VLAN (Virtual Local Area Network)

Gründe, Vorteile, Nachteile

- Die Bezeichnung Virtual Local Area Network (VLAN) bringt zum Ausdruck, dass es sich dabei um ein scheinbar eigenes Netzwerk innerhalb eines LAN oder auch WAN (VPN) handelt.
- Mithilfe von VLANs werden räumlich verteilte Computer zu Arbeitsgruppen zusammengefasst, etwa nach Fachabteilungen, wie z.B. Buchhaltung, Produktion und Entwicklungsabteilung.
- VLANs werden auf den Switches eingerichtet.
- Die logische Struktur des Netzes wird dadurch von der physischen Struktur getrennt.

VLAN (Virtual Local Area Network)

Gründe, Vorteile, Nachteile

- Durch die die Bildung von VLANs wird der Broadcast-Verkehr durch die Verkleinerung der Broadcast-Domänen reduziert.
- Erhöhung der Sicherheit durch Trennung der Netze und der Möglichkeit Access Control Lists (ACLs) einzusetzen. Die ACLs erlauben oder verbieten gezielt den Zugriff auf bestimmte Ressourcen.
- VLANs ermöglichen eine vereinfachte zentrale Administration.
- Die Verwaltung erfolgt über die Switche, ebenso können Regelsätze auf den Layer 3 – Switches konfiguriert werden.
- Als Nachteile sind die komplexere Konfiguration und die teureren Komponenten zu nennen.

VLAN (Virtual Local Area Network)

Typen

- Es wird zwischen zwei Typen von VLANs unterschieden:

1. Portbasierte VLANs
   - Auf einem managebaren Switch werden die Ports je einem VLAN fest zugeordnet.

2. Tagged VLANs
   - Den Ethernet-Frames wird eine Markierung (Tag) hinzugefügt, welche das VLAN kennzeichnen, für welches der Frame bestimmt ist.
   - Damit können VLANs über mehrere Switche hinweg ausgedehnt werden.

VLAN (Virtual Local Area Network)

Konfiguration

- VLANS werden auf einem VLAN-fähigen Switch konfiguriert.
- Am Switch wird festgelegt, welcher Port zu welchem Segment gehört.
- Der Switch leitet die Frames nur innerhalb desselben VLANs weiter. Rechner können nur mit Rechnern kommunizieren, die im selben Segment (VLAN) angesiedelt sind.
- Ein Verkehr zwischen den Segmenten ist in dieser Konstellation nicht möglich.

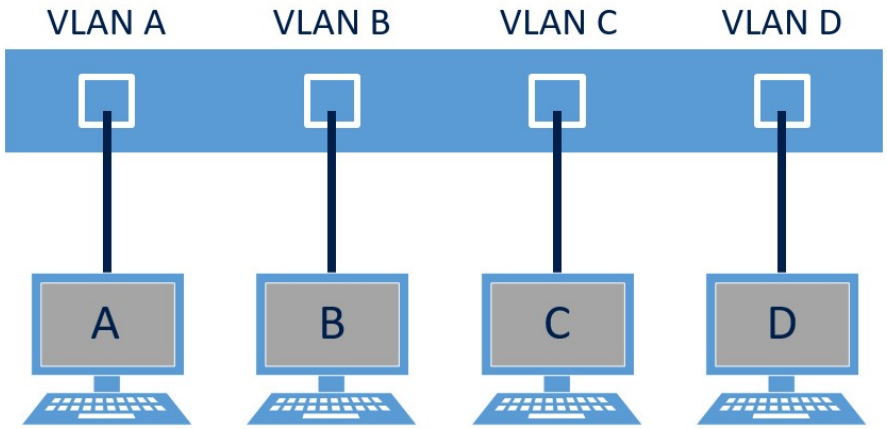

Abbildung 1: VLAN (eigene Darstellung)

VLAN (Virtual Local Area Network)

Tagging

- Müssen die Frames über mehrere Switche weitergeleitet werden, muß klar sein, zu welchem VLAN der Frame gehört.
- Dafür wird im Ethernet-Frame zwischen dem Adressblock und dem Type-/Length-Field eine Kennung, Tag genannt, eingefügt.
- Das Tag ist, genormt in IEEE 802.1Q (tagged VLANs), vier Byte lang und vergrößert damit einen Ethernet-Frame von 1.518 Byte auf 1.522 Byte.

Abbildung 2: Frame mit Tag (eigene Darstellung)

- !Ältere Switches und Hubs erkennen dies nicht an und verwerfen diese Pakete, da sie für Standard Ethernet zu groß sind!

VLAN (Virtual Local Area Network)

VLAN - Trunks

- Eine Verbindung zwischen Switches, die VLANs, also getaggte Pakete, transportiert, nennt man einen Trunk.
- Diese VLAN-Tags sind nur bei der Verbindung Switch-zu-Switch im Paket enthalten.
- Sendet ein Rechner, der in einem bestimmten VLAN ist, fügt der Switch den Tag ein, bevor er das Paket an den nächsten Switch verschickt.
- Kommen sie am Zielport an, entfernt der Switch die Tags, bevor er die Frames an die Endrechner schickt.

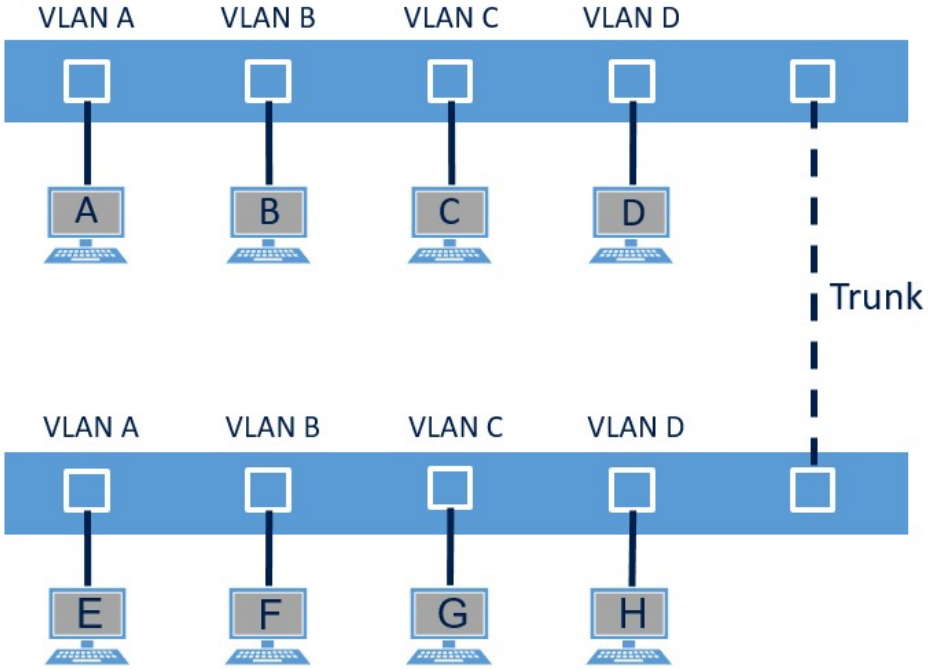

Abbildung 4: VLAN-Trunk (eigene Darstellung)

VLAN (Virtual Local Area Network)

Zuordnung der VLAN-ID

Die Zuordnung der Ports zu einem VLAN kann statisch oder dynamisch erfolgen.

1. Statische Zuordnung

- Jeder Port wird vom Administrator fest einem VLAN zugeordnet. Diese Zuordnung muß bei Bedarf manuell geändert werden.
- Vorteil ist die eindeutige Zuordnung der Ports.
- Nachteilig sind der hohe administrative Aufwand und die fehlende Mobilität der Geräte.

VLAN (Virtual Local Area Network)

Zuordnung der VLAN-ID

- **2. Dynamische Zuordnung**
  - Zugehörigkeit zu einem VLAN erfolgt auf Basis von Kriterien, wie MAC- oder IP-Adresse oder Authentifizierung.
  - Vorteile sind der geringere administrative Aufwand und Mobilität der Geräte.
  - Nachteilig sind Sicherheitsdefizite. (Z.B. sind MAC-Adressen leicht zu fälschen.)

VLAN (Virtual Local Area Network)

Verbindung der VLANs

- Ein Switch ist ein Gerät auf Layer II, er kann nicht routen.
- Die Trennung in verschiedene Segmente musste aber einen Layer höher angesetzt werden. Diese Aufgabe kann daher nur ein Router durchführen.
- VLAN A und B sind also auf Layer III getrennt, also verschiedene Netzwerke. Wird eine Kommunikation erwünscht, muss ein Router eingesetzt werden. Dieser arbeitet auf Layer III und besitzt in jedem VLAN ein Interface.

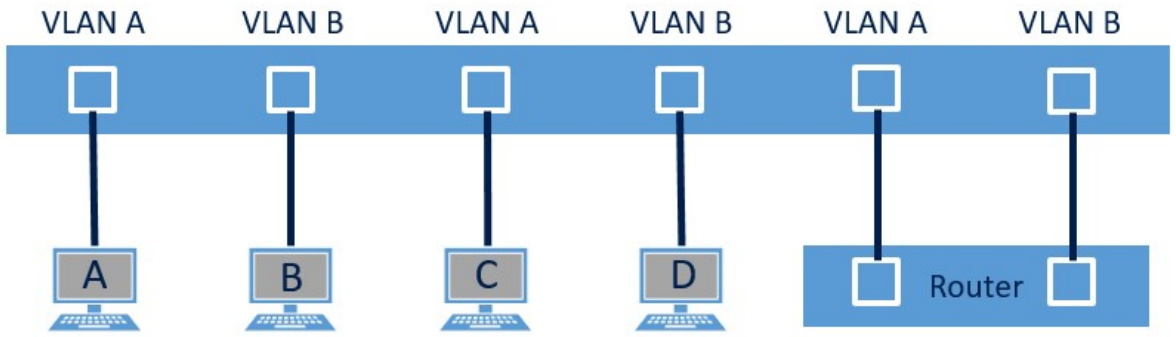

Abbildung 5: VLAN+Router (eigene Darstellung)

VLAN (Virtual Local Area Network)

Verbindung der VLANs

- Moderne Router sind in der Lage, die Layer II-Informationen zu lesen.
- Sie können über einen Trunk-Link angeschlossen zu werden.
- Der Switch übergibt die Pakete tagged an den Router.
- Der sucht das Destinationssubnetz und ändert dementsprechend den Tag.
- Dann gibt er das Paket an den Switch zurück.

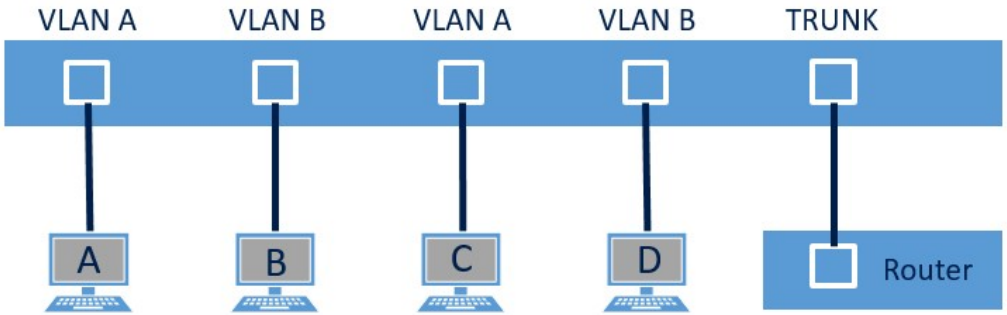

Abbildung 8: VLAN geroutet über Trunk (eigene Darstellung)

VLAN (Virtual Local Area Network)

Vorteile

- In einer voll geswitchten Umgebung mit VLANs können in den Büros eines Gebäudes die verschiedensten Subnetze definiert werden.
- Somit lassen sich zum Beispiel Büros von Abteilungen, obwohl in ganz anderen Gebäudeteilen untergebracht, in dasselbe Subnetz konfigurieren.
- Der Router routet den Verkehr zwischen den VLANs und stellt die Verbindung nach außen.

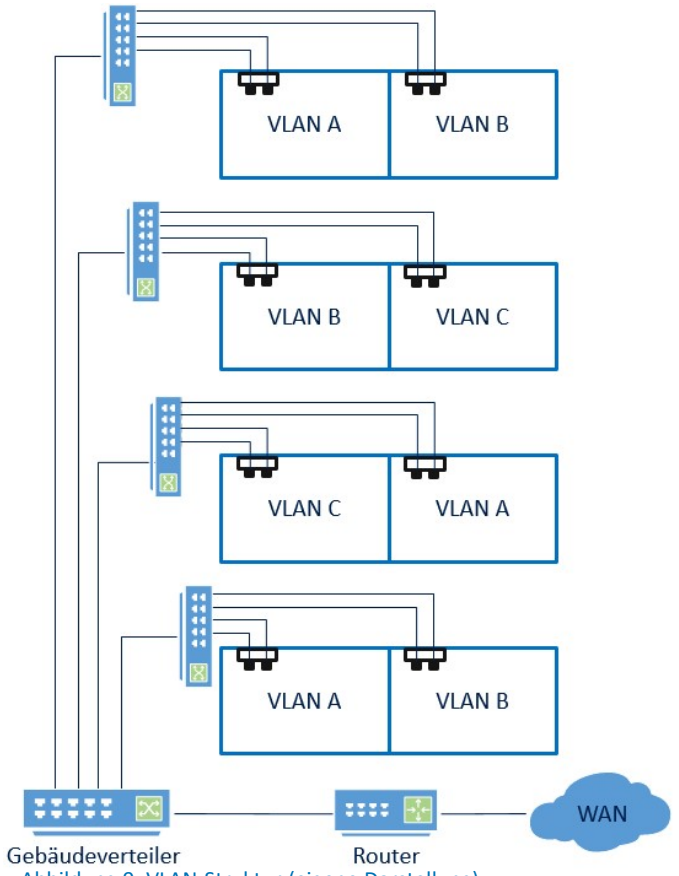

Abbildung 9: VLAN-Struktur (eigene Darstellung)

VLAN (Virtual Local Area Network)

Grenzen

- Über Router hinweg lassen sich Tags in der Regel nicht transportieren. Sind zum Beispiel zwei Gebäude durch Router verbunden, können in der Regel nicht in beiden dieselben VLANs benutzt werden.
- Eine Verbindung von Router zu Router ist eine reine Verbindung auf Layer III.
- Router können VLANs routen, die direkt an sie angeschlossen sind. Moderne Netzwerk-Core-Geräte sind eine Mischung aus Switch und Router, Layer-3-Switch.
- Es gibt Verfahren, mit denen sich die VLANs gekapselt über Layer III übertragen lassen. Dies ist aber unvorteilhaft, da es nur einen Default Gateway in jeder Broadcast-Domäne gibt. Zum Routing müssen also alle Daten wieder zurück übertragen werden.

VLAN (Virtual Local Area Network)

Grenzen

- Werden ganze Gebäude oder Firmenteile miteinander verbunden, handelt es sich in der Regel um MAN- oder WAN-Verbindungen. Diese sind auf Layer III geroutet.
- VLANs werden in der Regel nur in reinen Layer II-Umgebungen transportiert. Das bedeutet, dass eine Router-Verbindung auch nur reine Layer III-Daten transportiert.

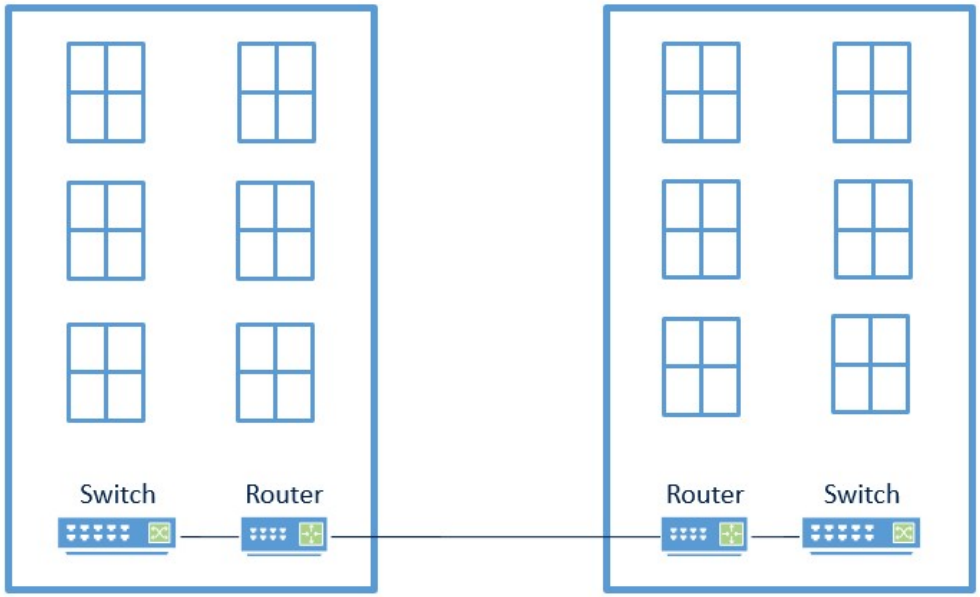

Abbildung 10: Routing (eigene Darstellung)

Quellen

Buchquelle

VLAN-Grundlagen (2019). In: 1&1 IONOS SE, 08.01.2019. Online verfügbar unter https://www.ionos.de/digitalguide/server/knowhow/vlan-grundlagen/, zuletzt geprüft am 18.05.2021.

Fischer, Werner (2010): VLAN Grundlagen. In: Thomas-Krenn.AG, 06.05.2010. Online verfügbar unter https://www.thomas-krenn.com/de/wiki/VLAN_Grundlagen, zuletzt geprüft am 18.05.2021.

Kersken, Sascha (2017): IT-Handbuch für Fachinformatiker. Der Ausbildungsbegleiter. 8. Auflage, revidierte Ausgabe. Bonn: Rheinwerk Verlag; Rheinwerk Computing.

Schnabel, Patrick (2013): Netzwerktechnik-Fibel. Grundlagen Netzwerktechnik ; Übertragungstechnik ; TCP/IP ; Anwendungen und Dienste ; Netzwerk-Sicherheit. 3. Aufl. Ludwigsburg.

Schreiner, Rüdiger (2014): Computernetzwerke. Von den Grundlagen zur Funktion und Anwendung. 5., erw. Aufl. München: Hanser.

VIELEN DANK!