Motivation: Strukturierung großer Netze Teil 2

Mit Hilfe des Subnettings konnte ein großes Netzwerk in mehrere Teilnetze aufgetrennt werden. Subnetting als alleiniges „Werkzeug“ zur Unterteilung eines Netzwerkes bringt allerdings noch eine große Zahl von Fallstricken mit sich und es stellt sich heraus, dass Subnetting um ein weiteres Verfahren ergänzt werden sollte.

Motivation: Probleme des Subnettings

Welchem Netzwerk (Subnetz) ein Host zugeordnet wird, hängt von seiner IP-Konfiguration (genauer von seiner IP und seiner Subnetzmaske) ab. Das bedeutet, dass die Zuordnung hostseitig erfolgt. Es ist somit denkbar, dass ein Host durch eine falsche Konfiguration im falschen Subnetz landet. Eine solche falsche Konfiguration kann versehentlich erfolgen; es ist allerdings auch denkbar, dass diese gezielt genutzt wird, um Zugriff auf andere Subnetze zu erhalten.

Geht man von einer strukturierten Verkabelung in einem Unternehmen aus, bei dem alle Etagen auf Coreswitches zusammenlaufen ergeben sich zusätzliche Probleme:

1. Die (automatische) Zuweisungen von IP-Adressen per DHCP ist kaum möglich, da der Server nicht erkennen kann, aus welchem Subnetz die Anfrage kommt. Anhand des DHCP-Discover kennt der Server lediglich die MAC-Adresse des anfragenden Hosts. Zwar ist es theoretisch denkbar, alle MAC-Adressen im DHCP-Server zu hinterlegen auf Basis dieser Datenbank IP-Adressen zu verteilen, dieses Verfahren ist allerdings unpraktisch, da neue Clients stets manuell vorab angelegt werden müssten.
2. Broadcaststürme: Aufgrund der Tatsache, dass im Falle der oben beschriebenen Topologie alle Hosts über Switches verbunden sind, können so genannte „Broadcaststürme“ enstehen. Jeder Host im Netzwerk der einen Broadcast abschickt erreicht damit alle anderen Hosts. Diese einerseits nette Eigenschaft führt andererseits bei sehr vielen Hosts im Netzwerk zu einer großen Menge an Traffic. Broadcasts verbreiten sich trotz Subnettings über das gesamte Netzwerk und verringern signifikant die Performanz des Netzes. Der Bereich, in dem Sich (Layer 2-) Broacasts ausbreiten können wird als „Broadcastdomain“ bezeichnet. Aus genannten Gründen ist es notwendig, Broadcastdomains nicht zu groß werden zu lassen. Subnetting hilft bei dieser Problemstellung nicht direkt weiter.

Eine Möglichkeit, die genannten Probleme zum Umgehen ist es, die Core-Switches durch Router (bzw. Layer-3 Switches) auszutauschen. Router unterbrechen gewissermaßen die Kommunikation auf Layer-2 und leiten entsprechend auch keine Broadcasts weiter.

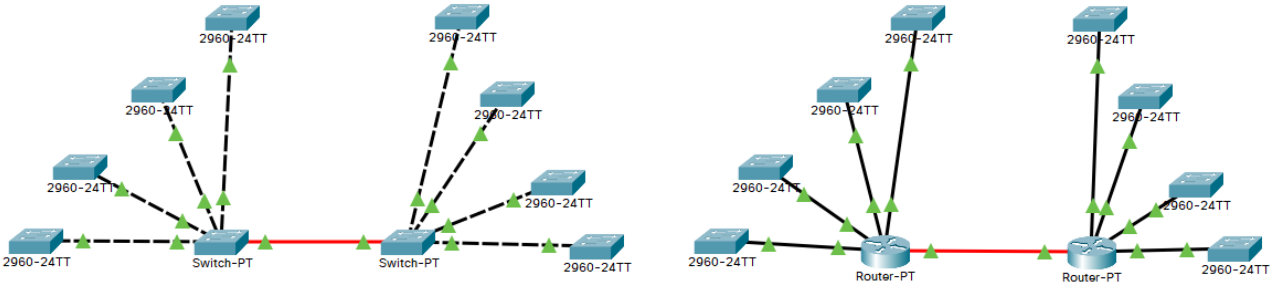
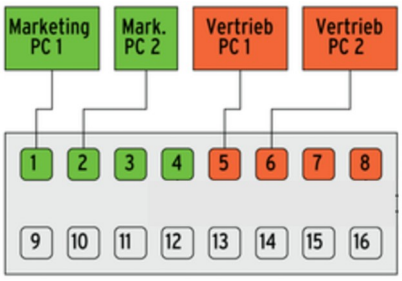


Schaubild 1: Strukturierte Verkabelung: Links Etagenswitches, die im Sekundärbereich mit Core-Switches verbunden sind. Die Core-Switches sind im Primärbereich über LWL verbunden. Rechts: Ersetzen der Coreswitches durch Router. An der Verkabelung ändert sich nichts, allerdings bewirken die Router, dass sich jeder Etagenswitch in einer eigenen Broadcastdomain befindet

Durch die Verwendung von Core-Routern statt Core-Switches ergibt sich nun pro Etagenswitch eine Broadcastdomain. Diese ist ggf. hinreichend klein, um Broadcaststürme zu vermeiden. Allerdings ergibt sich nun ein neues Problem: Jedes Subnetz korrespondiert nun mit einem Etagenswitch. Das bedeutet automatisch, dass die tatsächlich Position eines Clients (etwa die Etage in dem er steht) nun darüber entscheidet, welchem Subnetz er zugeordnet wird. Geht man beispielsweise davon aus, dass Subnetze abhängig von Abteilungen im Unternehmen zugewiesen werden, so müssten nun sich nun die Arbeitsplätze der Mitarbeiter einer Abteilung zwangsläufig auf einer Etage befinden. Wechselt ein Mitarbeiter die Abteilung, darf er auch gleich mit seinem Schreibtisch umziehen. Zwar ist diese „Lösung“ theoretisch denkbar, allein die praktische Umsetzung wird auf Widerstände stoßen.

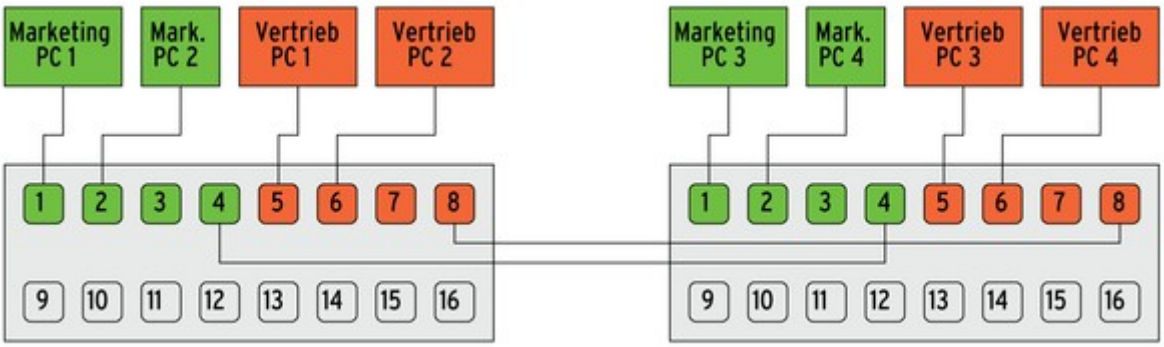
Lösung: Portbasierte VLANs



Moderne Switches bieten die Möglichkeit, so genannte virtuelle LANs einzurichten. Hierbei wird der Switch softwareseitig (virtuell) gewissermaßen in mehrere unabhängige Switches aufgeteilt und die einzelnen physikalischen Ports den einzelnen virtuellen Switchen zugeordnet. Die virtuellen Switches sind untereinander zunächst in keiner Weise verbunden. Jene Anordnung wird dann als VLAN bezeichnet. Moderne Switches können dabei bis zu 1000 VLANs gleichzeitig verwalten (also deutlich mehr als physikalische Ports vorhanden sind). Die folgende Abbildung zeigt einen Switch, dessen ersten 4 Ports einem bestimmten VLAN (Marketing) zugeordnet, während seine Ports 5-8 einem anderen VLAN (Vertrieb) zugeordnet sind. Beide virtuellen Switches haben nun keinerlei Kontakt zueinander. Damit ergeben sich – betrachtet man nur die ersten 8 Ports – nun auch zwei Broadcastdomains. Da beide VLANs nun keinerlei Kontakt zueinander haben, ist es theoretisch denkbar, in beiden VLANs die gleichen IP-Adressbereiche zu vergeben. Dies führt allerdings im weiteren Verlauf zu Problemen (diese werden später erläutert), weshalb hier nun das Thema VLANs mit dem entsprechenden Subnetting verbunden wird: Die Marketingabteilung erhält ihr eigenes VLAN (Layer 2) UND ihr eigenes Subnetz (Layer 3).

Verteilen von VLANs über mehrere Switches

Der Vorteil von VLANs ist nun, dass sie über mehrere Switches hinweg verteilt werden können. Wie normales Switches können nun auch die virtuellen Switches kaskadiert (also hintereinander geschaltet werden. Die folgende Abbildung zeigt, wie beide VLANs auf einen weiteren Switch erweitert werden können:

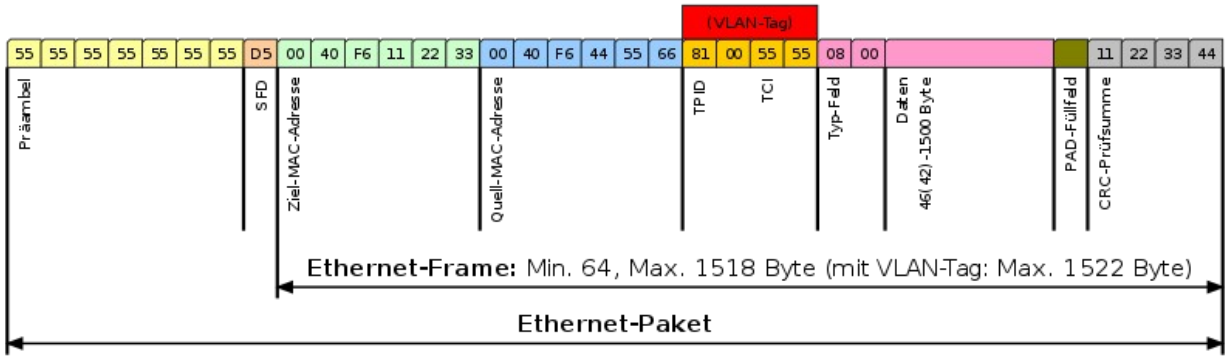


Hierzu wird pro VLAN ein Port zum kaskadieren verwendet. Damit befinden sich im obigen Beispiel alle 4 Marketing PCs in der gleichen Broadcastdomain und alle 4 Vertriebs-PCs ebenfalls. Es dürfte an dieser Stelle allerdings ersichtlich sein, dass dieses Verfahren im Falle sehr vieler VLANs schnell an seine Grenzen stößt. Wie oben erwähnt können aktuelle Switches bis zu 1000 VLANs verwalten. Auf dem oben gezeigten Weg können diese nicht verteilt werden. Legt man wieder eine strukturierte Verkabelung zugrunde, würde dies ferner bedeuten, dass im Sekundärbereich pro VLAN eine Leitung gezogen werden müsste. Dies ist natürlich völlig unpraktikabel, weshalb stattdessen das folgende Verfahren verwendet wird.

IEEE 802.1Q und VLAN-Trunks

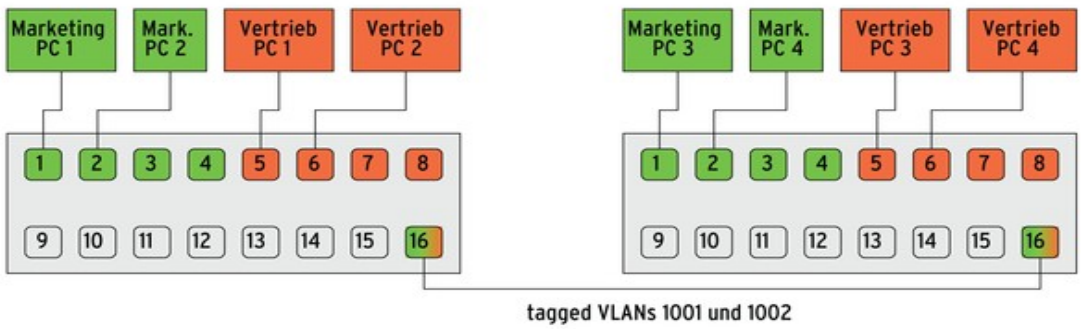
Bisher wurde davon ausgegangen, dass einem physikalischen Port nur ein VLAN zugeordnet werden kann. Der Standard 802.1Q ermöglicht nun so genannte Trunk-Ports (Stamm-Ports), auf denen mehrere VLANs übertragen werden können. Die Verbindungsleitungen zwischen den Switches in der vorigen Abbildung werden so gewissermaßen zu einer Leitung zusammengefasst. Werden nun allerdings Pakete aus verschiedenen VLANs über die gleiche Leitung übertragen, muss natürlich geklärt werden, welchem VLAN die Pakete jeweils zugeordnet sein sollen. 802.1Q erweitert dazu Ethernet-Frames um ein so genanntes VLAN-Tag, in dem schlicht die VLAN-Nummer mitübertragen wird.

Die folgende Abbildung zeigt einen Ethernet-Frame mit dem entsprechenden Tag:



Wird 802.1Q verwendet, wird gewissermaßen der klassische Ethernetstandard verändert, was bedeutet, dass eine Kommunikation nur erfolgen kann, wenn beide Switches 802.1Q beherrschen. Bei VLAN-fähigen Switches ist dies allerdings inzwischen nahezu immer der Fall. Damit verfügen Switches nun über zwei verschiedene Portarten:

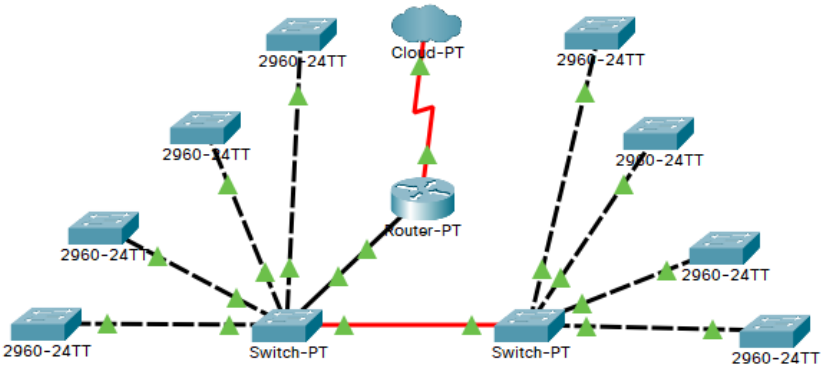
1. Access-Port: Als Access-Port werden die „ursprünglichen“ Ports bezeichnet, die mit lediglich einem VLAN assoziiert sind. An diesen Ports werden üblicherweise Hosts angeschlossen. Auf Layer-2 werden klassische Ethernetframes ohne VLAN-Tag verschickt und empfangen. Die Ports werden daher auch als „untagged“ bezeichnet. Theoretisch kann also jeder Access-Port mit einem weiteren Switch verbunden werden, der nicht VLAN-fähig ist. Dies bedeutet aber zugleich, dass angeschlossene Geräte keine Information darüber haben, in welchem VLAN sie sich befinden.
2. Trunk-Ports: Trunks dienen dazu, den Traffic verschiedener VLANs zu aggregieren (zusammenzufassen) und an einen Router oder einen nächsten Switch zu übertragen. Auf der Leitung werden Ethernetframes mit zusätzlichem VLAN-Tag verwendet, weshalb die Ports auch als „tagged-Port“ bezeichnet werden. Um Trunks verwenden zu können müssen beide Seiten 802.1Q-fähig sein.



VLANs, Subnetze und Default Gateway

Wie bereits erwähnt werden die eigentlich völlig unterschiedlichen Konzepte „VLAN“ und „Subnetting“ in der Praxis kombiniert. Legt man Subnetting zugrunde, benötigt jedes einzelne Subnetz sein eigenes Default Gateway um mit Geräten außerhalb des Netzwerks kommunizieren zu können. Die würde nun voraussetzen, dass der Internetrouter in einem Unternehmensnetzwerk so viele Anschlüsse bräuchte, wie es Subnetze im Unternehmensnetzwerk gibt, da ja für jedes Subnetz ein Interface mit eigener IP-Adresse bereitstehen muss[1]. Werden hingegen VLANs eingesetzt und innerhalb der VLANs die gleichen IP-Adressbereiche verwendet, so würde zu guter Letzt ein Router Pakete von verschiedenen Hosts mit jeweils gleicher Quell-IP erhalten. Theoretisch könnte er diese sogar noch an die jeweiligen Ziele weiterleiten, der Rückweg wäre allerdings unmöglich, da ein von außen Empfangenes Paket mit einer Ziel-IP keinem Host mehr eindeutig zuzuordnen wäre.

Daher wird üblicherweise jedem VLAN ein eigenes Subnetz zugeordnet. Damit gibt es eine direkte Entsprechung zwischen VLAN-Nummer und Netzadresse (bzw. IP-Bereich). Im weiteren wird nun erläutert, wie ein Router konfiguriert werden muss, damit er Traffic aus verschiedenen VLANs und damit verschiedenen Subnetzen weiterleiten kann.



Legt man die oben dargestellte Struktur zugrunde ist klar, dass die Verbindung zwischen dem linken Core-Switch und dem Router über einen Trunk hergestellt werden muss, damit alle VLANs Zugriff (beispielsweise) auf das Internet bekommen. Dies bedeutet aber auch, dass der Router als Default-Gateway für alle Subnetze agieren muss. Diese Anforderung wirkt – ausgehend von den obigen Ausführungen – zunächst widersinnig. Da die IP-Adresse des Default-Gateways eines Subnetzes immer im Adressbereich des Subnetzes selbst liegen muss, folgt daraus direkt, dass das Routerinterface mehre IP-Adressen gleichzeitig haben müsste. So widersinnig dies klingt, ist dies genau das, was im Router konfiguriert wird. Der Router ist über einen Trunk mit dem Firmennetz verbunden.

1 Zugegebenerweise könnten an dieser Stelle auch mehrere Router kaskadiert werden, aber es geht schlauer...

Für jedes VLAN bzw. Subnetz, was auf diesem Trunk transportiert wird, muss nun im Router ein so genanntes „Subinterface“ mit der IP-Adresse des entsprechenden Default-Gateway eingerichtet werden. Diese Subinterface sind ebenfalls virtuelle softwarebasierte Interfaces. Man kann also sagen, dass das Routerinterface im genannten Sinne über mehrere IP-Adressen verfügt. Die rechtsstehende Abbildung zeigt schematisch die Konfiguration des Routers. Statt also für jedes Subnetz ein Physikalisches Interface vorzusehen, wie es klassisch beim Subnetting nötig wäre, bietet die Kombination aus Subnetting und VLANs mit 802.1Q die Möglichkeit, sich auf ein physikalisches Interface zu beschränken und die benötigten Interfaces virtuell bereitzustellen. Dies reduziert sowohl Hardwarekosten als auch Verkabelungsaufwand deutlich.