

Switch (Netzwerktechnik)

Switch (vom Englischen für „Schalter“, „Umschalter“ oder „Weiche“, auch *Netzwerkweiche* oder *Verteiler* genannt) bezeichnet ein Kopplungselement in Rechnernetzen, das Netzwerksegmente miteinander verbindet. Es sorgt innerhalb eines Segments (Broadcast-Domain) dafür, dass die Datenpakete, sogenannte „Frames“, an ihr Ziel kommen. Im Unterschied zu einem auf den ersten Blick sehr ähnlichen Repeater-Hub werden Frames aber nicht einfach an alle anderen Ports weitergeleitet, sondern nur an den, an dem das Zielgerät angeschlossen ist – ein Switch trifft eine Weiterleitungsentscheidung anhand der selbsttätig gelernten Hardware-Adressen der angeschlossenen Geräte.

Der Begriff *Switch* bezieht sich allgemein auf eine Multiport-Bridge – ein aktives Netzwerkgerät, das Frames anhand von Informationen aus dem Data Link Layer (Layer 2) des OSI-Modells weiterleitet. Manchmal werden auch die präziseren Bezeichnungen *Bridging Hub* oder *Switching Hub* verwendet, im IEEE 802.3-Standard heißt die Funktion *MAC Bridge*. (*Packet*) „*Switching*“ ist aus der leitungsvermittelnden Technik entlehnt, tatsächlich wird nichts „geschaltet“.^[1] Der erste *EtherSwitch* wurde im Jahr 1990 von Kalpana eingeführt.

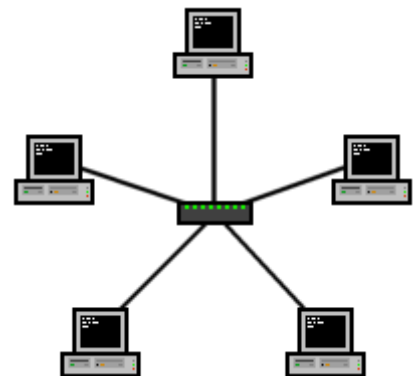
Das dem Switch vergleichbare Gerät auf Netzwerkschicht 1 (Layer 1) wird als (Repeater-)Hub bezeichnet. Switches, die zusätzlich Daten auf der Netzwerkschicht (Layer 3 und höher) verarbeiten, werden oft als Layer-3-Switches oder Multilayer-Switches bezeichnet und können die Funktion eines Routers erfüllen. Neben Ethernet-Switches gibt es Fibre-Channel-Switches, auch SAS-Expander werden immer häufiger als Switches bezeichnet. Fibre Channel (FC) definiert ein nicht routingfähiges Standardprotokoll aus dem Bereich der Speichernetzwerke, das als Variante von SCSI für die Hochgeschwindigkeitsübertragung großer Datenmengen konzipiert wurde. SAS (Serial Attached SCSI) ist der direkte Nachfolger der älteren parallelen SCSI-Schnittstelle.



5-Port-Switch



Switch mit 50 Ethernet-Ports



Ein Netzwerk mit zentralem Switch bildet eine Stern-Topologie.

Inhaltsverzeichnis

Eigenschaften und Funktionen

Layer-2- und Layer-3-Switches

Top of Rack Switch (ToR)

Management

Funktionsweise

Source Address Table

Unterschiedliche Arbeitsweisen

Port-Switching, Segment-Switching

Mehrere Switches in einem Netzwerk

Architekturen

Vorteile

Nachteile

Sicherheit

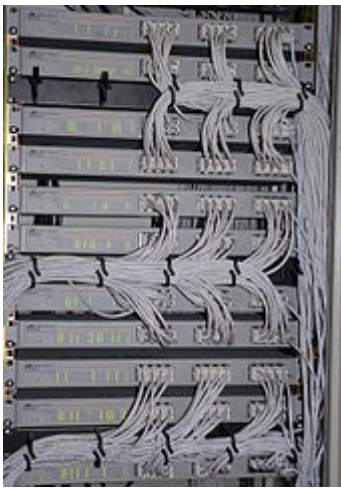
Kenngroßen

Geschichte

Weblinks

Einzelnachweise

Eigenschaften und Funktionen



24-Port-Switches

Einfache Switches arbeiten ausschließlich auf der Schicht 2 (Sicherheitsschicht) des OSI-Modells. Der Switch verarbeitet bei Erhalt eines Frames die 48 Bit lange

MAC-Adresse (z. B. 08:00:20:ae:fd:7e) und legt dazu einen Eintrag in der Source-Address-Table (SAT) an, in der neben der MAC-Adresse auch der physische Port, an dem diese empfangen wurde, gespeichert wird. Im Unterschied zum Hub werden Frames anschließend nur noch an den Port weitergeleitet, der für die entsprechende Zieladresse in

der SAT gelistet ist. Ist der Weg zur Zieladresse noch unbekannt (Lernphase), leitet der Switch das betreffende Frame an alle anderen aktiven Ports. Ein Unterschied zwischen Bridge und Switch ist die Anzahl der Ports: Bridges haben typischerweise nur zwei Ports, selten drei oder mehr, Switches hingegen haben als Einzelgeräte etwa 5 bis 50 Ports, modulare Switches auch mehrere Hundert. Von SOHO- über große Gebäudeinstallationen bis zu Rechenzentren ändern sich die Gehäuse fließend. Größere Geräte haben überwiegend Metallgehäuse und sind mit Montagewinkeln für den Einbau in 10"- oder 19"-Racks ausgestattet. Alle Ports sollten unabhängig voneinander gleichzeitig senden und empfangen können (non-blocking). Ein anderer möglicher Unterschied zu Bridges ist, dass manche Switch-Typen die

Cut-Through-Technik und andere Erweiterungen (s. u.) beherrschen. So verringert sich die Latenz, also die Verzögerung vom Absenden einer Anfrage und dem Eintreffen der Antwort darauf. Switches können auch mit Broadcasts umgehen; diese werden an alle Ports weitergeleitet. Bis auf wenige Ausnahmen gilt: Ein Switch ist eine Bridge, aber nicht jede Bridge ist ein Switch. Eine Ausnahme bilden Bridges, die verschiedene Protokolle wie Token Ring und Ethernet (MAC-Bridge oder LLC-Bridge) verbinden können. Eine solche Funktionalität ist bei



Modularer Switch mit 38 Ports von Cabletron Systems



Cisco 1900 Innenansicht

Switches nicht anzutreffen.

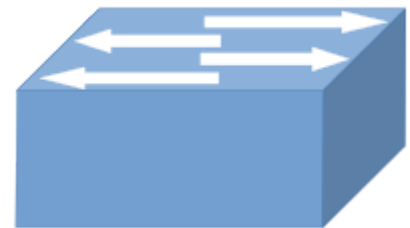
Für die angeschlossenen Geräte verhält sich ein Switch weitgehend transparent. Wenn die Kommunikation überwiegend zwischen den Geräten innerhalb eines Segments stattfindet, wird durch den Einsatz eines Switches die Anzahl der kursierenden Frames in den übrigen Segmenten drastisch reduziert. Muss ein Switch allerdings Frames in andere Segmente weiterleiten, führt sein Einsatz eher zu einer Verzögerung der Kommunikation (Latenz). Bei Überlastung eines Segments oder zu wenig Pufferspeicher im Switch kann es zum Verwerfen von Frames kommen. Dies muss durch Protokolle höherer Schichten wie TCP ausgeglichen werden.



Innenansicht eines vollintegrierten 5-Port-Switches

Layer-2- und Layer-3-Switches

Man unterscheidet zwischen Layer-2- und Layer-3- bzw. höheren Switches. Layer-2-Geräte sind häufig einfachere Modelle. Kleinere Geräte verfügen oft nur über grundsätzliche Funktionen und beherrschen meist keine Management-Funktionen (sind allerdings Plug-and-Play-fähig), oder nur mit einem geringen Funktionsumfang wie Portsperrungen oder Statistiken. Professionelle Layer-3- bzw. höhere Switches verfügen in der Regel auch über Management-Funktionen; neben den grundlegenden Switch-Funktionen verfügen sie zusätzlich über Steuer- und Überwachungsfunktionen, die auch auf Informationen aus höheren Schichten als Layer 2 beruhen können, wie z. B. IP-Filterung, Priorisierung für Quality of Service, Routing. Im Unterschied zu einem Router erfolgt bei einem Layer-3-Switch die Weiterleitungsentscheidung in der Hardware und somit schneller bzw. mit geringerer Latenz. Der Funktionsumfang von Layer-4-Switches und höher unterscheidet sich stark von Hersteller zu Hersteller, üblicherweise werden aber solche Funktionen in Hardware abgebildet wie Network Address Translation/Port Address Translation und Load Balancing.



(Cisco-)Symbol für einen Switch

Top of Rack Switch (ToR)

In Rechenzentrumsnetzwerken mit viel Datenverkehr, werden häufig pro Serverrack einer oder mehrere Switches zur Unterverteilung im Rack genutzt. Diese bezeichnet man als "Top of Rack Switch", sie sind im Normalfall oben im Rack verbaut. Besonders häufig Verwendung finden diese ToRs in der Spine-Leaf-Architektur, können aber auch in einem klassischen Sternnetzwerk verbaut werden.

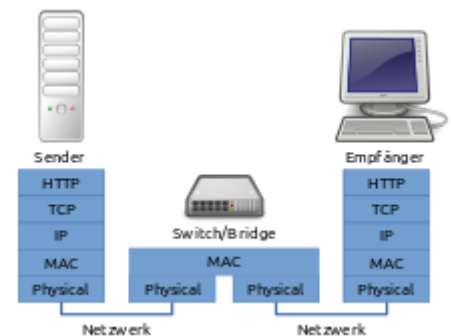
Ziel dieses Konzepts ist es, den Verkabelungsaufwand zwischen vielen Servern und Netzwerksystemen zu minimieren, die in größeren Rechenzentren mehrere zehntausend Systeme umfassen können. Seit SFF-8431 für IEEE_802.3ae sind "Direct-Attach Copper" (DAC) zur Rack-Verkabelung üblich. Die DACs haben typischerweise eine Länge von 2 m bis 7 m und sind passive Kupferkabel, die ohne ggf. fehleranfällige Laser oder Glasfaser auskommen. Die ToRs aggregieren den Datenverkehr der angeschlossenen Server und transportieren ihn dann gesammelt via Lichtwellenleiter zum Core-Netzwerk.^[2]

Management

Die Konfiguration oder Steuerung eines Switches mit Management-Funktionen geschieht je nach Hersteller über eine Kommandozeile (über Telnet oder SSH), eine Weboberfläche, eine spezielle Steuerungssoftware oder über eine Kombination dieser Möglichkeiten. Bei den aktuellen, „non-managed“ (Plug-and-Play-)Switches beherrschen manche höherwertige Geräte ebenfalls Funktionen wie tagged VLAN oder Priorisierung und verzichten dennoch auf eine Konsole oder ein sonstiges Management-Interface.

Funktionsweise

Im Folgenden wird, sofern nicht anders gekennzeichnet, von Layer-2-Switches ausgegangen. Die einzelnen Ein-/Ausgänge, die sogenannten „Ports“, eines Switches können unabhängig voneinander Daten empfangen und senden. Diese sind entweder über einen internen Hochgeschwindigkeitsbus (Backplane-Switch) oder kreuzweise miteinander verbunden (Matrix Switch). Datenpuffer sorgen dafür, dass nach Möglichkeit keine Frames verlorengehen.



Ein Switch zur Verknüpfung zweier Netzwerksegmente

Source Address Table

Ein Switch muss im Regelfall nicht konfiguriert werden. Empfängt er ein Frame nach dem Einschalten, speichert er die MAC-Adresse des Senders und die zugehörige Schnittstelle in der Source Address Table (SAT).

Wird die Zieladresse in der SAT gefunden, so befindet sich der Empfänger im Segment, das an der zugehörigen Schnittstelle angeschlossen ist. Das Frame wird dann an diese Schnittstelle weitergeleitet. Sind Empfangs- und Zielsegment identisch, muss das Frame nicht weitergeleitet werden, da die Kommunikation ohne Switch im Segment selbst stattfinden kann.

Falls die Zieladresse (noch) nicht in der SAT ist, muss das Frame an alle anderen Schnittstellen weitergeleitet werden. In einem IPv4-Netz wird der SAT-Eintrag meist bereits während der sowieso nötigen ARP-Adressenanfragen vorgenommen. Zunächst wird aus der ARP-Adressenanfrage eine Zuordnung der Absender-MAC-Adresse möglich, aus dem Antwort-Frame erhält man dann die Empfänger-MAC-Adresse. Da es sich bei den ARP-Anfragen um Broadcasts handelt und die Antworten immer an bereits erlernte MAC-Adressen gehen, wird kein unnötiger Verkehr erzeugt. Broadcast-Adressen werden niemals in die SAT eingetragen und daher stets an alle Segmente weitergeleitet. Frames an Multicast-Adressen werden von einfachen Geräten wie Broadcasts verarbeitet. Höher entwickelte Switches beherrschen häufig den Umgang mit Multicasts und senden Multicast-Frames dann nur an die registrierten Multicast-Adress-Empfänger.

Switches *lernen* also gewissermaßen die MAC-Adressen der Geräte in den angeschlossenen Segmenten automatisch.

Unterschiedliche Arbeitsweisen

Ein Ethernet-Frame enthält die Zieladresse nach der so genannten Datenpräambel in den ersten 48 Bits (6 Bytes). Mit der Weiterleitung an das Zielsegment kann also schon nach Empfang der ersten sechs Bytes begonnen werden, noch während das Frame empfangen wird. Ein Frame ist 64 bis 1518 Bytes lang, in den letzten vier Bytes befindet sich zur Erkennung von fehlerhaften Frames eine CRC-Prüfsumme (zyklische Redundanzprüfung). Datenfehler in Frames können erst erkannt werden, nachdem das gesamte Frame eingelesen wurde.

Je nach den Anforderungen an die Verzögerungszeit und Fehlererkennung kann man daher Switches unterschiedlich betreiben:



24-Port 10/100 Mbit Managed Switch

Cut-through

Fast-Forward-Switching

Eine sehr schnelle Methode, hauptsächlich von besseren Switches implementiert. Hierbei trifft der Switch beim eintreffenden Frame direkt nach der Ziel-MAC-Adresse eine

Weiterleitungsentscheidung und schickt das Frame entsprechend weiter, während es noch empfangen wird. Die Latenzzeit setzt sich zusammen aus lediglich den Längen der Präambel (8 Byte), der Ziel-MAC-Adresse (6 Byte) und der Reaktionszeit des Switches. Durch die frühestmögliche Weiterleitung kann das Frame aber nicht auf Fehlerfreiheit geprüft werden, und der Switch leitet auch eventuell beschädigte Frames weiter. Da eine Fehlerkorrektur in der Schicht 2 aber nicht existiert, belasten fehlerhafte Frames lediglich die betreffende Verbindung. (Eine Korrektur kann nur in höheren Netzwerkschichten stattfinden.) Manche Switches schalten bei zu häufigen Fehlern auch auf die langsamere, aber fehlerfreie Weiterleitung mit *Store-and-Forward* um bzw. herunter (s. u.).

Fragment-Free

Schneller als *Store-and-Forward*-, aber langsamer als *Fast-Forward-Switching*, anzutreffen vor allem bei besseren Switches. Bei dieser Methode prüft der Switch, ob ein Frame die im Ethernet-Standard geforderte minimale Länge von 64 Bytes (512 Bit) erreicht, und schickt es erst dann weiter zum Zielport, ohne eine CRC-Prüfung durchzuführen. Fragmente unter 64 Byte sind meist Trümmer einer Kollision, die kein sinnvolles Frame mehr ergeben.

Store-and-Forward

→ *Hauptartikel: Store and forward*

Die sicherste, aber auch langsamste Switch-Methode mit der größten Latenzzeit wird von jedem Switch beherrscht. Der Switch empfängt zunächst das ganze Frame (speichert dieses; „Store“), berechnet die Prüfsumme über das Frame und trifft dann seine Weiterleitungsentscheidung anhand der Ziel-MAC-Adresse. Sollten sich Differenzen zwischen der berechneten Prüfsumme und dem am Ende des Frames gespeicherten CRC-Wert ergeben, wird das Frame verworfen. Auf diese Weise verbreiten sich keine fehlerhaften Frames im lokalen Netzwerk. *Store-and-Forward* war lange die einzig mögliche Arbeitsweise, wenn Sender und Empfänger mit unterschiedlichen Übertragungsgeschwindigkeiten oder Duplex-Modi arbeiteten oder verschiedene Übertragungsmedien nutzten. Die Latenzzeit in Bit ist hier identisch mit der gesamten Paketlänge – bei Ethernet, Fast Ethernet und Gigabit Ethernet im Vollduplex-Modus sind das mindestens 576 Bit, Obergrenze ist die maximale Paketgröße (12.208 Bit) – plus der Reaktionszeit des Switches. Heute gibt es auch Switches, die einen *Cut-and-Store*-Hybridmodus beherrschen, der auch beim Übertragen der Daten zwischen langsamen und schnellen Verbindungen die Latenz senkt.^[3]

Error-Free-Cut-Through/Adaptive Switching

Eine Mischung aus mehreren der obigen Methoden, ebenfalls meist nur von teureren Switches implementiert. Der Switch arbeitet zunächst im Modus „Cut through“ und schickt das Frame auf dem korrekten Port weiter ins LAN. Es wird jedoch eine Kopie des Frames im Speicher behalten, über die dann eine Prüfsumme berechnet wird. Stimmt sie nicht mit dem im Frame gespeicherten CRC-Wert überein, so kann der Switch dem defekten Frame zwar nicht mehr direkt signalisieren, dass er fehlerhaft ist, aber er kann einen internen Zähler mit der Fehlerrate pro Zeiteinheit hochzählen. Wenn zu viele Fehler in kurzer Zeit auftreten, fällt der Switch in den *Store-and-Forward*-Modus zurück. Sinkt die Fehlerrate

wieder tief genug, schaltet der Switch in den Cut-Through-Modus um. Ebenso kann er temporär in den Fragment-Free-Modus schalten, wenn zu viele Fragmente mit weniger als 64 Byte Länge ankommen. Besitzen Sender und Empfänger unterschiedliche Übertragungsgeschwindigkeiten oder Duplex-Modi bzw. nutzen sie andere Übertragungsmedien (Glasfaser auf Kupfer), so müssen die Daten ebenfalls mit Store-and-Forward-Technik übertragen werden.

Heutige Netzwerke unterscheiden zwei Architekturen: das symmetrische und asymmetrische Switching gemäß der Gleichförmigkeit der Anschlussgeschwindigkeit der Ports. Im Falle eines asymmetrischen Switchings, d. h. wenn Sende- und Empfangsports unterschiedliche Geschwindigkeiten aufweisen, kommt das Store-and-Forward-Prinzip zum Einsatz. Bei symmetrischem Switching, also der Kopplung gleicher Ethernetgeschwindigkeiten, wird nach dem Cut-Through-Konzept verfahren.

Port-Switching, Segment-Switching

In den Anfangszeiten der Switching-Technik gab es die zwei Varianten: *Port-* und *Segment-Switching*. Diese Differenzierung spielt in modernen Netzwerken nur noch eine untergeordnete Rolle, da alle handelsüblichen Switches Segment-Switching an allen Ports beherrschen.

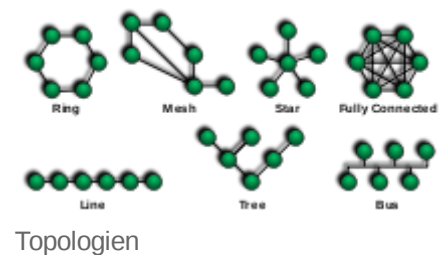
- Ein **Port-Switch** verwaltet pro Port nur einen SAT-Eintrag für eine MAC-Adresse. An solch einem Anschluss dürfen folglich nur Endgeräte (Server, Router, Workstation) und keine weiteren Segmente, also keine Bridges, Hubs oder Switches (hinter denen sich mehrere MAC-Adressen befinden) angeschlossen werden (siehe MAC-Flooding). Zusätzlich gab es oft einen sogenannten „Uplink-Port“, der die lokalen Geräte quasi „nach außen“ verbindet und für den diese Einschränkung nicht galt. Dieser Port hatte oft keine SAT, sondern wurde einfach für alle MAC-Adressen benutzt, die nicht einem anderen lokalen Port zugeordnet waren. Solche Switches arbeiteten in der Regel nach dem Cut-Through-Verfahren. Trotz dieser scheinbar nachteiligen Einschränkungen existierten auch Vorteile: Die Switches kamen mit extrem wenig Speicher aus (geringere Kosten) und auf Grund der Minimalgröße der SAT konnte auch die *Switching-Entscheidung* sehr schnell getroffen werden.
- Alle neueren Switches sind **Segment-Switches** und können an jedem Port zahlreiche MAC-Adressen verwalten, d. h. weitere Netz-Segmente anschließen. Hierbei gibt es zwei unterschiedliche SAT-Anordnungen: Entweder jeder Port hat eine eigene Tabelle von beispielsweise max. 250 Adressen, oder es gibt eine gemeinsame SAT für alle Ports – mit beispielsweise maximal 2000 Einträgen. Vorsicht: Manche Hersteller geben 2000 Adresseinträge an, meinen aber 8 Ports mit jeweils maximal 250 Einträgen pro Port.

Mehrere Switches in einem Netzwerk

Bei frühen Switches musste die Verbindung mehrerer Geräte meistens entweder über einen speziellen Uplinkport oder über ein gekreuztes Kabel (crossover cable) erfolgen, neuere Switches wie auch alle Gigabit-Ethernet Switches beherrschen Auto-MDI(X), sodass diese auch ohne spezielle Kabel miteinander gekoppelt werden können. Oft, aber nicht notwendigerweise sind Uplink-Ports in einer schnelleren oder höherwertigen (Ethernet-)Übertragungstechnik realisiert als die anderen Ports (z. B. Gigabit-Ethernet statt Fast Ethernet oder Glasfaserkabel anstatt Twistedpair-Kupferkabel). Im Unterschied zu Hubs können nahezu beliebig viele Switches miteinander verbunden werden. Die Obergrenze hat hier nichts mit einer maximalen Kabellänge zu tun, sondern hängt von der Größe der Adresstabelle (SAT) ab. Bei aktuellen Geräten der Einstiegsklasse sind oft 500 Einträge (oder mehr) möglich, das begrenzt die maximale Anzahl von Knoten (~Rechnern) auf ebendiese 500. Kommen mehrere Switches zum Einsatz, so begrenzt das Gerät mit der kleinsten SAT die maximale Knotenanzahl. Hochwertige Geräte können mit vielen tausend

Adressen umgehen. Läuft im Betrieb eine zu kleine Adresstabelle über, so müssen wie beim MAC-Flooding alle nicht zuzuordnenden Frames an alle anderen Ports weitergeleitet werden, folglich kann die Übertragungsleistung drastisch einbrechen.

Zur Steigerung der Ausfallsicherheit können bei vielen Geräten Verbindungen redundant aufgebaut werden. Dabei werden der mehrfache Transport von Broadcasts und Switching-Schleifen durch den per Spanning Tree Protocol (STP) aufgebauten Spannbaum verhindert. Eine andere Möglichkeit, ein Netz mit Schleifen redundant zu machen und gleichzeitig die Leistung zu steigern, ist das Meshing (IEEE 802.1aq – engl.: Shortest Path Bridging). Hier dürfen beliebige Schleifen zwischen meshing-fähigen Geräten gebildet werden; zur Leistungssteigerung können dann für Unicast-Datenverkehr (ähnlich wie beim Trunking) alle Schleifen (auch Teilschleifen) weiter genutzt werden (es wird kein einfacher Spannbaum gebildet). Multicast und Broadcast müssen vom Meshing-Switch gesondert behandelt werden und dürfen nur auf einer der zur Verfügung stehenden vermaschten Verbindungen weitergeschickt werden.



Wenn in einem Netzwerk Switches ohne weitere Vorkehrungen mit sich selbst verbunden oder mehrere Switches zyklisch in einer Schleife miteinander verbunden werden, entsteht eine Schleife, eine sogenannte Switching-Loop. Durch endloses Doppeln und Kreisen von Datenpaketen führt solch eine fehlerhafte Vernetzung in der Regel zu einem Totalausfall des Netzwerks.

Eine bessere Nutzung von mehrfach ausgeführten Verbindungen (Links) ist die Port-Bündelung (englisch: trunking, bonding, etherchannel – je nach Hersteller), wodurch bis zu acht [2009] gleichartige Verbindungen parallel geschaltet werden können, um die Geschwindigkeit zu steigern. Dieses Verfahren beherrschen professionelle Switches, die auf diese Weise untereinander, von Switch zu Switch oder aber von Switch zu Server verbunden werden können. Ein Standard ist mit LACP definiert (zuerst IEEE 802.3ad, später IEEE 802.1AX), das Zusammenschalten von Switches verschiedener Hersteller kann allerdings manchmal problematisch sein. Außer einigen herstellerspezifischen Protokollen existieren auch nicht ausgehandelte, sogenannte statische Bündel. So eine Portbündelung ist ebenfalls auf mehrere Links zwischen zwei Geräten beschränkt; drei oder mehr Switches zum Beispiel in einem aktiven Ring zu verbinden, ist damit nicht möglich. Ohne STP bildet sich entweder eine Switching-Schleife oder Frames erreichen nicht zuverlässig ihr Ziel, mit STP wird einer der Links blockiert und erst mit SPB können alle Links tatsächlich verwendet werden.

Stacking ist im Switching-Umfeld eine Technik, um mehrere unabhängige stacking-fähige Switches zu einem gemeinsamen logischen Switch mit höherer Portanzahl zusammen zu stellen und mit einem gemeinsamen Management zu konfigurieren. Stacking-fähige Switches bieten besondere Ports, die sogenannten Stacking-Ports, welche üblicherweise mit besonders hoher Übertragungsrate und geringer Latenzzeit arbeiten. Beim Stacking werden die Switches, die in der Regel vom selben Hersteller und aus derselben Modellreihe stammen müssen, mit einem speziellen Stack-Kabel miteinander verbunden. Eine Stacking-Verbindung ist normalerweise die schnellste Verbindung zwischen mehreren Switches und überträgt neben Daten auch Managementinformationen. Solche Schnittstellen können durchaus teurer sein als Standard-HighSpeed-Ports, die natürlich ebenfalls als Uplinks genutzt werden können; Uplinks sind immer möglich, aber: nicht alle Switches unterstützen das Stacking.

Architekturen

Den Kern eines Switches bildet das Switching Fabric, durch welches die Frames vom Eingangs- zum Ausgangsport transferiert werden. Das Switching Fabric ist vollständig in Hardware implementiert, um geringe Latenzzeiten und hohen Durchsatz zu gewährleisten. Zusätzlich zur reinen Verarbeitungsaufgabe

sammelt es statistische Daten, wie die Anzahl der transferierten Frames, (Frame-)Durchsatz oder Fehler. Die Vermittlungstätigkeit lässt sich auf drei Arten durchführen:

- **Shared Memory Switching:** Dieses Konzept lehnt sich an die Vorstellung an, dass Rechner und Switch in ähnlicher Weise arbeiten. Sie erhalten Daten über Eingangsschnittstellen, bearbeiten diese und geben sie über Ausgangsports weiter. Analog dazu signalisiert ein empfangenes Frame dem Switchprozessor über einen Interrupt seine Ankunft. Der Prozessor extrahiert die Zieladresse, sucht den entsprechenden Ausgangsport und kopiert das Frame in den Puffer. Als Folge ergibt sich eine Geschwindigkeitsabschätzung aus der Überlegung, dass wenn N Frame/s in den und aus dem Speicher ein- und ausgelesen werden können, die Vermittlungsrate $N/2$ Frame/s nicht übersteigen kann.
- **Bus Switching:** Bei diesem Ansatz überträgt der Empfangsport ein Frame ohne Eingriff des Prozessors über einen gemeinsamen Bus an den Ausgangsport. Den Engpass bildet der Bus, über den jeweils nur ein Frame zurzeit transferiert werden kann. Ein Frame, das am Eingangsport eintrifft und den Bus besetzt vorfindet, wird daher in die Warteschlange des Eingangsports gestellt. Da jedes Frame den Bus separat durchqueren muss, ist die Switchinggeschwindigkeit auf den Busdurchsatz beschränkt.
- **Matrix Switching:** Das Matrixprinzip ist eine Möglichkeit die Durchsatzbegrenzung des gemeinsam genutzten Busses aufzuheben. Ein Switch dieses Typs besteht aus einem Schaltnetzwerk, das N Eingangs- mit N Ausgangsports über $2N$ Leitungen verbindet. Ein Frame, das an einem Eingangsport eintrifft, wird auf den horizontalen Bus übertragen, bis es sich mit dem vertikalen Bus schneidet, der zum gewünschten Ausgangsport führt. Ist diese Leitung durch die Übertragung eines anderen Frames blockiert, muss das Frame in die Warteschlange des Eingangsports gestellt werden.

Vorteile

Switches haben folgende Vorteile:

- Wenn zwei Netzteilnehmer gleichzeitig senden, gibt es keine Datenkollision (vgl. CSMA/CD), da der Switch intern über die Backplane beide Sendungen gleichzeitig übermitteln kann. Sollten an einem Port die Daten schneller ankommen, als sie über das Netz weitergesendet werden können, werden die Daten gepuffert. Wenn möglich wird Flow Control benutzt, um den oder die Sender zu einem langsameren Verschicken der Daten aufzufordern. Hat man acht Rechner über einen 8-Port-Switch verbunden und jeweils zwei senden untereinander mit voller Geschwindigkeit Daten, sodass vier Full-Duplex-Verbindungen zustande kommen, so hat man rechnerisch die achtfache Geschwindigkeit eines entsprechenden Hubs, bei dem sich alle Geräte die maximale Bandbreite teilen. Nämlich 4×200 Mbit/s im Gegensatz zu 100 Mbit/s. Zwei Aspekte sprechen jedoch gegen diese Rechnung: Zum einen sind die internen Prozessoren besonders im Low-Cost-Segment nicht immer darauf ausgelegt, alle Ports mit voller Geschwindigkeit zu bedienen, zum anderen wird auch ein Hub mit mehreren Rechnern nie 100 Mbit/s erreichen, da desto mehr Kollisionen entstehen, je mehr das Netz ausgelastet ist, was die nutzbare Bandbreite wiederum drosselt. Je nach Hersteller und Modell liegen die tatsächlich erzielbaren Durchsatzraten mehr oder minder deutlich unter den theoretisch erzielbaren 100 %, bei preiswerten Geräten sind Datenraten zwischen 60 % und 90 % durchaus üblich.
- Der Switch zeichnet in einer Tabelle auf, welche Station über welchen Port erreicht werden kann. Hierzu werden im laufenden Betrieb die Absender-MAC-Adressen der durchgeleiteten Frames gespeichert. So werden Daten nur an den Port weitergeleitet, an dem sich tatsächlich der Empfänger befindet, wodurch Spionage durch Nutzung des Promiscuous Mode der Netzwerkkarte verhindert wird, wie sie bei Netzwerken mit Hubs noch möglich war. Frames mit (noch) unbekannter Ziel-MAC-Adresse werden wie Broadcasts behandelt und an alle Ports mit Ausnahme des Quellports weitergeleitet.

- Der Voll-Duplex-Modus kann benutzt werden, so dass an einem Port gleichzeitig Daten gesendet und empfangen werden können, wodurch die Übertragungsrate verdoppelt wird. Da in diesem Fall Kollisionen nicht mehr möglich sind, wird die physisch mögliche Übertragungsrate besser ausgenutzt.
- An jedem Port kann unabhängig die Geschwindigkeit und der Duplex-Modus ausgehandelt werden.
- Zwei oder mehr physische Ports können zu einem logischen Port (HP: Bündelung, Cisco: Etherchannel) zusammengefasst werden, um die Bandbreite zu steigern; dies kann über statische oder dynamische Verfahren (z. B. LACP oder PAgP) erfolgen.
- Ein physischer Switch kann durch VLANs in mehrere logische Switches unterteilt werden. VLANs können über mehrere Switches hinweg aufgespannt werden (IEEE 802.1Q).

Nachteile

- Ein Nachteil von Switches ist, dass sich die Fehlersuche in einem solchen Netz unter Umständen schwieriger gestaltet. Frames sind nicht mehr auf allen Strängen im Netz sichtbar, sondern im Idealfall nur auf denjenigen, die tatsächlich zum Ziel führen. Um dem Administrator trotzdem die Beobachtung von Netzwerkverkehr zu ermöglichen, beherrschen manche Switches *Port-Mirroring*. Der Administrator teilt dem (verwaltbaren) Switch mit, welche Ports er beobachten möchte. Der Switch schickt dann Kopien von Frames der beobachteten Ports an einen dafür ausgewählten Port, wo sie z. B. von einem Sniffer aufgezeichnet werden können. Um das Port-Mirroring zu standardisieren, wurde das SMON-Protokoll entwickelt, das in RFC 2613 beschrieben ist.
- Ein weiterer Nachteil liegt in der Latenzzeit, die bei Switches höher ist (100BaseTX: 5–20 µs) als bei Hubs (100BaseTX: < 0,7 µs). Da es beim CSMA-Verfahren sowieso keine garantierten Zugriffszeiten gibt und es sich um Unterschiede im Millionstelsekundenbereich handelt, hat dies in der Praxis selten Bedeutung. Wo bei einem Hub ein einkommendes Signal einfach an alle Netzteilnehmer weitergeleitet wird, muss der Switch erst anhand seiner MAC-Adresstabelle den richtigen Ausgangsport finden; dies spart zwar Bandbreite, kostet aber Zeit. Dennoch ist in der Praxis der Switch im Vorteil, da die absoluten Latenzzeiten in einem ungeswitchten Netz aufgrund der unvermeidbaren Kollisionen eines bereits gering ausgelasteten Netzes die Latenzzeit eines vollduplexfähigen (fast kollisionslosen) Switches leicht übersteigen. (Die höchste Geschwindigkeit erzielt man weder mit Hubs noch mit Switches, sondern indem man gekreuzte Kabel einsetzt, um zwei Netzwerk-Endgeräte direkt miteinander zu verbinden. Dieses Verfahren beschränkt jedoch, bei Rechnern mit je einer Netzwerkkarte, die Anzahl der Netzwerkteilnehmer auf 2.)
- Switches sind Sternverteiler mit einer sternförmigen Netzwerktopologie und bringen bei Ethernet (ohne Portbündelung, STP oder Meshing) keine Redundanzen mit. Fällt ein Switch aus, ist die Kommunikation zwischen allen Teilnehmern im (Sub-)Netz unterbrochen. Der Switch ist dann der Single Point of Failure. Abhilfe schafft die Portbündelung (FailOver), bei der jeder Rechner über mindestens zwei LAN-Karten verfügt und an zwei Switches angeschlossen ist. Zur Portbündelung mit FailOver benötigt man allerdings LAN-Karten und Switches mit entsprechender Software (Firmware).

Sicherheit

Beim klassischen Ethernet mit Thin- oder Thickwire genau so wie bei Netzen, die Hubs verwenden, war das Abhören des gesamten Netzwerkverkehrs noch vergleichsweise einfach. Switches galten zunächst als wesentlich sicherer. Es gibt jedoch Methoden, um auch in geswitchten Netzen den Datenverkehr anderer Leute mitzuschneiden, ohne dass der Switch kooperiert:

- MAC-Flooding – Der Speicherplatz, in dem sich der Switch die am jeweiligen Port hängenden MAC-Adressen merkt, ist begrenzt. Dies macht man sich beim MAC-Flooding zu Nutze, indem man den Switch mit gefälschten MAC-Adressen überlädt, bis dessen Speicher voll ist. In diesem Fall schaltet der Switch in einen *Failopen-Modus*, wobei er sich wieder wie ein Hub verhält und alle Frames an alle Ports weiterleitet. Verschiedene Hersteller haben – wieder fast ausschließlich bei Switches der mittleren bis hohen Preisklasse – Schutzmaßnahmen gegen MAC-Flooding implementiert. Als weitere Sicherheitsmaßnahme kann bei den meisten „Managed Switches“ für einen Port eine Liste mit zugelassenen Absender-MAC-Adressen angelegt werden. Protokolldateneinheiten (hier: Frames) mit nicht zugelassener Absender-MAC-Adresse werden nicht weitergeleitet und können das Abschalten des betreffenden Ports bewirken (*Port Security*).
- MAC-Spoofing – Hier sendet der Angreifer Frames mit einer fremden MAC-Adresse als Absender. Dadurch wird deren Eintrag in der Source-Address-Table überschrieben, und der Switch sendet dann allen Datenverkehr zu dieser MAC an den Switchport des Angreifers. Abhilfe wie im obigen Fall durch feste Zuordnung der MACs zu den Switchports.
- ARP-Spoofing – Hierbei macht sich der Angreifer eine Schwäche im Design des ARP zu Nutze, welches zur Auflösung von IP-Adressen zu Ethernet-Adressen verwendet wird. Ein Rechner, der ein Frame via Ethernet versenden möchte, muss die Ziel-MAC-Adresse kennen. Diese wird mittels ARP erfragt (ARP-Request Broadcast). Antwortet der Angreifer nun mit seiner eigenen MAC-Adresse zur erfragten IP (nicht seiner eigenen IP-Adresse, daher die Bezeichnung *Spoofing*) und ist dabei schneller als der eigentliche Inhaber dieser Adresse, so wird das Opfer seine Frames an den Angreifer senden, welcher sie nun lesen und gegebenenfalls an die ursprüngliche Zielstation weiterleiten kann. Hierbei handelt es sich nicht um einen Fehler des Switches. Ein Layer-2-Switch kennt gar keine höheren Protokolle als Ethernet und kann seine Entscheidung zur Weiterleitung nur anhand der MAC-Adressen treffen. Ein Layer-3-Switch muss sich, wenn er autokonfigurierend sein soll, auf die von ihm mitgelesenen ARP-Nachrichten verlassen und lernt daher auch die gefälschte Adresse, allerdings kann man einen „Managed Layer-3-Switch“ so konfigurieren, dass die Zuordnung von Switchport zu IP-Adresse fest und nicht mehr von ARP beeinflussbar ist.

Kenngrößen

- Forwarding Rate (Durchletrate): gibt an, wie viele Frames pro Sekunde eingelesen, bearbeitet und weitergeleitet werden können
- Filter Rate (Filterrate): Anzahl der Frames, die pro Sekunde bearbeitet werden
- Anzahl der verwaltbaren MAC-Adressen (Aufbau und max. Größe der Source-Address-Table)
- Backplanedurchsatz (Switching fabric): Kapazität der Busse (auch Crossbar) innerhalb des Switches
- VLAN-Fähigkeit oder Flusskontrolle.
- Managementoptionen wie Fehlerüberwachung und -signalisierung, Port-basierte VLANs, Tagged-VLANs, VLAN Uplinks, Link Aggregation, Meshing, Spanning Tree Protocol (Spannbaumbildung), Bandbreitenmanagement usw.

Geschichte


Die Entwicklung von Ethernet-Switches begann Ende der 1980er Jahre. Durch bessere Hardware und verschiedene Anwendungen mit einem hohen Bedarf an Bandbreite kamen 10-MBit-Netzwerke sowohl im Rechenzentrumsbetrieb als auch bei Campus-Netzen nun rasch an ihre Grenzen. Um einen effizienteren Netzwerkverkehr zu erhalten, begann man, Netze über Router zu segmentieren und Subnetze zu bilden.

Das reduzierte zwar Kollisionen und erhöhte die Effizienz, vergrößerte aber auch die Komplexität der Netze und steigerte die Installations- und Administrations-Kosten in erheblichem Maße. Auch die damaligen Bridges waren keine echten Alternativen, da sie nur wenige Ports hatten (meist zwei) und langsam arbeiteten – der Datendurchsatz war vergleichsweise gering und die Latenzzeiten zu hoch. Hier liegt die Geburtsstunde der ersten Switches: Das erste kommerziell verfügbare Modell hatte sieben 10-MBit-Ethernet-Ports und wurde 1990 vom US-StartUp-Unternehmen Kalpana (später von Cisco übernommen) angeboten. Der Switch hatte einen höheren Datendurchsatz als Ciscos High-End-Router und war weitaus günstiger. Zusätzlich entfielen Restrukturierungen: Er konnte einfach und transparent im bestehenden Netz platziert werden. Hiermit begann der Siegeszug der „geswitchten“ Netze. Schon bald danach entwickelte Kalpana das Port-Trunking-Verfahren Etherchannel, das es zur Steigerung des Datendurchsatzes erlaubt, mehrere Ports zu bündeln und gemeinsam als Uplink bzw. Backbone zu nutzen. Mitte der 1990er erreichten Fast-Ethernet-Switches (non Blocking, Full Duplex) Marktreife. Für Gigabit-Ethernet wurden Repeater-Hubs zwar noch im Standard definiert, es existieren aber effektiv keine. In 10-Gigabit-Netzwerken sind gar keine Hubs mehr definiert – alles wird „geswitcht“. Heute werden Segmente mit mehreren tausend Rechnern – ohne zusätzliche Router – einfach und performant mit Switches verbunden. Switches finden Verwendung in geschäftlichen oder privaten Netzwerken ebenso wie bei temporären Netzwerken wie LAN-Partys.



Kalpana EtherSwitch EPS-1500, einer der ersten Ethernet Switches.

Weblinks

 **Wiktionary: Switch** – Bedeutungserklärungen, Wortherkunft, Synonyme, Übersetzungen

- RFC 2613 – *Remote Network Monitoring MIB Extensions for Switched Networks Version 1.0*

Einzelnachweise

1. Lawrence G. Roberts: *The Evolution of Packet Switching*. (<https://web.archive.org/web/20160324033133/http://www.packet.cc/files/ev-packet-sw.html>) November 1978, archiviert vom Original (<https://giftbot.toolforge.org/deref.fcgi?url=http%3A%2F%2Fwww.packet.cc%2Ffiles%2Fev-packet-sw.html>) am 24. März 2016; abgerufen am 27. August 2019.
2. www.itwissen.info: *ToR (top of rack)*. (<https://web.archive.org/web/20210121055021/https://www.itwissen.info/ToR-top-of-rack-ToR-Switch.html>) Archiviert vom Original (<https://giftbot.toolforge.org/deref.fcgi?url=https%3A%2F%2Fwww.itwissen.info%2FToR-top-of-rack-ToR-Switch.html>) am 21. Januar 2021; abgerufen am 25. März 2021.
3. Hauser B.J., Lehrbuch der Kommunikationstechnik – Einführung in die Kommunikations- und Netzwerktechnik für Berufsschule und Studium (2011), S. 130f.

Abgerufen von „[https://de.wikipedia.org/w/index.php?title=Switch_\(Netzwerktechnik\)&oldid=220685336](https://de.wikipedia.org/w/index.php?title=Switch_(Netzwerktechnik)&oldid=220685336)“

Diese Seite wurde zuletzt am 1. März 2022 um 11:15 Uhr bearbeitet.

Der Text ist unter der Lizenz „Creative Commons Attribution/Share Alike“ verfügbar; Informationen zu den Urhebern und zum Lizenzstatus eingebundener Mediendateien (etwa Bilder oder Videos) können im Regelfall durch Anklicken dieser abgerufen werden. Möglicherweise unterliegen die Inhalte jeweils zusätzlichen Bedingungen. Durch die Nutzung dieser Website erklären Sie sich mit den Nutzungsbedingungen und der Datenschutzrichtlinie einverstanden.

Wikipedia® ist eine eingetragene Marke der Wikimedia Foundation Inc.