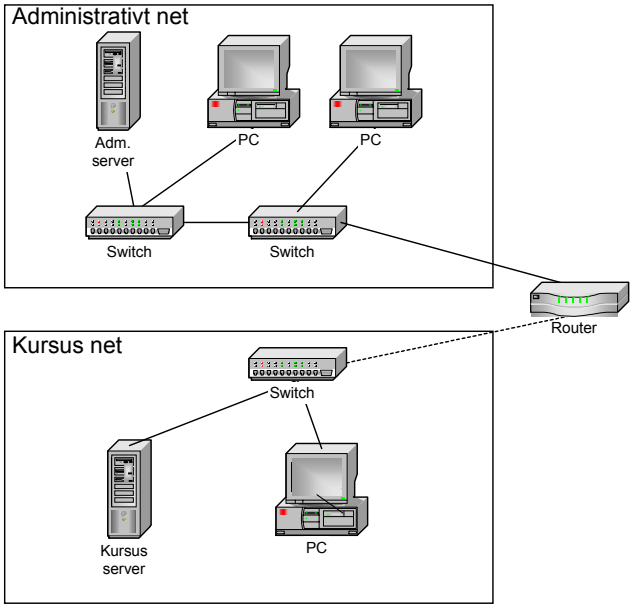
VLAN

I et traditionelt LAN (netværks adskilt af routere) indgår samtlige switche og samtlige porte i samme net, og disse kan uden videre kommunikere med hinanden - de indgår i et broadcast domain.

Ofte vil man have brug for at opdele et sådant net i flere separate net, som ikke uden hjælp fra en router, kan kommunikere med hinanden - eksempelvis af følgende årsager:

- Der er behov for såvel et administrativt som et kursusnet, og enhederne på disse net må ikke kun se hinanden.
- Der er problemer med for meget broadcast trafik i nettet - broadcast trafik anvendes typisk for at enheder kan finde hinanden indenfor samme broadcastdomain (typisk samme IP subnet).

Denne problemstilling kan løses ved at etablere to fysisk adskilte netværk, der er forsynet med hver deres switche, og som (hvis der skal være forbindelse på tværs af nettene) er koblet op på en fælles router.



En sådan løsning har følgende problemer:

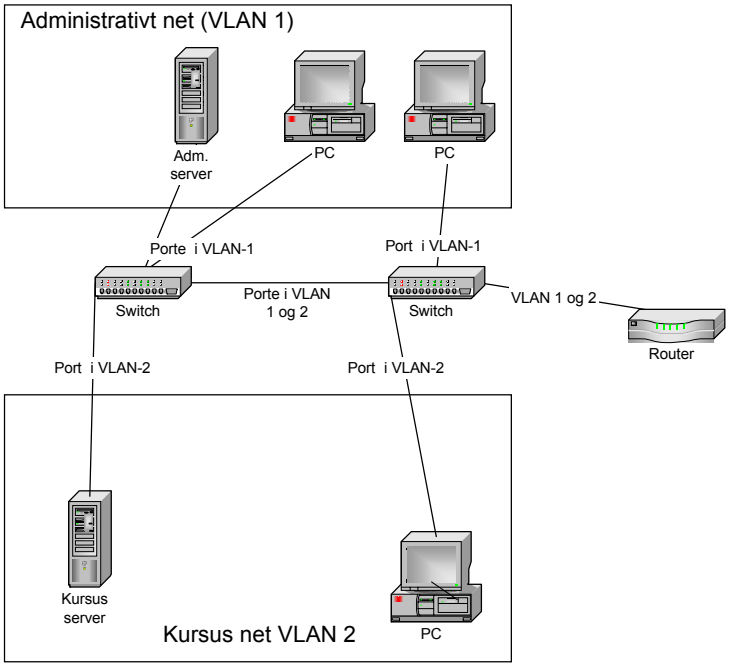
- Løsning er dyr i anskaffelse, idet der skal købes separat udstyr til de to net.
- Løsningen er ikke særlig fleksibel, idet ledige porte ikke kan flyttes mellem nettene.
- Såfremt nettene er placeret på flere fysisk adskilte lokationer, skal der anvendes en forbindelse mellem lokationerne pr net.

Alternativet til at lave to fysisk adskilte net er at anvende VLAN (standard IEEE 802.1Q), hvor man på de enkelte switche kan afgøre, hvilket net de enkelte porte skal høre til - eksempelvis kan port 1-10 høre til VLAN-1 (administration), mens port 11-24 anvendes til kursusnet (VLAN-2). Enhederne i disse to net vil ikke kunne se hinanden, idet switche ikke tillader kommunikation mellem VLAN's, hvorfor den eneste måde at etablere forbindelse mellem disse er ved at anvende en router.

Tilknytningen af en port til et VLAN kan ske ud fra bl.a. følgende metoder:

- Port baseret allokeret: dvs. hvor der manuelt defineres hvilket VLAN en given port hører til - dette er p.t. den mest udbredte form for VLAN.
- MAC adresse baseret: her defineres der pr MAC adresse (dvs. LAN adapter), hvilket VLAN den givne pc skal sidde i. Når en enhed bootes på en switch, med et MAC adresse baseret VLAN, kontrollerer switchen, hvilken MAC adresse som enheden har, og allokerer porten til det VLAN som den givne adresse hører til.
- IP adresse baseret: her defineres der hvilket VLAN en enhed med en given IP adresse skal placeres i (opdelingen laves normalt pr IP subnet).
- Protokol baseret: hvor der laves en VLAN til hver enkelt netværksprotokol - f.eks. IPX og TCP/IP.

I en switch hvor VLAN er aktiveret, kan en port sagtens være medlem af flere VLANs, hvilket sker ved at porten defineres som "tagged" i de enkelte VLAN, som den skal deltage i - at en port er tagged, betyder at der i samtlige datapakker, som sendes til/fra den pågældende port, tilføjes en entydig identifikation af hvilket VLAN den pågældende pakke hører til. Denne funktion bruges f.eks. når flere switche skal forbindes med hinanden, idet man så kun behøver en forbindelse (som dække samtlige VLAN's) mellem disse - tagged porte kan også anvendes ved opkobling af servere og routere.



VLAN har følgende fordele:

- Der skal anvendes mindre udstyr end ved oprettelse af separate net - en switch kan indgå i mange VLANs.
- Løsningen er dynamisk, idet man via software kan flytte en port i en switch fra et VLAN og til et andet - f.eks. hvis der i en periode ikke er brug for så mange porte på det administrative net, kan disse flyttes over på kursusnettet.
- Ved at bruge tagged porte kan man nøjes med en forbindelse mellem switchene (og de lokationer de måtte være installeret på) - uanset hvor mange VLANs der måtte være defineret.

Ulemperne ved VLAN er:

- VLAN standarden er på visse punkter åben for fortolkning, hvorfor man ikke skal være 100% sikker på, at switche fra forskellige leverandører kan anvendes sammen.
- Der skal anvendes en høj grad af disciplin ved konfigureringen af VLAN idet man let kan komme til at placere en port i et "forkert" VLAN, og dermed f.eks. placere en intern server på Internettet.
- Der skal laves en strategi for sikkerheden omkring switchene, idet der ikke kan tillades at en bruger, der sidder på eksempelvis kursusnettet, kan få adgang til switchenes konfiguration, idet dette vil give den pågældende bruger mulighed for at flytte eksempelvis servernes opkoblinger over på kursusnettet (som ofte er identisk med Internettet).