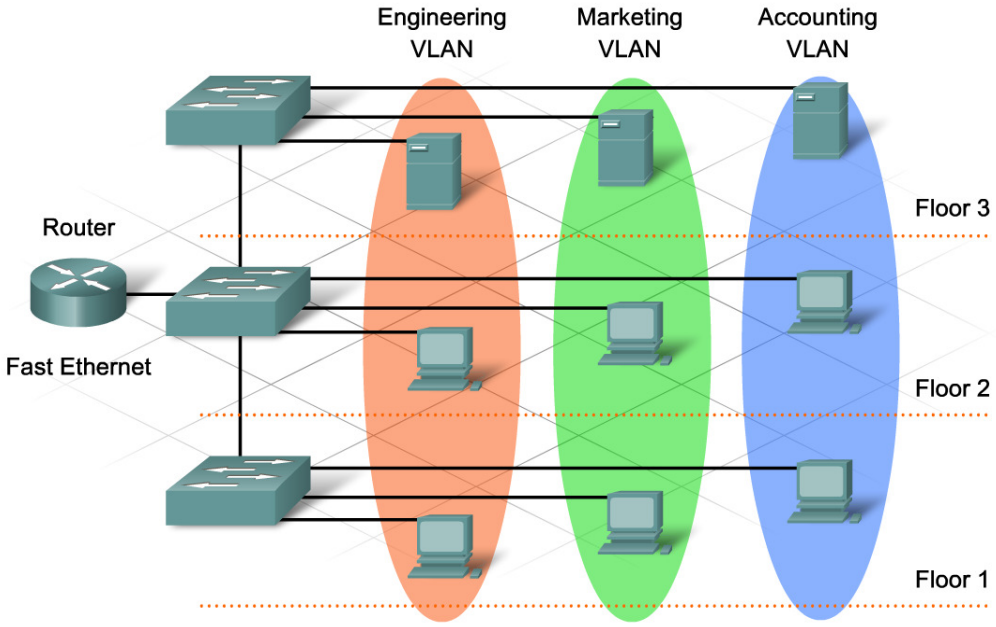
VLANs unterteilen ein bestehendes einzelnes physisches Netzwerk in **mehrere logische Netzwerke (Segmente)**. Jedes VLAN bildet eine eigene Broadcast-Domain. Die Teilnehmer eines Segments können sich dabei an beliebigen Orten im physikalischen LAN befinden. Eine Kommunikation zwischen zwei unterschiedlichen VLANs ist nur über einen Router möglich, der an beide VLANs angeschlossen ist. VLANs verhalten sich also so, als ob sie jeweils mit eigenen, voneinander unabhängigen Switches aufgebaut wären

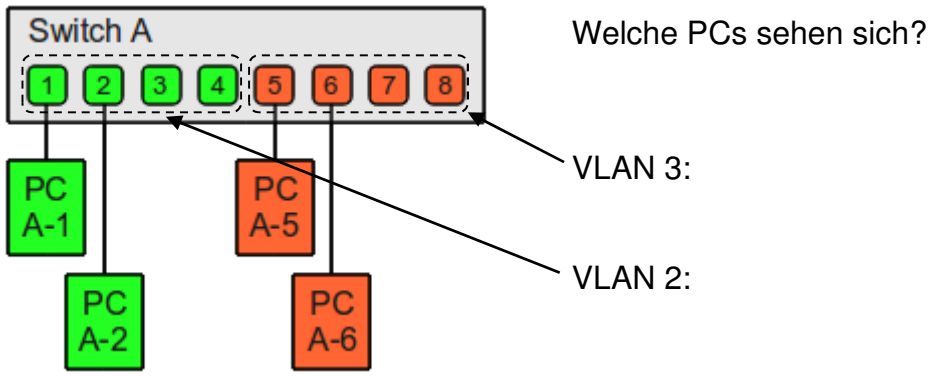


Man unterscheidet zwei Arten von VLANs:

- Portbasierte VLANs (untagged) to tag:
- Tagged VLANs

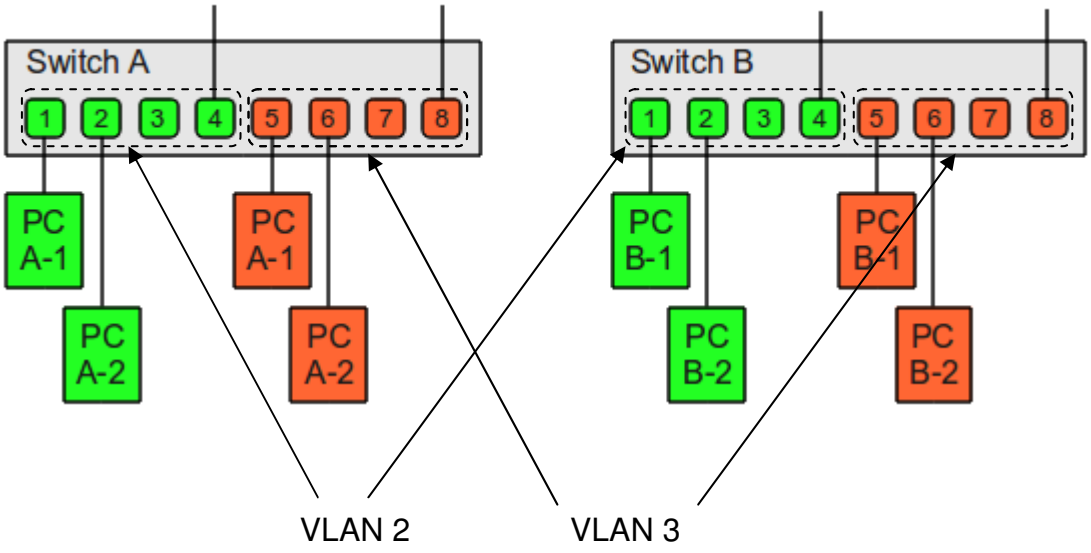
Portbasierte VLANs

Mit portbasierten VLANs unterteilen Sie einen einzelnen managebaren Switch einfach auf mehrere logische Switches. Im folgenden Beispiel teilen wir einen physischen 8-Port Switch (Switch A) auf zwei logische Switches auf:



Erstrecken sich zwei VLANs über zwei Switches, so benötigt man bei portbasierten VLANs zwei Patchkabel.

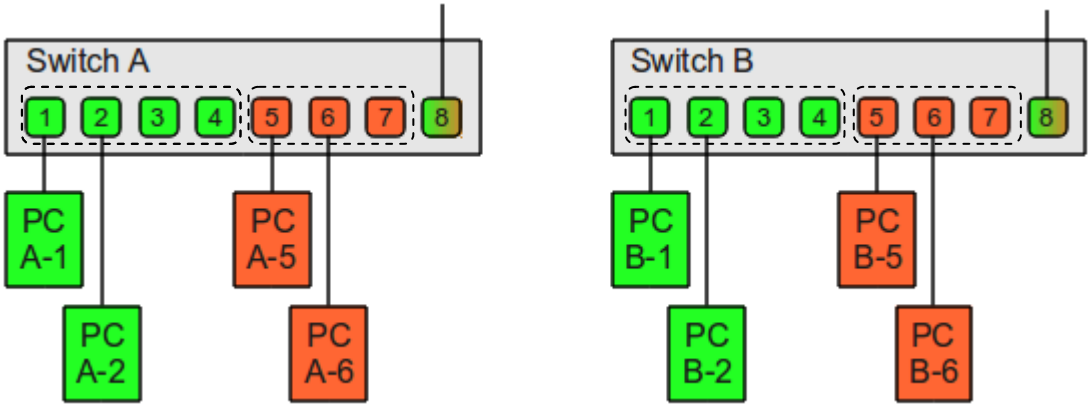
Aufgabe: Zeichnen Sie die Patchkabel ein!



Tagged VLANs

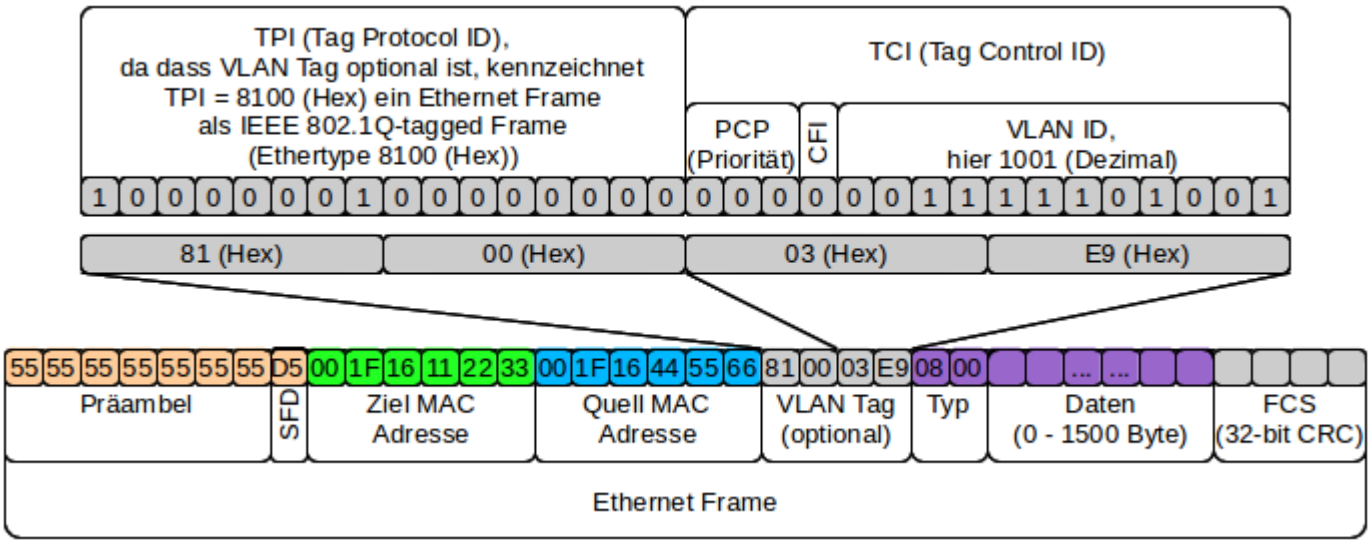
Bei tagged VLANs können mehrere VLANs über einen einzelnen Switch-Port genutzt werden. Die einzelnen Ethernet Frames bekommen dabei Tags angehängt, in dem jeweils die VLAN-ID vermerkt ist, zu dessen VLAN das Frame gehört. Wenn im gezeigten Beispiel beide Switches tagged VLANs beherrschen, kann damit die gegenseitige Verbindung mit einem einzelnen Patchkabel (trunk) erfolgen:

Aufgabe: Zeichnen Sie den Trunk ein!



Einbettung des VLAN-Tag (IEEE 802.1q tagged frame) **in den Ethernet Frame**

Der VLAN-Tag wird am Eingang des Switchports dem Ethernet-Header hinzugefügt und am Ausgang des Switchports wieder entfernt.



PCP (Priority Code Point): legt die Priorität des VLAN-Frames fest, Wert 7 (höchste Priorität), wird benutzt für die Klassifizierung von verschiedenen Daten (Type of Service ToS) wie Voice (5), Video (4), kritische Produktivdaten (3) usw.
CFI: (Canonical Format Indicator): bei Ethernet Switches ist das Bit immer auf "0" gesetzt

Aufgaben: Berechnen Sie die Tag Control ID (TCI) für Ihre Bank binär und im Hexcode; bei den Daten handelt es sich um Video-Daten.

Wieviele VLANs lassen sich maximal bilden?

Wiederholung zum Ethernet Frame:

Präambel: dient zur Synchronisation der Übertragung zwischen Sender und Empfänger.
SFD (Start Frame Delimiter=Trennzeichen): feste Bitsequenz; dient als Startmuster des Datenrahmens.
Typ: Das Typ-Feld gibt Auskunft über das Protokoll der nächst höheren Schicht.
PAD: Das PAD-Feld taucht in der Darstellung nicht auf, weil es oft nicht erforderlich ist. Es wird nämlich nur dann benötigt, wenn der Ethernet-Frame nicht die Minimalgröße von 64 Byte erreicht. In diesem Fall füllt das PAD-Feld den Ethernet-Frame bis zur Minimalgröße auf.
FCS (Frame Check Sequence): Die FCS wird beim Sender erstellt und an den Frame angehängt. Die Berechnung der FCS beginnt mit der Ziel-MAC-Adresse und endet mit dem PAD-Feld. Die Präambel, der SFD/SOF sowie die FCS selbst sind darin nicht enthalten. Der Empfänger des Frames macht selbst eine CRC-Berechnung und vergleicht die beiden Werte. Stimmen diese nicht überein, dann geht er davon aus, dass die Übertragung fehlerhaft war und verwirft den Datenblock.

Ferner unterscheidet man:

Statische VLANs

Hier wird einem Port eines Switches eine VLAN-Konfiguration fest zugeordnet. Er gehört dann zu einem Port-basierten VLAN oder zu einem tagged VLAN oder er ist ein Port, der zu mehreren VLANs gehört. Die Konfiguration eines Ports ist bei statischen VLANs fest durch den Administrator vorgegeben. Sie hängt nicht vom Inhalt der Pakete ab und steht im Gegensatz zu den dynamischen VLANs unveränderlich fest. Damit ist eine Kommunikation des Endgerätes an einem Port nur noch mit den zugeordneten VLANs möglich.

Dynamische VLANs

Wird ein Gerät an einen Switch angeschlossen, erhält dieser von dem Management System die Information, zu welchem VLAN-Segment die neue MAC-Adresse gehört. Der Switch ordnet das Gerät dann automatisch zu. So können Administratoren schnell und flexibel Änderungen im Netzwerk durchführen, ohne im Rechenzentrum Ports umstecken oder Konfigurationen im Switch ändern zu müssen. Da sich alle Inhalte von Frames praktisch beliebig manipulieren lassen, sollte in sicherheitsrelevanten Einsatzbereichen auf den Einsatz von dynamischen VLANs verzichtet werden.

Vorteile von VLANs:

-
-
-
-
-