

Netzwerk

Layer 2: VLAN

VLAN (Virtual Local Area Networks)
Logische Netzwerktrennung auf Layer 2

Vorteile:

- logische Trennung der Netzwerke bei einheitlicher physischer Netzstruktur (Sicherheit, Abgrenzung von IoT, VoIP, iSCSI/Backup usw.)
- jedes VLAN bildet eine eigene Broadcast-Domain (Traffic wird reduziert und kann in VLANs priorisiert werden)
- Übertragen mehrerer logisch getrennter VLAN-Netze ist über ein Kabel möglich (Trunking)
- ein Switch wird mit VLAN in mehrere virtuelle Switches geteilt, auch Switch-übergreifend

Grundlagen:

- max. 4096 VLANs
- VLAN-1 ist immer das Default-VLAN im Auslieferungszustand. Geräte ohne VLAN-Tag kommen per Default in VLAN-1.
- VLAN-7 nutzt die Telekom für VDSL und sollte frei gehalten werden
- VLAN-fähig sind Managed Switches, Router, Linux, VMWare, Windows je nach Netzwerkkarte, diverse Geräte wie NAS, WLAN-AccessPoints usw.
- jeder Port und jedes Gerät kann Teil nur eines VLANs sein, aber es können ihm mehrere VLANs zugeordnet werden (Trunk)
- VLAN-Trunks müssen alle VLAN-IDs hinterlegt haben, die sie übertragen sollen. Oder sie sind so konfiguriert, dass sie alle VLANs weiter leiten. Dynamische, selbstlernende VLAN-Trunks sind heute Standard.
- VLAN-Tags werden vom Ziel-Switch entfernt, wenn der Empfänger-Switchport UNTAGGED ist. Ansonsten gehen die TAGGED Pakete bis zum VLAN-taggingfähigen Zielgerät.
- Verbinden verschiedener VLANs ist durch gezieltes Routing (Layer 3) möglich
- Verschiedene VLANs können identische Netzwerkadressen haben, dann ist aber kein Routing möglich.

Verfahren:

- Switch wird pro Port genau einem VLAN zugewiesen (VLAN-ID)
- jeder Port kann Member von mehreren VLANs sein und deren Pakete übertragen (PVID)
- innerhalb eines Switches erfolgt die Kommunikation meist portbasierend, zwischen den Switchen paketbasierend.

1. (U) Port-basierend (untagged)

- statische Netzstruktur, unterteilt einen physischen Switch in mehrere logische Switches

Seite 1 / 3

(c) 2024 Uwe Kernchen <news@uwe-kernchen.de> | 2024-04-25 18:43

URL: <https://uwe-kernchen.de/phpmyfaq/index.php?action=faq&cat=4&id=340&artlang=de>
(C) <https://uwe-kernchen.de>

Netzwerk

- am Port liegen alle Daten des jeweiligen VLAN an, es werden aber keine VLAN-Informationen nach außen weiter gereicht

2. (T) TAG-basierend (paketbasiert, framebasiert, tagged)

- Datenpakete werden mit VLAN-TAG an das nächste Gerät weiter geleitet (Gegenseite muss auch getagged sein)
- die Kommunikation verschiedener VLANs kann über ein Kabel erfolgen
- VLAN-TAG wird in IEEE 802.1q festgelegt, Cisco, 3Com u.a. haben teilweise abweichende Standards
- Anwendung: Uplinks zwischen Switchen, AccessPoints, Hyper-V- und ESX-Servern, VoIP-Telefonen...

Umsetzung:

VLANs werden üblicherweise zwischen Switchen und Routern konfiguriert, Endgeräte haben einen ungetaggten Port mit der passenden VLAN-ID.

- VLAN tagged
Tagged Port eingehend: Die VLAN-Markierung wird überprüft aber nicht verändert
Tagged Port ausgehend: Die VLAN-Markierung wird überprüft aber nicht verändert
- VLAN untagged - pro Port gibt es max. 1 untagged VLAN
Untagged Port eingehend: Die VLAN-Markierung wird laut PVID (häufig identisch mit der untagged VLAN ID) intern im Switch hinzugefügt
Untagged Port ausgehend: Die VLAN-Markierung wird überprüft und beim Versenden entfernt
- PVID (Port VLAN ID) - je nach Hersteller, typisch: Netgear, MikroTik, TP-Link
 - bestimmt das VLAN, in das untagged Frames geforwardet werden die an dem Port reinkommen.
 - heisst bei anderen Herstellern native Vlan oder dual Mode VLAN.
 - Jedem Port muss eine PVID zugewiesen werden (standardmäßig PVID 1).
 - Um die Standard-PVID eines Ports zu ändern, muss zunächst ein VLAN erstellt werden, das den Port als Mitglied enthält.
This is a term used for non-Cisco switches.
- Auto-PVID - bei vielen Herstellern ist die PVID automatisch = VLAN-ID

VLAN-Portdefinition im Lancom Router:

Netzwerk

Port-Tabelle - Eintrag bearbeiten

VLAN-Port: LAN-2: Lokales Netzwerk 2

VLAN-Tagging-Modus: Access (Niemals) ▾

☒ Auf diesem Port Pakete e VLANs gehören

Port-VLAN-ID:

OK Abbrechen

* VLAN am PC:

- Intel oder Realtek Netzwerkkarten unterstützen VLAN
- bei Realtek ist das Realtek Diagnostics Programm erforderlich
- 1. Original LAN-Karte wird deaktiviert (keine IP)
- 2. je VLAN wird eine virt. Netzwerkkarte angelegt

* VLAN in VM-Workstation:

1. VLANs über die physische Netzwerkkarte definieren (siehe oben)
2. entsprechende virtuelle Netzwerkkarte mit VLAN der gewünschten VM zuweisen

Dynamische VLANs

Zuordnung zu einem VLAN anhand von MAC-Adresse, IP-Adresse, Protokolltyp oder Anwendungsebene/Portnummer.

Damit kann beispielsweise VoIP priorisiert werden oder ein Mobilgerät unabhängig von seinem Port einem VLAN zugeordnet werden.

- gute FAQ: <https://administrator.de/knowledge/vlan-installation-routing-pfsense-mikrotik-dd-wrt-cisco-rv-routern-110259.html>
- siehe auch: [Lancom VLAN](#)

Eindeutige ID: #1339

Verfasser: Uwe Kernchen

Letzte Änderung: 2023-06-16 08:58