VLAN

> Ein VLAN ist eine Struktur, in welcher Netzwerkswitche in mehrere „logische Switche“ aufgeteilt und voneinander isoliert werden.
> Jedes VLAN bildet ein eigenes Netz. Jedes LAN bildet eine Broadcastdomäne. Broadcasts bleiben somit im eigenen VLAN und gelangen nicht in andere. Damit zwei Rechner in unterschiedlichen VLANs miteinander kommunizieren können, müssen diese über einen Router verbunden werden.

VLAN Typen

Uplinks einzelner logischer Switche, werden physikalisch zu einem Link zusammengefasst. Damit die Datenframes der einzelnen logischen virtuellen Netzwerke dem jeweiligen VLAN zugeordnet werden können, müssen die Frames mit VLAN-Tags modifiziert werden. Die Zugehörigkeit zum virtuellen Netzwerk muss zusätzlich im Frame (Layer-2, Ethernet-Frame) transportiert werden.

Tagged und Untagged VLANs

Der PC schickt einen normalen Datenframe heraus. Der Switch macht die Zuordnung zum virtuell LAN und erweitert den Frame mit dem Tag. Das so gekennzeichnete Ethernet-Frame wird wie gewohnt durch das Netzwerk transportiert. Der letzte Switch entfernt diesen VLAN-Tag wieder, bevor er die Daten an den Zielrechner schickt.

Untagged VLAN bedeutet, dass der komplette Switchport dem VLAN angehört. Egal welches Gerät angeschlossen wird, wird automatisch im definierten VLAN landen. Untagged VLAN ist auch als portbasierten VLAN bekannt.

VLAN-Trunking

Mit VLAN-Trunking lassen sich Switches so verschalten, dass sie mehrere verschiedene VLANs untereinander zu Netzwerken verbinden. VLAN-Trunking ist in der Lage, die Informationen mehrerer virtueller LANs über eine einzige Leitung zu übertragen. Es lassen sich einzelne oder gebündelte Ports für das Trunking verwenden.

Bei portbasierten VLANs (d. h. bei Paketen, die kein Tag besitzen) wird zum Weiterleiten eines Datenpakets über einen Trunk hinweg üblicherweise vor dem Einspeisen in den Trunk ein VLAN-Tag hinzugefügt, welches kennzeichnet, zu welchem VLAN das Paket gehört. Der Switch auf Empfängerseite muss dieses wieder entfernen. Bei tagged VLANs (nach **IEEE 802.1Q**) hingegen werden die Pakete entweder vom Endgerät (z. B. Tagging-fähigem Server) oder vom Switch am Einspeiseport mit dem Tag versehen. Daher kann ein Switch ein Paket ohne jegliche Änderung in einen Trunk einspeisen.

Kollisions- und Broadcastdomäne

> Kollisionsdomäne: alle Stationen auf einem gemeinsamen Medium

Teilen sich mehrerer Endgeräte ein Medium (Netzwerkkabel, WLAN, etc.), spricht man von einem shared medium. Zusammen bilden sie eine **Kollisionsdomäne**. Senden zwei oder mehrere Endgeräte gleichzeitig, so kommt es zu Kollisionen auf dem Medium. Steigt die Anzahl der Endgeräte, so steigt auch die Anzahl der Kollisionen. Sind zu viele Stationen vorhanden, dann ist gar keine Kommunikation mehr möglich und das Medium ist dauernd (durch Kollisionen) belegt.

> Broadcastdomäne: alle Stationen eines Netzes

Eine Broadcast-Meldung ist eine Rundsendung an alle Netzwerkteilnehmer. Die Menge der Stationen, die eine Broadcastmeldung empfangen, bildet eine **Broadcastdomäne**.

> Durch VLANs verringert sich der Traffic auf einer Kollisionsdomäne durch Reduzierung der Broadcastmeldungen, da VLANs die Broadcastdomäne verkleinern.

Created 2022-10-27 12:53:03 UTC by Joshua Lieder
Updated 2022-11-17 13:50:06 UTC by Joshua Lieder