hinweise.

Fehlersuche bei Layer-2-Schleifen

Sinnvolle Schritte:

1. Symptome prüfen:
   Broadcast-Sturm, MAC Flapping, hohe Last

2. Switch-Logs prüfen:
   STP-Meldungen, Port-Changes

3. Topologie prüfen:
   Welche Switches sind mehrfach verbunden?

4. Kabelwege prüfen:
   versehentliche Schleifen suchen

5. STP-Status prüfen:
   Root Bridge, blockierte Ports

6. Testweise verdächtige Verbindung trennen

7. Ursache sauber dokumentieren und korrigieren

Merksatz:

Bei Schleifenproblemen Topologie und STP prüfen.

Typische Ursachen in der Praxis

Häufige Praxisursachen:

- jemand steckt beide Enden eines Patchkabels in zwei Netzwerkdosen
- zwei kleine Switches werden mehrfach miteinander verbunden
- unmanaged Switch ohne STP wird angeschlossen
- Access Point oder Bridge ist falsch verkabelt
- Trunk-Ports sind falsch konfiguriert
- Link Aggregation wurde nicht korrekt eingerichtet
- STP wurde deaktiviert
- Root Bridge ist ungünstig gewählt

Merksatz:

Kleine Verkabelungsfehler können große Layer-2-Probleme auslösen.

Unmanaged Switches und STP

Ein unmanaged Switch hat oft keine oder nur sehr eingeschränkte Konfigurationsmöglichkeiten.

Problem:

STP ist eventuell nicht vorhanden
oder nicht kontrollierbar.

Wenn ein unmanaged Switch falsch angeschlossen wird, kann er Schleifen verursachen.

In professionellen Netzen sollte man daher vorsichtig sein, wenn zusätzliche kleine Switches angeschlossen werden.

Merksatz:

Unmanaged Switches können in Firmen-LANs ein Risiko sein.

BPDU Guard

BPDU Guard ist eine Schutzfunktion auf Switches.

Sie kann Ports deaktivieren, wenn dort unerwartet STP-BPDUs empfangen werden.

Typischer Einsatz:

```
Access-Ports für Endgeräte
```

Warum?

```
An einem normalen PC-Port sollte normalerweise kein weiterer Switch hängen.
```

Wenn dort BPDUs auftauchen, könnte ein nicht autorisierter Switch angeschlossen worden sein.

Merksatz:

```
BPDU Guard schützt Access-Ports vor unerwarteten Switch-Verbindungen.
```

Root Guard

Root Guard verhindert, dass ein unerwünschter Switch Root Bridge wird.

Das ist wichtig, damit die geplante STP-Topologie erhalten bleibt.

Typischer Einsatz:

```
Ports zu weniger vertrauenswürdigen Switches oder Bereichen
```

Merksatz:

```
Root Guard schützt die geplante Root Bridge.
```

Storm Control

Storm Control ist eine Schutzfunktion gegen übermäßigen Broadcast-, Multicast- oder Unicast-Verkehr.

Ein Switch kann begrenzen, wie viel solcher Verkehr pro Port erlaubt ist.

Wenn ein Grenzwert überschritten wird, kann der Switch reagieren.

Mögliche Reaktionen:

- Verkehr begrenzen
- Frames verwerfen
- Port sperren
- Ereignis protokollieren

Merksatz:

Storm Control begrenzt übermäßigen Layer-2-Verkehr.

Schutzmaßnahmen gegen Layer-2-Schleifen

Sinnvolle Maßnahmen:

- STP oder RSTP aktivieren
- Root Bridge gezielt planen
- BPDU Guard auf Access-Ports nutzen
- Root Guard an passenden Stellen nutzen
- Storm Control konfigurieren
- Link Aggregation korrekt einrichten
- unmanaged Switches vermeiden oder kontrollieren
- Netzwerkdosen dokumentieren
- Ports für Endgeräte klar konfigurieren
- Monitoring und Logs prüfen

Merksatz:

Schleifenschutz besteht aus STP, sauberer Konfiguration und Kontrolle.

STP und Fehlersuche nicht verwechseln

Wenn ein Port durch STP blockiert wird, ist das nicht automatisch ein Fehler.

Es kann genau das gewünschte Verhalten sein.

STP blockiert Ports, um Schleifen zu verhindern.

Problematisch ist es erst, wenn:

ein wichtiger Weg unerwartet blockiert wird

oder

STP falsch geplant ist

oder

eine Schleife nicht verhindert wird.

Merksatz:

STP-Blocking kann normal und gewollt sein.

Einordnung in das OSI-Modell

Thema	Schicht
Ethernet-Frame	2
Switch	2
MAC-Adresse	2
VLAN	2
Broadcast-Domäne	2
STP	2
RSTP	2
LACP / Link Aggregation	2
IP-Adresse	3
Routing	3
TTL	3

Merksatz:

STP schützt Layer 2.

TTL gehört zu Layer 3.

Was STP nicht macht

STP macht nicht:

- IP-Routing
- Firewall-Regeln
- VLAN-Erstellung
- DHCP-Vergabe
- DNS-Auflösung
- Verschlüsselung
- Benutzerverwaltung
- Anwendungsschutz

STP hat eine klare Aufgabe:

Schleifen auf Schicht 2 verhindern.

Merksatz:

STP ist Schleifenschutz,
kein Routing- oder Sicherheitskonzept für alles.

Typische IHK-Fragen

In AP1 und AP2 kann zum Beispiel gefragt werden:

- Warum sind Schleifen auf Schicht 2 gefährlich?
- Was ist ein Broadcast-Sturm?
- Warum gibt es bei Ethernet-Frames keine TTL wie bei IP?
- Was bedeutet STP?
- Welche Aufgabe hat STP?
- Was ist eine Root Bridge?
- Was ist eine BPDU?
- Was ist ein Root Port?
- Was ist ein Designated Port?
- Was ist ein blockierter Port?
- Was ist RSTP?
- Was ist der Unterschied zwischen STP und Link Aggregation?
- Was ist MAC Flapping?
- Welche Schutzmaßnahmen gibt es gegen Layer-2-Schleifen?

Typische Prüfungsfallen

Layer-2-Schleifen sind gefährlich,
weil Frames im Kreis laufen können.

Ethernet-Frames haben keine TTL wie IP-Pakete.

Broadcasts können sich bei Schleifen stark vervielfachen.

STP verhindert Schleifen.

STP entfernt keine Kabel,
sondern blockiert Ports logisch.

Root Bridge ist der zentrale Bezugspunkt für STP.

Niedrigste Bridge-ID gewinnt die Root-Bridge-Wahl.

BPDU = STP-Nachricht.

RSTP ist schneller als klassisches STP.

Link Aggregation ist nicht dasselbe wie STP.

MAC Flapping kann auf eine Schleife hinweisen.

Ein blockierter STP-Port ist nicht automatisch ein Fehler.

Wichtige Begriffe kurz erklärt

Begriff	Kurze Erklärung
Layer-2-Schleife	Kreis im Switch-Netz, über den Frames immer wieder laufen
Broadcast-Sturm	sehr viele Broadcasts überlasten das Netz
MAC Flapping	MAC-Adresse erscheint ständig an unterschiedlichen Ports
STP	Spanning Tree Protocol, verhindert Schleifen
Root Bridge	zentraler Bezugspunkt im STP
Bridge-ID	Kennung zur Wahl der Root Bridge

Begriff	Kurze Erklärung
STP-Priorität	Wert zur Beeinflussung der Root-Bridge-Wahl
BPDU	Bridge Protocol Data Unit, STP-Nachricht
Root Port	bester Port Richtung Root Bridge
Designated Port	aktiver Port für ein Segment
Blocked Port	blockierter Port zur Schleifenvermeidung
RSTP	Rapid Spanning Tree Protocol
MSTP	Multiple Spanning Tree Protocol
Link Aggregation	mehrere physische Links als ein logischer Link
LACP	Protokoll für Link Aggregation
BPDU Guard	Schutz vor unerwarteten BPDUs auf Access-Ports
Root Guard	Schutz der geplanten Root Bridge
Storm Control	Begrenzung übermäßigen Layer-2-Verkehrs

IHK-sichere Kurzformulierung

Layer-2-Schleifen entstehen, wenn es in einem Switch-Netz mehrere aktive Kreiswege gibt, über die Ethernet-Frames endlos weitergeleitet werden können. Da Ethernet-Frames keine TTL wie IP-Pakete besitzen, können sich Broadcasts und unbekannte Unicast-Frames stark vervielfachen. Die Folge kann ein Broadcast-Sturm mit hoher Netzwerklast und Verbindungsproblemen sein. STP, das Spanning Tree Protocol, verhindert solche Schleifen, indem es eine schleifenfreie Baumstruktur berechnet und redundante Ports logisch blockiert. RSTP ist eine schnellere Weiterentwicklung von STP. Link Aggregation ist davon zu unterscheiden, da sie mehrere physische Verbindungen zu einer logischen Verbindung bündelt.

Merksätze

Layer-2-Schleifen sind gefährlich.

Ethernet-Frames haben keine TTL.

Broadcast-Sturm = zu viele Broadcasts.

Schleifen können ein LAN lahmlegen.

MAC Flapping kann auf Schleifen hinweisen.

STP = Spanning Tree Protocol.

STP verhindert Layer-2-Schleifen.

STP blockiert Ports logisch.

Root Bridge = zentraler Bezugspunkt.

Niedrigste Bridge-ID gewinnt.

BPDU = STP-Nachricht.

Root Port = bester Weg zur Root Bridge.

Designated Port = aktiver Port im Segment.

Blocked Port = blockiert zur Schleifenvermeidung.

RSTP = schnelleres STP.

MSTP = mehrere Spanning-Tree-Instanzen.

Link Aggregation ist nicht STP.

LACP bündelt mehrere Links.

BPDU Guard schützt Access-Ports.

Root Guard schützt die Root-Bridge-Planung.

Storm Control begrenzt übermäßigen Verkehr.

STP-Blocking ist nicht automatisch ein Fehler.