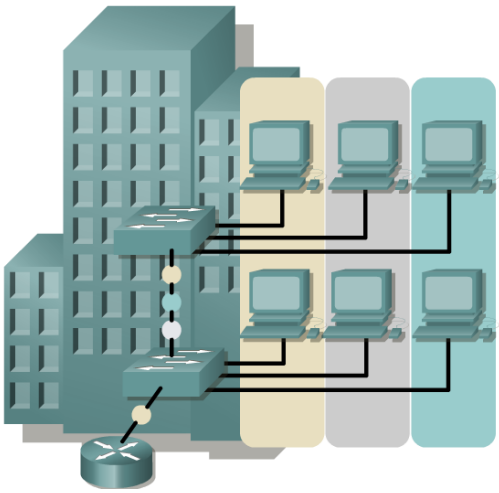
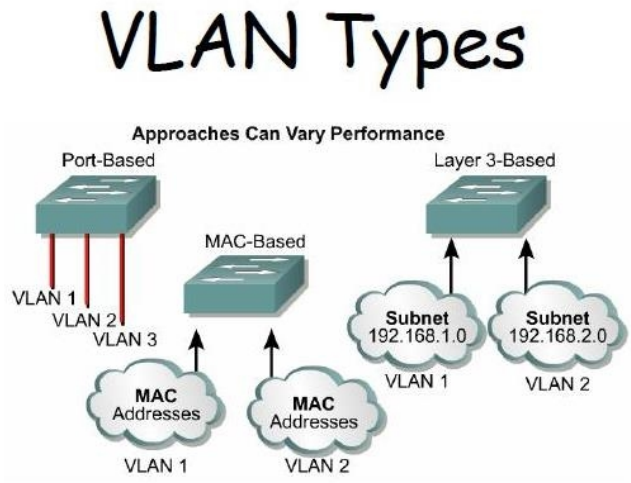
## VLAN - virtuelle lokale Netzwerke



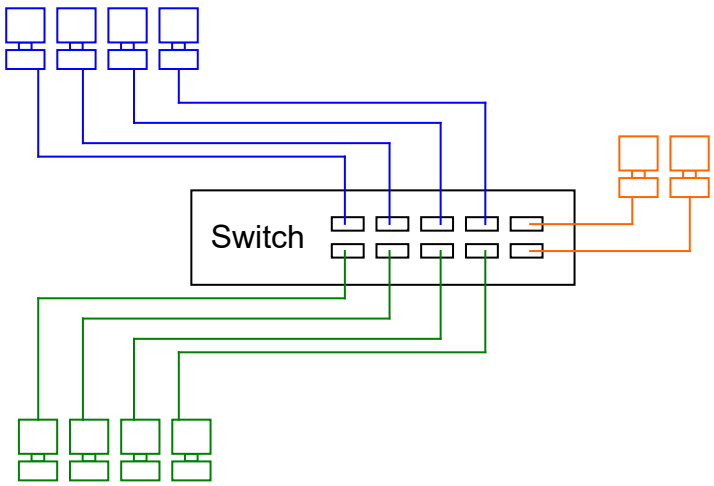
**VLAN =** Netzstruktur mit allen Eigenschaften eines gewöhnlichen LAN, jedoch ohne räumliche Bindung. Ermöglicht u.a. weiter entfernte Knoten zu einem virtuellen lokalen Netzwerk zu verbinden. Die logische Segmentierung erfolgt mit Switches.




Üblich sind drei VLAN-Typen:
portbasiert
MAC-Adressen basiert - selten implementiert
protokollbasiert

### 1. Port-basierende VLANs (Statisches VLANs)

Die Ports eines Switches werden unterschiedlichen VLANs zugeordnet. An einem Port können immer nur Angehörige desselben VLANs angeschlossen sein.




\+ Die starre Zuordnung zwischen Port und VLAN vereinfacht die Fehlersuche.
\+ Broadcasts sind auf das jeweilige VLAN begrenzt (hohe Sicherheit).
\- Geringe Flexibilität bei Umzügen, der Umzug einer Station muß durch den Administrator im VLAN-Manager nachgeführt werden.
\- Soll eine Station zu mehreren VLANs gehören, sind mehrere NICs nötig.

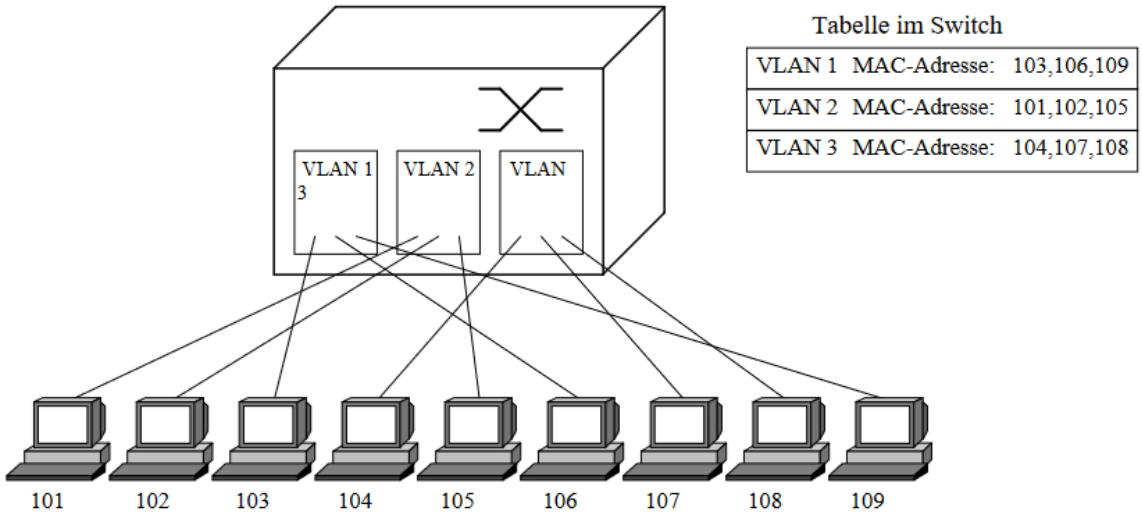
➔ Weit verbreitetesVerfahren. Standardisiert durch IEEE 802.1Q.

### Dynamische VLANs

Bei der dynamischen Implementierung eines VLANs wird die Zugehörigkeit eines Frames zu einem VLAN anhand bestimmter Inhalte des Frames getroffen. Da sich alle Inhalte von Frames praktisch beliebig manipulieren lassen, sollte in sicherheitsrelevanten Einsatzbereichen auf den Einsatz von dynamischen VLANs verzichtet werden. Dynamische VLANs stehen im Gegensatz zu den statischen VLANs. Die Zugehörigkeit kann beispielsweise auf der Basis der **MAC-** oder **IP-Adressen** geschehen, oder auch auf Anwendungsebene nach den **TCP-/UDP - Portnummern**. In der Wirkung entspricht dies einer automatisierten Zuordnung eines Switchports zu einem VLAN.

### 2. Level-2-VLANs

Die Zugehörigkeit zu einem VLAN richtet sich nach der **MAC-Adresse**. Der Switch muß bei jedem empfangenen Datenpaket entscheiden, zu welchem VLAN es gehört. So können an einem Port auch Stationen verschiedener VLANs angeschlossen sein.




+ Der Umzug von Stationen ist leicht möglich, da die Zuordnung zum VLAN ja erhalten bleibt.
- Aufwendige Konfiguration, da die MAC-Adressen aller Endgeräte erfasst werden müssen. Aufwändig bei mehreren Switches.

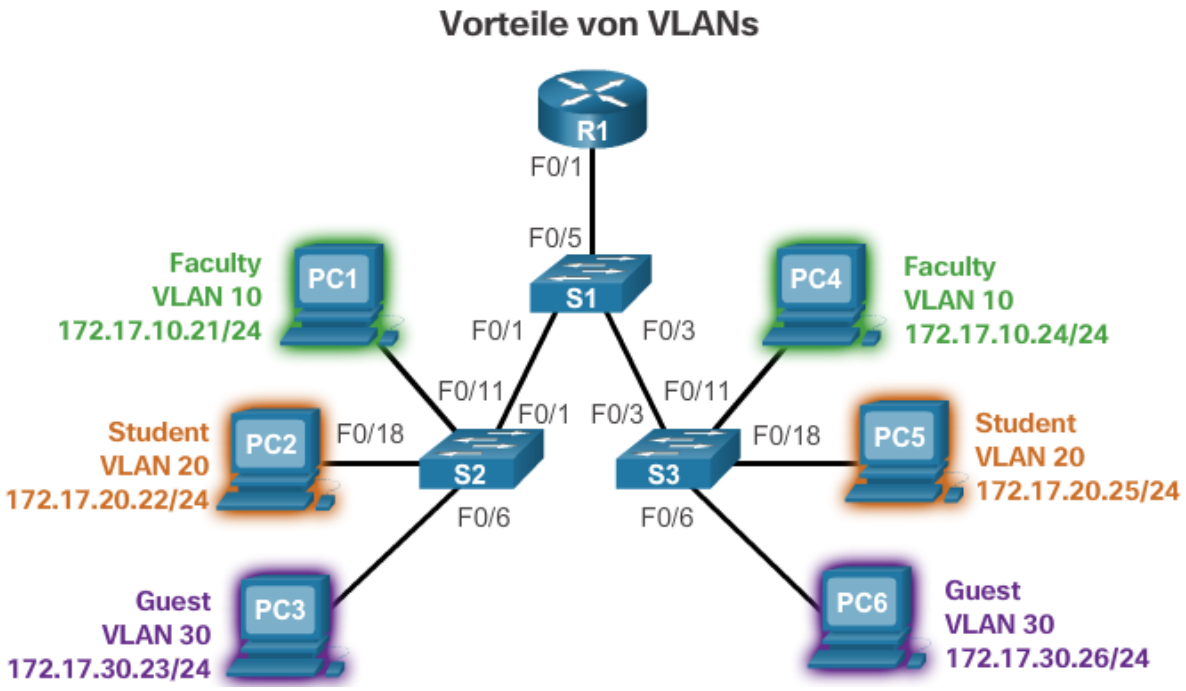
Sobald jedoch mehrere Switches vernetzt sind, muß sichergestellt werden, daß die Adreßtabellen in allen Switches konsistent sind. Dazu müssen regelmäßig Informationen über das Netz übertragen werden. Genau dies ist aber das **Hauptproblem der VLANs**. Jeder Hersteller verwendet für diesen Informationsabgleich eigene Verfahren. Deshalb verstehen sich die Switches verschiedener Produzenten oft nicht. U. a. gibt es:

- den regelmäßigen Austausch der Adreßtabellen mit MAC-Adressen und VLAN-Nummer. Die Tabellen werden etwa einmal pro Minute ausgetauscht.
- das Frame Tagging, bei dem die VLAN-Nummer als Tag vor das MAC-Paket gesetzt. Die zulässige Paketlänge kann dabei überschritten werden.
- das Zeitmultiplexverfahren, bei dem der Backbone zwischen den Switches in Zeit-Slots aufgeteilt wird, die fest den einzelnen VLANs zugeordnet sind.

### 3. Protokoll-basierende VLANs

Layer-3-Switches bieten zusätzliche Möglichkeiten durch Basis-Routing-Funktionalität. Der externe Router wird somit oft überflüssig. Diese Variante ist langsamer, da auch Layer-3-Informationen ausgewertet werden müssen. Die Zuordnung einzelner Datenpakete zu verschiedenen virtuellen LANs geschieht durch Auswertung der Subnetzadressen oder portbasiert. Innerhalb eines VLAN wird auf Layer 2 geswitcht.

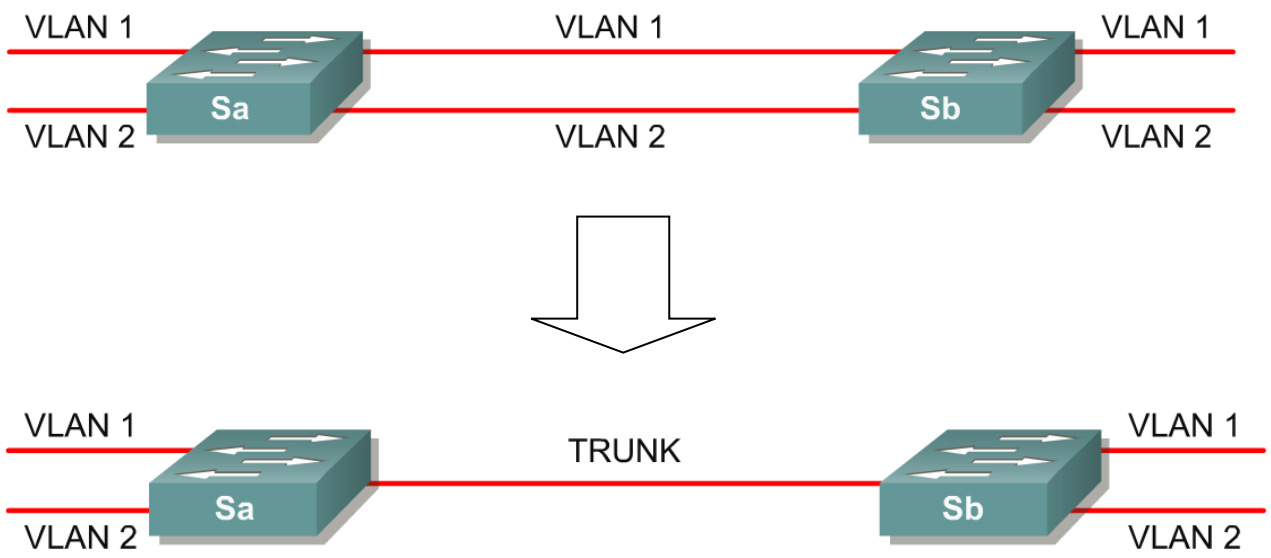
## Vorteile von VLANs



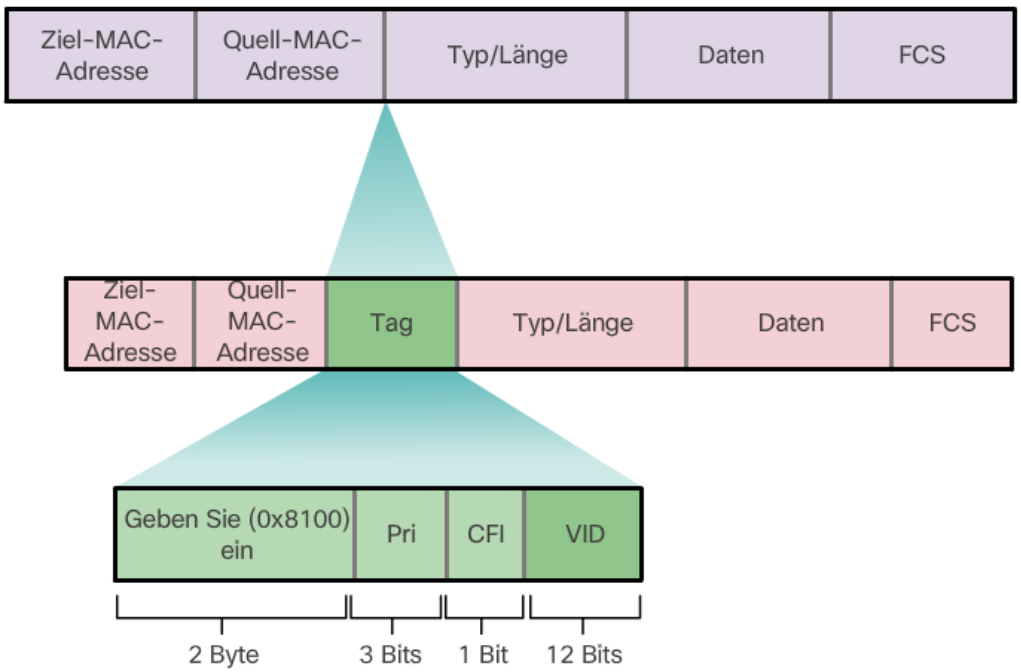

Benutzerproduktivität und Netzwerkflexibilität sind wichtig für Wachstum und Erfolg von Unternehmen. VLANs erleichtern die Entwicklung passender Netzwerke für die Ziele einer Organisation. VLANs bieten die folgenden wesentlichen Vorteile:

- **Sicherheit** – Gruppen mit sensiblen Daten können vom Rest des Netzwerks getrennt werden, um die Gefahr der Weitergabe vertraulicher Informationen zu reduzieren. In der Abbildung sehen Sie, dass sich die Computer der Fakultät im VLAN 10 befinden und komplett vom Datenverkehr der Studenten und Gäste getrennt sind.
- **Niedrigere Kosten** – Kosteneinsparungen durch Minimierung teurer Netzwerkupgrades und effizientere Nutzung vorhandener Bandbreiten und Uplinks.
- **Bessere Leistung** – Durch die Aufteilung flacher Schicht-2-Netzwerke in mehrere logische Arbeitsgruppen (Broadcast-Domänen) wird unnötiger Datenverkehr im Netzwerk reduziert und die Leistung verbessert.
- **Kleinere Broadcast-Domänen** - Durch die Aufteilung eines Netzwerks in VLANs wird die Anzahl der Geräte in der Broadcast-Domäne reduziert. In der Abbildung sehen Sie sechs Computer im Netzwerk und drei Broadcast-Domänen: Fakultät, Student und Gast.
- **Bessere IT-Effizienz** - VLANs erleichtern die Verwaltung des Netzwerks, da Benutzer mit ähnlichen Netzwerkanforderungen dasselbe VLAN verwenden. Wenn ein neuer Switch bereitgestellt wird, können alle bereits für das entsprechende VLAN konfigurierten Richtlinien und Prozeduren bei der Zuweisung der Ports implementiert werden. Außerdem können die IT-Mitarbeiter die Funktion der einzelnen VLANs durch die Vergabe passender Namen identifizieren. In der Abbildung hat VLAN 10 den Namen „Faculty“, VLAN 20 den Namen „Student”, und VLAN 30 den Namen „Guest“.
- **Einfachere Projekt- und Anwendungsverwaltung** - VLANs aggregieren Benutzer und Netzwerkgeräte zur Erfüllung geschäftlicher oder geografischer Anforderungen. Separate Funktionen erleichtern die Verwaltung von Projekten und die Arbeit mit spezialisierten Anwendungen. Ein Beispiel für eine solche Anwendung ist eine E-Learning-Entwicklungsplattform für die Fakultät.

**VLAN-Trunk**




**Felder in einem Ethernet-802.1Q-Frame**




Das VLAN-Markierungsfeld enthält die Felder Typ, Priorität, kanonische Formatkennung und VLAN-ID:

- **Typ** – Ein 2-Byte-Wert, der als TPID-Wert (Tag-Protokoll-ID) bezeichnet wird. Für Ethernet hat dieses Feld den Hexadezimalwert 0x8100.
- **Benutzerpriorität** – Ein 3-Bit-Wert, der die Implementierung von Stufen oder Diensten unterstützt.
- **Kanonische Formatkennung (CFI)** – Eine 1-Bit-Kennung, die die Übertragung von Token Ring-Frames über Ethernet-Verbindungen ermöglicht.
- **VLAN-ID (VID)** – Eine 12-Bit-VLAN-ID, die bis zu 4096 VLAN-IDs unterstützt.