21. VIRTUELLA NÄTVERK, VLAN

VLAN, ***Virtuella LAN*** skall ej förväxlas med ***WLAN***, ***Wireless LAN***. VLAN är en teknik som utvecklats för att på enhetsnivå segmentera och dela upp nätverkstrafik. Med enhetsnivå menar jag olika nätverksenheter, unikt identifierade av deras ***MAC-adress***. Varje enhet som ansluts till ett nätverk har nämligen en helt egen, unik MAC-adress. Detta gäller alla typer av enheter som skall kunna kommunicera i ett nätverk, datorer, skrivare, routrar, intelligenta switchar m.m. Alla dessa har av respektive tillverkare erhållit ett unikt nummer, MAC-adress.

Med hjälp av VLAN-tekniken kan man styra så att kommunikationen i nätverket styrs till enheten med rätt MAC-adress.

Detta utnyttjas i ***Switchar***. Alla datorer, servrar och andra enheter man kopplar in i switchen identifieras tack vare sin unika ***MAC-adress***. Denna skickas ju alltid med i ***Ethernet-paketet*** och tillhör skikt 2, ***Datalänkskiktet***.

Switch

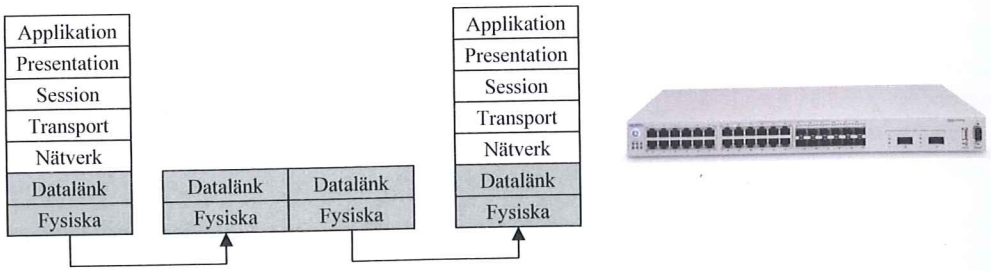
När switchen erhåller paket på någon port så identifierar den vilken MAC-adress som avsändaren av paketet har. MAC-adressen läggs in i en databas, switchdatabasen. Fortsättningsvis så vet nu switchen till vilken port som paket adresserade till denna MAC-adress skall skickas.

Om switchen erhåller att paket adresserat till en mottagare vars MAC-adress ännu inte har identifierats så skickas detta till samtliga portar. Efter en stund när switchen varit igång ett tag så har den dock lärt sig till vilka portar alla datorer i nätverket är kopplade och då fungerar den optimalt.

Till en och samma port kan flera MAC-adresser kopplas i switchdatabasen. Detta behövs om man i en switch kopplar in en annan switch eller en hub. Då måste ju alla MAC-adresser som är kopplade till porten kunna sparas.

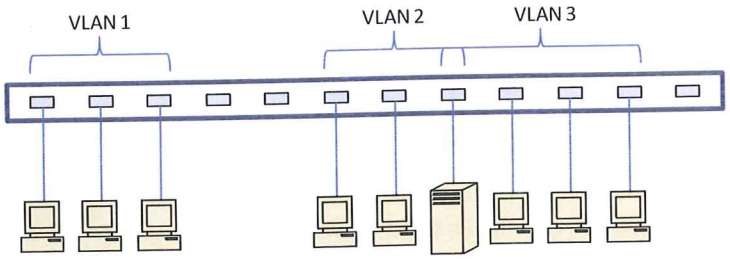
Switchen undersöker de kommunicerande datorernas MAC-adresser och öppnar endast upp förbindelse mellan de två datorer som skall kommunicera med varandra. Detta minskar drastiskt trafiken på nätverket eftersom de datorer som inte kommunicerar inte störs av någonting på nätverket. I en switch kan dessutom flera förbindelser mellan olika portar öppnas samtidigt vilket gör att flera datorer kan kommunicera med varandra samtidigt.

Switchar är idag mycket mer vanliga än hubbar. Många routrar och brandväggar har även inbyggd switch. Switchen arbetar i OSI-modellens datalänkskikt, skikt 2.



VLAN

Det finns också switchar som kan delas upp i s.k. ***VLAN, Virtuella LAN***. Detta innebär att några av portarna i switchen kopplas samman och isoleras från de andra portarna. Dessa kan då användas då man önskar flera, från varandra oberoende nätverk utan kontakt med varandra.



Belastningen på nätverket minskar då eftersom trafiken inom ett VLAN stannar där utan att påverka andra portar och andra VLAN i switchen. Man erhåller också högre säkerhet då man enkelt kan hindra åtkomst till servrar och viktiga resurser på nätverket genom att placera dessa i andra VLAN.

Man kan även låta någon eller några portar i switchen ingå i flera VLAN. Då kan flera VLAN ha åtkomst till en server eller till en internetförbindelse utan att de har tillgång till varandra.

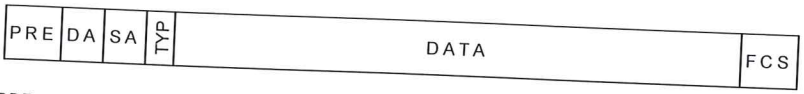
Varje ***Virtuellt nätverk, VLAN*** som man skapar får ett unikt nummer, ***1 – 4094***. VLAN med ID 0 eller 4095 är reserverade. VLAN med ID 0 ingår inte i något VLAN.

Exempel på hur man konfigurerar en VLAN Switch visas längre fram i detta kapitel.

802.1Q protokollet

Att skicka information om VLAN-tillhörighet i vanlig Ethernet-kabel är möjligt tack vare en utökning av Ethernet-protokollet. Det definieras i standarden ***802.1Q***.

Det vanliga Ethernet-paketet ser ut så här:



PRE — Preamble, ett synkroniseringsfält bestående av 8 bytes där de 7 första har värdet 10101010, 10101010 osv

DA — Destination adress, Mottagarens MAC-adress, 6 bytes

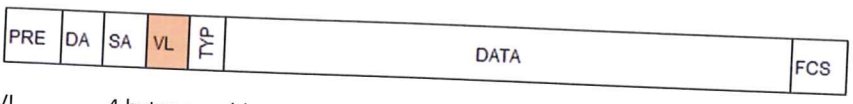
SA — Source adress, Sändarens MAC-adress, 6 bytes

Typ — Anger typ av nätprotokoll som används, 2 bytes, IP har koden 0800

Data — Själva datan som skickas. Max 1492 bytes

FCS — Checksumma. Används för felkontroll, 4 bytes

Genom att lägga in ytterligare 4 bytes i Ethernet-paketet så möjliggörs VLAN-tekniken.



VL — 4 bytes som bl.a. anger VLAN ID.

Dessa fyra bytes (32 bitar) fördelas så här:

TPID — 2 bytes, 16 bitar som har innehållet 1000 0001 0000 0000. Detta identifierar paketet som ett VLAN-paket.

TCI — 2 bytes, 16 bitar. Består i sin tur av tre delar:

PCP — Prioritetskod, 3 bitar. Anger prioritet 1-7 där 1 innebär lägst prioritet och 7 högst prioritet. Värdet 0 innebär bästa möjliga nivå.

CFI — 1 bit. Har värdet 0 för Ethernet

VID — VLAN-ID, 12 bitar. Anger VLAN-ID, 1-4094. Värdet 0 innebär att datapaketet inte tillhör något VLAN. Värdet 4095 kan ej användas.

TPID	TCI		
	PCP	CFI	VID
16 bit	3 bit	1 bit	12 bit

Trafikprioritering

Med ***802.1Q*** så kan man både prioritera trafiken i nätet och styra det till olika VLAN. Genom att ange olika värden på Prioritetsfältet, ***PCP***, så kan man prioritera vilken trafik som skall ha förtur i nätet.

Man använder idag det lokala nätverket till mycket mer än bara ren datatrafik. Telefoni i datanätet, s.k. IP-telefoni blir allt vanligare. Likaså att man skickar videotrafik från t.ex. videokonferenssystem. Dessa andra typer av trafik ställer andra krav på nätverket.

Datatrafiken har som krav att komma fram på ett säkert sätt och någorlunda fort men en fördröjning på någon sekund för t.ex. e-post innebär ju oftast inte några problem. Däremot för video och ljud får det inte alls bli någon fördröjning i trafiken. Om man skall kunna parata med varandra i telefon så accepterar man inte avbrott eller fördröjningar. Inte ens om dessa är under en sekund.

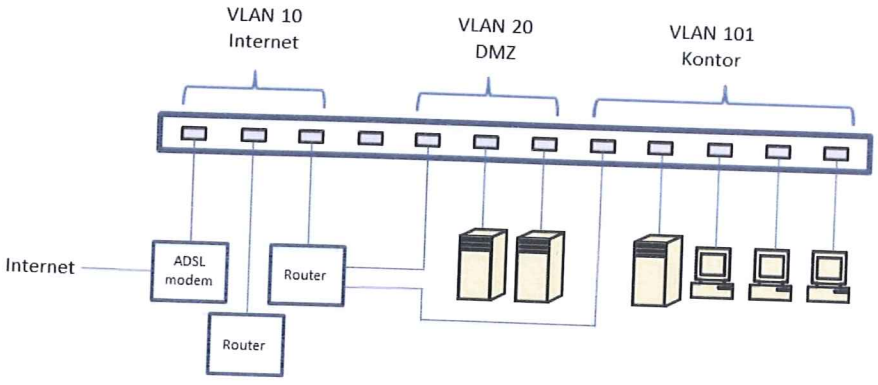
Man bör därför i nätverk som man även använder för t.ex. IP-telefoni använda sig av nätverksutrustning som stöder trafikprioritering enligt 802.1Q -standarden.

VLAN i praktiken

För att du som läsare skall förstå hur man kan utnyttja VLAN-tekniken så skall jag här ge några exempel på hur man kan göra.

Exempel 1: Switchen i Serverrummet

I ett företags serverrum så har man behov av många switch-portar. Man har också flera olika nätverk som inte får ha kontakt med varandra. Istället för att då köpa flera olika separata switchar så kan man använda en stor switch och dela upp den i flera VLAN. Då kan man dessutom enkelt efter hand anpassa hur många portar man behöver ha i respektive VLAN.

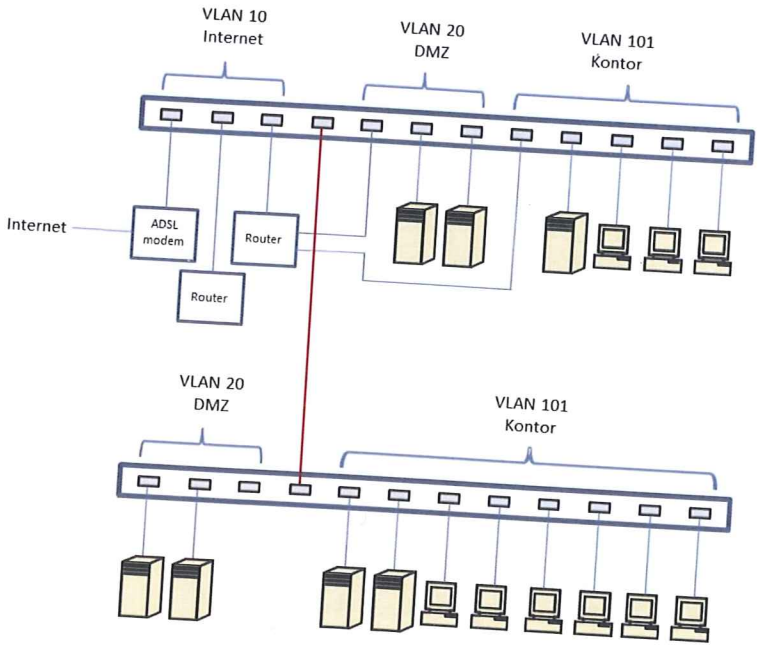


DMZ står för ***DeMilitarized Zone*** och är ett mellanting mellan det oskyddade Internet utanför brandväggen och det interna nätverket innanför brandväggen. I DMZ placerar man ofta servrar som skall kommunicera mot internet, (mailserver, webbserver DNS-server osv).

Exempel 2: Flera switchar i Serverrummet

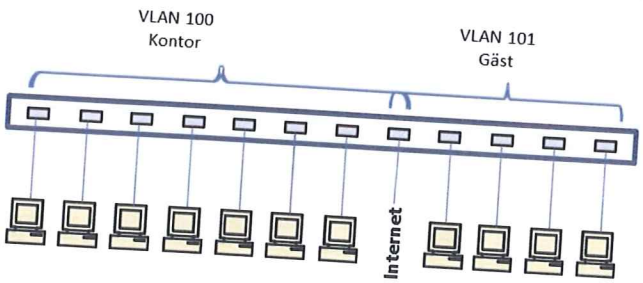
Om man behöver utöka med flera switchar i serverrummet eller om man har flera serverrum så måste man kunna flytta med de olika VLAN:en till de andra servarna. Då kan man konfigurera switchen så att flera VLAN skickas ut på en port. Detta kan man göra tack vare 802.1Q-protokollet.

I en helt vanlig nätverkskabel mellan de båda switcharna kan man skicka flera VLAN. Man måste då konfigurera switcharna så att de skickar dessa signaler på denna port.



Exempel 3: Flera separata nätverk behöver tillgång till internet

Om man har flera olika nätverk, som inte skall kunna ha kontakt med varandra, men som alla skall kunna nå internet via en gemensam länk så kan man ***Trunka*** ihop flera VLAN i en port i switchen. Observera att trafiken på Trunk-porten inte kommer använda 802.1Q-protokollet utan det blir helt vanlig nätverkstrafik. Båda VLAN:en delar alltså på Trunk-porten men kan inte se varandra.



Exempel 4: Trådlöst nätverk med flera olika VLAN

Om man vill ha flera olika trådlösa nätverk, kopplade till olika VLAN, så kan man åstadkomma detta med 802.1Q-protokollet. Lite mer avancerade trådlösa Accesspunkter har stöd för fler än ett trådlöst nät och kan dessutom avkoda VLAN med 802.1Q-protokollet. Man skickar helt enkelt ut de VLAN man vill ha på en port i switchen och kopplar sedan Accesspunkten till denna.