

Lappeenrannan Teknillinen Yliopisto
Tietotekniikanosasto
010626000 Lähiverkot erikoistyökurssi

01062000 Lähiverkot – erikoistyökurssi
Seminaari
VLAN

Esa Nuutinen, 0086450
Tite 4.

Lyhenteet

ATM = Asynchronous Transfer Mode

CRC = Cyclic Redundancy Check

ICV = Integrity Check Value

IEEE = The Institute of Electrical and Electronics Engineers, Inc.

LAN = Local Area Network

LANE = Local Area Network Emulation

LEC = LAN Emulation Client

LES = LAN Emulation Server

MAC = Medium Access Control

MDF = Management Defined Field

PDU = Protocol Data Unit

PVC = Permanent Virtual Circuit

SAID = Security Association Identifier

SDE = Security Data Exchange

SNMP = Simple Network Management Protocol

SVC = Switched Virtual Circuit

TDM = Time-Division Multiplexing

VID = VLAN ID

VLAN = Virtual Local Area Network

WAN = Wide Area Network

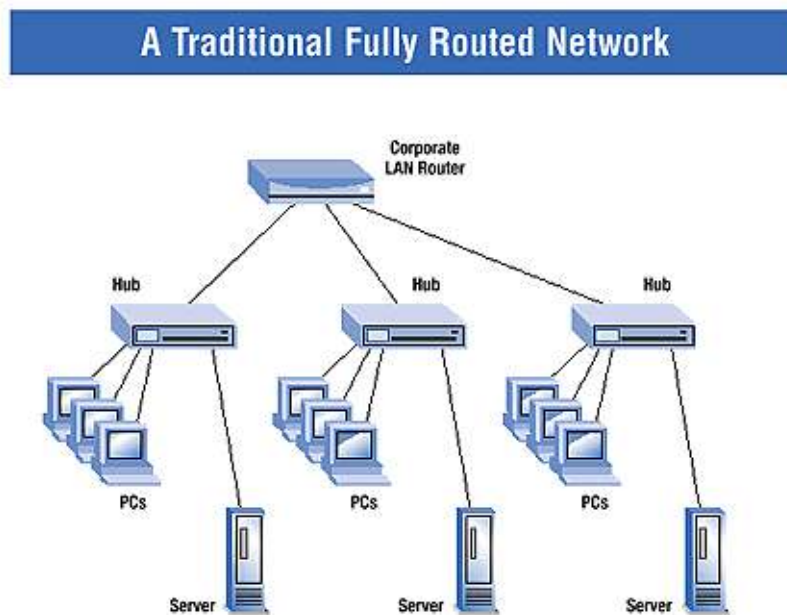
Sisällysluettelo

1.0 Johdanto.....	4
2.0 VLAN.....	6
2.1 Mikä VLAN on?.....	6
2.2 Porttien mukaan ryhmitellyt VLAN:t.....	7
2.3 MAC osoitteiden mukaan ryhmitellyt VLAN:t.....	8
2.4 Verkkokerroksen perusteella ryhmitellyt VLAN:t.....	9
2.5 Pakettien siirto kytkimen välillä.....	10
2.5.1 Implicit.....	10
2.5.2 Explicit.....	10
2.6 VLAN:n konfigurointi.....	11
2.6.1 Manuaalinen konfigurointi.....	11
2.6.2 Puoliautomaattinen konfigurointi	12
2.6.3 Täysin automaattinen konfigurointi	12
2.7 Kytkimien välinen kommunikointi.....	12
2.7.1 Taulukkojen ylläpito signalaleilla.....	12
2.7.2 Kehysten merkitseminen.....	12
2.7.3 TDM	12
2.7.4 VLAN ja ATM (LANE).....	13
2.8 Standardit.....	14
2.8.1 IEEE 802.10.....	14
2.8.2 IEEE 802.1Q.....	16
2.8.3 802.1P	17
3.0 VLAN:n edut ja haitat.....	19
4.0 VLAN:n käytännössä.....	21
5.0 Yhteenveto.....	22
6.0 Tenttikysymykset.....	23
Lähteet.....	24

1.0 Johdanto

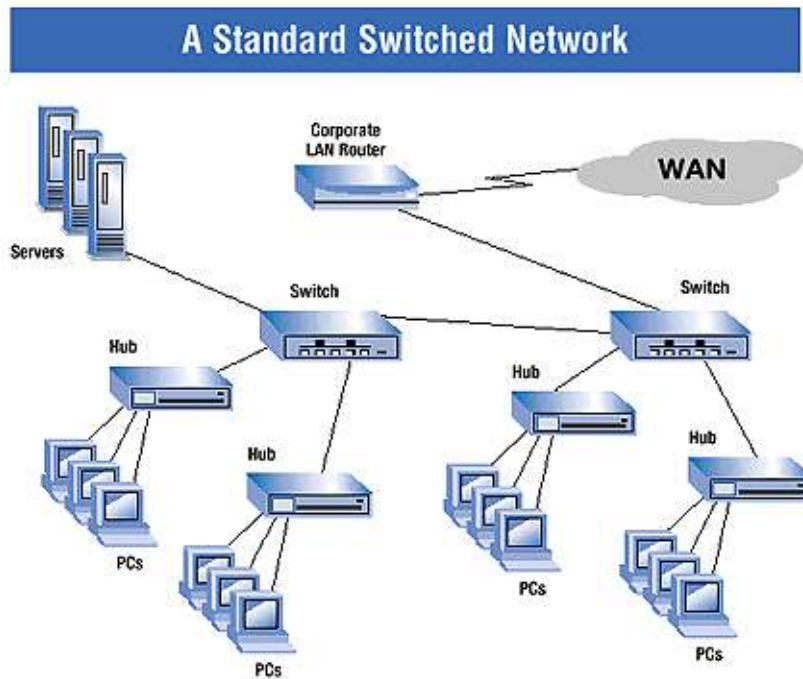
1980 luvulla verkot rakennettiin yksinkertaisen verkkoarkkitehtuurin varaan. Verkon osat liitettiin yhteen reitittimellä kuvan 1 mukaisesti. Tämä mahdollisti sen, että kaikki verkkoressurit olivat käytettävissä kyseiseen reitittimeen liitetyillä koneilla, sillä reititin ohjasi tarvittavan liikenteen verkkojen osien, mutta verkon sisäinen liikenne tai broadcast liikenne ei siirtynyt. Näin verkko ei tukkeutunut turhasta liikenteestä. Perinteiset reitittimet ovat kuitenkin hitaita, monimutkaisia ja kalliita.

[2]



Kuva 1. Perinteinen reitittimellä kytketty verkko. [2]

Verkkoliikenteen lisääntymisen ja koneiden nopeutumisen myötä verkkoliikenteen määrä kasvoi ja vaadittiin suurempia nopeuksia. Kytkimet olivat seuraava ratkaisu ongelmaan. Verkko jaettiin segmentteihin, joista jokainen segmentti liitettiin toisiinsa kytkimellä kuvan 2 mukaisesti. Kytkimiä voitiin kytkeä toisiinsa ja näin muodostui kokonainen sisäinenverkko, joka voitiin yhdellä reitittimellä kytkeä esimerkiksi Internetiin tai muuhun ulkoiseen verkkoon. Tarvittaessa kaikki resurssit ovat käytettävissä kytkimien välityksellä. Broadcast ja multicasta liikenne kulki kytkimen läpi edelleen kaikille. Kytkimien myötä verkkolaitteiden hinnat ja monimutkaisuus laskivat tiedonsiirto nopeuksien kasvaessa. [2]



Kuva 2. Kytetty verkko. [2]

Verkkojen koon ja liikennemäärien kasvaessa verkkoja jaettiin aina vaan pienempiin segmentteihin. Ongelmaksi on muodostunut broadcast liikenteen määrä, joka kuluttaa suurissa verkoissa kapasiteettia turhaan. Reitittimiä käytetään edelleen, mutta lähinnä niissä verkon osissa, joissa nopeus ei ole tärkeää, sekä yhdistämään yrityksen lähiverkko ulkopuoliseen verkkoon, esimerkiksi Internetiin. VLAN (Virtual Local Area Network) on kehitetty ratkaisemaan nykyisten verkkojen ongelmia. [2]

2.0 VLAN

2.1 Mikä VLAN on?

VLAN:n määritelmä ei ole täysin yksiselitteinen. Käytännössä tällä kuitenkin tarkoitetaan sitä, että ryhmä tietokoneita kuuluu samaan broadcast domainiin. Toisin sanoen vaikka työasemat fyysisesti sijaitisivat eri verkko segmenteissä, VLAN:n avulla ne kuitenkin näyttäisivät siltä, kuin ne sijaitisivat samassa verkkosegmentissä. [1] VLAN:n on mainostettu ratkaisevan nykyisten verkkojen ongelmia, niin suorituskyvyn kuin joustavuudenkin osalta. [2]

VLAN:ssa koneen fyysisellä sijainnilla ei ole siis enää merkitystä, koska hän voi kytkeytyä verkkoon toisessa verkko segmentissä, mutta hänelle tilanne näyttää samalta kuin jos hän olisi kytkeytynyt verkkoon ”oikeassa” segmentissä. Myös eri verkkoresurssien oikeudet voidaan määritellä, eli esimerkiksi on mahdollista rajata jotkut palvelimet niin, että ne näkyvät vain yrityksen insinööreille. VLAN:n käyttöönotolla on mahdollista korjata olemassa olevan verkon suunnitelussa sattuneista virheistä ja päästä eroon mahdollisista rajoituksista. [2]

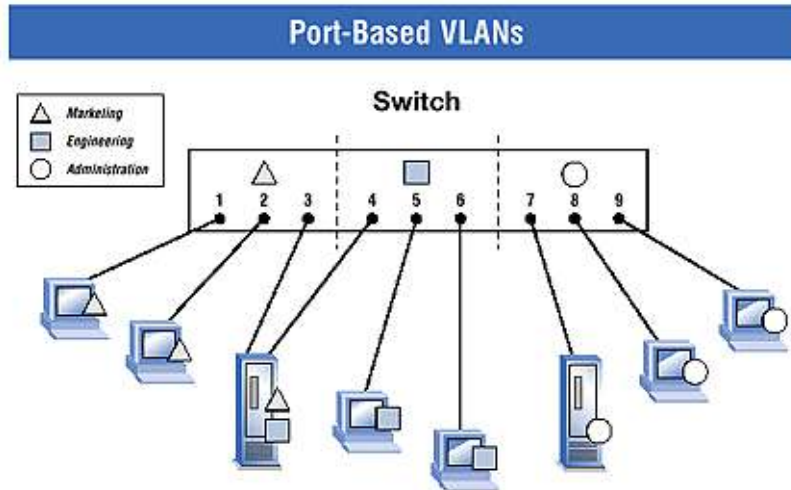
Verkossa joka oli toteutettu reitittimien avulla, segmenttien koko vaihteli tyypillisesti 30-100 käyttäjän välillä. Kytkimien avulla segmenttien kokoa oli mahdollista pienentää. Tällaisissa verkoissa reitittimen rooli on toinen ja se yhdistää lähinnä enää LAN:n WAN:iin (Wide Area Network) esimerkiksi Internetiin. Kytkimet eivät estä broadcast yms. lähetyksiä, vaan ne leviävät verkoissa entistä suuremmille käyttäjämäärälle. Pelkillä kytkimillä toteutetussa verkon osassa saattaa hyvinkin olla yli 500:kin käyttäjää. Näin sama broadcast liikenne kulkeutuu heille kaikille. Kytkimien kehityksen myötä verkko koostuu yhä suuremmasta määrästä pieniä segmenttejä, segmenttien käyttäjämäärän samalla pienentyessä. [1]

VLAN tekniikka voidaan jakaa kolmeen eri pääkategoriaan. Porttien mukaan ryhmiteltyihin, MAC-osoitteiden perusteella ryhmiteltyihin tai verkkokerroksen (protokollien) mukaan ryhmiteltyihin

VLAN:hin. Lisäksi jotkut valmistajat ovat kehittäneet omia ratkaisuja, jossa näitä tapoja on voitu yhdistellä tarpeen mukaan. [1][2]

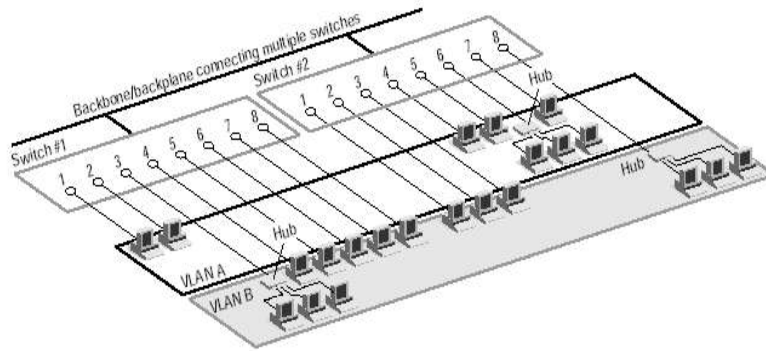
2.2 Porttien mukaan ryhmitellyt VLAN:t

Tässä menetelmässä VLAN-ryhmät määritellään kytkimen porttien perusteella. Esimerkiksi portit 1-3 voivat kuulua myyntipuolen VLAN:n, portit 4-6 insinöörien VLAN:n ja portit 7-9 hallinnon VLAN:n. Esimerkki kuvassa 3.



Kuva 3. Porttien mukaan ryhmitelty VLAN. [2]

Ratkaisu on kaikkein yleisin tapa toteuttaa VLAN, johtuen konfiguroinnin suoraviivaisuudesta. Aikaisemmin tämän tyyppiset ratkaisut tukivat vain yhtä reitintä, mutta nyt toisen sukupolven ratkaisuisissa on mahdollista tehdä sama portteihin perustuva ryhmittely myös kytkimille pelkkien yksittäisten koneiden sijaan. Kuvan 4 esimerkissä portit 1 ja 2 kytkimessä #1 sekä portit 4, 5, 6, ja 7 kytkimessä #2 muodostavat VLAN:n A ja loput muodostavat VLAN:n B. [1]



Kuva 4. Porttien mukainen ryhmittely VLAN kahdella kytkimellä. [1]

Portteihin perustuva ryhmittely tapa on siis kaikkein yleisin helppoutensa vuoksi. Siinä on kuitenkin omat haittansakin. Esimerkiksi jokaisen kytkimen porttiin kytketyssä keskittimessä olevan laitteen täytyy kuulua samaan ryhmään kaikkien muiden laitteiden kanssa. Kuvassa 4 näkyvässä kytkimen #1 3-porttiin kytketyn keskittimen takana olevien koneiden on pakko kuulua VLAN B:hen. [1] [2]

Jos käyttäjä siirtyy paikasta toiseen ja liittää koneensa toiseen porttiin, on ylläpitäjän muutettava konfiguraatiota manuaalisesti ja määriteltävä kyseisen portin VLAN-ryhmä oikeaksi. Etuna normaaliin LAN:n on, että nyt ylläpitäjä selviää tekemällä muutoksen konfigurointi ohjelmalla, sen sijaan että hänen olisi käveltävä kaapille jossa kytkin on ja vaihdeltava verkkokaapeleita paikasta toiseen. Periaatteessa tämän tyyppinen ratkaisu ei helpota ylläpidon työtä paljontaan, vaikka ylläpidon työtaakan keventymistä mainostetaan yhtenä hankintaperusteista.

2.3 MAC osoitteiden mukaan ryhmitellyt VLAN:t

Kun käyttäjiä ryhmitellään VLAN:ssa MAC osoitteiden perusteella, on ratkaisu ominaisuuksiltaan etujen ja haittojen osalta hyvin erilainen kuin porttien perusteella ryhmiteltävä VLAN. MAC-osoite on siis jokaiseen verkkolaitteeseen tallennettu osoite, jonka perusteella se voidaan yksilöidä. Teoriassa kaikilla verkkolaitteilla pitäisi olla valmiiksi tallennettuna oma yksilöllinen MAC-osoite. [1] [2]

Jokaisessa kytkimessä on taulukko verkkolaitteiden MAC osoitteista, sekä VLAN-ryhmästä, johon kyseisen osoitteen omaava verkkolaite kuuluu. Menetelmän suurin etu seuraa juuri tästä, kun laitteen

MAC-osoite ja VLAN-ryhmä on tallennettu, toimii konfigurointi automaattisesti, vaikka laite fyysisesti liitettäisiinkin eri paikkaan tai porttiin. Näin verkko on periaatteessa konfiguroitu käyttäjien mukaan ja osoitteet on sidottu käyttäjien verkkolaitteisiin. Toisaalta kun järjestelmää konfiguroidaan ensimmäisen kerran, on sen tekeminen paljon työläämpää kuin esimerkiksi aikaisemmin mainitussa portteihin perustuvassa menetelmässä. Toisena rajoituksena on se, että yksi laite ei voi käytännössä kuulua useampaan VLAN-ryhmään. Teoriassa tämän pitäisi toimia, mutta käytännössä tästä voi seurata suuriakin ongelmia reititystä yms. ajatellen. [1] [2]

Konfiguroinnin helpottamiseksi jotkut valmistajat ovat kehitelleet työkaluja, joiden avulla on mahdollista ainakin osittain alustaa MAC pohjainen verkko sen ensimmäisen tilan perusteella. Eli verkkolaitteiden MAC-osoitteet luetaan ja tallennetaan kytkimelle. VLAN luodaan siten, että esimerkiksi jokaisesta kytkimeen liitetystä keskittimestä tehdään oma ”aliverkko”. Toisin sanoen ne kuuluvat samaan VLAN:n. Käytännössä tämäkin tapa vaatii ylläpidon toimenpiteitä, koska VLAN ryhmittelyä täytyy todennäköisesti korjata. Oletettavaa on, että alkuperäinen verkon asetelma ja luodut VLAN:t eivät välttämättä vastaa todellista tilannetta. [1]

Toinen ongelma, joka tästä menetelmästä aiheutuu ovat suorituskyky ongelmat, jos yhden portin alla on useisiin eri VLAN ryhmiin kuuluvia käyttäjiä. Myös verkon koon kasvaessa suureksi, kasvaa kytkimien välisen tiedonsiirron tarve melkoisesti, koska käyttäjätietoja on välitettävä paljon kytkinten välillä. Ongelmana mainitaan myös kannettavien tietokoneiden telakointiasemat. Jos käyttäjällä on mahdollisuus käyttää useampaa telakointi asemaa ei MAC-perusteinen systeemi toimi, koska MAC-osoite on tallennettu telakointiasemaan ja jos käyttäjä siirtyy toiseen paikkaan ja liittää koneensa toiseen telakointiasemaan vaihtuu myös MAC-osoite. Tässä tilanteessa käyttäjätietoja on edelleen päiviteltävä jatkuvasti manuaalisesti. [1] Tämä ongelma ei ole yleinen, mutta tätä käytettiin esimerkkinä kuvaamaan MAC perusteisen VLAN:n ongelmia ja rajoituksia.

2.4 Verkkokerroksen perusteella ryhmitellyt VLAN:t

VLAN:t jotka perustuvat OSI-mallin kolmanteen kerrokseen (Network layer), ottavat huomioon protokollan tyyppin (jos useampaa protokollaa tuetaan) tai verkkokerroksen osoitteen määrittellessään

VLAN-ryhmää. Kytkin tuktii paketista IP-osoitteen, selvittäessään VLAN-ryhmää.

Etuina voidaan pitää sitä, että VLAN:t voidaan jakaa protokolla tyyppien mukaan. Käyttäjien vapaa liikkuvuus on myös mahdollista ilman että verkko osoitetta on konfiguroitava uudestaan. Suorituskyky on kuitenkin edelleen ongelma verrattuna aikaisempiin malleihin. Osoitteen selvittäminen paketista vie enemmän aikaa kuin esimerkiksi MAC- osoitteen lukeminen (Linkkikerros). Myös protokollien välillä on eroa suorituskyvyssä. Esimerkiksi TCP/IP protokollaa käytettäessä tehokkuus on parempi, kuin IPX tai AppleTalk:ia. Lisäksi reitittämättömät protokollat kuten NetBIOS:ta käytettäessä ei voida määrittellä toimimaan verkkokerrokseen perustuvissa VLAN:ssa.

2.5 Pakettien siirto kytkimen välillä

Jos kaikki koneet olisivat yhden kytkimen takana, pakettien siirto oikeaan paikkaan olisi yksinkertaista, koska yksi kytkin tietäisi aina tarkasti kuka on missäkin ryhmässä jne. Käytännössä tällaista tilannetta ei kuitenkaan koskaan tule. Niinpä tähän tilanteeseen on kaksi erityyppistä ratkaisua: implicit ja explicit. [2]

2.5.1 Implicit

Implicit tarkoittaa sitä, että jäsenyys ilmaistaan MAC-osoitteen perusteella. Tässä tapauksessa jokaisella kytkimellä, joka tukee ko. VLAN-ryhmää on oltava muistissaan taulukko, joka sisältää tiedon kaikkiin ko. ryhmään kuuluvien MAC-osoitteista. Käytännössä, jos kytkimeen ei ole liitettyä yhtään ko. ryhmän jäsentä, ei kytkimen tarvitse tallettaa kenenkään kyseisen VLAN ryhmään kuuluvien MAC-osoitteita. Tässä ratkaisussa kytkimet voivat joutua pitämään muistissaan varsin isoja taulukoita. Lisäksi taulukot on pidettävä ajantasalla ja tämä tietenkin lisää verkon kuormitusta. [2]

2.5.2 Explicit

Expliciittisessä tapauksessa jokaiseen pakettiin lisätään tagi, joka ilmaisee sen, mihin VLAN ryhmään käyttäjä kuuluu. Cisco ISL ja IEEE 802.1q VLAN määrittely käyttävät tätä tapaa. Koska tämä on määriteltä standardissa, on siitä tullut oletustapa kaikkiin VLAN:hin. [2]

Käytännössä menetelmä on varsin yksinkertainen. Paikallinen kytkin käyttää konfiguroitua tapaa (porttien, verkkokerroksen tai MAC-osoitteen perusteella ryhmitely) selvittääkseen mihin ryhmään tiedon lähettänyt käyttäjä kuuluu. Jos saman kytkimen alla on muita käyttäjiä, jotka kuuluvat samaan ryhmään, lähetetään paketti heille normaalisti. Jos/kun verkko koostuu useammasta kytkimestä, lisää paikallinen kytkin pakettiin tagin, joka ilmaisee VLAN-ryhmän johon lähettäjä on kuulunut ja lähettää paketin eteenpäin muille kytkimille. Kun muut kytkimet vastaanottavat paketin, ne lukevat tagista lähettäjän ryhmän ja lähettävät paketin kaikille samaan ryhmään kuuluville käyttäjille. [2][1]

Kytkimien välillä pakettia siirettäessä voidaan käyttää molempia tapoja. Jos käytetään MAC osoitteisiin perustuvaa ryhmittelyä on käytettävä tapa lähes aina implisiittinen. Muissa tapauksissa yleisempi tapa on explisiittinen. [2]

2.6 VLAN:n konfigurointi

VLAN:ien konfigurointia on mahdollista automatisoida. Automaation aste voi vaihdella manuaalisesta automaattiseen. Tähän vaikuttaa se millä tavalla VLAN on toteutettu. Esimerkiksi portteihin perustuvaa VLAN:a käytettäessä ei täysin automaattinen konfigurointi tule kysymykseen, kuten aikaisemminkin mainittiin. Lisäksi eri valmistajilla on erityyppisiä ratkaisuja tähän, joten valittu laitteistokin vaikuttaa konfiguroinnin toteuttamiseen.

2.6.1 Manuaalinen konfigurointi

Manuaalinen konfigurointi tarkoittaa sitä, ettei mitään ole automatisoitu. Verkon ylläpitäjät voivat hallita kaikkia tapahtuvia muutoksia ja joutuvat näin tekemäänkin. Menetelmän etuna on tietenkin se, että kaikkia muutoksia hallitaan ja verkon tila on aina tiedossa. [1] Käytännössä ratkaisu voi toimia pienissä verkoissa, joissa muutoksia tapahtuu vain harvoin. Kun verkossa on satoja koneita tai jos muutoksia tapahtuu usein, ei tämä enää ole kovinkaan käytännöllistä. Vaikkakin hallintatyökalujen kautta tapahtuva verkon konfigurointi saattaa olla yksinkertaisempaa verrattuna normaaliin ratkaisuun, on kuitenkin epäkäytännöllinen ratkaisu. Jotta verkon ylläpito on järkevää manuaalisesti, tarkoittaa se sitä, että verkon on oltava pieni. Siispä herääkin kysymys onko tälläisessä verkossa todella tarvetta VLAN kytkimille ja laitteille, vai voitaisiinko koko homma hoitaa yksinkertaisesti samalla tavalla kuin

se on hoidettu aikaisemminkin.

2.6.2 Puoliautomaattinen konfigurointi

Puoliautomaattinen konfigurointi tarkoittaa ratkaisuja, jossa automaation aste vaihtelee. Käytännössä tällä tarkoitetaan sitä, että joko verkon alkukonfigurointi on automaattinen, muutosten hallinta on automaattinen tai molemmat ovat automaattisia. Vaikka molemmat olisi hoidettu automaattisesti, eroaa ratkaisu täysin automaattisesta siinä, että ylläpidolla on kuitenkin aina mahdollista muuttaa konfigurointia manuaalisesti. [1]

2.6.3 Täysin automaattinen konfigurointi

Automaattisessa tavassa työasemat automaattisesti ja dynaamisesti liittyvät oikeaan ryhmään. Ryhmä määritellään sovelluksen, käyttäjätunnuksen tai ylläpitäjän määrittelemien sääntöjen mukaisesti.[1]

2.7 Kytkimien välinen kommunikointi

Kytkimien väliseen kommunikointiin on kehitetty kolme eri tapaa. Taulukkojen ylläpito signaalien välityksellä, tagien lisääminen kehyksiin ja TDM (Time-Division Multiplexing). [1]

2.7.1 Taulukkojen ylläpito signaleilla

Kun verkkoon kytketään uusi laite ensimmäistä kertaa ja se lähettää tietoa broadcastina kytkin selvittää laitteen MAC osoitteen tai portin johon se on liitetty. Tätä tietoa verrataan kytkimen muistiin tallennettuihin tietoihin, jonka jälkeen tieto lähetetään muille verkon kytkimille. Jos VLAN ryhmään kuuluva kone vaihdetaan kuulumaan toiseen ryhmään, päivitetään tiedot manuaalisesti ylläpitäjän työkaluilla. Kun verkko laajenee ja kytkinten määrä kasvaa, kasvaa myös lähetettävien ja muistissa pidettävien tietojen määrä huomattavasti. [1]

2.7.2 Kehysten merkitseminen

Jos käytetään kehyksien merkitsemistä, jokaiseen MAC-kerroksen kehykseen joka välitetään kytkimien kautta merkitään mihin VLAN ryhmään ne kuuluvat. Tämä lisää tietenkin overheadia verkkoliikenteeseen. Mutta toisaalta kytkinten välisen kommunikoinnin määrä ja muistissa pidettävien

taulukoiden koko pienenee. [1]

2.7.3 TDM

TDM (Time-Division Multiplexing) on kolmas tapa toteuttaa tämä. Tätä on käytetty vähiten kaikista näistä kolmesta. Periaate on sama kytkinten välisessä komminuikoinnissa kuin WAN ympäristössä tukemaan erityyppistä verkkoliikennettä. Tässä jokaiselle VLAN ryhmälle varataan oma kanava. Tämä vähentää verkkoliikenteen overheadia, mutta tuhlaa kaistaleveyttä. Jokaiselle kanavalle on varattu vuoronperään tietyn aikayksikön mittainen aika, jolloin tietoa siirretään. Toinen kanava ei kuitenkaan voi käyttää toiselle kanavalle tarkoitettua aikaa, vaikka kyseinen kanava ei siirtäisikään tietoa. [1]

2.7.4 VLAN ja ATM (LANE)

VLAN:t oli alunperin tarkoitettu vain LAN kytkimille, mutta käyttöalue on ulotettu myös ympäristöihin, jossa on ATM verkkoja ja ATM:n suoraan liitettyjä laitteita. Tämä osa-alue on niin laaja ja liittyy suurimmalta osin ATM tekniikkaan, joten tätä ei tulla käymään tässä seminaari esityksessä kovinkaan tarkasti läpi. [1]

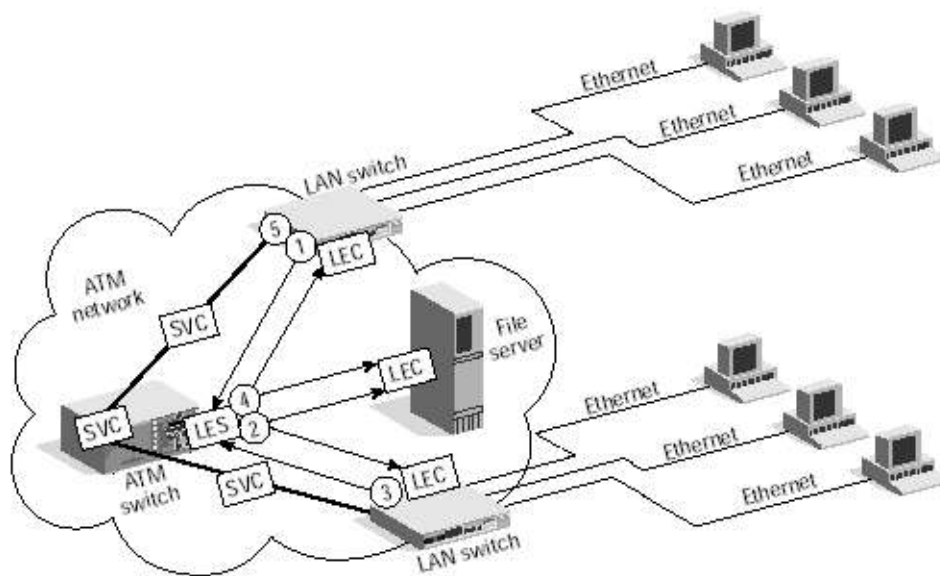
Tapaus jossa yhtään laitetta ei ole suoraan kytketty ATM-verkkoon, vaan ainoastaan reitittimiä on kytketty ATM:llä toisiinsa, on varsin yksinkertainen. Tällaisessa tapauksessa voidaan käyttää ATM permanent virtula circuit (PVC) piiriä. Tämä luo loogisen linkin, jonka kautta kaikki VLAN liikenne voi kulkea kytkimeltä toiselle. VLAN on täysin läpinäkyvä ATM kytkimille, eli ne toisin sanoen vain välittävät paketit toiselle välittämättä niiden sisällöstä. [1]

Käytännössä organisaatiot, jotka käyttävät ATM-tekniikkaa, kytkevät useinmiten myös palvelimia ja muita laitteita suoraan ATM:n. Tämä tekee tilanteesta huomattavasti monimutkaisemman. Verkossa pitää silloin toimia sekä yhteydettömät LAN protokollat, että yhteyspohjainen ATM. Järjestelmä on toteutettu siten, että ATM kantaa vastuun koko hommasta. Se emuloi broadcast LAN:n ominaisuudet (LAN Emulation (LANE)), ja tarjoaa osoitteiden muunnoksen MAC-osoitteesta ATM-osoitteeksi. LANE standardi määriteltiin 1995 ATM forumin toimesta. LANE:ssa on määritelty LAN Emulation server (LES), joka hoitaa osoitteiden konvertoinnin MAC-osoitteesta ATM-osoitteeksi. Tieto

lähetetään LAN Emulation clienteleille (LEC), jotka koostuvat siis kytkimistä ja ATM-verkkokorteista. Kuvassa 5 on esitetty LANE:n toimintaa. [1]

1. LAN kytkin vastaanottaa paketin ethernetiin kytketyltä työasemalta, jonka pitäis päätyä toiselle ethernetiin kytketylle työasemalle ATM verkon toisella puolella. LEC (LAN kytkin) lähettää LES:lle pyynnön konvertoida MAC osoite ATM osoitteeksi. LES on tässä esimerkissä sisään rakennettuna ATM kytkimessä.
2. LES lähettää multicast viestin kaikille muille LEC:ille, jotka ovat samassa verkossa.
3. Ainoastaan LEC jolla on kohteen (MAC) osoite muistissaan vastaa LES:lle.
4. LES broadcastaa tämän vastauksen kaikille LEC:ille.
5. Kohdan yksi kytkin tunnistaa tämän vastauksen ja saa vastaanottajan ATM osoitteen, jonka jälkeen se avaa kytketyn virtuaalisen piirin (switched virtual circuit (SVC)) ja siirtää paketit kohteeseen.

Tässä tapauksessa LAN kytkin näkee ATM:n ainoastaan yhtenä porttinaan ja kaikki ATM:n kytketyt laitteet olisivat jäsenenä tietyssä VLAN:ssa. [1]



Kuva 5. ATM ja VLAN. [1]

2.8 Standardit

VLAN:a varten on esitetty useampia standardeja, joiden tarkoituksena on ollut pääasiassa ollut päästä

eroon ongelmista, jotka aiheutuvat siitä, kun eri valmistajat tekivät omia toistensa kanssa yhteensopimattomia ratkaisuja.

2.8.1 IEEE 802.10

Vuonna 1995 Cisco ehdotti IEEE 802.10 standardia, joka alunperin oli suunniteltu mahdollistamaan LAN:ssa turvallinen yhteys. Ciscon ajatuksena oli, että 802.10 standardin headeria käytettäisiin uudestaan turvallisuus tiedon tallentamisen sijaan kehysten merkitsemiseen. Periaatteessa tämä olisi mahdollista, mutta käytännössä suurin osa valmistajista ja IEEE:n jäsenistä vastusti yhden standardin käyttöä useampaan tarkoitukseen. [1]

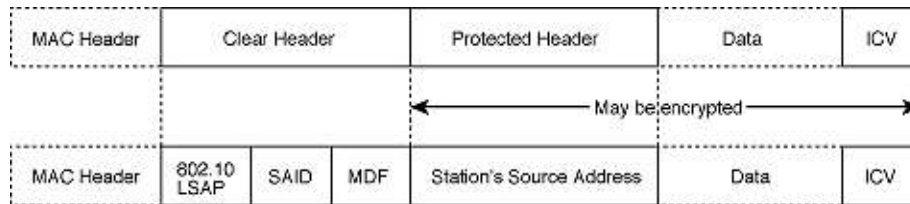
Ciscon ratkaisussa siis olisi hyödynnetty LAN/MAN Security (SILS) standardia, joka oli vahvistettu 1992. Standardin aluperäinen tarkoitus oli mahdollistaa autentikointi ja kryptaus, jossa siis voitiin varmistaa siirretyn datan luotettavuus ja muuttumattomuus siirrettäessä se verkon läpi. [5]

802.10 standardissa määriteltiin Protocol Data Unit (PDU), joka tunnettiin Security Data Exchange (SDE) PDU:na. Tämä on siis MAC kerroksen kehys, jossa 802.10 otsikko kenttä lisätään MAC headerin, ja kehyksen datan väliin. Kehys sisälsi kaksi headeria, sisemmän ja ulomman kuvassa 6 (sisempi=Protected Header ja ulompi (Clear header). [5]

Clear Header sisältää Security Association Identifierin (SAID). Tarvittaessa myös MDF (Management-Defined Field (MDF) on käytettävissä, joka voi sisältää tietoa helpottamaan PDU:n käsittelyä. Protocol Header sisältää saman MAC osoitteen kuin MAC header, jotta osoitteen validointi on mahdollista. Näin voidaan tunnistaa lähettäjä. Integrity Check Value (ICV) varmistaa, ettei kukaan pääse muuttamaan dataa. [5]

Jos IEEE 802.10 protokollaa käytettäisiin Ciscon esittämällä tavalla VLAN:ssa, on VLAN ID eli tieto siitä mihin VLAN ryhmään lähettäjä kuuluu, tärkein osa header tietoja. Tämän ID:n perusteella tieto voidaan välittää kaikille ko. ryhmään kuuluville. Jos muut laitteet saavat paketin, jonka ID ei täsmää yhdenkään ko. kytkimeen kytkettyyn laitteen VLAN ID:hen, ne eivät välitä sitä millekään. Vastaavasti

jos laite löytyy, palautetaan ko. kehys alkuperäiseen muotoonsa ja lähetetään niille vastaanottajille, jotka kuuluvat samaan ryhmään. Koska paketit olisivat olleet normaaleja MAC kehyksiä, olisivat ne menneet läpi myös vanhemmista laitteista, jotka eivät tue VLAN:ja. [5] Menetelmää on käytetty ilmeisesti ainakin vanhemmissa Ciscon laitteissa, mutta oikeaa standardia siitä ei tullut.



Kuva 6. Ciscon ehdotus VPN pakettien tag-merkinnöistä. [5]

2.8.2 IEEE 802.1Q

Vuonna 1998 saatiin valmiiksi ehdotus VLAN standardista IEEE 802.1Q [10]. Siinä oli määritelty erityyppisiä VLAN ratkaisuja. Lisäksi tämän avulla pyrittiin pääsemään eroon ongelmista, joka pakotti käyttämään yhteensopivuus syistä vain yhden valmistajan kytkimiä. Ongelmahan aiheutui siitä, että eri tyyppisiä menetelmiä käytettiin eri valmistajien laitteissa. [3]

Tässä standardissa määriteltiin portteihin, MAC osoitteisiin ja protokoliin perustuva VLAN. Lisäksi standardissa on määritelty aiemmin läpikäyty ATM VLAN. [6]

Standardin mukaisesti, ylläpitäjä voi konfiguroida jokaisen portin kuulumaan haluttuun VLAN ryhmään. Kytkinten välinen liikenne hoidetaan lisäämällä VID tagi kaikkiin kehyksiin. Sen arvo voi olla mikä tahansa 1 ja 4094 välillä. Jokaisella VLAN ryhmällä täytyy olla oma VID tunnus. [3]

Käytännössä kytkin joka on VLAN standardin 802.1Q kanssa yhteensopiva, tarkistaa onko linjan toisessa päässä joku yhteensopiva laite, esimerkiksi toinen kytkin. Jos laite on vanhemman mallinen kytkin, paketti lähetetään sille ilman tagia, jos se taas on yhteensopiva, saa se paketin tagin kanssa. Näin ratkaistaan ongelma, joka aiheutuu tilanteesta, jossa esimerkiksi vanhempien tulostimien tai PC:den verkkokortit eivät ole 802.1Q yhteensopivia. Tällainen laite hylkäisi paketin, koska ei ymmärrä mukana tulevaa tagia. Myös Ethernet kehyksen koko kasvatettiin 802.1Q:ssa 1518 tavusta 1522 tavuun.

Tämä voi aiheuttaa sen, että vanhemmat verkkokortit tai kytkimet eivät välitä kehystä eteenpäin, koska se on vanhempaa standardia suurempi. [3]

Taulukossa 1 ja 2 on kuvattu IEEE standardin 802.1P mukainen kehys. 802.1Q:n kehys on lähes vastaava, mutta siinä ei kehyksen prioriteetin määritteleviä bittejä oltu vielä määritelty.

7	1	6	6	2	2	2	42-1496	4
Preamble	SFD	DA	SA	TPID	TCI	Type length	DATA	CRC

Taulukko 1. Normaali kehys. [6]

- Preamble. Kertoo vastaanottajalle, että kehys on tulossa. Synkronisoi vastaanoton.
- SFD. (Start-of-frame-delimiter)
- DA. (Destination address) Kertoo, kenen pitäisi vastaanottaa kehys.
- SA. (Source address) Kertoo, kuka oli lähettäjä.
- TPID. Arvo 8100 hexoina. Jos tämä arvo on 8100, merkitsee se sitä, että se on IEEE 802.1Q tai IEEE 802.1P:n mukainen.
- TCI kentässä on seuraavaa dataa:

3 bits	1 bit	12 bits
User Priority	CFI	Bits of VLAN ID to identify possible VLANs.

Taulukko 2. TCI kentän data. [6]

- User Priority: Määrittelee paketin prioriteetin.
- CFI. (Canonical Format Indicator). On aina nolla ethernet kytkimille. Tätä käytetään yhtensopivuus syistä ethernet ja Token Ring verkkojen kanssa.
- VID: VLAN ID on standardin 802.1Q mukainen verkkotunnus. Arvoa 0 on käytetty tunnistamaan prioriteetti kehykset. Myös arvo 4096 on varattu muuhun käyttöön. Mahdollisia VLAN ryhmiä voi siis olla maksimissaan 4094 kappaletta.

- Legth/type. Kertoo joko MAC-numeron tavujen määrän, joka on tallennettu data kehykseen tai kehyksen tyyppiin.
- Data.
- FCS (Frame check sequence). Sisältää CRC arvon. Varmistaa kehysten eheyden.

2.8.3 802.1P

IEEE 802.1P standardissa määritellään signalointitekniikka verkkoliikenteen priorisointia varten linkki/MAC kerroksessa. Standardi on muunnos 802.1Q:sta, ja ne toimivat rinnakain. Tämän standardin mukaan VLAN tagi on jaettu kahteen osaan 12-bitin VLAN ID:hen ja 3 bitin priorisointi osaan. Priorisointi kenttää ei ole määritelty 802.1Q standardissa. [4]

802.1P:tä tukevat suurin osa valmistajista, käytännössä valmistajat voivat päättää, kuinka priorisointi käytännössä toteutetaan. Vaikka prioriteetti tasoja on määritelty 8, tukevat monet valmistajat vain muutamia näistä. Arvo 0 tarkoittaa pienintä prioriteettia ja 7 suurinta. Käytännös kuitenkin tason 7 paketin prioroiteetti on usein sama kuin tason 4 prioriteetti. [4]

3.0 VLAN:n edut ja haitat

VLAN:n avulla verkko segmenttien koko voidaan määritellä koostumaan pelkästään yhdestä käyttäjästä. Mikä siis vastaisi tilannetta, jossa jokainen käyttäjä olisi riittänyt koneensa suoraan kytkimeen keskittimen sijaan. Tämä ei kuitenkaan välttämättä ole kovin käytännöllinen vaihtoehto. Käyttäjien määrän/VLAN ryhmän koon, joka vastaaanottaa saman broadcast liikennettä sanotaan VLAN ratkaisuihin voivan olla jopa yli 1000 käyttäjää. Käytännössä suorituskyky kuitenkin varmasti kärsii jo tällaisissa määrissä. Tosin verkon suorituskyky on huomattavasti parempi, kuin ilman VLAN:a, koska normaalisti kaikki kytkimiin tuleva broadcast liikenne leviää kaikille, mutta VLAN:n avulla se voidaan rajata vain oikeisiin paikkoihin. [1]

VLAN:n helpottaa verkon ylläpitoa. Se voi automaattisesti seurata työasemien liikkeitä. Ennen jos joku on siirtänyt koneensa uuteen paikkaan ja kytkisi sen eri keskittimeen tai kytkimeen tms. on IP osoite täytynyt konfiguroida manuaalisesti oikeaksi. VLAN:ssa käyttäjä sen sijaan saa pitää oman IP osoitteensa automaattisesti, olettaen että VLAN on näin konfiguroitu toimimaan. [1]

Verkkojen segmentointi on mahdollista toteuttaa joustavasti, eikä se ole riippuvainen verkon fyysisestä rakenteesta. Samoja resursseja tarvitsevat laitteet voidaan ryhmitellä omiin verkkosegmentteihinsä sijainnista riippumatta. Lisäksi hallinta on helpompaa, koska kaikki muutokset ja siirrot voidaan lähestulkoon aina hoitaa hallinta ohjelmilla, sen sijaan että muutokset tehtäisiin kytkinkaapeissa tai kaapeleita vetämällä. [2]

Suorituskyvyn paranemisen lisäksi VLAN lisää myös turvallisuutta, koska se voi luoda virtuaalisia rajoja ja toimia ikään kuin eräänlaisena palomuurina. [2]

Suurimpina ongelmina on ilmeisesti edelleenkin pienet epäyhteensopivuudet eri laitevalmistajien tuotteiden välillä. Lisäksi kustannukset ovat jonkin verran korkeammat normaaliin LAN:n verrattuna. Tosin nykypäivänä ero ei ole enää kovinkaan merkittävä. Valmistajasta riippuen hinnat näyttivät

vaihtelevan hiukan kalliimmista jopa kaksinkertaisiin verrattaessa VLAN tuotteita verrattaessa lähes vastaaviin LAN tuotteisiin. Hintojen vertailu oli kuitenkin vaikeaa, koska juuri vastaavilla ominaisuuksilla varustettua kytkintä ilman VLAN tukea oli mahdotonta löytää. Yllättävän monissa kytkimissä näytti olevan ainakin jonkinlainen VLAN tuki. VLAN tukevien verkkokorttien hinnat näyttivät lähtevän 40 eurosta ylöspäin. Tosin nämä eivät ole välttämättömiä, sillä VLAN:ia tukemattomia laitteita varten kytkin poistaa ylimääräisen tiedon, ja näin pakettien pitäis kulkea perille ilman suurempia ongelmia. [7][8][9]

Lyhyen vertailun perusteella kytkimien hinta muodostuu lähinnä muista kuin VLAN:n liittyvistä ominaisuuksista. Käytännössä kaikissa VLAN:a tukevissa palvelimissa oli lähes samnkaltaiset ylläpitomahdollisuudet. Suurin osa tuki ylläpitoa SNMP:tä, www:n, telnet:n yms. protokollien kautta. Kaikki valmistajat tukivat IEEE standardin 802.1Q (ja useimmat myös 802.1P) mukaisia VLAN:ja. Lisäksi Ciscolla ja muutamalla muulla valmistajalla oli tuettuna myös jotain omia standardoimittomia menetelmiä ainakin joissain reitittimissä. Lisäksi tietyt valmistajat tarjosivat mukaan omia verkon hallinta työkalujaan, osalla ne sisältyivät jo hintaan, mutta joillakin ne täytyi hankkia erikseen. Näissäkin kytkimissä täytynee kuitenkin olla perus työkalut ylläpitoa ajatellen, mutta ilmeisesti valmistajan ohjelmisto tarjoaisi jotain lisäominaisuuksia, joita ei perus työkaluissa ole mukana. [7][8][9]

4.0 VLAN:n käytännössä

VLAN:ja mainostetaan sillä, että ne säästävät ylläpito kuluja ja muita ns. näkymättömiä kuluja, jotka eivät liity itse laitteistohankintoihin. Asia ei ole läheskään näin selkeä. Käytännössä ylläpitäjien aika kuluu osittain ainoastaan eri asioihin kuin aikaisemmin.

VLAN tuo vapautta verkon suunnitteluun. Käytännössä kaikki on edelleen suunniteltava huolella, jos VLAN:n suomista eduista halutaan ottaa kaikki irti. Esimerkkinä voidaan mainita tilanteet, jossa yhden 24 porttiseen kytkimeen on kytkeytynyt 24 käyttäjää, josta jokainen kuuluu eri VLAN-ryhmään. Tässä tilanteessa kytkimen on siis käsiteltävä kaikki paketit ja välitettävä ne oikealla käyttäjälle. Tilanne ei tällaisessa tapauksessa ole verkon kapasiteetin osalta paljontaan parempi kuin normaalissa LAN:ssa, päin vastoin. Tilanne on huomattavasti parempi ja verkkokapasiteettia säästyy huomattavasti, jos kytkimeen kytkeytyneet käyttäjät kuuluvat esimerkiksi vain 2 eri VLAN-ryhmään. Näin kytkimelle muualta tuleva liikenne ja itse kytkimen kuormitus pienenee huomattavasti.

Tilanne jossa käyttäjiä on esimerkiksi kahden eri kytkimen takana, ja kolmannen takana on käyttäjien tarvitsema palvelin, mutta ei yhtään palvelimen käyttäjää. On varsin epäkäytännöllistä, että broadcast pyynnöt menevät kolmeen paikkaan kahden paikan sijasta, mikä siis myöskin lisää verkon kuormitusta. Palvelimet kannattaisi siis kytkeä samaan kytkimeen, missä sitä eniten tarvitsevat käyttäjät ovat.

VLAN ryhmien koon on oltava järkevä. Jos kaikki tai huomattava osa käyttäjistä kuuluu samaan VLAN ryhmään on siitä saatava hyöty merkityksetön. Myös liian pienet ryhmät kuormittavat verkkoa turhaan. Pienissä yrityksissä VLAN on todennäköisesti täysin tarpeeton. Nykyisten lähiverkkojen kapasiteetti todennäköisesti riittää hyvin käyttäjien määrän ollessa muutamia kymmeniä. Tällaisessa tapauksessa VLAN:sta on todennäköisesti vain enemmän vaivaa ja kustannuksia kuin todellista hyötyä.

VLAN:n hankkimista harkitsevassa organisaatiossa on tarkasti mietittävä ja laskettava tarjoaako VLAN riittävästi vastinetta rahoilleen. Pienille yrityksille VLAN tuskin on järkevä vaihtoehto. Tämä kuitenkin vaihtelee tapauskohtaisesti. Mitään yleispätevää ohjetta ei tähän ole.

5.0 Yhteenveto

VLAN on melko uusi tekniikka. Käytännössä sille on tarvetta ainakin suurten yrityksen verkkoissa. Hinnaltaan tekniikka ei enää nykypäivänä ole kovinkaan kallista, verrattuna muihin normaaleihin ethernet verkkotekniikoihin. VLAN tarjoaa helpotusta suuren verkon ylläpitoon, koska muutokset voidaan pääasiassa hoitaa ohjelmallisesti. Ylläpidon työtä se ei välttämättä vähennä, vaikka sen avulla tekniikkaa mainostetaankin. Nopeuksien paranemisen lisäksi VLAN parantaa yrityksen tietoturvaa. Sen avulla voidaan rajoittaa tarpeettomien työntekijöiden pääsyä palvelimille ja resursseihin, joita heidän ei ole tarvetta käyttää tai joihin heidän ei haluta pääsevän käsiksi. Itse VLAN tekniikoita on paljon. Tiettyjen laitevalmistajien laitteiden välillä on ennen ollut yhteensopivuus ongelmia ja joidenkin laitteiden välillä ilmeisesti vieläkin. Tekniikka on tosin nykyään standardoitu, joten yhteensopivuus ongelmien pitäisi pääosin olla historiaa. Tämä on myös laskenut itse tekniikan hintaa, koska enää ei ole niin suurta tarvetta ostaa kaikkia tuotteita samalta valmistajalta.

Vaikein vaihe tässäkin tekniikassa on edelleen sen käyttöönotto. Käyttöön oton jälkeen osa verkon ylläpidosta on mahdollista automatisoida, mikä varmasti osittain vähentää ylläpidon työtä.

Tällä tekniikalle löytyy varmasti käyttäjiä. Pääasiassa se on tarkoitettu ratkaisemaan isompien yritysten LAN:n kapasiteetti ja tietoturva ongelmia. Pienempien yritysten tai yhteisöjen verkossa tällä tekniikalle tuskin on tarvetta. Todennäköisesti se vain monimutkaistaisi entisestään pienen yrityksen verkon ylläpitoa. Tekniikan hankkimista harkitsevan on tarkasti mietittävä, onko heillä todellisuudessa tarvetta tälle tekniikalle. Ja jos päätetään siirtyä osittain tai kokonaan VLAN laitteisiin, on verkon arkkitehtuuri silti suunniteltava huolella, jotta tekniikasta saadaan kaikki potentiaali irti.

6.0 Tenttikysymykset

1. Millä eri tavoilla VLAN kytkimet kommunikoivat keskenään?
2. Miten VLAN käyttäjät voidaan ryhmitellä?
3. VLAN:n edut ja haitat?

Lähteet

- [1] Decisys, 5.1996, The Virtual LAN Technology Report [verkkodokumentti], 3Com, Saatavissa: http://www.3com.com/other/pdfs/solutions/en_US/20037401.pdf [viitattu 12.2.2004]

- [2] Intel, 1997, Virtual LANs, [verkkodokumentti], Intel, Saatavissa: http://www.intel.com/network/connectivity/resources/doc_library/tech_brief/virtual_lans.htm [viitattu 12.2.2004]

- [3] Xilinx, IEEE 802.1Q, [verkkodokumentti], Xilinx, Saatavissa: http://www.xilinx.com/esp/networks_telecom/optical/net_tech/ieee8021q.htm [viitattu 13.2.2004]

- [4] Xilinx, IEEE 802.1P, [verkkodokumentti], Xilinx, Saatavissa: http://www.xilinx.com/esp/networks_telecom/optical/net_tech/ieee8021p.htm [viitattu 13.2.2004]

- [5] Cisco, 15.7.1995, VLAN Interoperability, [verkkodokumentti], Cisco, Saatavissa: <http://www.cisco.com/warp/public/537/6.html> [viitattu 14.2.2004]

- [6] Javvin, VLAN: Virtual Local Area Network and IEEE 802.1Q, [verkkodokumentti], Javvin, Saatavissa: <http://www.javvin.com/protocolVLAN.html> [viitattu 14.2.2004]

- [7] D-Link Systems, Inc. Product Categories, [verkkodokumentti], Saatavissa: <http://www.d-link.com/products/category.asp?cid=5> [viitattu 22.2.2004]

- [8] 3Com Product, Offering, [verkkodokumentti], Saatavissa: http://www.3com.com/prod/fi_FI_EMEA/prodlist.jsp?tab=cat&cat=4 [viitattu 22.2.2004]

- [9] Products, Cisco Systems, [verkkodokumentti]. Saatavissa:
<http://www.cisco.com/en/US/products/index.html> [viitattu 22.2.2004]
- [10] IEEE, 7.5.2003, IEEE Standards for local and Metropolitan area network. Virtual bridged local area networks, IEEE, [verkkojulkaisu]. Saatavissa:
<http://ieeexplore.ieee.org/iel5/8557/27089/01203093.pdf?isNumber=27089&prod=STD&arnumber=1203093&arSt=&ared=&arAuthor=> [viitattu: 14.2.2004]. ISBN 0-7381-3663-8.