

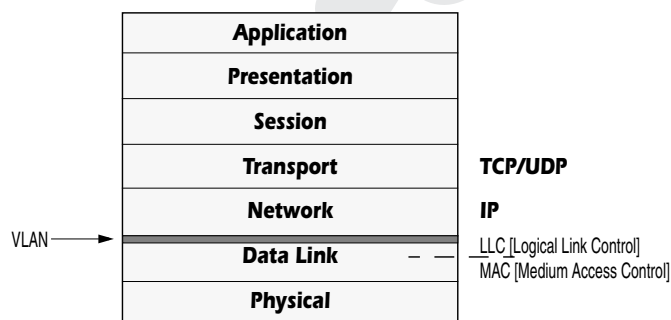
Frem fra glemselen: VLAN

VLAN? Virtuelle lokalnett? Vi smakte på dem på 90-tallet, og de smakte vondt. Finnes det noen god grunn til at vi skal gjennom den samme øvelsen én gang til?

Fra leverandørsiden får vi et rungende ja på dette spørsmålet, og enkelte brukermiljøer kan fortelle om gode erfaringer – VLAN er åpenbart ikke hva det en gang var. Dermed gir vi oss i kast med nøkkel-spørsmålene: Hva og hvorfor, hvilke forandringer har skjedd siden forrige runde, hva er medaljens bakside – og ikke minst: Trenger vi VLAN?

Virtuelle lokalnett

Ideen fremgår på sett og vis av navnet: Virtuelle lokalnett betyr at vi smetter inn et ekstra administrasjonslag mellom det såkalte link-nivå (*data link layer*) og transport-protokollen. Vi ser umiddelbart (figur 4)



Figur 4 Virtuelle lokalnett implementeres gjennom å innføre et ekstra 'lag' mellom mediets lavnivå-protokoller og transportprotokollen.

at dette representerer en komplikasjon av et bilde som ikke utmerker seg med sin enkelhet fra før. Samtidig er det ganske innlysende at vi derigjennom tilfører en styringsmulighet og en fleksibilitet. Dermed blir spørsmålet – som også er hovedtema for denne artikkelen: Står prisen i et rimelig forhold til gevinsten?

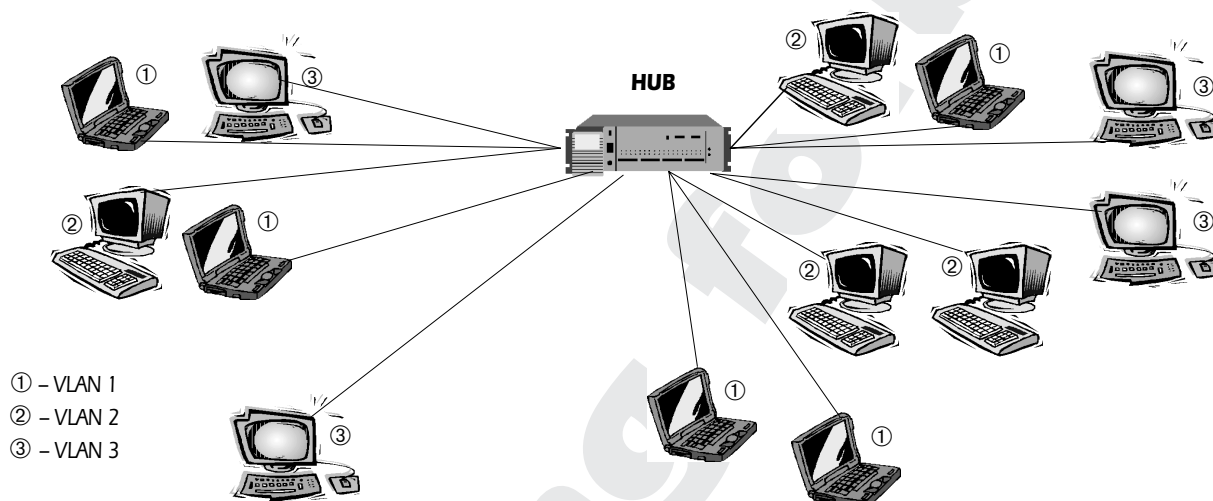
Motivasjon

Ideen om virtuelle lokalnett oppsto i kjølvannet av den voldsomme ekspansjonen på lokalnettsiden på 90-tallet. Overgangen fra delte koaksialkabler til såkalte strukturerte kablingssystemer, dvs. parkabel i stjerne-topologi, åpnet for en ny grad av kontroll og struktur – med én eller noen få beslektede noder per fysisk forbindelse frem til nærmeste kabelskap. HUBene som knyttet det hele sammen, var en vide-reutvikling av tradisjonelle broer.

Rutere var kostbare og hørte til unntakene, og protokollene var i de fleste miljøer en broket samling som gjorde sitt ytterste for å ta knekken på hverandre. Såkalte *broadcast*-stormer kombinert med ustabilitet og overbelastet utstyr hadde lenge gjort hverdagen til et mareritt for

nettverks-administratorer flest, og motiverte overgangen til en ny arkitektur der isolasjon av feil ble en selvfølge i stedet for en umulighet. Utsiktene til konvergens mot én eller et par-tre protokoller var imidlertid beskjedne.

VLAN skulle bringe kontrollnivået et skritt videre: Ved å etablere et logisk skille mellom grupper av noder på samme HUB, skulle det bli enklere å holde styr på trafikken, administrere brukerne og øke stabiliteten. At tilsvarende effekt kunne oppnås ved å bruke rutere i stedet for broer, var uinteressant: Rutere var kostbare, hadde sine egne ytelsesproblemer å slite med, og aller viktigst: En rekke av protokollene fungerte kun i lokalnett, og kunne ikke rutes.⁸



Figur 5 Tradisjonelt VLAN-oppsett via en HUB – koblingen mellom gruppe (VLAN) og medlem (node) gjøres på portnivå eller på hardware-adresse.

Bra, men ikke godt nok

Om ideen var aldri så god, ble det aldri riktig fart i sakene for 1. generasjons VLAN. I etterpå-klokskapens grelle lys, er det lett å finne årsakene til fiaskoen:

- ✓ HUBene hadde ytelsesproblemer allerede. Et ekstra lag av programvare forverret problemet.
- ✓ Programvare og protokoller for administrasjon av de virtuelle lokalnettene, var underutviklet og manglet standardisering. Vi måtte velge én leverandør – eller ingen ting.
- ✓ Dårlige driftsverktøy gjorde at drømmen om å administrere brukernes tilhørighet fra skjermen i stedet for ved flytting av kabler, ble til et mareritt.

Å lage VLANs som strakk seg utover én enkelt HUB ble en formidabel oppgave – konseptet skalerte kort og godt ikke, mer på grunn av manglende verktøy enn svakheter i konseptet. Videre var mulighetene

⁸ Eksempler på slike protokoller er DLC (DATA LINK CONTROL [IBM]) og LAT (LOCAL AREA TRANSPORT [Digital]).

for kobling mellom gruppe (VLAN) og bruker (node) begrenset til adresse eller port:

- ✓ Adresse: En tabell i HUBen inneholder en oversikt over alle hardware-adresser som er akseptable og deres VLAN-tilhørighet, gjerne med en egen gruppe for ukjente eller uregistrerte adresser. Metoden er åpenbart administrasjonsintensiv i et dynamisk miljø.
- ✓ Port: En tilsvarende tabell som for eksempel assosierer portene 1, 3, 8, 9 og 11 til VLAN-1; 2, 4, 14, 15 og 16 til VLAN-2 og så videre. Med et effektivt verktøy kan dette fungere bra, men skalerbarheten er fortsatt beskjeden.

Neste generasjon

Idet vi nærmet oss årtusenskiftet, dukket imidlertid ideen opp på nytt. Kaoset fra 90-tallet var på vei ut, med konvergering mot Ethernet på teknologisiden og IP på protokollsiden. Dessuten – og minst like viktig – var tilblivelsen av en egen lavnivå-protokoll (egentlig en protokollutvidelse for Ethernet, under navnet 802.1Q) for VLAN fra IEEE. Eksistensen av en slik standard ville for det første gjøre skalerbarheten for VLANs langt bedre, og for det andre muliggjøre samspill mellom utstyr fra flere leverandører. Standarden ble endelig vedtatt i desember 1998.⁹

Mens standarden var en viktig katalysator for å få VLAN på banen igjen, var motivasjonen – eller salgargumentene – overfor markedet fortsatt nært beslektet med tilsvarende fra første generasjons VLAN:

- ✓ **Et fjernstyrt patchepanel:** Brukerne flytter seg stadig oftere, og arbeidet med fysiske omkoblinger i den forbindelse er både tidkrevende og feilbefengt. Å kunne gjøre operasjonen fra et verktøy på skjermen og umiddelbart teste resultatet, er attraktivt – uansett sammenheng.
- ✓ **Isolasjon av trafikk:** Å sørge for at trafikken kun havner der den hører hjemme, er ikke bare en optimalisering, men også et bidrag til sikkerheten. Med våre dagers kablingsstruktur betyr det først og fremst styring/filtrering av *broadcast*- og *multicast*-trafikk.
- ✓ **Mobilitet for brukerne:** Effekten av det elektroniske patchepanelet vi beskrev ovenfor, er at brukerne ser det samme nettverket, uansett hvor de er plugget inn. Dette gir forutsigbarhet og stabilitet, med færre problemer og spørsmål som følge.
- ✓ **Automatisk konfigurering av subnett:** 90-tallets protokollkaos er erstattet av IP over alt¹⁰ – et gigantisk fremskritt på

9 802.1Q-standard er basert på en tidligere standard for Ethernet-svitsjer som ikke er forberedt for VLAN, 802.1D. 802.1Q øker størrelsen på en Ethernet-ramme med 4 bytes, og legger forholdene til rette for QoS-mekanismer i tillegg til VLAN-støtte. Arbeidet med 802.1Q startet i juli 1995.

10 Novells NetWare er forbausende seiglivet, og IPX-protokollen er definitivt fortsatt i live. Selv NetWare har imidlertid tatt konvergensen mot IP til følge, og en stor prosent av dagens NetWare-miljøer benytter kun IP som transport-protokoll.

alle måter. Selv et homogent IP-nett har imidlertid rikelig av løpende oppgaver og problemstillinger, herunder administrasjon av subnett. Et avansert VLAN kan automatisere deler av denne jobben gjennom å gjenkjenne brukere og plassere dem i riktig subnett uten manuell intervensjon.

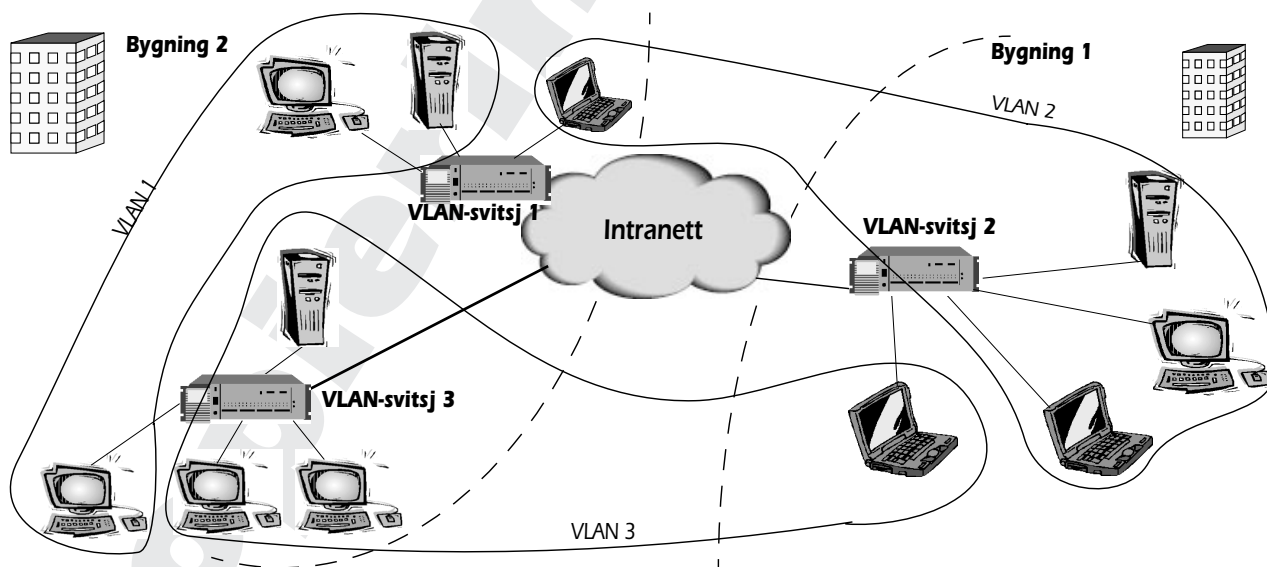
De teknologiske fremskrittene som fant sted mellom 1. og 2. generasjon, var også i høyeste grad kvalifiserende for å bringe liv i ideen om VLAN:

- ✓ HUBene var blitt til intelligente svitsjer med høy kapasitet.
- ✓ Verktøyene var blitt vesentlig bedre, og standardene for fjernstyring av utstyr likeså [SNMP, RMON2].
- ✓ Den nye VLAN-standarden, som utvidet Ethernet-protokollen fysisk og funksjonelt, gjorde det mulig å implementere VLAN med et nytt nivå av dynamikk og skalerbarhet.

Spesielt det siste punktet er viktig her: Mens første generasjons VLAN fokuserte på noder, adresser og porter, kan dagens produkter rette oppmerksomheten mot trafikken, datastrømmen. Funksjonen blir rett og slett mer lik en ruter, som basert på nettverks-adresse i hver enkelt pakke og egne rutingtabeller, formidler trafikken videre dit den hører hjemme.

Muligheter, begrensninger

Det betyr at vi i prinsippet kan bygge virtuelle, svitsjede lokalnett av vilkårlig størrelse ved hjelp av svitsjer med VLAN-støtte og tilhørende styringsverktøy. Figur 6 viser forenklet hvordan dette kan se ut i et større intranett som dekker flere geografiske lokasjoner. Hvorvidt dette er en hensiktsmessig arkitektur, skal vi komme tilbake til nedenfor.



Figur 6 Med en utvidet Ethernet-protokoll (802.1Q) kan virtuelle lokalnett strekke seg over større områder og flere svitsjer. I og med at protokollene ligger på lag 2 i stakken (se figur 4), kan et VLAN ikke passere en ruter.

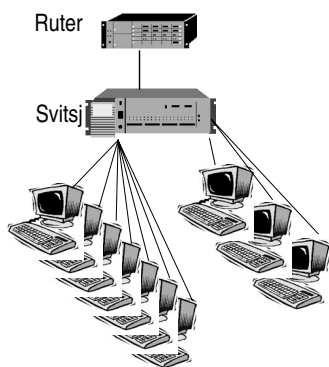
VLAN-protokollen gir nye frihetsgrader med hensyn til hvordan et VLAN kan struktureres og skales. Kombinert med Ethernet-baserte

forbindelser over lange distanser (se egen artikkel på side 4), kan lokalnett-segmenter dekke store geografiske områder. Enkelte tjeneste-leverandører har sågar valgt å basere seg på en slik modell for å tilby områdenett eller fjernnett for kunder – som alternativ til å bruke rutere. Mulighetene for å introdusere QoS-mekanismer i ligningen er ofte et nyttig argument i den forbindelse – om ikke alltid like relevant. At løsningen blir topologisk enkel (flat struktur) og gir god ressursutnyttelse, er det imidlertid ingen tvil om.

Struktur og automatikk

Mens 802.1Q-standarden dramatisk utvider dekningsområdet og anvendeligheten til VLAN, åpner overgangen til intelligente og effektive svitsjer for nye strukturer og grupperingsmekanismer. Vi kan for eksempel etablere omfattende nettverk med mer eller mindre automatiske VLAN-strukturer etter følgende kriterier:

- ✓ Portbasert – avansert, fjernstyrt patchpanel. Karakteristisk for første generasjons VLAN, og med større nytteverdi i dag enn noen gang tidligere.
- ✓ Adressebasert: Et hakk mer sofistikert enn de tidlige portbaserte systemene. Senderens hardware-adresse avgjør hvilke porter som mottar trafikken.
- ✓ Protokoll-basert: Svitsjen fordeler trafikken i henhold til hvilken protokoll som kjøres på nivå 3. For eksempel Appletalk på port 1,5,10, IPX på port 2,3,4,6, IP på port 7,13,14 osv. Middels avanserte enheter kan ha overlappende soner, slik at en port kan tilhøre flere protokoll-grupper. Videre kan grupperingen skje automatisk ved at svitsjen gjenkjenner trafikk-typen og allokterer portene etter dette.
- ✓ Subnett-basert: Automatisk portallokering basert på IP-subnett. Noder på ulike subnett kan ikke kommunisere direkte seg imellom, selv om de befinner seg på samme fysiske segment, uten at en ruter er til stede. For å ta effektivt vare på slike situasjoner, har det dukket opp svitsjer med innebygde IP-rutere på markedet (se margrammen).
- ✓ Applikasjonsbasert: Svitsjen strekker sine undersøkelser til strekkelig langt inn i hver enkelt pakke til å kunne detektere hvilke applikasjoner eller applikasjonsgrupper som kjøres, og foretar gruppering av VLAN basert på dette.¹¹ Funksjonen er primært orientert mot båndbreddeintensive anvendelser som video *multicasting* og videokonferanser, men er i beskjeden praktisk bruk. Båndbreddebehovet for slike anvendelser blir ofte overestimert.



En 'router on a stick' eller 'one armed router' sørger for at noder tilhørende ulike subnett, men som befinner seg på samme segment, kan kommunisere. Som regel tar en slik ruter seg også av kommunikasjon med verden utenfor, og kan i noen tilfeller være inkludert i selve svitsjen.

Kostbar usynlighet

En viktig kvalifikasjon for 802.1Q-utvidelsen har naturlig nok vært at den ikke skal ødelegge kompatibiliteten Ethernet er kjent for. Kravet har en rekke tekniske implikasjoner som vi ikke skal komme inn på i

¹¹ Enkelte leverandører kaller dette LAYER 7 SWITCHING.

denne sammenheng, utover å konstatere at resultatet er tilfredsstillende: VLAN-pakker formidles uten komplikasjoner av svitsjer som ikke 'forstår' VLAN – de legger ikke engang merke til forandringen. Utstyr som mottar pakkene for håndtering på høyere nivå (klienter, tjenere, rutere – ofte kalt 'endesystemer'), forkaster dem umiddelbart, fordi de ikke gjenkjenner pakketyper. Slike 'taggede' pakker, som de gjerne kalles, skal ikke frem til endesystemer, men pakkes ut av den svitsjen mottakeren er tilkoblet. Derfor er det både akseptabelt og nødvendig at 'taggede' pakker blir forkastet når de havner på avveie.

Nå kan slike endesystemer gjerne oppdateres til å forstå de utvidede pakkene direkte. I tilfellet applikasjonssvitsjing er slik støtte en nødvendighet. I praksis forekommer imidlertid dette knapt, og fordelene med at millioner av systemer kan fortsette å fungere uten den aller minste forandring, er åpenbare.

Mens skalerbarhet er en av de viktigste følgene av den nye VLAN-protokollen, skal vi ikke la oss forlede til å tro at den er ubegrenset. Selv om protokollen er enkel og lagt til rette for optimal effektivitet i Ethernet-omgivelser,¹² er det et faktum at prosesseringen blir av en helt annen størrelsesorden enn ren pakkessvitsjing. Stor trafikk og store nettverk kan derfor gi ytelsesproblemer om de ikke struktureres optimalt. For eksempel er det viktig å velge hvor det er nødvendig med VLAN-svitsjing og hvor det er overflødig. Logikken er ikke umiddelbart innlysende, men i et stort svitsjet VLAN-nettverk, trenger ikke sentrale svitsjer å vite noe om VLAN – på samme måte som sentrale rutere ikke trenger å vite noe om enkeltnoder: De forholder seg til nettverkene og overlater til kantrutere – og i VLAN-tilfellet kantsvitsjer – å ta seg av detaljer som har med klienter, tjenere og andre endenoder å gjøre.

VLAN og sikkerhet

Med dagens sterke fokus på IT-sikkerhet kommer VLAN hyppig på banen som en antatt viktig faktor. Separasjon av trafikk er, som vi var inne på ovenfor, et bidrag til sikkerheten.

Mens dette er et faktum, er det også nødvendig å være oppmerksom på at VLAN ikke er noen sikrings-mekanisme. Trafikkseparasjon er positivt, men gir ingen reell sikkerhet utover nivået vi finner på offentlige toaletter: Vi lukker og stenger døren etter oss, men har ingen illusjoner om at den vil stoppe en inntrenger som virkelig vil inn.

Utbredte misforståelser rundt VLAN og sikkerhet, representerer faktisk en viktig innvending mot hele konseptet. Det kan ikke understrekes sterkt nok at VLAN er et teknisk/administrativt verktøy, ikke et relevant bidrag til sikkerheten. «Do not depend on electronic measures for security», sier nettverks- og svitsj-eksperten Rich Seifert, som blant annet har vært en drivkraft i utviklingen av 802.1Q-standarden. Han fortsetter:

«It should be emphasized that there is no such thing as total electronic security. While VLAN technology can isolate

¹² 802.1Q-standarden er tilpasset Ethernet, Token Ring og FDDI, med hovedvekt på førstnevnte.

traffic [...], such mechanisms will not prevent all security attacks. VLAN isolation simply makes the intruder's job more difficult, and will prevent intrusions only from those attackers who are unwilling to expend the effort necessary to break the level of protection provided.»¹³

I et adresse-basert VLAN, der gruppe-tilhørigheten avgjøres på bakgrunn av en nodes hardware-adresse, kan en inntrenger 'låne' adressen til en node som er avslått eller frakoblet, og derigjennom få full aksess til nettverket. En annen kjent variant er at inntrengerer først bryter seg inn i en av svitsjene eller skaffer seg passordet til administrasjonssystemet, og derigjennom ordner trafikkflyten etter behov.

Trenger vi VLAN?

Et kanskje overraskende, men høyst relevant spørsmål. Alle sine attraktive sider til tross, er ikke VLAN noen vidundermedisin for overbelastede, kompliserte eller administrasjonsintensive nettverk. Det skal gjøres grundige og kritiske evalueringer av alternativene – i de fleste tilfeller en kombinasjon av svitsjede lokalnett, VLANs og rutede subnett – før valgene foretas, der blant andre følgende faktorer vektlegges:

- ✓ Ruting gir ekte segmentering og full kontroll med trafikken, også i sikkerhetsmessig forstand.
- ✓ Svitsjing er i utgangspunktet enklere og raskere enn ruting, men forskjellen er beskjeden når VLAN introduseres.
- ✓ VLAN gir store frihetsgrader som inspirerer kreativiteten hos arkitektene. Resultatet blir ofte det motsatte av hva intensjonen var – med høyere kompleksitet og lavere stabilitet.
- ✓ Store svitsjede nett bidrar til å spare IP-adresser, men NAT er i mange tilfeller en mer rasjonell løsning, som alltid er sikrere.
- ✓ Svitsjing og VLAN er nivå 2 teknologi, og fjerner ikke behovet for rutere.

VLAN øker kompleksiteten i nettverket ved å introdusere et nytt nivå. For noen år siden kunne vi føre både økonomiske og ytelsesmessige argumenter for en slik komplikasjon, fordi rutere var mer kostbare og mindre effektive enn de er i dag. Jo dypere vi graver i VLAN-teknologien, desto flere fellestrekk får den med ruting på nivå 3 – funksjonelt, teknologisk, effektivitetsmessig og økonomisk.

Utviklingen har feid en vesentlig del av fundamentet bort fra den nye generasjonen VLAN, hvilket ikke gjør den unyttig, men forsterker viktigheten av å gjøre kvalifiserte valg. VLAN øker alltid kompleksiteten, og gevinsten må være vesentlig i forhold til denne 'kostnaden' for at valget skal være interessant. Der ruting koster og yter det samme, skal det gode argumenter til for å velge VLAN. ■

¹³ Sitatet er hentet fra Rich Seiferts bok "The Switch Book" (John Wiley & Sons 2000, ISBN 0-471-34586-5) side 437.