

Switching Grundlagen

In diesem Kapitel erfahren Sie

- was Switches für Funktionen bereitstellen und wie sie sich von ihren Vorgängern – den Bridges – unterscheiden.
- welche Methoden zur Weiterleitung von Ethernet Frames zur Verfügung stehen
- wie Switches ihre Weiterleitungstabelle verwalten und Weiterleitungsentscheidungen treffen
- welche Probleme entstehen, wenn Switches redundant verkabelt werden um multiple Switching Pfade bereitzustellen (Redunanz, Ausfallsicherheit)

Vorfahren eines Switches

Geschichtlicher Überblick – Geräte und Topologien bei Verwendung von Ethernet als LAN Technologie:

1. Bustopologie mit **Koaxial**-Verkabelung
 - physikalische und logische Bustopologie
 - Broadcast-Domain = Collision Domain
2. Sterntopologie mit **Hub**
 - physikalische Sterntopologie, logische Bustopologie
 - Broadcast-Domain = Collision Domain
3. Sterntopologie mit **Bridge**
 - physikalische und logische Sterntopologie (P2p Verbindungen)
 - Microsegmentation: Jeder Bridge Port ist eine separate Collision Domain
4. Sterntopologie mit **Switch**
 - physikalische und logische Sterntopologie (P2p Verbindungen)
 - Microsegmentation: Jeder Switch Port ist eine separate Collision Domain
 - Full-Duplex Funktion: Kollisionsfrei, CSMA/CD abgeschaltet
 - VLAN fähig

Switching Methoden

Switching Methoden beschreiben wie Layer-2 Geräte Frames empfangen, verarbeiten und weiterleiten. Dabei existieren insgesamt 3 Methoden:

Methode	Switch empfängt ein Frame ..
Store and Forward	Switch lädt das gesamte Frame in den Puffer des Ports Switch überprüft die CRC (Cyclic Redundancy Check) im Frame Trailer .. Switch sendet das Frame, wenn CRC korrekt
Fragment-Free	Switch lädt nur die ersten 64 Byte des Frame in den Puffer des Ports → Aussortierung von Kollisionsfragmenten (.. die immer < 64 Byte sind) .. Switch sendet das Frame, wenn Frame > 64 Byte
Cut-Through	Switch lädt nur die ersten 20 Byte des Frame in den Puffer des Ports → Präambel (8 Byte), DST MAC (6 Byte) und SRC MAC (6 Byte) .. Switch sendet das Frame

	Store & Forward	Fragment Free	Cut Through
Geschwindigkeit der Datenweiterleitung	normal	schnell	sehr schnell
Weiterleitung von Kollisionsfragmenten	nein	nein	ja
Weiterleitung fehlerhafter Frames (CRC Fehler)	nein	ja	ja

Welche Switching Methode ein Cisco Switch verwendet bzw. zur Verfügung stellt kann oft nur im Datenblatt des Geräts ermittelt werden – zumeist wird die Fast Forward oder Cut Through Methode verwendet. Die administrative Manipulation der Switching Methode ist nur auf wenigen Geräten mit entsprechendem IOS möglich.

Grundfunktionalität von Switches

learning

automatischer Aufbau der Weiterleitungstabelle: MAC Address Table (MAC Table)

Ablauf

1. Switch empfängt einen Frame.
2. Switch liest die MAC Adresse des Senders (Inhalt des Ethernet **SRC MAC** Headerfeldes) und vergleicht sie mit den Einträgen in seiner MAC Table
3. Wenn noch kein Eintrag für die MAC Adresse vorhanden ist,
→ wird die MAC Adresse zusammen mit der Port ID (Portnummer) und der VLAN ID des Empfangsports als Eintrag in der MAC Table gespeichert.
4. Wenn bereits ein Eintrag für die MAC Adresse vorhanden ist,
→ wird der Timer für den Eintrag zurückgesetzt (auf default age time: 300 Sekunden). Der Timer wird verwendet, um alte Einträge (Geräte die keinen Traffic senden) aus der MAC Table zu entfernen.

Einem Port können mehrere MAC Adressen zugeordnet werden (mehrere MAC Adressen innerhalb der MAC Table mit gleicher Port ID), eine MAC Adresse kann jedoch nicht mehreren Ports zugeordnet werden.

Wird eine Verbindung entfernt, entfernt der Switch sofort auch alle Einträge innerhalb der MAC Table, die sich auf den Port beziehen.

show mac address-table

forwarding/flooding/filtering

Weiterleitung von Frames nach Informationen innerhalb der MAC Table

Ablauf

1. Switch empfängt einen Frame.
2. Switch liest die MAC Adresse des Empfängers (**DST MAC**) aus und vergleicht sie mit den Einträgen in seiner MAC Table
- Möglichkeiten:
 - **Unicast traffic** – DST MAC in der MAC Table
→ (Forwarding) sendet das Frame nur über den ermittelten Port weiter ..
→ (Filtering) .. und ausdrücklich nicht über andere Ports
 - **Unkown Unicast** – DST MAC nicht in der MAC Table.
→ (Flooding) sendet das Frame über alle Ports mit Ausnahme des Empfangsports
 - **Multicast traffic** - DST MAC ist eine Multicast-Adresse (OUI = 0100.5E)
→ (Flooding) sendet das Frame über alle Ports mit Ausnahme des Empfangsports
 - **Broadcast traffic** - DST MAC ist eine Broadcast-Adresse (FFFF.FFFF.FFFF)
→ (Flooding) sendet das Frame über alle Ports mit Ausnahme des Empfangsports
 - **Empfangsport und Zielpport sind identisch**
→ (Filtering) Der Switch leitet das Frame nicht weiter
 - **MAC Tabelle voll** (Besonderheit) – es können keine Einträge mehr aufgenommen werden. HINWEIS: die Kapazität der MAC Table ist i.d.R. ausreichend.
→ (Flooding) sendet alle Frames über alle Ports mit Ausnahme des Empfangsports

remove loops

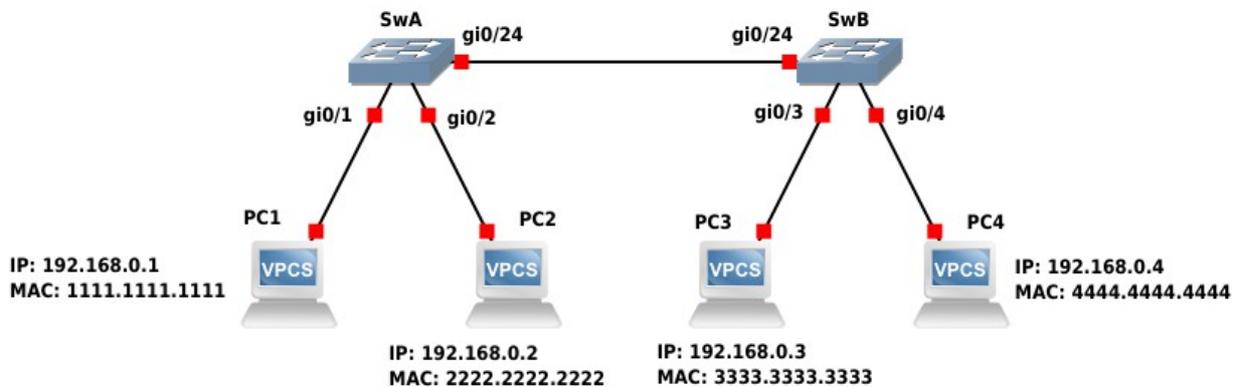
Vermeidung von Layer 2 Switching Loops in redundanten L2 Topologien.

Achtung: NUR falls folgenden IEEE Standards auf dem Gerät unterstützt werden (.. was auf allen zeitgemäßen professionelleren Switches i.d.R. der Fall ist):

- IEEE 802.1d → STP - Spanning Tree Protocol
- IEEE 802.1w → RSTP - Rapid Spanning Tree Protocol
- IEEE 802.1s) → MSTP - Multiple Spanning Tree Protocol

Packet Delivery Switching

.. am Beispiel eines ARP Request/Reply



HINWEIS: Nach dem die Switches frisch gebootet wurden, ist die MAC Table leer.

1. **PC1** möchte PC4 pingen und stellt fest, dass im ARP Cache die MAC Adresse zum Zielhost 192.168.0.4 nicht auffindbar ist.

→ PC1 sendet einen ARP Request ins Netzwerk.

DST MAC: ffff.ffff.ffff

SRC MAC: 1111.1111.1111

2. **SwA** empfängt das Frame auf dem Port gi 0/1.

Learning:

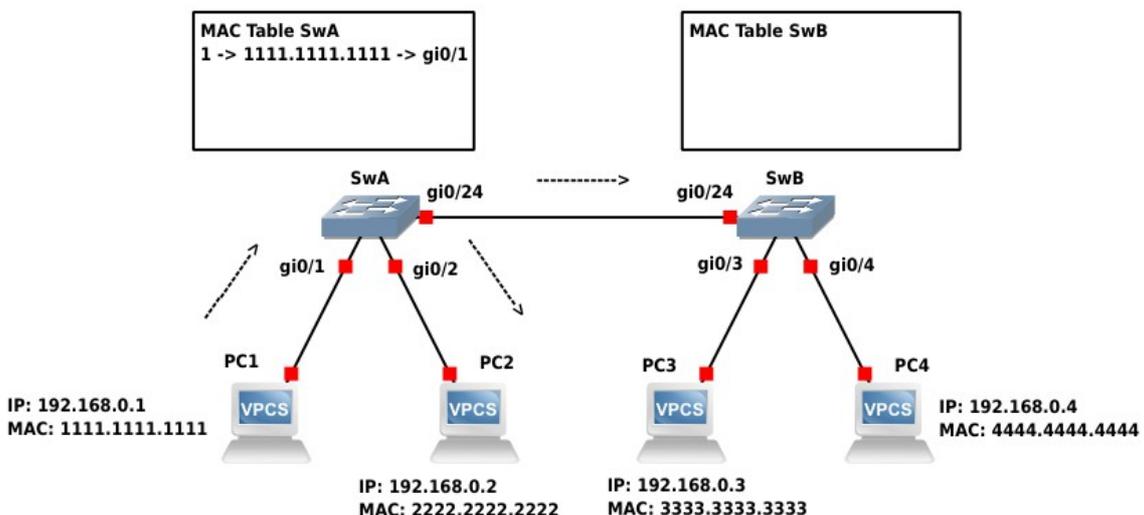
SwA überprüft, ob die **SRC MAC** 1111.1111.1111 bereits in der MAC Table existiert:

NEIN: er trägt die SRC MAC 1111.1111.1111 zusammen mit dem Empfangsport gi0/1 und die VLAN ID auf dem Port in seine MAC Table ein und startet einen Timer (300 Sekunden).

Forwarding/Flooding/Filtering:

SwA liest die **DST MAC** ein und stellt fest, dass es sich um Broadcast Datenverkehr handelt

→ Flooding: SwA flutet das Frame über alle aktiven Ports (gi02 und gi0/24) mit Ausnahme des Empfangsport



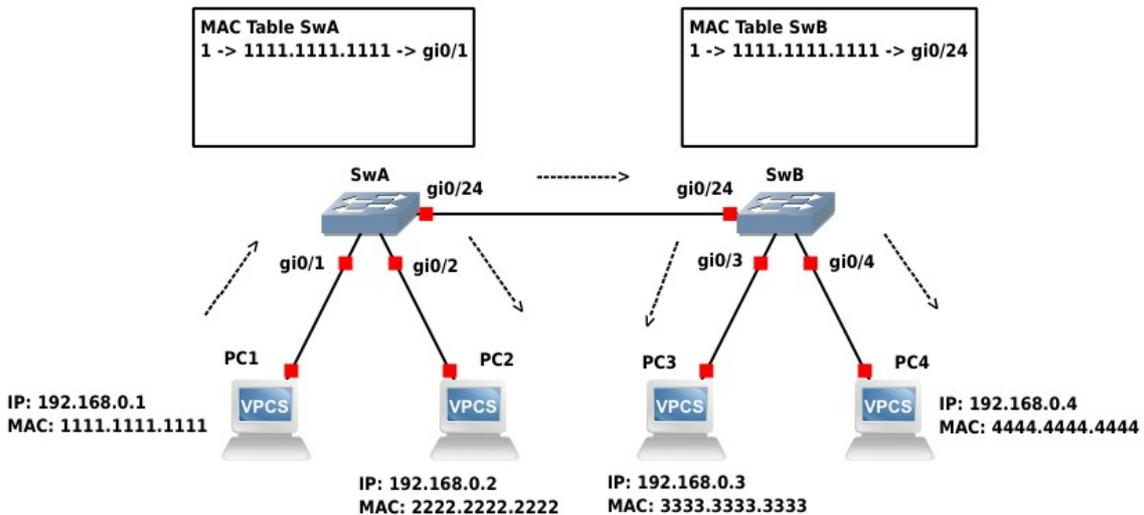
3. **SwB** empfängt das Frame auf dem Port gi 0/24.

Learning:

SwA überprüft, ob die **SRC MAC** 1111.1111.1111 bereits in der MAC Table existiert:
NEIN: er trägt die SRC MAC 1111.1111.1111 zusammen mit dem Empfangsport gi0/1 und die VLAN ID auf dem Port in seine MAC Table ein und startet einen Timer (300 Sekunden).

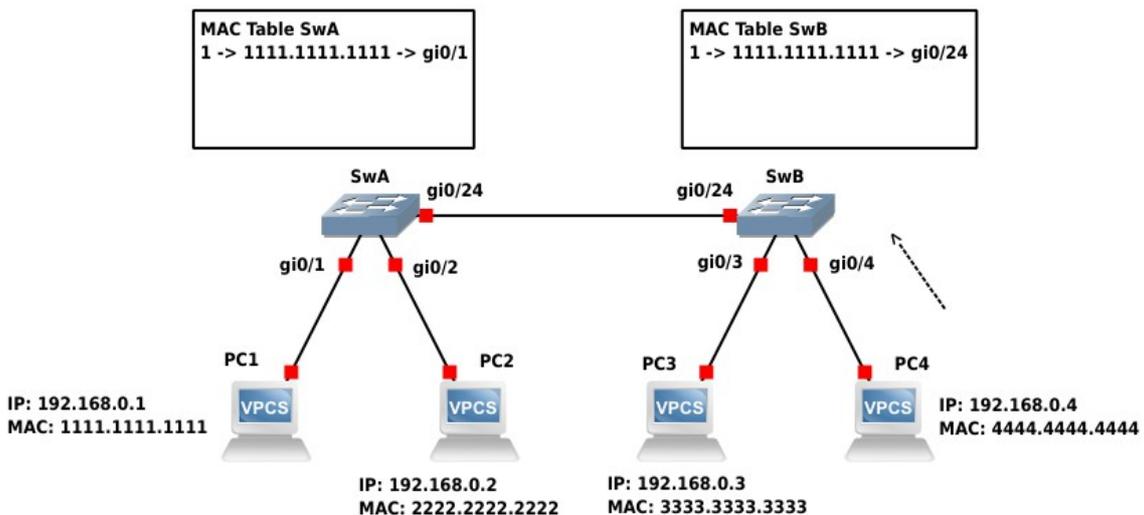
Forwarding/Flooding/Filtering:

SwB liest die **DST MAC** ein und stellt fest, das es sich um Broadcast Datenverkehr handelt
→ **Flooding**: SwB flutet das Frame über alle aktiven Ports (gi0/3 und gi0/4) mit Ausnahme des Empfangsport.



4. **PC4** verarbeitet den ARP Request von PC1 und sendet eine ARP Response via Unicast an PC1 zurück:

DST MAC: 1111.1111.1111
SRC MAC: 4444.4444.4444



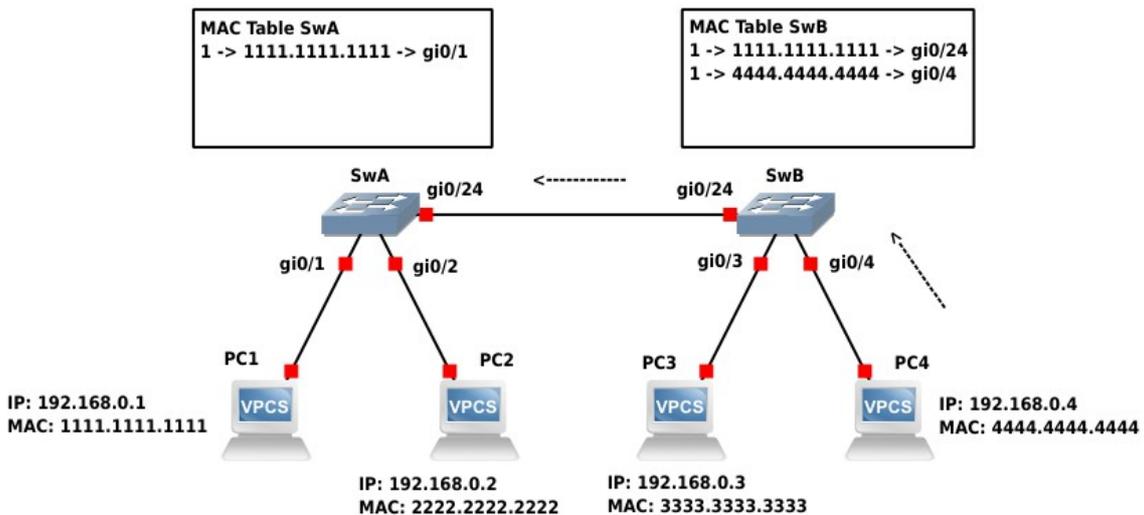
5. **SwB** empfängt das Frame auf dem Port gi 0/4.

Learning:

SwA überprüft, ob die **SRC MAC** 4444.4444.4444 bereits in der MAC Table existiert:
NEIN: er trägt die SRC MAC 4444.4444.4444 zusammen mit dem Empfangsport gi0/4 und die VLAN ID auf dem Port in seine MAC Table ein und startet einen Timer (300 Sekunden).

Forwarding/Flooding/Filtering:

SwB liest die **DST MAC** ein und stellt fest, das es sich um Unicast Datenverkehr handelt
→ **Forwarding**: SwB sucht und findet die DST MAC 1111.1111.1111 in seiner MAC Table, ermittelt den korrekten Ausgangsport: gi0/24 und sendet das Frame NUR über Port gi0/24.



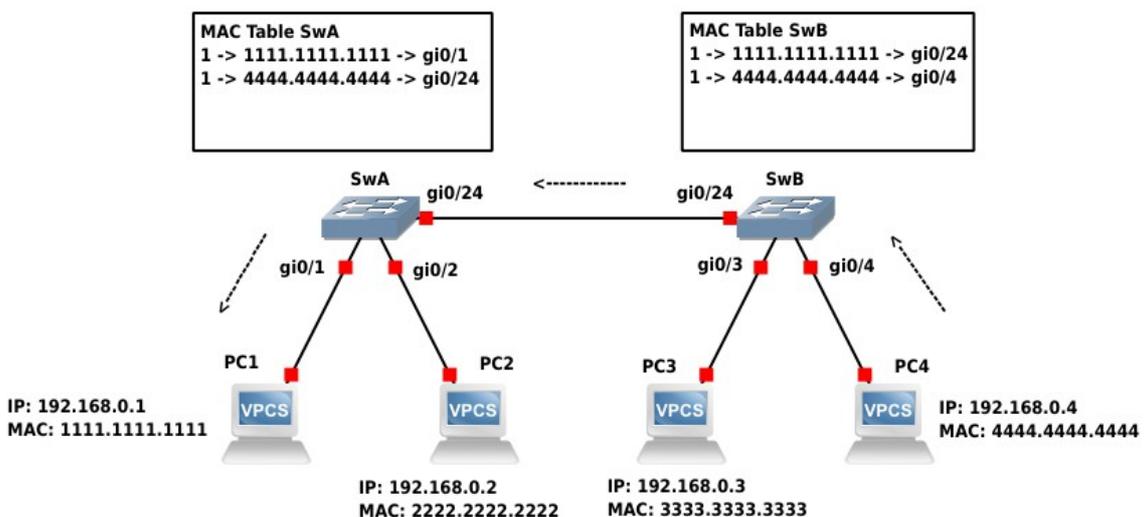
6. **SwA** empfängt das Frame auf dem Port gi 0/24.

Learning:

SwA überprüft, ob die **SRC MAC** 4444.4444.4444 bereits in der MAC Table existiert:
NEIN: er trägt die SRC MAC 4444.4444.4444 zusammen mit dem Empfangsport gi0/24 und die VLAN ID auf dem Port in seine MAC Table ein und startet einen Timer (300 Sekunden).

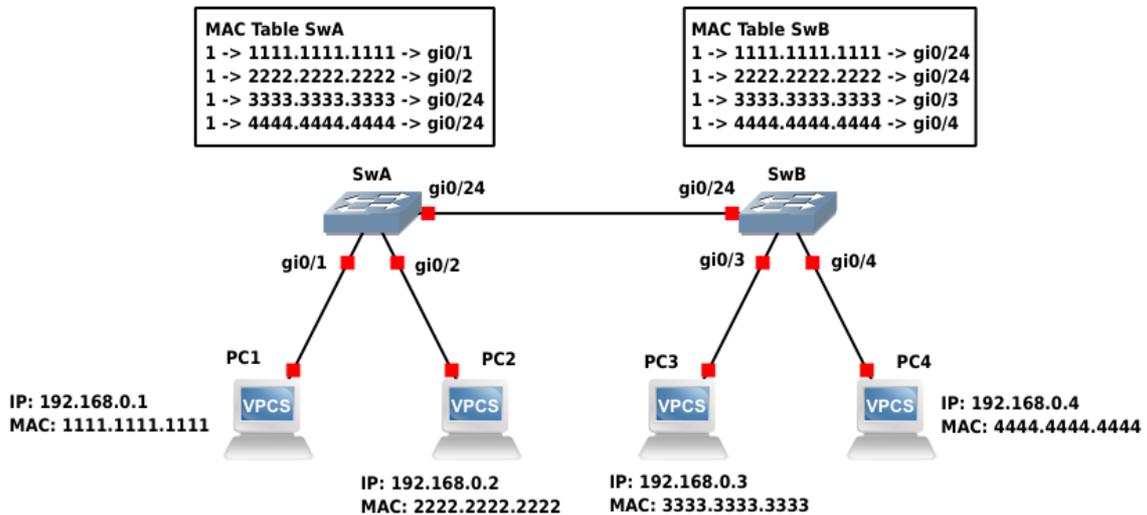
Forwarding/Flooding/Filtering:

SwB liest die **DST MAC** ein und stellt fest, das es sich um Unicast Datenverkehr handelt
→ **Forwarding**: SwB sucht und findet die DST MAC 1111.1111.1111 in seiner MAC Table, ermittelt so den korrekten Ausgangsport gi0/1 und sendet das Frame NUR über Port gi0/1.



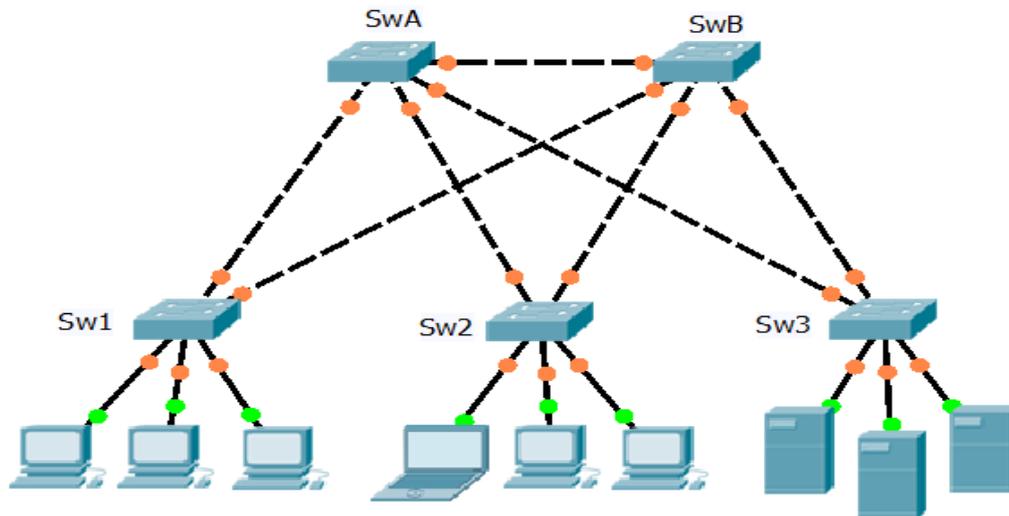
7. PC1 empfängt das ARP Reply Frame und trägt PC4 vollständig in seinen ARP Cache ein.

WENN ALLE PCs innerhalb der Topologie kommuniziert haben, sind auch die MAC Tabellen auf SwA und SwB komplett gefüllt:



Switching Loops

In LAN Topologien werden Switches meist redundant verbunden, um die Ausfallsicherheit im Netzwerk zu erhöhen.



Durch redundante Verbindungen stehen multiple "Switching Pfade" von jeder Quelle zu jedem Ziel zur Verfügung.

ACHTUNG: Falls keine Abwehrmassnahmen getroffen wurden – Aktivierung von STP – führen redundante Switching Topologien jedoch unvermeidlich zu Switching Loops.

L2 Switching Loop Problematiken

- reduzieren die verfügbare Bandbreite im Netzwerk drastisch (**Broadcast Storm**)
→ durch unendliche Weiterverteilung eines identischen Broadcast, Multicast oder unknown Unicast Frames (Flooding) im Netzwerk.
- verursachen Probleme auf Switches (**Inconsistent MAC Table**)
→ durch rasant wechselnde Einträge innerhalb der MAC Table, die so keine Folgerichtigkeit mehr aufweist
- verursachen Probleme auf allen Geräten im LAN (**Multiple Frame Transmission**)
→ die sich permanent wiederholende Zustellung eines identischen Frames, kann bei Geräten, die dieses immer wieder empfangen, zu Fehlern führen

ACHTUNG:

- Layer 2 Switching Loops enden nicht (!) automatisch nach einem gewissen Intervall (wie Routing Loops), ..
- .. führen zu enormen Datenverlusten und ..
- .. machen eine "normale" Datenkommunikation unmöglich !

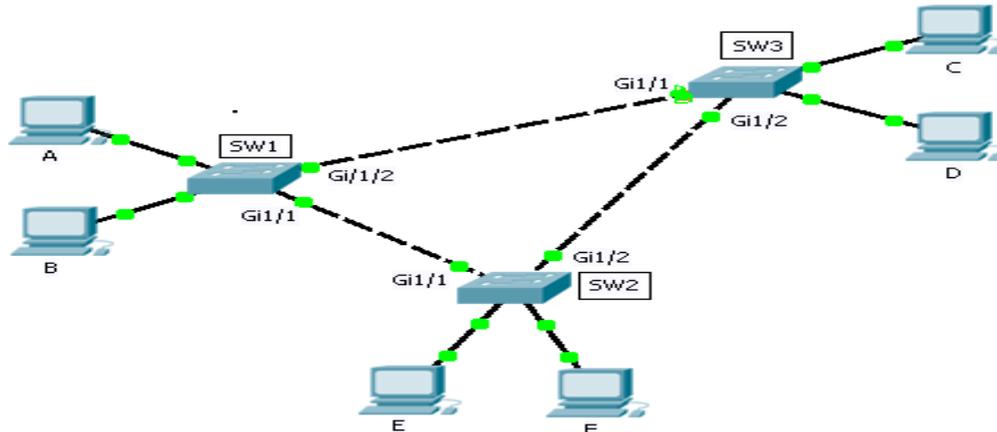
Durch Verwendung des **STP (Spanning Tree Protocols)** werden Layer 2 Switching Loops verhindert:

- STP stellt in einer redundanten Switching Topologie genau einen (1) aktiven Pfad zur Verfügung, über den jedes Gerät mit jedem andern Gerät kommunizieren kann ..
.. dabei werden existente, redundante Pfade durch "Abschalten" (blocking state) von Switchports deaktiviert: relevanter Datenverkehr wird nicht über den Switchport gesendet/empfangen.
- Fällt der aktive Pfad aus, wird ein vormals deaktivierter, redundanter Pfad für die Dauer des Ausfalls wieder freigeschaltet: durch wieder "Anschalten" (forwarding state) des/der entsprechenden Switchports.

Switching Loop Problematiken (Beispiel)

Broadcast Storm, Inconsistent MAC Table, Multiple Frame Transmission

L2 Switching Loops werden hauptsächlich ausgelöst durch das Flooding (Grundfunktion) von Broadcast, Multicast und unknown Unicast Frames. Beim Flooding werden die Frames von einem Switch über alle Ports weitergeleitet - außer über den entsprechenden Empfangsport. Beispiel: **Host A** möchte **Host D** erreichen und sendet einen **ARP Request (Broadcast)**



1.
SW1 erhält das Frame von Host A
SW1 MAC Table: **MAC Host A ↔ Port Fa 1/1** (nicht in der Topologie dargestellt)
SW1 **flutet** das Frame über alle Ports (nicht Empfangsport) → an Host B und SW1, SW2
2.
SW2 erhält das Frame von SW1
SW2 MAC Table: **MAC Host A ↔ Port Gi 1/1**
SW2 **flutet** das Frame über alle Ports (nicht Empfangsport) → an Hosts E,F und SW3

SW3 erhält das Frame von SW1
SW3 MAC Table: **MAC Host A ↔ Port Gi 1/1**
SW3 **flutet** das Frame über alle Ports (nicht Empfangsport) → an Hosts C,D und SW2
3.
SW2 erhält das Frame von SW3
SW2 MAC Table: ~~MAC Host A ↔ Port Gi 1/1~~ **MAC Host A ↔ Port Gi 1/2**
SW2 **flutet** das Frame über alle Ports (nicht Empfangsport) → an Hosts E,F (**2x**) und SW1

SW3 erhält das Frame von SW2
SW3 MAC Table: ~~MAC Host A ↔ Port Gi 1/1~~ **MAC Host A ↔ Port Gi 1/2**
SW3 **flutet** das Frame über alle Ports (nicht Empfangsport) → an Hosts C,D (**2x**) und SW1
4.
SW1 erhält das Frame von SW2
SW1 MAC Table: ~~MAC Host A ↔ Port Fa 1/1~~ **MAC Host A ↔ Port Gi 1/1**
SW1 **flutet** das Frame über alle Ports (nicht Empfangsport) → an Hosts A,B (**2x**) und SW3

SW1 erhält das Frame von SW3 (.. fast zeitgleich)
SW1 MAC Table: ~~MAC Host A ↔ Port Gi 1/1~~ **MAC Host A ↔ Port Gi 1/2**
SW1 **flutet** das Frame über alle Ports (nicht Empfangsport) → an Hosts A,B (**3x**) und SW 2
- 5 ff.
.. und so weiter und so weiter → unendlich

! SWITCHING LOOP ! KEIN Datenverkehr mehr möglich ! Netzwerk überlastet/ausgefallen !

Selbstkontrolle – Aufgaben und Übungen

1. Mit welcher Grundfunktion wird die MAC Table eines Switches automatisch erzeugt und welche Informationen werden in die MAC Table aufgenommen?
2. Was bedeutet Flooding im Zusammenhang mit den Switching Grundfunktionen?
3. Welche Art Datenverkehr leitet ein Switch nur über den ermittelten Ausgangsport weiter und wie nennt man diese Grundfunktion eines Switches?
4. Woran erkennt ein Switch Multicast Datenverkehr und wie leitet er ihn weiter?
5. Welchen Datenverkehr kann ein Administrator auf einem Host in einem Switched Netzwerk empfangen und z.B. mit dem Wireshark analysieren?
6. Wodurch werden Switching Loops ausgelöst?
7. Auf welcher OSI Schicht arbeiten Switches?

Selbstkontrolle – Lösungen

1. Mit welcher Grundfunktion wird die MAC Table eines Switches automatisch erzeugt und welche Informationen werden in die MAC Table aufgenommen?

Learning

SRC MAC des empfangenen Frame, Port ID des Empfangsports

2. Was bedeutet Flooding im Zusammenhang mit den Switching Grundfunktionen?

Senden eines Frames über alle aktiven Ports, mit Ausnahme des Empfangsports.

3. Welche Art Datenverkehr leitet ein Switch nur über den ermittelten Ausgangsport weiter und wie nennt man diese Grundfunktion eines Switches?

Unicast

forwarding

4. Woran erkennt ein Switch Multicast Datenverkehr und wie leitet er ihn weiter?

DST MAC Adresse (0100.5e)

Flooding

5. Welchen Datenverkehr kann ein Administrator auf einem Host in einem Switched Netzwerk empfangen und z.B. mit dem Wireshark analysieren?

Unicast Datenverkehr des Hosts

Multicast Datenverkehr aller Geräte im Netzwerk

Broadcast Datenverkehr aller Geräte im Netzwerk

6. Wodurch werden Switching Loops ausgelöst?

Durch redundante Verkabelung von Switches

7. Auf welcher OSI Schicht arbeiten Switches?

OSI 2