

### Switches als Kopplungselement

Switches sind die zentralen Verbindungsgeräte in einem Ethernet-basierten Netzwerk. An einen Switch werden alle anderen Geräte im Netzwerk (inkl. weiterer Switches) angeschlossen. Damit erzeugt ein Switch eine Sterntopologie, deren Sternpunkt der Switch selbst ist. Ein Switch arbeitet auf Layer 1 und 2 des OSI-Referenzmodells, er besitzt also physikalische Anschlüsse (Layer 1) und verfügt über die Fähigkeit, Datenverkehr anhand der MAC-Adresse zu managen (Layer 2). Heutzutage kommen im professionellen Umfeld so genannte "Layer-3-Switches" bzw. "Multilayerswitches" zum Einsatz, die über weitreichendere Funktionen verfügen als klassische Switches. Auf "Layer-3-Switches" wird allerdings erst an späterer Stelle eingegangen.

### Was und wie switcht ein Switch

Der Name "Switch" bedeutet so viel wie Schalter. Ein Switch schaltet also gewissermaßen Datenverkehr durch. Die Entscheidung, wohin Datenverkehr geschaltet werden soll trifft der Switch anhand der Ziel-MAC-Adresse, die im Ethernetframe, der weitergeleitet werden soll, eingetragen ist. Im folgenden Beispiel möchte PC1 mit PC2 kommunizieren. Der verschickte Ethernetframe enthält als Zieladresse die MAC-Adresse von PC2. Diese liest der Switch aus und leitet den entsprechenden Frame ausschließlich an PC2 weiter. PC3

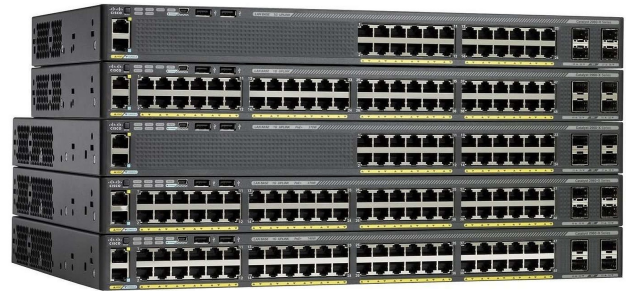


Abbildung 1: Verschiedene Switches des Herstellers Cisco aus der Catalyst-Serie

und PC4 erhalten den Frame nicht. Gleichzeitig möchte PC3 mit PC4 kommunizieren. Der betroffene Frame enthält als Zieladresse auf Layer 2 die MAC-Adresse von PC4. Diesen Frame leitet der Switch entsprechend ausschließlich an PC4 weiter. Das Besondere an einem Switch (im Vergleich zu den inzwischen beliebig stark veralteten Hubs) ist, dass beide Frames zeitgleich übertragen werden können, ohne dass sich die Übertragungen gegenseitig beeinflussen. Nimmt man beispielsweise an, dass an einem voll belegten 24-Port-Switch mit Gigabit-Interface jeweils "Hostpaare" miteinander kommunizieren wollen, so könnte theoretisch jedes dieser Paare mit 1Gbit/s kommunizieren. In diesem Sinne "schaltet" (switcht) ein Switch Verbindungen zwischen Hosts. Erreicht den Switch ein Frame, dessen Zieladresse ihm unbekannt ist, so gibt er diesen Frame an allen seinen Ports aus. Dieses Verhalten wird als "Flooding" bezeichnet.

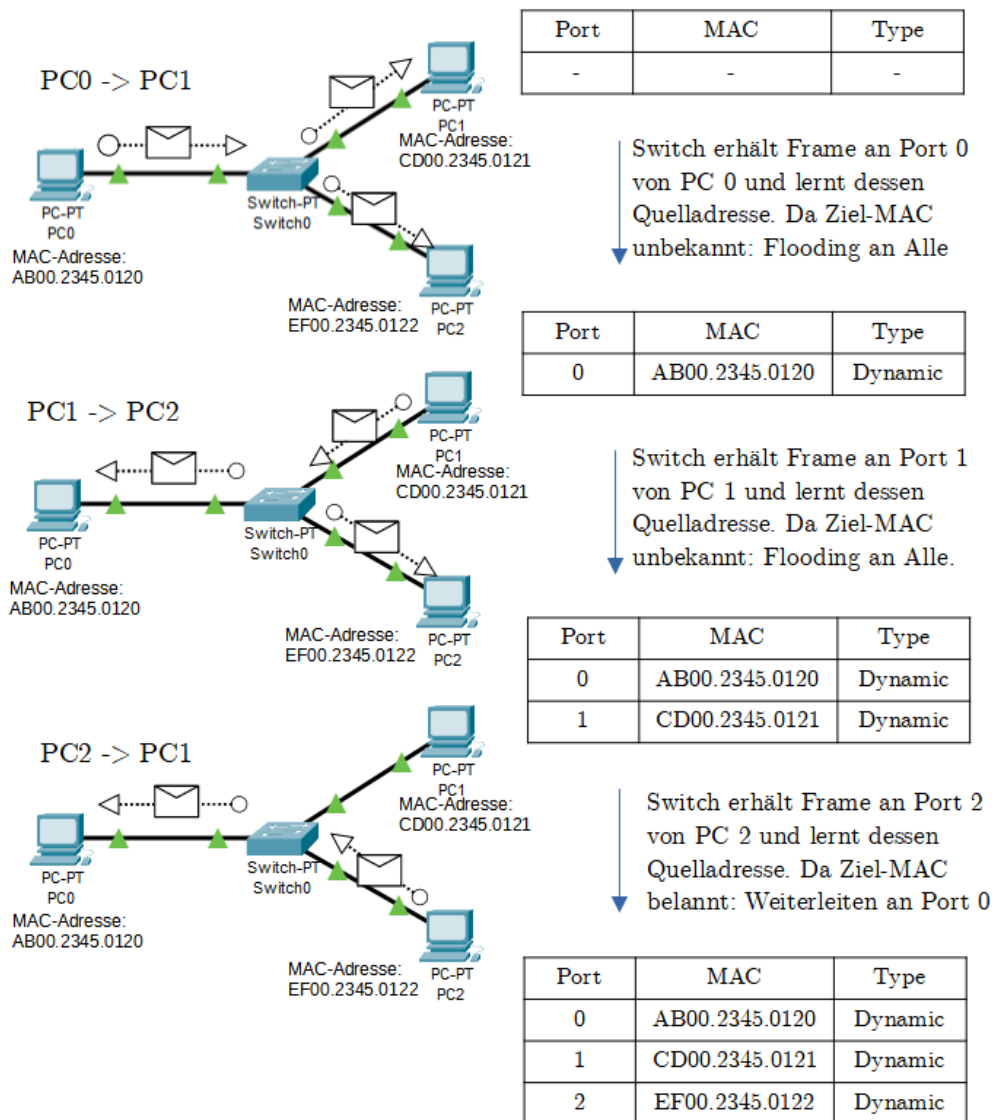
### Die MAC-Address-Table

In obigem Beispiel wurde stillschweigend angenommen, der Switch wisse, an welchem seiner Ports welcher Host mit welcher MAC-Adresse angeschlossen ist. Dies ist nach einer gewissen Zeit in einem bestehenden Netzwerk auch der Fall. Für diesen Zweck führt ein Switch eine so genannte "MAC-Address-Table" (auch als Source-Address-Table (SAT) bezeichnet), die insgesamt aus 3 Spalten besteht: Portnummer, MAC-Adresse und Typ. Der Switch trägt damit in die Tabelle ein, an welchem seiner

physikalischen Ports (Layer 1) welche MAC-Adressen (Layer 2) angeschlossen sind. Die Tabelle kann wahlweise manuell konfiguriert werden (Typ: Static) oder der Switch "lernt" im laufenden Betrieb und füllt die Tabelle selbstständig (Typ: Dynamic). Bei der Zuordnung von Port zu MAC-Adresse handelt es sich nicht um eine 1zu1-Beziehung. Für einen Port können mehrere MAC-Adresse gespeichert werden (Segment switching)

### Lernen der MAC-Adressen

Wie zuvor erwähnt ist ein Switch in der Lage seine SAT selbstständig zu füllen. Man nennt dies "lernen". Empfängt der Switch einen Ethernetframe an einem seiner Ports, liest er die Quelladresse des Frames aus und ordnet diese direkt dem Empfangsport zu. Der Switch hat folglich ausgelernt, wenn an jedem seiner Ports alle "angeschlossenen MAC-Adressen" einmal aufgetaucht sind. Im folgenden Beispiel ist zu Beginn die SAT des Switches leer. PC0 ist mit Port 0, PC1 mit Port 1 und PC2 mit Port 2 verbunden.



Nun ist die SAT vollständig gefüllt. Alle weiteren Pakete, die zwischen den PCs ausgetauscht werden sollen, würden zielgerichtet an den Empfänger weitergeleitet

### Verbinden mehrerer Switches: Kaskadierung

Da Switches nur mit begrenzter Portzahl erhältlich sind, ist es oftmals notwendig, mehrere Switches untereinander zu verbinden. Dies ist ohne weitere über die normalen Ports eines Switches möglich. In der Praxis kann es allerdings sinnvoll sein, Switches über schnellere Ports (beispielsweise 10GBaseT statt 1GBaseT) zu verbinden. In vielen Switches stehen so genannte SFP-Steckplätze (Small Formfactor-Pluggable) zur Verfügung, in die entsprechende Module eingebaut werden können. Mit Hilfe von SFP-Modulen kann ein Switch etwa um eine schnellere optische Schnittstelle erweitert werden. Ein Beispiel zeigt die rechts stehende Abbildung. Wird ein Switch (Switch1) an einem Port mit einem weiteren Switch (Switch2) verbunden, so sind aus Sicht von Switch1 mehrere MAC-Adressen (eben alle Hosts, die mit Switch2 verbunden sind) an diesem Port angeschlossen. Dies zeigt die Notwendigkeit des zuvor genannten segment switching.



Abbildung 2: Cisco-Switch mit SFP-Ports und SFP-Modulen

### Managed und Unmanaged Switches

Switches sind in vielen Umgebungen Plug'n'Play-fähig. Damit ist eine Konfiguration nicht unbedingt notwendig. Im Consumer- und Kleingewerblichen Bereich sind daher unmanaged Switches die Regel, also Switches, die nicht konfigurierbar sind. Im professionellen Umfeld werden konfigurierbare Switches (managed) eingesetzt. Solche Switches verfügen oft über eine spezielle Konfigurationsschnittstelle (bei Cisco: Console-Port), werden Konsolenprogramme wie Telnet oder SSH konfiguriert oder bieten ein Webinterface für diesen Zweck an. Im professionellen Umfeld ist die Konfiguration über ein Konsolenprogramm meist schneller, da hier bspw. Skripte ausgeführt werden können.