Vorteil: Die meisten Fehler und Kollisionen treten während den ersten 64 Byte auf. Nachteil: Dieses Verfahren wird trotz seiner effektiven Arbeitsweise selten genutzt.

2.5.2 Switch-MAC-Tabellenverwaltung

Switches haben den Vorteil, im Gegensatz zu Hubs, dass sie Datenpakete nur an den Port weiterleiten, an dem die Station mit der Ziel-Adresse angeschlossen ist. Als Adresse dient die MAC-Adresse, also die Hardware- Adresse einer Netzwerkkarte. Diese Adresse speichert der Switch in einer internen Tabelle. Empfängt ein Switch ein Datenpaket, so sucht er in seinem Speicher unter der Zieladresse (MAC) nach dem Port und schickt dann das Datenpaket nur an diesen Port. Die MAC-Adresse lernt ein Switch mit der Zeit kennen. Die Anzahl der Adressen, die ein Switch aufnehmen kann, hängt ab von seinem Speicherplatz.

Ein Qualitätsmerkmal eines Switches ist es, wie viele Adressen er insgesamt und pro Port speichern kann. An einem Switch, der nur eine Handvoll Computer verbindet, spielt es keine Rolle wie viele Adressen er verwalten kann. Wenn der Switch aber in einem großen Netzwerk steht und an seinen Ports noch andere Switches und Hubs angeschlossen sind, dann muss er evt. mehrere tausend MAC-Adressen speichern und den Ports zuordnen können. Je größer ein Netzwerk ist, desto wichtiger ist es, von vornherein darauf zu achten, dass die Switches genügend Kapazität bei der Verwaltung von MAC-Adressen haben.

2.5.3 Layer3-Switches

Der Ausdruck Layer-3-Switch ist etwas irreführend, denn es handelt sich um Multifunktionsgeräte, die eine Kombination aus Router und Switch darstellen.

2.6 Kollisions- und Broadcastdomänen

Eine Kollisionsdomäne ist ein Netzwerksegment in einem CSMA/CD-Netz (etwa Ethernet). Alle Stationen, die physisch miteinander verbunden sind, befinden sich in der gemeinsamen Kollisionsdomäne. Repeater und Hubs trennen Kollisionsdomänen nicht.

Bridges trennen Kollisionsdomänen, da sie auf OSI-Schicht 2 arbeiten. In einem geswitchten Netz besteht die Kollisionsdomäne nur aus zwei Stationen, dem Client und dem Switchport.

Eine **Broadcast-Domäne** ist ein logischer Verbund von Computern in einem lokalen Netzwerk, der sich dadurch auszeichnet, dass ein Broadcast alle Domänenteilnehmer erreicht.

Ein lokales Netzwerk auf der zweiten Schicht des OSI-Modells (Sicherungsschicht) besteht durch seine Hubs, Switches und/oder Bridges aus einer Broadcast -Domäne. Erst durch die Unterteilung in VLANs oder durch den Einsatz von Routern, die auf Schicht 3 arbeiten, wird die Broadcast-Domäne aufgeteilt.

Eine Broadcast-Domäne besteht aus einer oder mehreren Kollisionsdomänen.

2.7 VLANs (Virtual LANs)

Durch die Switching-Technik (OSI-Ebene 2) können sehr große LANs aufgebaut werden, ohne starke Bandbreiteneinbußen zu verursachen. Switches können sehr viele angeschlossene Stationen gleichzeitig verwalten (begrenzt durch die Größe ihrer MAC address table). Vorteil eines großen geswitchten Netzes ist die einfache Erreichbarkeit aller Stationen, die Einsparung von Routern und deren Verwaltung und eine geringe Latenz der Datenpakete.

Aus folgenden Gründen will man ein solches Netz oft wieder unterteilen:

- Die Broadcast-Last wird sehr hoch.
- Man möchte die Netze kompakt und überschaubar halten, z.B. nach Abteilungen getrennt, aber ohne VLANs kann jede Station jede andere direkt ansprechen (Sicherheitsproblem)

Eine Lösung dieser Probleme sind VLANs. Mit Hilfe von VLANs können auf einem Switch oder über mehrere Switches hinweg virtuell getrennte Netze betrieben werden. Diese Technik eignet sich auch für die standortübergreifende Vernetzung (z.B. per ATM) mehrerer VLANs über einen Switch bzw. Router.

Schon aus Ressourcengründern lässt sich ein Netz nicht überall über getrennte Switches aufbauen. Physisch getrennt verkabelte Netze sind aber auch unflexibel und Änderungen nur mit hohem Aufwand möglich. VLAN stellt unabhängig von der physischen Struktur eine logische Struktur des Netzes zur Verfügung.

Technologien

- **Port-based VLANs**: Hier wird ein managebarer Switch in mehrere logische Switches segmentiert. Ein Port gehört dann immer nur zu einem VLAN, um die so segmentierten Netze bei Bedarf zu verbinden kommt z.B. ein Router zum Einsatz; meist kann ein Layer-3-Switch auch diese Aufgabe erfüllen-
- **Tagged VLANs:** Hier tragen die Netzwerkpakete eine Markierung, welche die Zugehörigkeit zu einem VLAN anzeigt.

Funktionsweise nach IEEE 802.1Q: Jedem VLAN wird eine eindeutige Nummer zugeordnet. Man nennt diese Nummer VLAN ID. Ein Gerät, das zum VLAN mit der ID=1 gehört, kann mit jedem anderen Gerät im gleichen VLAN kommunizieren, nicht jedoch mit einem Gerät in einem anderen VLAN wie z.B. ID=2, 3, ...

Um zwischen den VLANs zu unterscheiden, wird nach IEEE 802.1Q das Ethernet-Frame um 4 Byte (= 32 Bit) erweitert. Davon sind 12 Bit zur Aufnahme der VLAN ID vorgesehen, so dass insgesamt 4096 - 2 = 4094 VLANs möglich sind (die VLAN-IDs "0" und "4095" sind reserviert und nicht zulässig).

TPID *(Tag Protocol Identifier):* Fester Wert 0x8100. Bedeutung: Frame trägt die 802.1Q/802.1p-Tag- Information.

Priorität *(user_priority)* – Benutzer-Prioritätsinformationen.

CFI *(Canonical Format Indicator):*

- Wert 0: das Format der MAC-Adressen ist kanonisch (LSB zuerst)
- Wert 1: Format ist nicht-kanonisch. Benutzung im Token Ring/Source-Routed-FDDI-Media- Zugang, um die bit order der Adressinformationen des verkapselten Frames zu kennzeichnen.

VID *(VLAN Identifier):* VLAN-Nummer, zu dem der Rahmen gehört.