Aktive Netzwerkkomponenten

Michael Dienert

24. April 2020

Inhaltsverzeichnis

1 Einige wichtige Begriffe

1.1 Hierarchisch organisierte Netze

Access : Switches mit VLAN-Support, PoE, Port Security; Stellt Switchports für Hosts bereit → Interface to End Devices.

> Die Access-Schicht verbindet **End**-Geräte mit dem Netzwerk und kontrolliert, welche Geräte miteinander über das Netz kommunizieren dürfen.

Distribution : Switches mit Layer3-Support, ACLs

- VLANS, Subnetze, Inter-VLAN-Routing
- Redundante Verbindungen
- ACLs

Core : Zusammenfassen des Datenverkehrs vom Distribution-Layer: schnelle Switches (very high forwarding rate); Core-Layer = High-Speed-Backbone, nur schnelles Switching, kein Routing, keine ACLs

1.2 Kollisions- und Broadcastdomänen

Collision Domain : alle Geräte, die auf Layer 1 miteinander verbunden sind, bilden eine Kollisionsdomäne. Dies kann entweder eine Punkt-zu-Punkt Verbindung zwischen zwei Geräten sein oder eine Busleitung, die mehrere Teilnehmer über einen gemeinsamen Bus verbindet. Ein Ethernet-Segment stellt somit eine Kollisionsdomände dar. Bridges und Switches *filtern* Kollisionen und **trennen** damit Kollisionsdomänen voneinander.

> **jeder beschaltete** Switchport stellt eine Kollisionsdomäne dar.

Broadcast Domain : in einer Broadcastdomäne erreicht ein von einem Teilnehmer gesendeter Broadcast **alle** anderen Netzteilnehmer. Ein Broadcast wird nicht geroutet, gelangt also **nicht** über einen Router hinweg:

> Switches filtern Broadcasts **nicht**; Eine Ansammlung untereinander verbundener Switches stellt eine Broadcastdomände dar. Router trennen BC-Domains ⇒ VLANs und Subnetze bilden jeweils eine BC-Domain.

2 Repeater

2.1 Repeater in der Funktechnik

Der Begriff Repeater stammt aus der Funktechnik. Damit werden Anlagen bezeichnet, die ein Funksignal empfangen und mit leicht veränderter Trägerfrequenz wieder aussenden (Abb. 1). Für das dabei verwendete, kombinierte Empfangs- und Sendegerät nennt man **Transceiver** (Transmitter-Receiver).

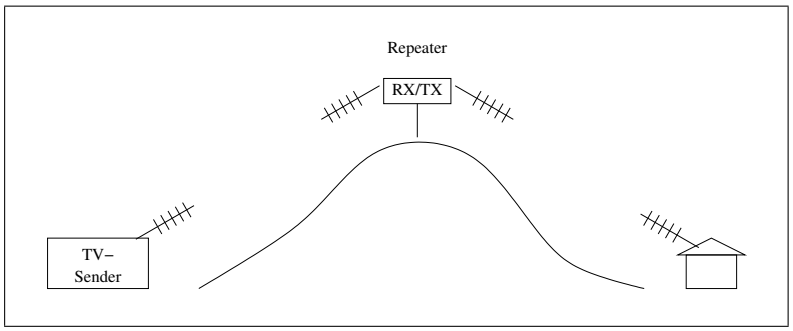

Abbildung 1: Repeater zur Vermeidung von Funkschatten

2.2 Repeater in der Netzwerktechnik

Ein klassischer Netzwerk-Repeater verbindet zwei 10Base2 oder 10BASE5 Ethernet-Segmente. Er arbeitet auf der Netzwerkschicht 1. Abb. 2 zeigt den internen Aufbau.

Wie man sieht, besteht der Repeater einfach nur aus zwei hintereinandergeschalteten Transceivern, die das Ethernet-Signal in je ein RX- und TX-Signal aufteilen.

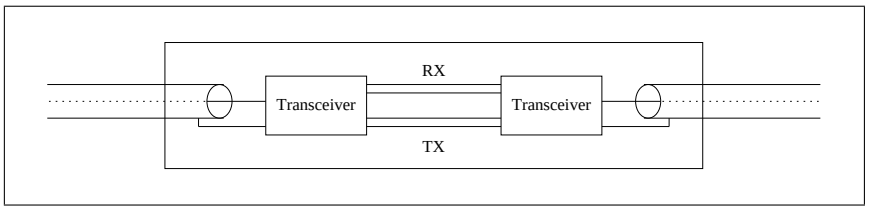

Abbildung 2: Klassischer Repeater zur Verbindung zweier Ethernetsegmente

Die Abb. 3 wiederum zeigt das Blockschaltbild eines Transceivers. Der Transceiver enthält je einen Verstärker (Dreieckssymbol) für die Sende- (TX) und die Empfangsrichtung (RX).

Zusätzlich sind noch je zwei Übertrager (Trafos) vorhanden. Diese wandeln das asymmetrische Signal auf der Koax-Leitung in ein symmetrisches Signal, wie es z.B. auf TP-Leitungen verwendet wird. Zusätzlich sorgen sie noch für eine Potentialtrennung: Nur Wechselspannungen werden von den Trafos weitergeleitet. So wird sichergestellt, dass keine hohen Ausgleichströme durch die Netzwerkleitungen fliessen. Ausgleichsströme können entstehen, wenn das Massepotential an den Enden einer Übertragungsstrecke unterschiedlich ist.

2.2.1 Remote-Repeater

Bei einem Remote-Repeater werden die beiden Transceiver durch ein bis zu 1000m langes Stück LWL verbunden (Abb. 4.

3 Hubs

Hubs verbinden mehrere Twisted-Pair-Segmente über je einen Transceiveranschluss mit dem **Ethernet**.

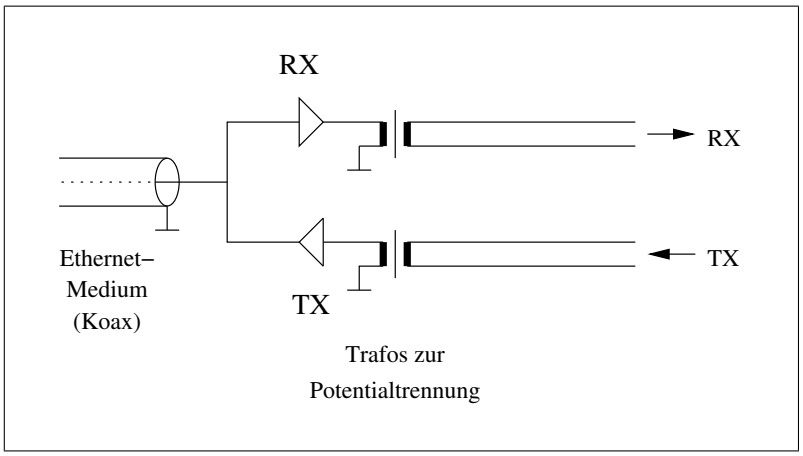

Abbildung 3: Blockschaltbild eines Transceivers

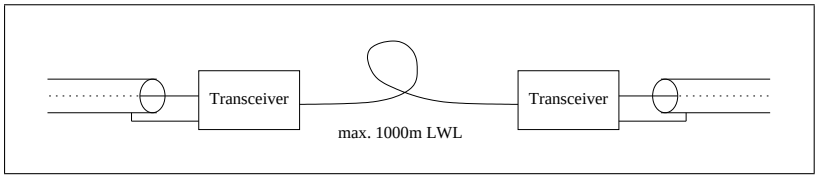

Abbildung 4: Blockschaltbild eines Remote-Repeaters

Abb. 5 zeigt das Blockschaltbild.

Hubs als Multiport-Repeater arbeiten ebenfalls auf Schicht 1.

Der Ausdruck **Hub** heisst auf Deutsch **Nabe**. Er soll verdeutlichen, dass von einem Hub mehrere TwistedPair-Segmente wie die Speichen eines Rades abgehen. Virtuell wird damit die Busstruktur des Ethernets in eine Sternstruktur überführt.

In der Realität hat man es aber nach wie vor mit dem Ethernet-Bus zu tun: Das Ethernetsegment ist einfach nur in den Hub integriert.

Auch die Transceiver, die bei Koax-Ethernet in der Nähe der Hosts oder sogar direkt auf den Netzwerkkarten sitzen, sind ebenfalls ins Gehäuse des Hubs gewandert.

> Da im Innern des Hubs der gesamte Datenverkehr immer noch über eine Leitung geht, ist mit einem Hub kein Full-Duplex-Betrieb möglich und **alle Twisted-Pair-Anschlüsse des Hubs bilden eine Kollisionsdomäne**.

4 Bridges

Die Anschlüsse eines Repeaters oder Hubs bilden eine Kollisionsdomäne, für die die Längenbeschränkungen des Ethernets gilt.

Um diese Einschränkung aufzuheben, wurden Bridges entwickelt:

> Eine Bridge trennt Ethernet-LANs physikalisch: fehlerhafte Pakete oder Kollisionen gelangen nicht über die Bridge hinweg.

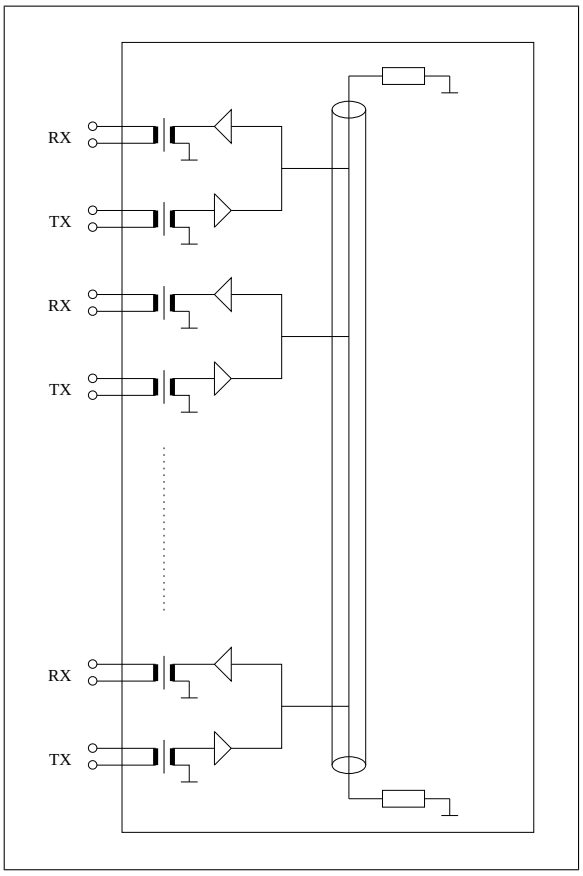

Abbildung 5: Blockschaltbild eines Hubs

Damit das funktioniert, muss die Bridge auf Schicht 2 arbeiten: eine Bridge liest *vollständig* die ankommenden Ethernet-Frames ein und wertet die Rahmenprüfsumme (FCS) sowie Quell- und Zieladressen aus.

Durch das Einlesen und Analysieren des Rahmens entstehen Verzögerungen.

Wie man in Abb. 6 erkennt, enhält eine Bridge eine CPU mit ROM für das Betriebssystem und RAM für das Speichern einer Adresstabelle:

Während des Betriebs lernt die Bridge, auf welcher Seite welche physikalische Adresse (= Hardwareadresse, MAC-Adresse) ist und speichert diese Information in einer Adresstabelle.

Ist diese Tabelle aufgebaut, werden Pakete, deren Zieladresse auf der selben Seite wie die Quelladresse liegt, verworfen. D.h. die Bridge lernt selbstständig, welche Pakete weitergeschickt werden müssen und welche nicht.

Durch diese Filterung werden unnötige Kollisionen vermieden und die Längenbeschränkungen des Ethernets aufgehoben.

Hier nocheinmal zusammengefasst die Vor- und Nachteile einer Bridge:

- Trennung von Kollisions-Domänen
- Erhöhter Durchsatz, da Segmente sich nicht gegenseitig durch Kollisionen aus-

bremsen.

- Werden in einem Netzwerk mehrere Bridges eingesetzt, kommunizieren diese miteinander um Netzwerkschleifen zu verhindern (Spanning-Tree-Protokoll).
- Da jedes Paket zur Analyse gepuffert werden muss, erzeugen Bridges Vwerzögerungen.

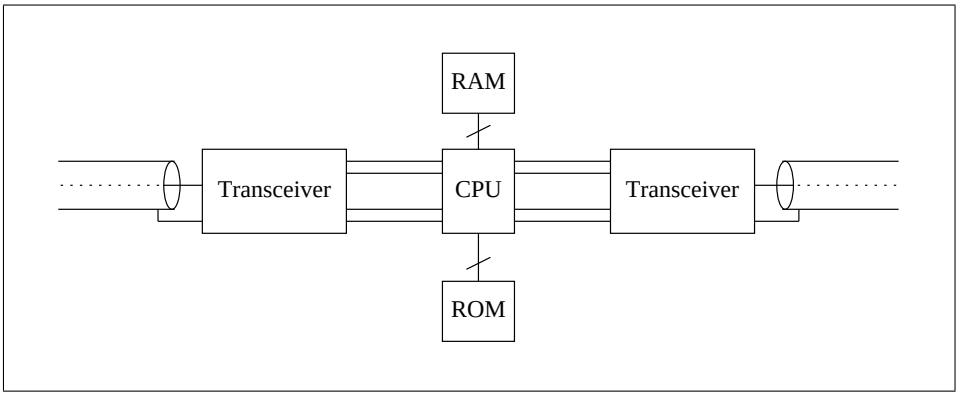

Abbildung 6: Blockschaltbild einer Bridge

5 Switches

Ein Switch ist die Weiterentwicklung einer Bridge mit mehr als 2 Ports.

5.1 Bauformen

Es werdem 3 verschiedene Arten unterschieden:

Shared Memory Switch - die Transceiver aller Ports werden von einer zentralen CPU mit Daten versorgt. Die Kommunikation zwischen 2 Ports findet dabei über **einen** zentralen Speicher statt. Da sich alle Ports diesen zentralen Speicher teilen müssen, entsteht an dieser Stelle ein Flaschenhals.

Common Bus Switch - jeder Transceiver erhält einen eigenen, lokalen Pufferspeicher. Die einzelnen Speicher werden über einen zentralen Bus, der mit hoher Bandbreite arbeitet, verbunden.

Crosspoint Matrix - das ist eine Weiterentwicklung der Common-Bus-Technik, bei der die einzelnen Speicher über einen Kreuzschienenverteiler verbunden werden. Abb. 7 zeigt das Schema.

5.2 Betriebsarten

Neben den drei Bauformen unterscheidet man noch zwischen folgenden Switch-Betriebsarten:

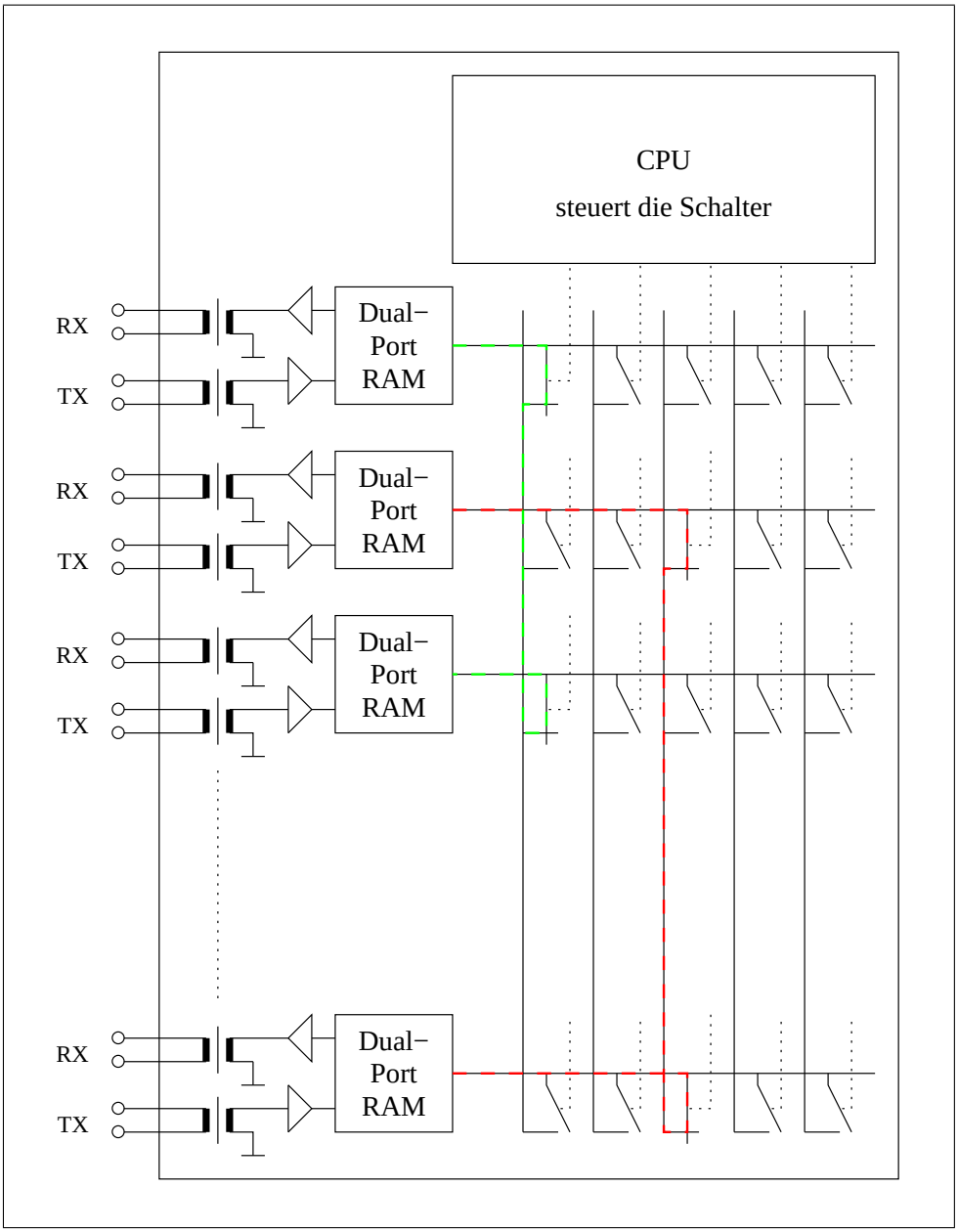

Abbildung 7: Blockschaltbild eines Switches mit Crosspoint-Matrix

Cut-Through-Switching - auch On-The-Fly-Switching genannt: das ankommende Paket wird so schnell als möglich zum Zielport weitergeleitet. D.h. sobald der Frame bis zur Zieladresse gelesen wurde, kann der entsprechende Port ausgewählt werden.

Nachteil dieses Verfahrens: da die Rahmenprüfsumme nicht ausgewertet wird, werden auch defekte Rahmen weitergeleitet.

Vorteil: geringe Latenzzeit

Rechenbeispiel für 10MBit/s:

$$t_{verzogerung} = (8+6) \cdot 8 \cdot 0.1\mu s + 9.6\mu s \approx 20\mu s$$

Erklärung: 8 Bytes Preamble, 6 Bytes Zieladresse, $0.1\mu s$ pro bit, $9.6\mu s$ Inter-Frame-Gap

Fragment-Free-Switching - das ist eine Variante von Cut-Through mit dem Unterschied, dass bei Fragment-Free die ersten 64 Bytes eines Rahmens eingelesen werden.

Vorteil gegenüber Cut-Through: falls am entsprechenden Switch-Port eine Kollision auftritt, wird diese erkannt und das Jamming-Signal gesendet.

Store-And-Forward-Switching - diese Betriebsart entspricht derjenigen von Bridges: der gesamte Rahmen wird eingelesen, gepuffert und die Prüfsumme wird ausgewertet.

Verzögerung je nach Frame-Länge. Z.B. bei 10MBit/s: $67 \cdots 1230\mu s$

6 Layer3-Switching

Layer3-Switching ist eine Kombination aus Switching (Layer2) und Routing (Layer3). Funktioniert nur in reinen IP-Netzen (Kein IPX).

Funktion: Der Switch liest **sämtliche** Ethernet-Frames des ersten IP-Pakets, analysiert Source- und Destination IP-Adresse und *routet* das Paket (Layer3). Alle Folgepakete dieser Kommunikationspartner können anschliessend auf Layer2 auf Basis der MAC-Adressen im reinen Switch-Betrieb weitergeleitet werden.

7 Port Security

Mittels Port Security kann man die Anzahl an MAC-Adressen, die an einenm Switchport auftauchen dürfen einschränken. Je nach Konfiguration kann man dabei genau eine MAC-Adresse oder auch eine begrenzte Menge erlauben.

Dabei gibt es 3 Arten, wie diese MAC-Adressen eingetragen werden:

Static Secure MAC-Address: hier wird genau eine MAC-Adresse erlaubt und diese wird manuell eingetragen

Dynamic Secure MAC-Address: hier kann man eine begrenzte Zahl MAC-Adressen erlauben, die der Switch in der Adresstabelle speichert. Diese werden bei einem Neustart des Switches gelöscht. Diese Einstellung schützt vor dem Angriff "*MAC-Address-Flooding*".

Sticky Secure MAC-Address: wie Dynamic Secure MAC-Address, nur werden die gelernten MAC-Adressen der Running-Config hinzugefügt. Durch Kopieren der Running-Config in die Startup-Config können diese Adressen dauerhaft gelernt bleiben.

Fall an einem Switchport eine Verletzung der eingestellten Sicherheitsrichtlinie auftritt, kann man den Switch konfigurieren, sich wie folgt zu verhalten:

Shutdown: der Switchport wird gestoppt, d.h. er sendet und empfängt keine Frames mehr. Dieser Zustand kann nur manuell wieder beseitigt werden. Der Shutdown-Modus ist die Default-Einstellung.

Protect: der Switchport leitet Frames mit der nicht erlaubten MAC-Adresse einfach nicht weiter.

Restrict: keine Weiterleitung von Frames und zusätzlich ein Eintrag in die Syslog-Datei sowie ein Hochzählen eines *Violation Counters*

8 VLANs

Ein VLAN ist ein von einem oder mehreren Switches logisch abgeteiltes Netz, das eine eigene **Broadcastdomäne** bildet.

Das bedeutet:

- Broadcasts sind nur innerhalb eines VLANs sichtbar
- Das Adress-Resolution-Protocol löst IP-Adressen mit Broadcast-Anfragen auf: IP-Adressen die **nicht** im **eigenen** VLAN liegen werden nicht aufgelöst. Auch dann nicht, wenn die Hosts aus verschiedenen VLANs am selben Switch angeschlossen sind.
- Um Pakete zwischen VLANs auszutauschen, muss Routing auf Schicht 3 stattfinden.
- Die Hosts im eigenen VLAN sind dagegen ohne Routing erreichbar.

8.1 Bildung von VLANs

portbasierte VLANs: in welchem VLAN ein Switchport liegt wird manuell konfiguriert: d.h. bestimmte Ports eines oder mehrerer Switches werden zusammengefasst (gruppiert) und damit einem VLAN zugeordnet. Diese VLAN-Port-Zuordnung ist fest (=statisch).

dynamische VLANs = Layer-2-VLANs: hier hängt die Zugehörigkeit zu einem VLAN von der MAC-Adresse ab: der Switch prüft bei jedem ankommenden Frame die Quell-MAC-Adresse und ordnet den *Switchport über den das Paket hereinkommt* dynamisch dem gewünschten VLAN zu.

Die Zugehörigkeit zum VLAN wird in einer Tabelle gespeichert. Erstrecken sich ein VLAN über mehrere Switches, müssen diese Tabellen auf allen Switches synchronisiert werden.

protokoll-basierte VLANs = Layer-3-VLANs: bei Layer-3-VLANs erfolgt die Zuordnung zu einem VLAN auf Basis der Layer-3-Adresse

8.2 Mehrere VLANs auf einer Leitung: Trunking

Möchte man VLANs einrichten, die sich über mehr als einen Switch erstrecken, hat man folgendes Problem: zwischen den Switches benötigt man für jedes VLAN eine eigene Leitung und auf jeder Seite jeweils einen Switchport. Bei mehreren VLANs hätte man damit nicht nur eine einzelne Uplink-Leitung sondern ein ganzes *Bündel*. Solch ein Leitungsbündel wird auf englisch *Trunk* genannt.

Grund: überträgt man die Frames verschiedener VLANs über eine Leitung zu einem Switch, kann der Switch die ankommenden Frames nicht mehr den definierten VLANs zuordnen.

Abhilfe: man erweitert die Ethernet-II-Frames um 4 Bytes, die direkt vor dem Type-Feld eingefügt werden. Diese 4 Bytes enthalten u.A. eine VLAN-ID. Man nennt diese 4 Bytes **VLAN-Tag** (Tag = Schildchen).

12 bit innerhalb dieser 4 Bytes legen die Zugehörigkeit zu einem bestimmten VLAN fest. Abb. 8 zeigt die Details:

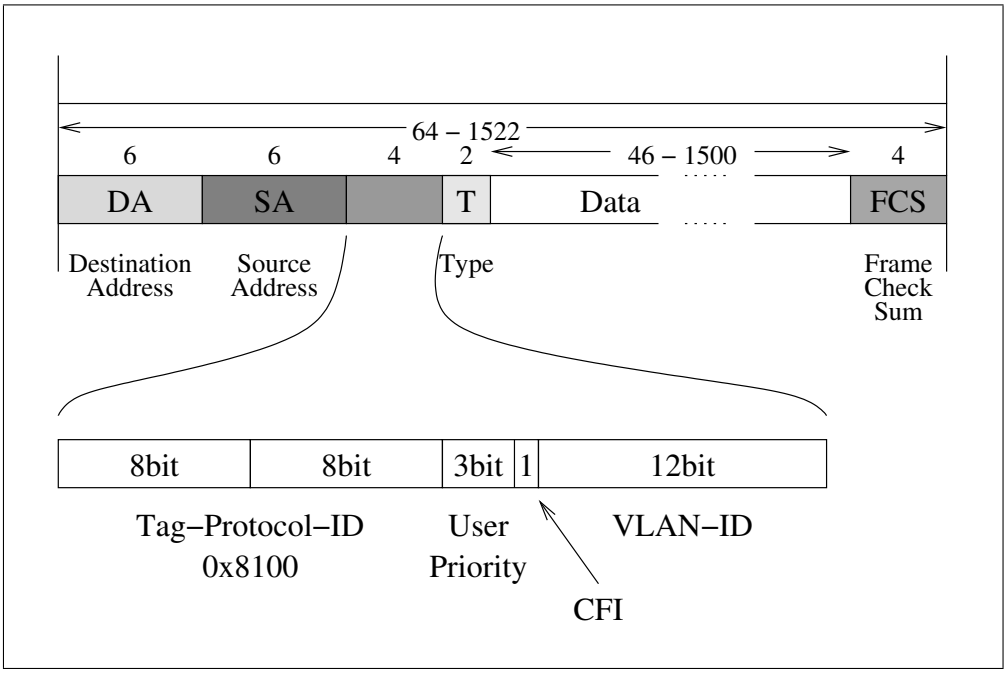

Abbildung 8: Ethernet-Frame mit VLAN-Tag nach IEEE802.1Q

Tag-Protocol-ID (TPID): fester Wert 0x8100, diese ID identifiziert den Frame als IEEE802.1Q-Frame

Priority Code Point (PCP): mit diesem 3-bit-Wert können Frames bevorzugt transportiert werden. Niedrigste Priorität: 001=1, Standard-Priorität:000=0, höchste Priorität:111=7

Canonical Format Indicator (CFI): für Kompatibilität zwischen Ethernet und TokenRing. Bei Ethernet ist CFI=0

VLAN-Identifier (VLAN-ID): 12bit VLAN-ID.

Durch die VLAN-ID kann ein Switch nun auch Frames, die über einen einzelnen Port eintreffen wieder den richtigen VLANs zuordnen.

Das Einfügen des VLAN-Tags gestattet es also, verschiedene VLANs auf einer gemeinsamen Leitung zwischen Switches zu übertragen. Natürlich müssen sich die VLANs dabei die zur Verfügung stehende Bandbreite teilen.

8.2.1 Trunk-Port oder Tagged-Port

Da man sich durch das VLAN-Tagging das Verlegen eines Leitungsbündels (engl. **Trunk**) spart, nennt man im Cisco-Umfeld Ports, die Frames mit VLAN-Tag empfangen und senden können **Trunk-Ports**.

Bei Geräten von HP dagegen, spricht man von einem **Tagged-Port**.

8.2.2 Access-Ports und Untagged-Ports

Da das VLAN-Tag direkt nach der Quell-Mac-Adresse eingefügt wird, wird ein Gerät, das 802.1Q nicht unterstützt, den Rahmen als ungültig ansehen und verwerfen.

Nun sind die meisten Netzwerkkarten noch nicht VLAN-fähig. Das heisst, der Switch muss an allen Ports, an denen Computer mit normalen Netzwerkkarten angeschlossen sind, das VLAN-Tag wieder entfernen, bevor der Rahmen ausgesendet wird.

Solche Ports heissen bei Cisco **Access-Ports** und bei HP **Untagged-Ports**

9 Spanning-Tree

STP benötigt 3 Schritte, um zu einer schleifenfreien Netztopologie zu kommen:

1. Wahl der Root-Bridge: Um eine schleifenfreie Topologie zu erhalten, wird ausgehend von einer sog. **Root Bridge** eine Baumstruktur im Netzwerk erzeugt. Der erste Schritt zu dieser Struktur ist also die Festlegung der Root Bridge.

Werden die Switches (Bridges) eines Netzwerks eingeschaltet, geht jedes Gerät zunächst davon aus, selbst Root Bridge zu sein und versendet BPDUs. Die Switchports befinden sich dabei im Blocking-Status, d.h. leiten keine Datenframes weiter, tauschen aber BPDUs aus. Die Bridge mit der kleinsten Bridge-ID (siehe Abb. 9, Aufbau der Bridge-ID) gewinnt das Rennen und wird Root Bridge.

> Nur Root Bridges **erzeugen** BPDUs. Alle Nicht-Root Bridges versenden nur BPDUs, wenn sie eine BPDU empfangen haben, d.h. sie leiten BPDUs lediglich weiter (Relaying).

2. Festlegung der Root Ports Alle Nicht-Root Bridges müssen nun genau einen Root-Port festlegen:

> Root-Port wird der Switchport, der der Root Bridge bezüglich der Pfadkosten am nächsten liegt. D.h. Root-Port wird der Port, der die BPDU mit den geringsten Pfadkosten von der Root Bridge empfangen hat. Bei gleichen Pfadkosten entscheidet die Port-ID (bei redundanten Verbindungen).

Bandbreite/	STP Kosten
10 MBit/s	100
100 MBit/s	19
1 GBit/s	4
10 GBit/s	2

Tabelle 1: STP Wegkosten

Hier die STP-Wegkosten:

3. Bestimmung der Designated Ports Jedes **Segment** im Netzwerk muss genau einen Designated Port haben. Ein Segment ist dabei einfach eine Punkt-zu-Punkt Verbindung zwischen zwei Switchports.

Der Port eines Segments mit den geringsten Pfadkosten in Richtung der Root Bridge wird Designated Port. Bei gleichen Wegkosten, wird der Port der Bridge mit der kleineren Bridge-ID zum Designated-Port. Alle Ports ausser den Designated Ports und den Root Ports sind im Status *Blocking*, d.h. sie leiten keine Frames weiter.

Aus voriger Aussage folgt, dass die Root Bridge ausschliesslich Designated Ports besitzt.

BPDU : Bridge Protocol Data Unit; werden alle 2s versandt (Hello-Timer)

Bridge-ID :

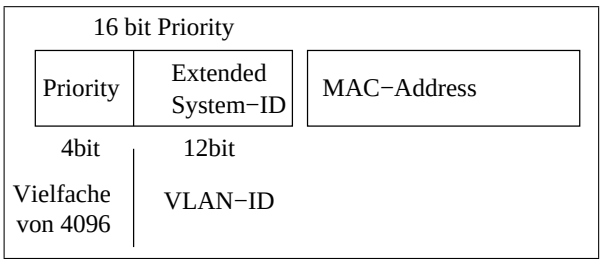

Abbildung 9: Aufbau der Bridge-ID

Root-Bridge : Die Bridge mit der **kleinsten** Bridge-ID wird Root-Bridge.

Network-Diameter : Da STP in der Default-Einstellung mit einem Network-Diameter von 7 “Hops” arbeitet, ist nach 14 s die Root-Bridge bestimmt.

Max-Age : empfängt ein Switch 20s lang keine BPDUs (also 10 aufeinanderfolgende BPDUs), wird ein neuer Root-Election-Prozess gestartet.

Forward-Delay : Zeit, die im Listening und Learning Status verbracht wird

Port-States :

STP	RSTP
Blocking (20s)	
Listening (15s)	Discarding (Schleifen auflösen)
Learning (15s)	Learning (MAC-Adr. Tabelle füllen
Forwarding	Forwarding
Disabled	Discarding

Pfadkosten

Strecke	Kosten
10Gbit/s	2
1Gbit/s	4
100MBit/s	19
10 MBit/s	100

Port-Rollen :

Root-Ports :

- Root-Ports sind der Root-Bridge am nächsten, d.h. haben kleinste Pfadkosten Richtung Root-Bridge
- Nur ein Port pro Switch kann Root-Port sein; haben mehrere Ports gleiche Pfadkosten, entscheidet die Port-Priority
- Die Root-Bridge selbst hat nur Designated-Ports

Designated und Non-Designated Ports :

- Jedes Segement = Verbindung Switch-Switch hat genau einen **Designated Port**,der andere Port wird **Non-Designated-Port**, wenn die Verbindung nicht Richtung Root-Bridge weist (also sozusagen zwei Äste des Baums **quer** verbindet).
- Dabei wird wieder über die Wegekosten entschieden: Der Port mit den geringsten Wegkosten Richtung Root-Bridge wird Designated Port.
- Bei gleichen Wegkosten wird der Port auf dem Switch mit der kleineren Bridge-ID zum Designated Port.

Edge-Ports :

- entspricht Portfast; Edge-Ports gehen sofort in den Forwarding-State
- Edge-Ports werden zu normalen ST-Ports, sobald sie ein BPDU empfangen

Alternate-Ports (nur bei RSTP) :

- Entspricht Non-Designated-Port einer "Querverbindung" (s.o.) bei STP; im Normalfall im Discarding-State
- Wird zu einem Designated-Port und wechselt in den Forwarding-State, wenn der Pfad über den Designated-Port ausfällt.

Backup-Port (nur bei RSTP) :

- Nur bei redundanten (parallelen) Verbindungen; Normalszustand: Discarding
- Wechselt nach Forwarding, wenn paralleler Pfad ausfällt

Link-Types :

- Point-to-Point : Full-Duplex; nur Point-to-Point Designated Ports können bei RSTP den Schnellübergang Discarding $\rightarrow$ Forwarding machen.
- Shared Link : Half-Duplex, z.B. Verbindung zu einem Hub.