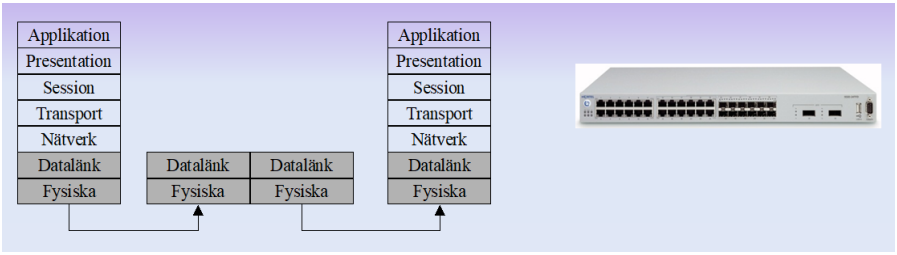
4.4 Virtuella nätverk (VLAN)

Vad är ett virtuellt nätverk?

Varje enhet, vare sig dator, skrivare, router, switch eller någon annan hårdvara som ansluts till ett nätverk, har en egen unik MAC-adress, som den har erhållit av resp. tillverkare. MAC-adresser är fasta *fysiska* adresser, inpräntade i hårdvaran, där *MAC* står för *Media Access Control*.

VLAN (Virtual Local Area Network) är en teknik som etablerar kommunikation i ett befintligt nätverk på enhetsnivå genom att använda MAC-adressen. Förbindelsen kallas ofta för en *"tunnel"* mellan två punkter, eftersom MAC-adresser fungerar på det s.k. *datalänkskiktet* (skikt 2) i *OSI*-modellen *(Open Systems Interconnection)*, en nivå lägre än IP-adresser som fungerar på *nätverksskiktet* (skikt 3) i *OSI*-modellen, se förra avsnitt. Därför är också nätverksenheten som organiserar kommunikationen inte längre routern utan en *switch:*

Switch



När switchen erhåller data identifierar den först vilken MAC-adress som avsändaren har. MAC-adressen sparas i en databas på switchen. Fortsättningsvis vet nu switchen vart data adresserad till denna MAC-adress ska skickas.

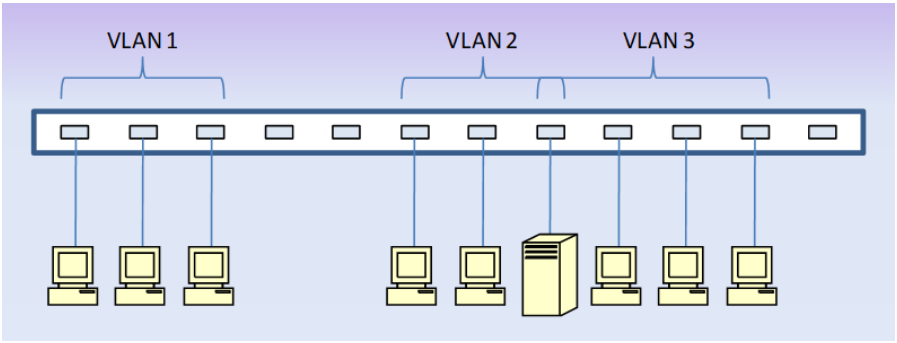
Om switchen erhåller data adresserad till en mottagare vars MAC-adress ännu inte har identifierats, skickas den till switchens samtliga portar, i väntan på ytterligare in-

formation. Efter en stund, när switchen varit igång ett tag, har den lärt sig till vilka portar alla enheter i nätverket är kopplade och då fungerar den optimalt.

Till en och samma port kan flera MAC-adresser kopplas. Switchen undersöker de kommunicerande datorernas MAC-adresser och öppnar endast upp en förbindelse mellan de två datorer som ska kommunicera med varandra, så att de datorer som inte kommunicerar, inte störs. Detta minskar trafiken på nätverket avsevärt. I en switch kan dessutom flera förbindelser mellan olika portar öppnas samtidigt, så att flera datorer kan kommunicera samtidigt med varandra. En sådan teknik minimerar inte bara nätverkstrafiken utan höjer även säkerheten.

VLAN Switch

Det finns switchar som kan delas upp i flera VLAN-switchar. Detta innebär att några av switchens portar kopplas samman och isoleras från de andra, Dessa kan då användas när man vill ha flera, från varandra oberoende nätverk utan kontakt med varandra. Så här kan ett exempel på en sådan uppdelning av portar se ut:



Varje VLAN-switch man skapar får ett unikt nummer. Det finns 1-4094 möjligheter. Nr. 0 och 4095 är dock reserverade för andra ändamål och kan inte delas ut.

VLAN 802.1Q protokollet

Att skicka information med VLAN-teknik i ett vanligt nätverk är möjligt tack vare en utökning av Ethernet-protokollet som har standarden ***802.1Q***. Detta grös genom att lägga ytterligare 4 bytes till i Ethernet-datapaketet, som bl.a. anger *VLAN- ID*.

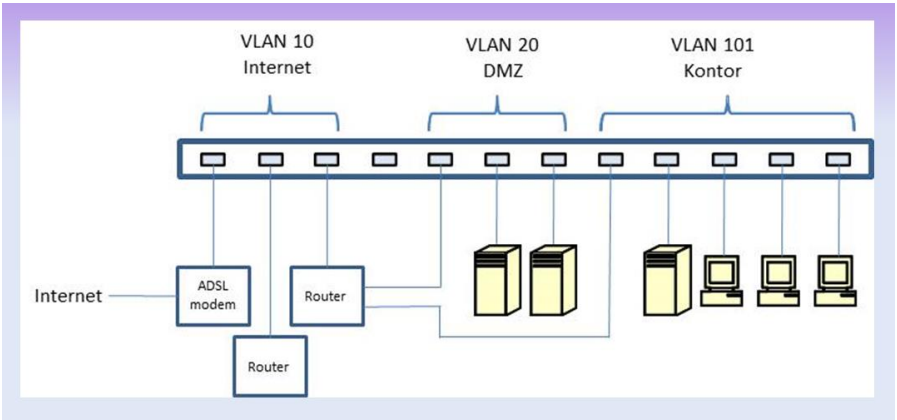
Med ***802.1Q*** kan man både prioritera trafiken i nätet och styra det till olika VLAN. I dagens datatrafik har IP-telefoni, videotrafik, filmstreaming osv. som varken tål fördröjning eller avbrott, inkluderats så att kommunikation utan trafikprioritering inte längre är tänkbar. 802.1Q-protokollet bidrar till att säkerställa denna prioritering.

VLAN i praktiken

Ex. 1: Switchen i serverrummet

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

Så här kan en sådan konfiguration se ut:



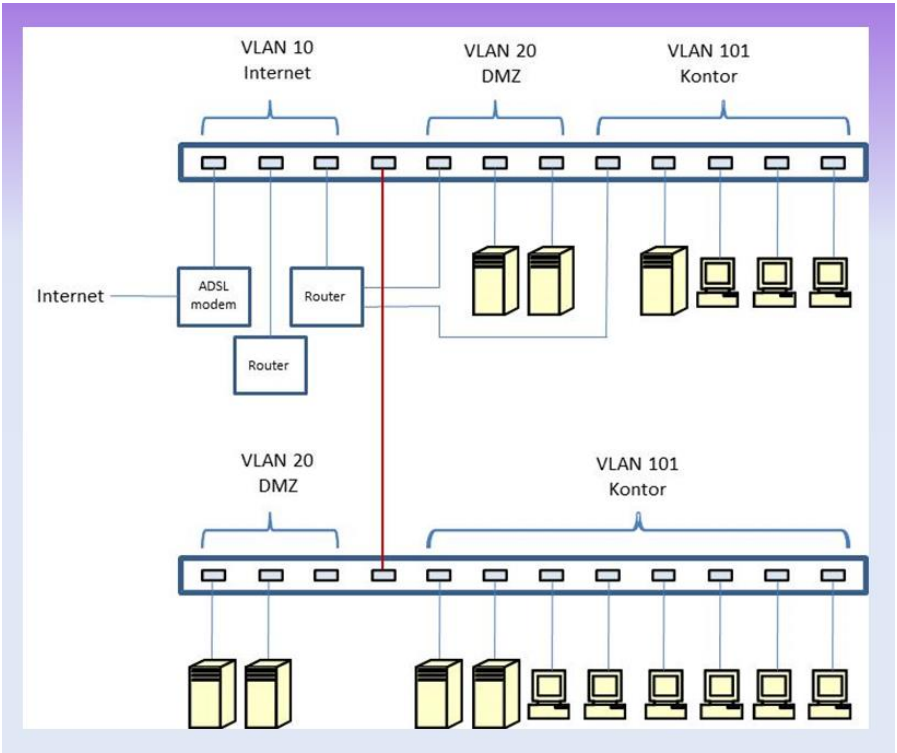
DMZ som man ser i VLAN 20 står för DeMilitarized Zone och är ett mellanting mellan det oskyddade Internet utanför brandväggen och det interna nätverket innanför brandväggen. I DMZ placerar man ofta servrar som ska kommunicera mot Internet, typ mailservrar, webbservrar, DNS-servrar osv.

Ex. 2: Flera switchar i serverrummet

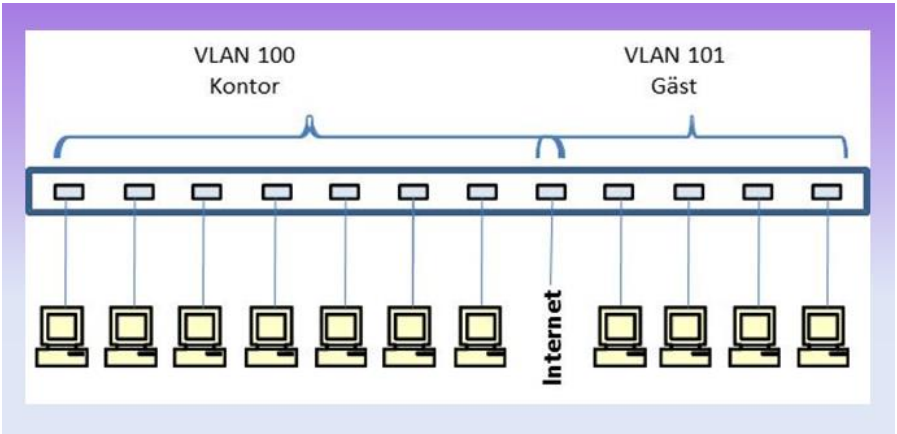
Om man behöver utöka med flera switchar i serverrummet eller om man har flera serverrum måste man kunna flytta de olika VLANs till de andra servrarna. Då kan man konfigurera switchen så att flera VLANs skickas ut på en port. Detta kan man göra tack vare 802.1Q-protokollet.

Via en vanlig nätverkskabel mellan de båda switcharna kan man skicka flera VLANs. Då måste man konfigurera switcharna så att de skickar sina data till denna port.

Så här kan konfigurationen se ut:



Ex. 3: Flera separata nätverk med tillgång till Internet



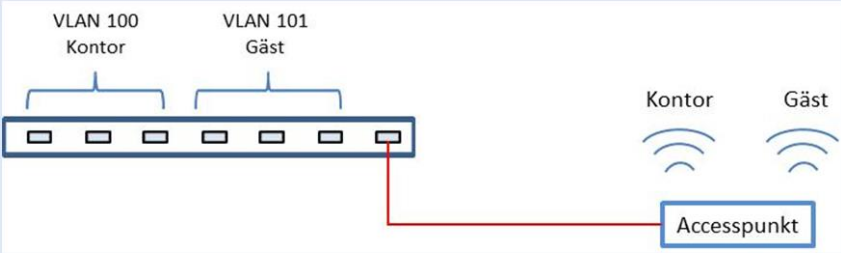
Om man har flera olika nätverk, som inte ska kunna ha kontakt med varandra, men som alla ska kunna nå Internet via en gemensam länk, kan man föra ihop flera VLANs i en port i switchen. Denna port kalls då för *Trunk*-port, som är en port som

kommunicerar med flera VLANs. Trafiken på Trunk-porten kommer inte behöva använda 802.1Q-protokollet utan det blir helt vanlig nätverkstrafik. Båda VLANs. delar på Trunk-porten utan att kunna se varandra.

Trådlösa VLAN

Ex. 4: Trådlöst nätverk med flera olika VLANs

Om man vill ha flera olika trådlösa nätverk, kopplade tll olika VLANs, så kan man åstadkomma det med 802.1Q-protokollet. Man skickar helt enkelt ut de VLANs man vill ha, på en port i switchen och kopplar sedan accesspunkten till denna port:



Besvara nu frågorna 4.345-4.346 på sid 150 om avsnitt 4.4 om Virtuella nätverk (VLAN).

.