Tutkimusraportti
BVAL73-011120

Tilaaja: TEKES, teollisuus

TIETOVERKKOJEN JA TIEDONSIIRRON DIAGNOSTIIKKA

Jussi Lehtonen, Jyrki Tervo, Jari Halme

Espoo 21.8.2001

A Työraportti	
B Julkinen tutkimusraportti	X
Tutkimusraportti luottamuksellinen saakka	

Raportin nimi

Tietoverkkojen ja tiedonsiirron diagnostiikka

Toimeksiantaja/rahoittaja ja tilaus pvm/nro **TEKES, teollisuus**	Raportin numero **BVAL73-011120**
Projektin nimi Koneiden ja laitteiden kunnon ja käyttöolosuhteiden monitorointi ja diagnostiikka	Suoritteen numero V9SU00893
Laatija(t) Jussi Lehtonen, Jyrki Tervo, Jari Halme	Sivujen/ liitesivujen lukumäärä 33/ -

Avainsanat

Tietoverkot, tiedonsiirto, diagnostiikka, langaton tiedonsiirto

Tiivistelmä

Raportissa luodaan katsaus joihinkin nykyisiin tietoverkkoratkaisuihin ja tiedonsiirtotekniikoihin sekä tarkastellaan tiedonsiirron kunnonvalvontaa ja diagnostisointia. Perinteiset lähiverkot (LAN, Local Area Network) ovat tietokoneita ja oheislaitteita yhdistäviä tiedonsiirtoverkkoja, joissa siirretään binääristä dataa tietokoneiden välillä. Verkon ylläpidossa käytetään laitehallinnan työkaluja, joiden avulla ylläpitäjä voi seurata verkkoon kytkettyjen laitteiden tilaa ja toimintaa, jolloin verkkovikojen haitat pienenevät vianhaun nopeutuessa. Vika on epänormaali tila, joka vaatii ylläpidon huomiota tai toimintaa, jotta se saadaan korjattua. Vika havaitaan useimmiten vääränä verkon toimintana tai suurena määränä virheilmoituksia. Vianhallinnan tehtävänä on mahdollisimman nopeasti määritellä vian paikka, eristettävä vika paikantamalla ja tunnistamalla se, määriteltävä verkon asetukset uudelleen, korjattava tai vaihdettava vialliset komponentit tai korjattava virheet. Protokolla on kuvaus tavasta, jolla tietoliikenteen eri osapuolet kommunikoivat toistensa kanssa. Käytetyin protokollapino on TCP/IP, jota käytetään myös internetissä. Tietoliikenteen virheiden korjausmenetelminä käytetään lähinnä kahta tapaa: ARQ (Automatic Repeat ReQuest) ja FEC (Forward Error Correction). SNMP kehitettiin TCP/IP-protokollaa käyttävien verkkojen verkonhallintajärjestelmäksi. Tietoverkkojen ongelmien ratkaisuun on saatavilla monipuolisia vianetsintätyökaluja, mm. Protokolla-analysaattori. Internet on maailmanlaajuinen verkkojen verkosto. Internet yhdistää TCP/IP-koneet ja -lähiverkot IP-reitityksellä. Intranet-verkot ovat sisäisiä verkkoja, joissa käytetään julkisen internetin protokollia ja ratkaisuja tietojärjestelmien toteutukseen. Verkon dynamiikka (ohimenevät ruuhkat, reitin vaihdokset) vaikuttaa merkittävästi internetin suorituskykyyn. Verkon dynamiikka ilmenee kadonneina tai viivästyneinä lähetyksinä. Viat johtuvat usein reitittimen toiminnasta. Langattomassa lähiverkossa (WLAN, Wireless Local Area Network) tiedonsiirto tapahtuu pääasiassa vapailla, viranomaisluvista riippumattomilla radiotaajuuksilla. Langattoman verkon vikatilanne voi johtua yhden tai useamman verkon komponentin pettämisestä. Kriittisiä komponentteja ovat mm. kytkimet, tukiasemat, tietokannat, päätelaitteet ja langattomat linkit.

Allekirjoitukset, Espoo 21.8.2001

Kenneth Holmberg	Jussi Lehtonen	
Tutkimuspäällikkö	Tutkija	Tarkastanut

Jakelu (asiakkaat ja VTT):

Alkusanat

Tämä raportti liittyy osaltaan KÄKI-teknologiaohjelman menetelmäprojektiin M9 – Koneiden ja laitteiden kunnon ja käyttöolosuhteiden monitorointi ja diagnostiikka. Projektin ovat rahoittaneet TEKES, Metso Paper, Rautaruukki Raahe Steel, Lillbacka, Metso Minerals, Outokumpu PoriCopper, sekä VTT. Raportissa on luotu yleiskatsaus tietoverkkoihin ja tiedonsiirtoon sekä niiden diagnostiikkaan. Kiitämme hankkeeseen osallistuneita yrityksiä ja projektin rahoittajia työtä kohtaan osoitetusta mielenkiinnosta, asiantuntevista kommenteista ja taloudellisesta tuesta.

Espoo, Elokuussa 2001

Tekijät

Sisällysluettelo

1 Johdanto

Tietoverkkojen koko ja monimutkaisuus ovat kasvaneet valtavasti viimeisten vuosien aikana. Tyypillinen verkko voi koostua sadoista tai tuhansista solmupisteistä, joiden liikenne ja kaistanleveys vaihtelevat huomattavasti. Tosiaikaiset sovellukset vaativat entistä parempaa luotettavuutta ja suurempaa tiedonsiirtokapasiteettia. Näiden muutosten myötä myös verkon hallinta ja kunnonvalvonta on muuttunut aikaisempaa hankalammaksi ja monimuotoisemmaksi. Koska vikatilanteilta ei yleensä pystytä välttymään, on vikojen nopea havainnointi ja tunnistus sekä nopea vikatilanteista toipuminen ratkaisevaa tietoverkon toiminnan luotettavuuden kannalta.

Tietoverkkojen hallinta ja kunnonvalvonta on nopeasti kehittyvä tietotekniikan osa-alue. Verkon hallinnan ongelmiin on esitetty ja esitetään jatkuvasti erilaisia periaateratkaisuja sekä sovellusohjelmia, joten sovellusratkaisut ja arkkitehtuurit ovat lakkaamattomassa muutostilassa. Tässä raportissa luodaan katsaus joihinkin nykyisiin tietoverkkoratkaisuihin ja tiedonsiirtotekniikoihin sekä tarkastellaan tiedonsiirron kunnonvalvontaa ja diagnostisointia. Lisäksi arvioidaan alan kehitysnäkymiä yleisellä tasolla.

2 Signaalit

Onnistuneen tiedonsiirron edellytyksenä on hyvä signaalin laatu. Signaalilla tarkoitetaan tässä yhteydessä sähköpulssia tai sähkömagneettista säteilyä, jolla tietoa kuljetetaan kahden pisteen välillä. Signaalin laadun kehittyminen on mahdollistanut nykyiset suuret siirtonopeudet. Signaalinkäsittely on parantunut nopeiden signaaliprosessorien ansiosta, joiden avulla signaali voidaan tulkita oikein vaikeissakin olosuhteissa.

Signaaleihin sisältyy yleensä useita eri taajuuksia. Yleisesti pätee, että kaikki signaalit muodostuvat erilaisten taajuuksien siniaaltokomponenteista. Signaalin spektri koostuu kaikista sen sisältämistä taajuuksista. Koko spektrin laajuutta kutsutaan absoluuttiseksi kaistanleveydeksi. Aluetta, jolla pääosa signaalista sijaitsee kutsutaan efektiiviseksi kaistanleveydeksi. Kaistanleveydet vaihtelevat siirtotiestä riippuen sadoista Hz:stä GHz-alueelle. Siirtotien kapasiteetti ilmoitetaan bitteinä sekunnissa (bps).

Signaaleihin liittyy monia niiden laatua heikentäviä fysikaalisia ilmiöitä, jotka on otettava huomioon tiedonsiirrossa. Näitä ovat mm.:

- signaalin vaimeneminen eli amplitudin pieneneminen pitkällä matkalla
- kohina, joka johtuu mm. atomien lämpöliikkeistä
- kulkuaikavääristymä eli eri taajuuksien kulkeminen johtimissa eri nopeuksilla
- huojunta eli lähetettävän signaalin venyminen ja kutistuminen
- dispersio eli pulssin leviäminen valokuituyhteyksissä heijastuskulmien vaihtelujen vuoksi
- ylikuuluminen eli sähkömagneettisen induktion aiheuttama signaalin kopioituminen

- heijastuminen eli liitoskohdasta tai päättämättömästä johtimesta heijastuvan pulssin aiheuttama vääristymä lähetettyyn signaaliin

Siirtotien ja vallitsevien olosuhteiden hallinnalla on mahdollista arvioida ympäristön vaikutukset vastaanotettuun tietoon ja siten poistaa signaaliin kohdistuneet häiriötekijät [1].

3 Lähiverkot (LAN, Local Area Network)

Perinteiset lähiverkot (LAN, Local Area Network) ovat tietokoneita ja oheislaitteita yhdistäviä tiedonsiirtoverkkoja, jossa siirretään binääristä dataa tietokoneiden välillä. Tästä johtuen liikennöinnin yksityiskohdat on määriteltävä tarkasti. Lähiverkon tiedonsiirtonopeus vaihtelee yleensä 10 – 1000 Mbps:n välillä verkkoratkaisusta riippuen. Yleisimmät lähiverkkototeutukset rajoittavat verkon ääripisteiden välisen etäisyyden muutamaan kilometriin. Lähiverkkoon voidaan liittää myös IP-puhelimia ja videoneuvottelulaitteita, reaaliaikaista liikennettä voidaan kuljettaa lähiverkossa muun datan joukossa ja samoja yhteyksiä voidaan soveltaa myös puhelinliikenteeseen

Monet nykyiset lähiverkkotekniikat ovat kytkentäisiä, jolloin jokaisella päätelaitteella on oma yhteys kytkimeen. Kytkin välittää datan vain vastaanottajalle sanomaan sisältyvän osoitteen perusteella. Kytkentäisissä verkoissa voidaan luoda virtuaaliverkkoja ja estää saman fyysisen verkon eri osien välinen liikenne määrittelemällä päätteet eri virtuaaliverkkoihin. Näin samaa lähiverkkoa voivat käyttää esimerkiksi eri organisaatiot tietoturvaa vaarantamatta [2].

3.1 Ethernet

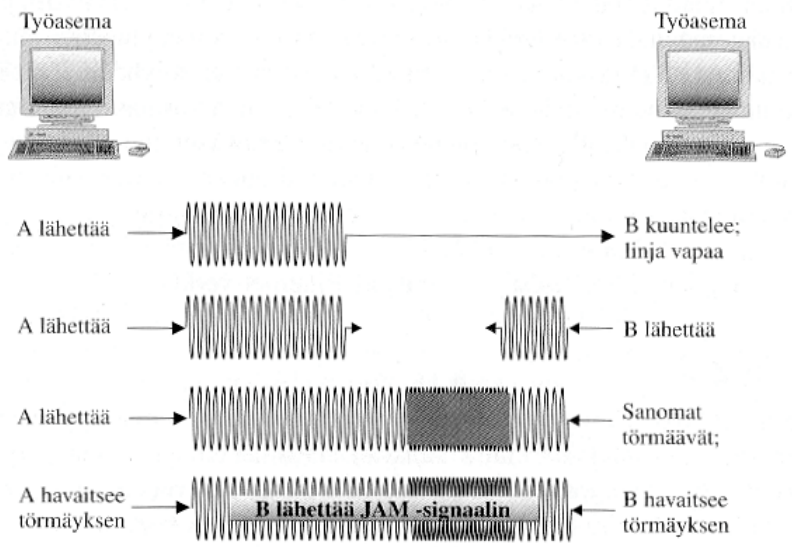
Ethernet oli ensimmäinen IEEE 802.3- standardin mukainen lähiverkko. Ethernet on edelleen yleisin käytössä oleva lähiverkko johtuen siinä käytettyjen ratkaisujen ja tekniikoiden yksinkertaisuudesta. Vasta viime vuosikymmenellä on Ethernetille kehitetty kilpailevia ratkaisuja, jotka nekin perustuvat pääosin Ethernet-tekniikkaan.

Ethernet-verkon yleisin siirtonopeus on 10 Mbit/s. Verkon topologia, eli tapa jolla verkon laitteet kytketään toisiinsa, on yleensä tähtimäinen tai väylä. Tähtikytkennässä jokaisella verkkoon kytketyllä laitteella on yhteys keskittimeen (hub), joka välittää sanomia verkon osapuolten välillä. Keskitin on edelleenkin useimmiten toistin (repeater), jolloin verkon kaikki laitteet pystyvät kuuntelemaan verkon lähetyksiä. Väyläratkaisussa taas kaikki laitteet ovat kytkettynä samaan väylään. Myös tässä kytkennässä laitteet voivat seurata kaikkea verkon liikennettä.

Toistimilla toteutettu verkko muodostaa yhden törmäysalueen eli segmentin. Ethernet-segmentin kuormitus ei saisi ylittää 4 – 7 Mbit/s kuin väliaikaisesti. Kuormituksen kasvaessa törmäysmäärät lisääntyvät, jolloin suurin osa ajasta menee odotteluun. Tämä taas johtaa verkkoon liitettyjen työasemien lähetyspuskurissa odottavien sanomien määrän kasvuun. Liialliset törmäykset siis heikentävät yleensä verkon suorituskykyä. Tiedostonsiirto käyttää suuria kehyksiä (frame), jolloin verkon kuormitus voi olla jopa 80% ilman ongelmia. Sen sijaan mm. tietokantakyselyt käyttävät pieniä kehyksiä, jolloin kehysten määrän kasvaessa myös törmäysvaara suurenee voimakkaasti jo 40%: n kuormituksella.

Nykyisin yleisin käytössä oleva Ethernet-kaapelointistandardi on 10BaseT, jossa yhteydet on toteutettu työasemien osalta parikaapelointina ja aluekaapelointi valokuitukaapeleilla. 10BaseT-standardin mukainen verkkotopologia on fyysinen tähtikytkentä, jossa työasemat on kytketty toistimena toimivaan keskittimeen. Suurin kaapelipituus on 100 metriä. Tarvittaessa keskitin osaa poistaa vialliseen laitteeseen kytketyn portin käytöstä, jolloin yhden laitteen virhetilanne ei katkaise koko verkon liikennettä.

Väylänvarausjärjestelmänä Ethernet-verkoissa käytetään CSMA/CD-kanavanvarausta (Carrier Sense Multiple Access/Collision Detect), joka jakaa siirtokapasiteettia eri laitteiden välillä (kuva 1). Mikä tahansa asema voi lähettää vapaaseen kanavaan. Lähetyksen aikana asema kuuntelee väylän liikennettä ja lopettaa lähetyksen, jos havaitsee muuta liikennettä. Jos verkkoon pääsee samanaikaiset lähetykset, asemat huomaavat lähetetyn tiedon muutoksen, päättelevät törmäyksen tapahtuneen ja varmistavat tilanteen JAM-signaalilla, joka tuhoaa lähetyksen. Törmäyksen jälkeen lähetykseen osallistuneet asemat arpovat toisistaan riippumattomat odotusajan ja lyhyemmän ajan saanut asema lähettää ensin viestin uudelleen.



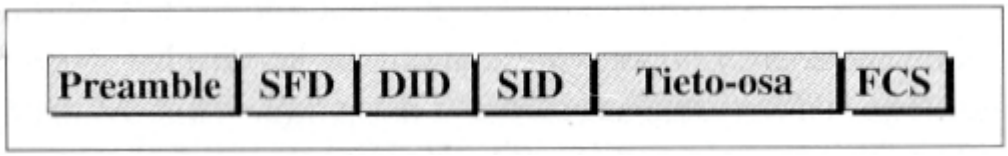
Kuva 1. CSMA/CD-vuoronvarauksen periaate [1].

Ethernetin MAC-kerros (Medium Access Control) kuuluu OSI:ssa määriteltyyn siirtoyhteyskerrokseen. MAC:in tehtävänä on huolehtia tiedon luotettavasta siirtämisestä asemalta toiselle. CSMA/CD:n tehtävänä on kilpavarausväylän vuoronvaraus. MAC-kehyksen tehtävänä on tunnistaa eri asemat (laitteet), havaita siirtovirheet, erottaa kehykset ja tunnistaa protokollat.

Ethernet-verkossa jokaisen segmentin asema kuulee lähetyksen. Lähettävä laite osoittaa vastaanottavan laitteen fyysisen osoitteen MAC-osoitteella, joka on jokaiseen laitteeseen tai tietoliikenneohjaimeen ohjelmoitu yksikäsitteinen osoite. Yleisin lähiverkoissa käytössä oleva MAC-osoite on 48-bittinen koodi.

Tiedonsiirto Ethernet-verkoissa tapahtuu kehyksinä (frame), joiden suurin standardinmukainen pituus on 1518 merkkiä. Sanoma koostuu viidestä osasta (kuva 2), jotka ovat:

- Preamble, jonka tehtävän on synkronoida vastaanottajan ja lähettäjän kellot
- SFD (Start of Frame Delimiter) rajaa kehyksen alkuosan
- DID (Destination IDentification) vastaanottajan MAC-osoite
- SID (Source IDentification) lähettäjän MAC-osoite
- Varsinainen data, johon sisältyy täyte, jos data-osa on lyhempi, kuin 64 merkkiä
- FCS (Frame Check Sum) eli 32-bittinen tarkistusluku, CRC (Cyclic Redundancy Check-32)



Kuva 2. Tiedonsiirtokehyksen periaate [1].

Ethernet-kehyksestä riippuen data-osaa voi edeltää erilaisia ohjaustietoja, mm. sanoman tyyppi, protokollatunnus, sanoman pituus, vastaanottajan ja lähettäjän sovellustunnukset tai organisaatiotietoa [1,2].

Ethernet-lähiverkkojen kapasiteetti on riittänyt hyvin pitkään. Vasta muutaman viimeisen vuoden aikana työasemien ja verkko-ohjelmistojen kasvanut suorituskyky ja siirrettävien tietomäärien kasvu on osoittanut Ethernetin kapasiteetin joissain tapauksissa riittämättömäksi. CSMA/CD-vuoronvarausjärjestelmä ei takaa mitään tiettyä palvelutasoa, koska segmentin työasemat kilpailevat kanavan siirtokapasiteetista. Tämä on ongelma varsinkin reaaliaikaisen tiedonsiirron sovellusten kohdalla, esimerkiksi äänen- ja kuvansiirron sovelluksissa.

Käytetty tekniikka ei myöskään tarjoa ratkaisuja työasemien, palvelimien ja verkkoon kytkettyjen muiden laitteiden keskitettyyn hallintaan. Eräät verkkoprotokollat (DHCP, SNMP ja RMON), työasema- ja palvelinjärjestelmien laajennukset sekä verkkokäyttöjärjestelmien ominaisuudet korjaavat tilanteen osittain mahdollistamalla joitakin keskitettyjä määrittely-, hallinta- ja monitorointitoimia. Ethernet on jaetun median verkko, mikä mahdollistaa periaatteessa kaikkien verkkoon kytkettyjen asemien tarkkailun ja kuuntelemisen luvattomasti. Viimeaikaiset tietoturvasovellukset ovat tosin tuoneet lisää turvallisuutta myös Ethernet-verkkoihin.

Ethernet-verkon ongelmia voidaan ratkaista mm. jakamalla verkko pienempiin osiin (mm. kytkentäinen Ethernet), skaalaamalla nykyisiä tekniikkoja (mm. 100Mbit/s ja Gigabit Ethernet) ja uusilla verkkotekniikoilla. Kytkentäisessä Ethernetissä verkko on jaettu useisiin törmäysalueisiin kytkimille, jolloin kytkimen eri portteihin liitetyt työasemat saavat kukin oman törmäyksettömän 10 Mbit/s kanavan. Kytkin välittää viestit oikeaan osoitteeseen MAC-osoitteen avulla. Kytkentäisellä Ethernetillä saavutetaan noin kaksinkertainen kapasiteetti perinteiseen Ethernetiin verrattuna. Skaalatut Ethernet-verkot ovat perustoiminnoiltaan samanlaisia normaalin Ethernet-verkon kanssa - erot ovat lähinnä siirtonopeudessa, joka on

nostettu 10-100-kertaiseksi ja käytettävissä kaapeleissa. Skaalattuja verkkoja käytetään enimmäkseen runkoverkkoina [2].

3.2 Muut lähiverkot

Ethernetin lisäksi on kehitetty myös muita lähiverkkoratkaisuja, jotka eivät perustu CSMA/CD-vuoronvaraukseen ja 802.3-kehykseen. Tärkeimmät näistä ovat IBM:n kehittämä Token Ring, samaa vuoronvarausta käyttävä FDDI (Fiber Distributed Data Interface), Ethernet- tai Token Ring-kehystä ja omaa Demand Priority-vuoronvarausta käyttävä 100VG AnyLAN sekä ATM-verkko [2].

Token Ring

Token ring on IBM:n kehittämä rengasmuotoinen lähiverkko, jossa käytetään tähtimäistä parikaapelointia ja jonka asemat muodostavat renkaan. Vuoronvarausjärjestelmänä käytetään renkaassa kiertävää valtuusmerkkiä (token), jonka asema voi siepata. Valtuusmerkin saanut asema lähettää viestin viereiselle asemalla, joka tarkistaa kohteen ja lähettää viestin eteenpäin. Viestin saavuttua kohdeasemalle, se kopioidaan puskuriin ja lähettää sanoman takaisin renkaaseen merkiten sen samalla kopioiduksi. Sanoma palautuu lopulta lähettäneelle asemalle, joka tarkistaa sanoman perillemenon, poistaa kopioidun sanoman verkosta ja siirtää valtuusmerkin eteenpäin. Vuoronvarausmenetelmä takaa kaikille verkkoon kytketyille asemille tietyn lähetyskaistan.

Token Ring- verkoissa käytetään 48-bitin MAC-osoitteita. Token Ring käyttää siirtokaistaa tehokkaammin kuin Ethernet-verkkojen CSMA/CD. Alkuperäinen Token Ring toimi 4 Mbit/s siirtonopeudella, mutta vuonna 1988 julkistettiin 16 Mbit/s siirtonopeutta käyttävä uusi versio. Uusin versio nostaa siirtonopeudeksi 100 Mbit/s. Paremmista ominaisuuksista huolimatta Token Ring ei ole saavuttanut Ethernetin suosiota, koska käyttäjät eivät ole halunneet sitoutua yhden laitevalmistajan (IBM) verkkoratkaisuihin [2].

FDDI (Fiber Distributed Data Interface)

FDDI on valokuituun perustuva lähiverkkoratkaisu. Topologialtaan verkko on rengasmainen ja sen siirtonopeus on 100 Mbit/s. Valtuudenvälitysjärjestelmä on samanlainen kuin Token Ringissä. Renkaan suurin mitta on 100 km ja samaan renkaaseen voidaan kytkeä jopa 1000 asemaa. Verkkoon liitetyt asemat voivat olla joko varmistettuun kaksoisrenkaaseen kytkettyjä DAS-asemia tai keskittimeen varmistamattomalla yhteydellä kytkettyjä SAS-asemia. DAS-asemia yhdistävä verkko on vikasietoinen, sillä asemat pystyvät käyttämään vaihtoehtoista reittä vikatilanteessa. FDDI-verkkoja käytetään lähinnä ATK-keskusten runkoverkkoina sekä kaupunki-, tehdasalue- ja kampusverkkoina. Korkean hinnan vuoksi FDDI-tekniikka ei ole vielä yleisessä käytössä Suomessa [2].

100VG AnyLAN

100VG AnyLAN-tekniikka on Hewlett-Packardin ja IBM:n ehdotusten perusteella standardoitu 100 Mbit/s-lähiverkkotekniikka, joka poikkeaa Ethernetistä mm. kehyksen ja vuoronvarausmenetelmän osalta. Työasemat on kiinnitetty tähtimäisesti keskittimeen. Asema

varaa siirtotien omalla protokollallaan ja lähettää sanoman saatuaan siihen luvan. Vain vastanottava asema kuulee lähetetyn sanoman. Vuoronvaraus on samantyyppinen kuin Token Ringissä, joten törmäyksiä ei tapahdu. 100VG AnyLAN-verkko koostuu keskittimistä, joihin työasemat, palvelimet, muut keskittimet ja tietoliikennelaitteet kytketään. Siirtokaistan käyttö tapahtuu keskittimen suorittamien kiertokyselyiden avulla, joihin palvelua tarvitseva asema vastaa. Keskittimen vastaanottaessa tiedonsiirtopaketin ohjataan se ainoastaan kohdeosoitteen mukaiseen porttiin. Huolimatta 100VG AnyLANin paremmasta suorituskyvystä Ethernetiin verrattuna, tekniikka ei ole saavuttanut kovin suurta suosiota, mikä johtunee laitetarjonnan keskittymistä vain muutamalle valmistajalle [2].

ATM

ATM (Asynchrous transfer mode) on uusin lähiverkkotekniikka, joka yhdistää piirikytkentäisen ja pakettikytkentäisen tekniikan edut. ATM:n ominaisuuksia ovat vakioviive, taattu kapasiteetti, joustavuus ja kanavoinnin tehokkuus. ATM:n avulla voidaan välittää perinteisten lähiverkkosovellusten lisäksi laadukasta HiFi-ääntä ja täyskuvavideota. Datan siirto tapahtuu lyhyissä kiinteänmittaisissa paketeissa, joita lähetetään laitetasolla ATM-solmujen kautta. Verkon topologia on tähtimäinen, jossa päätelaitteet on liitetty ATM-solmuun. ATM-solun pituus on 53 tavua, joka koostuu 5 tavun otsikosta ja 48 tavun tieto-osasta. Tämä mahdollistaa viiveiden ennustettavuuden, jolloin ATM:llä voidaan siirtää reaaliaikaista tietoa. ATM-verkkojen siirtonopeudet ovat 25 - 2500 Mbit/s, sillä niissä ei ole virheenkorjausta tai vuonohjausta, kuten tavallisissa pakettikytkentäisissä verkoissa. ATM-verkoissa luotetaan siis nykyaikaisten siirtoteiden virheettömyyteen ja vastuu virheenkorjauksista on siirretty äärijärjestelmille. ATM-tiedonsiirrossa päätesolmujen välille muodostetaan virtuaaliyhteys. Lähettävä solmu pyytää kytkimeltä tarvittavia yhteysparametreja, jonka jälkeen ensimmäinen ATM-kytkin etsii reitin lähetettävälle tiedolle. Yhteysparametreja hyväksikäyttäen muodostaa kytkin virtuaaliyhteyden välittävien solmujen kautta. Muodostettua reittiä käytetään koko yhteyden ajan. Lähiverkkoprotokollia ei voida sellaisenaan käyttää ATM-verkoissa. Tämän vuoksi käytetään erilaisia emulaatioita, jotta tietoa voidaan siirtää esimerkiksi ATM:n ja muiden lähiverkkojen välillä. Käytössä ovat ainakin LAN emulaatio (LANE), klassinen IP-protokolla ja MPOA (Multiprotocol over ATM) [2].

Virtuaaliset lähiverkot

Kytkentäiset verkot voidaan jakaa myös virtuaaliverkkoihin (VLAN) kytkimen porttien, MAC-osoitteen, protokollatiedon, verkko-osoitteen tai sovelluksen mukaan. Virtuaaliverkossa liikkuvissa kehyksissä on mukana tieto siitä, mihin verkkoon ne kuuluvat. Tämän tiedon perusteella kytkimet välittävät kehyksen vain kyseiseen virtuaaliverkkoon kuuluviin portteihin. Vain saman verkon asemat voivat "keskustella" suoraan. VLANin avulla verkko voidaan määritellä esimerkiksi organisaation ja tehtävien mukaiseksi riippumatta päätteiden fyysisestä sijainnista [2].

3.3 CAN (Controlled Area Network)

CAN on integroitu tietoliikenneratkaisu reaaliaikaisiin sovelluksiin. Se kehitettiin alunperin autoissa käytettäväksi, mutta nykyisin sitä käytetään myös monissa teollisuusautomaatio- ja

valvontasovelluksissa. CANin siirtonopeus on enimmillään 1 Mbit/s. CAN-väylän fyysinen media on yleensä suojaamaton tai suojattu kierreparikaapeli, mutta myös tavallista parikaapelia käytetään. Väylä toimii hyvin vaikeissakin olosuhteissa ja sillä on erinomainen virheiden havaitsemis- ja eristyskyky. Tiedonsiirto toimii vaikka toinen johtimista menee poikki, joutuu oikosulkuun tai maadoittuu [3].

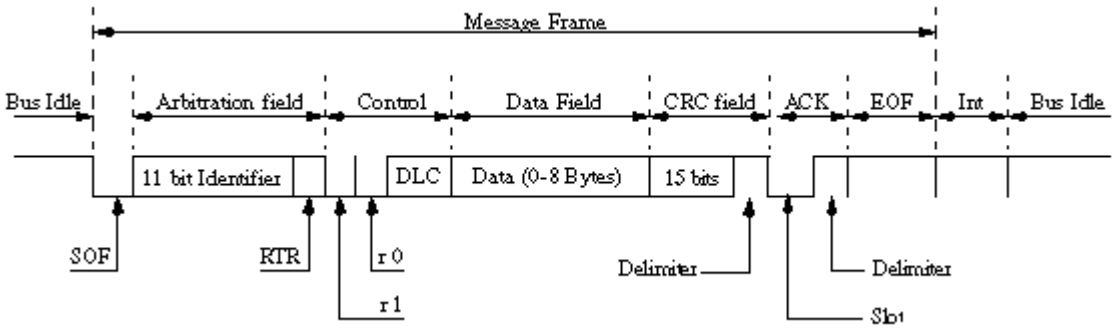
ISO 11898-standardissa määritelty CAN-spesifikaatio käsittää vain fyysisen tason ja datalinkkitason. Ensimmäisessä määritellään väylän fyysiset ja sähköiset ominaisuudet sekä laitteisto, jolla tieto muutetaan signaaleiksi. Jälkimmäinen tunnistaa ja ymmärtää viestien formaatin. Tämä taso koodaa fyysiselle tasolle lähetettävät viestit ja purkaa fyysiseltä tasolta vastaanotetut viestit. CAN-ohjaimien datalinkki-taso on yleensä toteutettu laitteistotasolla.

Monet CAN-sovellukset tarvitsevat palveluja, jotka ylittävät datalinkkitason perustoiminnan, esimerkiksi pidemmän kuin 8-bittisen tiedon lähetys tai vastaanotto. Nämä palvelut voidaan toteuttaa sovellustasolla, joita ovat kehittäneet monet eri organisaatiot. Käytettyjä sovellustasoja ovat mm. CAL (CAN Application Layer), CANopen, PCAL (CALin implementaatioita), DeviceNet™ (CAN 2.0A:n perustuva teollisuusautomaatiosovellus) ja SDS™ (Smart Distributed System, koneiden ohjaussovellus). Viesteissä ei käytetä lähettävän tai vastaanottavan kohteen osoitteita, vaan viestiin liitetään yksilöllinen tunniste. Verkon kaikki asemat vastaanottavat viestin ja suorittavat hyväksymistestin, jolla määritetään onko viestin sisällöllä merkitystä kyseiselle asemalle. Jos viesti on merkityksellinen, vastaanottava asema käsittelee sen. Muussa tapauksessa viesti hylätään. Tunniste määrittelee myös viestin prioriteetin käyttämällä CSMA/CD-vuoronvarausta, jossa on parannettu säilyttävä vuoronvaraustekniikka. Kahden tai useamman aseman lähettäessä yhtä aikaa säilyttävä vuoronvaraustekniikka varmistaa, että viestit lähetetään kiireellisyysjärjestyksessä.

CAN-viestien prioriteetti määräytyy tunnisteen numeroarvon perusteella. Tunnisteiden numeeriset arvot määritellään järjestelmää suunniteltaessa. Korkein prioriteetti on pienimmän numeerisen arvon saaneella tunnisteella. Järjestelmä takaa väylän resurssien jaon tarpeiden mukaan, toisin kuin esimerkiksi Ethernet tai TokenRing, ja rajoittavana tekijänä on vain väylän suurin tiedonsiirtokapasiteetti.

Tiedonsiirto tapahtuu kehyksien avulla, jotka "kantavat" viestit lähettävästä asemasta vastaanottaviin asemiin. Käytössä on kaksi tiedonsiirtoprotokollaa, 2.0A ja 2.0B, joista ensimmäisessä on 11 bitin tunnisteet ja jälkimmäisessä 11 ja 29 bitin tunnisteet (kuva 3). Standardiversiossa (2.0A) viestikehys koostuu seitsemästä osasta:

- kehyksen alku (SOF, Start of Frame)
- tunniste (arbitration)
- kontrolli (Control)
- data
- tarkiste (CRC, Cyclic Redundancy Check))
- kuittaus (ACK, Acknowledge)
- kehyksen loppu (EOF, End of Frame)



Kuva 3. CANin 2.0A-kehys [3].

2.0B-protokolla kehitettiin, jotta CAN saataisiin yhteensopivaksi muiden autoissa käytettävien tiedonsiirtoprotokollien kanssa. Protokolla eroaa 2.0A:sta lähinnä tiedonsiirtokehyksen osalta ja on yhteensopiva 2.0A:n kanssa. Joitakin rajoituksia lukuun ottamatta molempia protokollia voidaan käyttää samassa verkossa.

CANin sisältöihin suuntautunut viestinvälitysjärjestelmä tarjoaa laajan joustavuuden systeemien kokoonpanojen määrittelyssä. Pelkästään olemassa olevaa tietoa vastaanottavien asemien liittäminen verkkoon on mahdollista tekemättä muutoksia laitteistoihin tai ohjelmistoihin. Eri ohjainten tarvitsemat mittaustulokset voidaan välittää väylää pitkin, joten jokainen ohjain ei tarvitse erillistä anturia [3].

3.4 Lähiverkkojen ongelmat ja diagnostisointi

Lähiverkkojen laajentuminen ja sovellusten siirtäminen verkkoon on asettanut verkon käytettävyydelle suuria haasteita. Vikojenhallinta on muuttunut entistä vaikeammaksi tietoverkkojen muututtua dynaamisemmiksi ja heterogeenisimmiksi. Verkon ylläpidossa käytetään laitehallinnan työkaluja, joiden avulla ylläpitäjä voi seurata verkkoon kytkettyjen laitteiden tilaa ja toimintaa, jolloin verkkovikojen haitat pienenevät vianhaun nopeutuessa [2,11].

Verkonhallinta voidaan jakaa viiteen osa-alueeseen [2]:

- Vikatilanteiden hallinta (fault management) - verkon ongelmien havainnointi, kirjaaminen, ilmoittaminen käyttäjille ja korjaaminen.
- Määrittelyjen hallinta (configuration management) - verkkoelementtien määrittelytietojen seuraaminen, josta saatavia tietoja käytetään vianeristyksessä, vianhaussa ja verkon suunnittelussa.
- Suorituskyvyn hallinta (performance management) - verkon suorituskyvyn ylläpitäminen hyväksyttävällä tasolla. Keinoina ovat vasteajan, kapasiteetin ja kuormitusasteen mittaaminen.
- Käytön ja laskutuksen hallinta (accounting management) - käytön tunnuslukujen mittaaminen verkon käytön seuraamiseksi. Mittauksia voidaan hyödyntää kapasiteettisuunnittelussa, käyttäjäkohtaisten rajoitusten toteutuksessa tai laskutuksen perusteena.

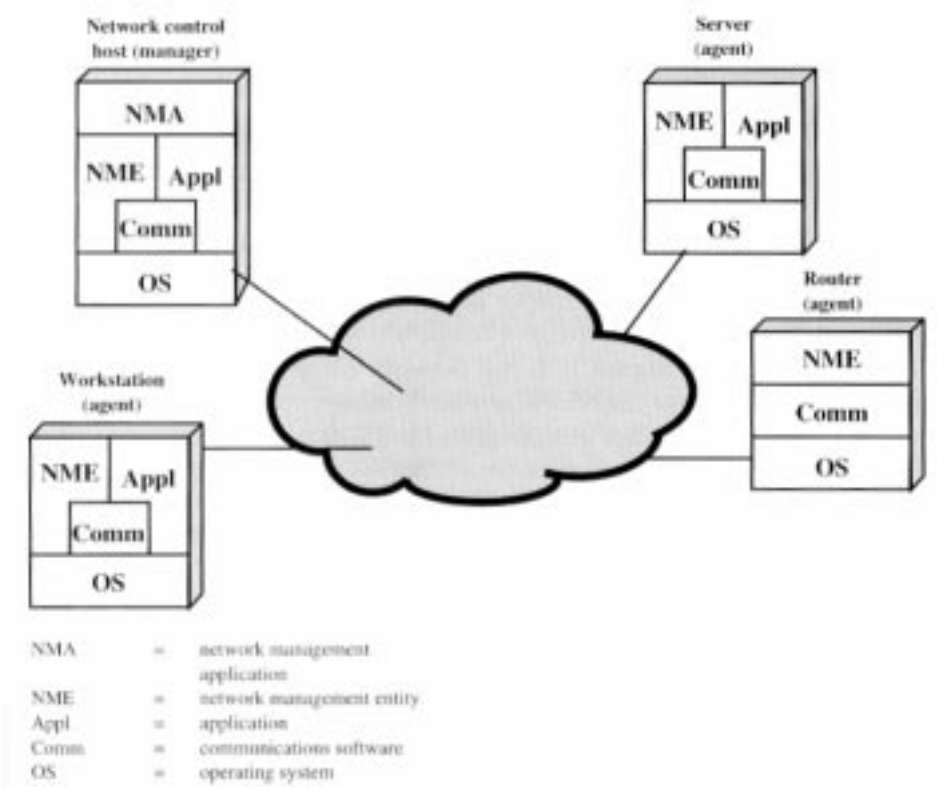
- Turvallisuuden hallinta (security management). Verkkoresurssien kontrollointi, verkko-oikeuksien hallinta.

Lähiverkoissa kokonaisuuden ylläpito sisältää seuraavia tehtäviä [2]:

- verkon ja järjestelmien ylläpito ja operointi
- vikojen etsiminen, korjaaminen ja ehkäiseminen
- muutoksista johtuvat ylläpitotehtävät
- kokonaisuuden ja osien kuormitusseuranta ja kapasiteettisuunnittelu

Verkonhallinta toteutetaan yleensä protokollatasolla. Yleisin hallintaprotokolla on TCP/IP-verkkojen SNMP (Simple Network Management Protocol). Kappaleessa 5.3 on esitetty tarkemmin protokollakerroksen kunnonvalvontaa.

Verkonhallintasysteemi on kokoelma työkaluja verkon valvontaan ja hallintaan. Järjestelmä koostuu verkkoon liitettävistä laitteistoista ja ohjelmistoista. Verkonhallinnan ohjelmisto sijaitsee isäntäkoneissa ja tiedonsiirron käsittelykomponenteissa (mm. reitittimissä, silloissa, edustakoneissa, pääteklusterien ohjaimissa). Verkon aktiiviset elementit lähettävät säännöllisesti palautetietoa verkon tilasta hallintakeskukselle (NCC, Network Control Center). Kuvassa 4 on esitetty verkonhallintajärjestelmän arkkitehtuuri [12].



Kuva 4. Verkonhallintajärjestelmän arkkitehtuuri [12].

Verkon jokainen solmupiste sisältää verkonhallintaan tarkoitettuja ohjelmia (NME, Network Management Entity), jotka keräävät tietoja tiedonsiirrosta, tallentavat tilastoja paikallisesti ja

toteuttavat verkonhallintakeskuksen komentoja. Komentoja ovat mm. kerätyn tilastotiedon lähettäminen hallintakeskukseen, parametrin vaihto, status-informaatio ja toiminnan testaaminen lähettämällä testiviestejä.

Ainakin yksi verkon isäntäkoneista määritellään verkon manageriksi, jossa on verkonhallinnan sovellusohjelmisto (NMA, Network Management Application). Ohjelmiston avulla verkon ylläpitäjä antaa komennot NME-ohjelmille verkon solmupisteisiin. Muita verkon solmupisteitä kuin manageria kutsutaan agenteiksi. Agenttien tehtävänä on tarkkailla hallittavien objektien tilaa ja raportoida niistä ylläpidolle. Lisäksi agentit vastaanottavat ylläpidon ohjeita objekteille suoritettavista toimenpiteistä. Useimmiten käytetään kahta tai useampaa verkonhallinnan isäntäkonetta, jolloin yhden koneen kaatuessa verkon toimintoja voidaan ohjata varajärjestelmän avulla.

Vika on epänormaali tila, joka vaatii ylläpidon huomiota tai toimintaa, jotta se saadaan korjattua. Vika havaitaan useimmiten vääränä verkon toimintana tai suurena määränä virheilmoituksia. Esimerkiksi katkenneet tai taittuneet kaapelit voivat aiheuttaa signaalin katkeamisen tai vääristymän. Lähiverkkojen vikatilanteita ovat mm. reititinsilmukat ja isäntäkoneen (host) kaatuminen. Virheet puolestaan ovat yksittäisiä datavirheitä tietoverkon viesteissä, joita verkonhallintaprotokollien virheenkorjausmekanismit pystyvät yleensä korjaamaan verkon toiminnan häiriintymättä. Verkon vikatoleranssia voidaan parantaa käyttämällä korvautuvia komponentteja ja vaihtoehtoisia tiedonsiirtoreittejä. Viat ilmaistaan etukäteen määriteltyinä hälytyksinä. Hälytysviesteissä annetaan informaatiota joka koostuu vian kohdanneen järjestelmän nimestä, vian oireista, vian paikasta tietoverkossa, vian havaitsemisen ajasta ja vian syystä. Useimmiten järjestelmä ei kuitenkaan pysty antamaan kaikkea em. informaatiota. Varsinkin vian paikka ja syy jäävät usein selvittämättä, koska tietoverkon eri laitteilla on vain rajoitettua tietoa koko järjestelmän toiminnasta [12 - 14].

Vian tapahtuessa vianhallinnan tehtävänä on mahdollisimman nopeasti [12]:

- määriteltävä vian paikka reaali-ajassa verkon protokolliin ja laitteisiin liitettyjen mekanismien avulla
- eristettävä vika paikantamalla ja tunnistamalla se vika-algoritmien avulla ja mahdollisten viallisten komponenttien testauksella, jotta muun verkon toiminta voi jatkua häiriytymättä
- määriteltävä verkon asetukset uudelleen toimimaan ilman viallisia komponentteja
- korjattava tai vaihdettava vialliset komponentit tai korjattava virheet ohjelmiston avulla verkon palauttamiseksi alkuperäiseen tilaan

Tietoverkkojen vikojen hallintaan on kehitetty useita järjestelmiä, joita ovat mm. asiantuntijajärjestelmät, tietokantatekniikat, FSM-järjestelmät (Finite State Machine) ja todennäköisyyteen perustuvat menetelmät. Näissä järjestelmissä vikatyypit on spesifioitava etukäteen, jotta viat voidaan havaita. Tämä ominaisuus rajoittaa kehitettyjen järjestelmien suorituskykyä, koska kaikkien mahdollisten vikojen määritteleminen etukäteen ei ole mahdollista [11, 15].

Asiantuntijajärjestelmät sopivat parhaiten selkeisiin ongelmiin toimintaympäristössä, joka ei ole kovin dynaaminen. Tapauskohtaisten diagnostiikkajärjestelmien avulla voidaan etsiä ratkaisuja useisiin yhtäaikaisiin ongelmiin, esimerkiksi tiedonhankinnan pullonkauloihin.

FSM on "virtuaalinen kone", jota käytetään hahmojen tunnistukseen ja identifioimiseen. Tämä menetelmä pystyy käsittelemään sekä epätäydellistä tietoa että odottamattomia vikoja. Edellä mainitut järjestelmät ovat kuitenkin herkkiä "hälytyskohinalle" eli hälytysviestin viiveelle tai katoamiselle, joten niiden käyttö reaaliaikaisissa sovelluksissa on rajoitettua. Todennäköisyyteen perustuvat menetelmät käyttävät mm. Bayes-verkkoa ja etukäteistietoa vikojen tunnistukseen [16].

Uusimpia lähestymistapoja ovat olleet mm. koodattuun tapahtumakorrelaatioon perustuvat menetelmät. Ongelman aiheuttaneet tapahtumat on esitetty koodilla, jonka avulla ongelma tunnistetaan. Havaittujen oireiden perusteella määritellään minkä ongelman koodi sopii oireisiin. Syy-yhteyskuvaajaa käytetään esittämään tapahtumien välisiä syy-seuraus-yhteyksiä. Lisäksi vianhallintaan on esitetty useita erilaisia uusia menetelmiä, mm. neuroverkkoja, integroituja hajautettuja AI-järjestelmiä (AI, Artificial Intelligence), mukautuvia oppivia järjestelmiä, ajoitettua tapahtumakorrelaatiota ja sumeaa logiikkaa [11,13,15,16].

Esimerkkinä tietoverkossa tapahtuvasta vianhallinnasta on esitetty CAN-verkon virheidenvalvonta- ja korjausmekanismi.

CANin virheidenvalvonta- ja korjausmekanismit

CAN käyttää viittä virheiden havaitsemismekanismia, jotka ovat CRC (Cyclic Redundancy Check), kehystarkistus, kuittausvirheiden tarkistus, bittien valvonta ja bittien lisäys. Jokainen viesti sisältää 15 bitin pituisen CRC-koodin. Lähettävä asema laskee CRC:n ja sen arvo perustuu viestin sisältöön. Kaikki viestin hyväksyneet vastaanottavat asemat suorittavat tarkistuslaskelman ja ilmoittavat, jos CRC-arvo poikkeaa lähetetystä. Kehystarkistusta varten viestikehyksessä on etukäteen määritetty bittiarvoja, joiden täytyy sijaita tietyissä paikoissa lähetyksen aikana. Jos vastaanottava asema havaitsee väärän bitin jossakin näistä paikoista, tuloksena on virheilmoitus. Kuittausvirhe ilmoitetaan, jos lähettävä asema ei vastaanota kuittaussignaalia vastaanottajalta. Kaikki lähettävät asemat tarkkailevat ja vertailevat automaattisesti todellista väylän bittivirtaa lähetettävään tasoon. Jos nämä kaksi poikkeavat toisistaan, tuloksena on virheilmoitus. Tiedonsiirron eheyttä tarkkaillaan tavujen lisäyksellä. Viiden peräkkäisen samanlaisen bittitason lähettämisen jälkeen lähettävä asema lisää automaattisesti tarkistusbitin bittivirtaan. Vastaanottavat asemat poistavat automaattisesti tarkistusbitit ennen viestin käsittelyä. Jos siis jokin vastaanottavista asemista vastaanottaa *kuusi* peräkkäistä bittiä samalla tasolla, tuloksena on virheilmoitus. Minkä tahansa aseman havaittua yhden tai useampia em. virheitä, havaitseva asema keskeyttää tiedonsiirron lähettämällä virhekehyksen (error frame), jolla estetään muita asemia hyväksymästä viestiä ja varmistetaan tiedon yhtenäisyys koko verkon alueella.

Virheen eristäminen on mekanismi, jolla pystytään erottamaan toisistaan hetkelliset virheet ja pysyvät viat. Hetkellisiä virheitä voivat aiheuttaa esimerkiksi jännitepiikit. Pysyvät viat johtuvat useimmiten viallisista liitännöistä, kaapeleista, lähettimistä ja vastaanottimista sekä pitkään kestävistä ulkoisista häiriöistä. Kun järjestelmä ilmoittaa virheestä, CAN-verkon jokainen asema lisää arvon toiseen virherekistereistään. Vastaanottovirheet ovat 1 arvoisia ja se lisää vastaanottovirherekisterin summaa. Lähetysvirheet ovat 8 arvoisia ja ne kasaantuvat lähetysvirherekisteriin. Jos virheitä tulee lisää virherekisterien arvo kasvaa. Virheettömät viestit puolestaan vähentävät virherekisterien arvoa ja virheiden loppuessa rekisterit saavat

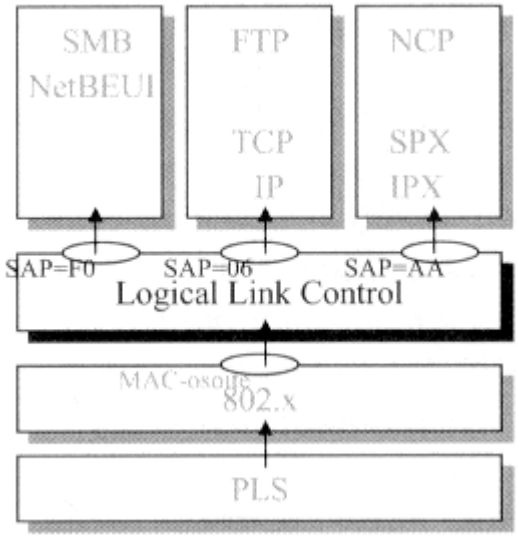
arvon nolla. Virherekisterin yhteenlaskettu arvo määrää aseman virhetilan, joita on kolme erilaista: aktiivinen, passiivinen ja irtikytkeytyminen.

Aktiivinen tila on aseman normaalitila. Tässä tilassa asema on täysi toimiva ja molempien virherekisterien arvo on vähemmän kuin 127. Jos jommankumman virherekisterin arvo ylittää 127 asema menee passiiviseen tilaan, jossa asema voi edelleen lähettää ja vastaanottaa viestejä, mutta aseman havaitsemien virheiden ilmoituskykyä on rajoitettu. Jos virhetilanne jatkuu ja rekisterin arvo ylittää 255, asema kytkee itsensä pois väylästä. Vialliset laitteet saadaan näin pois väylästä kunnes käyttäjä kytkee sen uudelleen. Muiden asemien tiedonsiirto toimii kuitenkin edelleen häiriintymättä.

CANin virheiden havaitsemiskyky on erittäin perusteellinen. Globaalit virheet havaitaan 100% varmuudella. Useiden virheiden havainnointimekanismien ansioista paikallisten virheiden mahdollisuus jäädä huomaamatta on vain noin 10^{-11} [3].

4 Siirtotien ohjaus - LLC (Logical Link Control)

LLC - siirtotien ohjausta käytetään muodostamaan yhteinen siirtotiestä ja verkkotyypistä riippumaton rajapinta lähiverkkojen ja eri verkkoprotokollien välille. LLC huolehtii myös kuljetettavan datan protokollatunnistuksesta ja useiden yhteyksien luomisesta samojen MAC-osoitteiden välille. LLC:tä voidaan käyttää myös virheenkorjaukseen, viallisten kehysten uudelleenlähettämiseen ja yhteyden muodostamiseen. Siirtotien ohjaus häivyttää eri verkkoprotokollat MAC-kerroksen lähiverkkoratkaisuilta. Kuvassa 5 on esitetty LLC:n periaatteellinen malli [2].



Kuva 5. LLC-ohjauksen malli [2]

5 Protokollat

Protokolla (protocol) eli yhteyskäytäntö on kuvaus tavasta, jolla tietoliikenteen eri osapuolet kommunikoivat toistensa kanssa. Protokollan avulla osapuolet saadaan toimimaan yhteisten pelisääntöjen puitteissa. Sääntöjä tarvitaan mm. seuraaviin tehtäviin [4]:

- bittien yhtäläinen sähköinen esittäminen
- yhteisen siirtotien käyttöoikeuden jakaminen
- virheiden havaitseminen ja korjaaminen
- vastaanottajan osoittaminen
- yhteyden kytkentä verkon solmussa
- ruuhkan hallinta

Verkkokerroksen protokollat lähiverkkojen ja etäverkkojen palveluja datapakettien kuljettamiseen. Ohjelmistolla toteutettua liitäntää verkkokerroksen ja sovelluskerroksen välillä kutsutaan protokollapinoksi. Maailman käytetyin protokollapino on TCP/IP, jota käytetään myös internetissä. Muita protokollapinoja ovat mm. IPX/SPX ja NetBEUI.

5.1 TCP/IP (Transmission Control Protocol/Internet Protocol)

TCP/IP:n verkkokerroksessa (IP) käytetään yhteydettömien pakettien reititystä. Yhteydettömyys tarkoittaa sanoman lähettämistä verkon läpi ilman varmistusta sen perillemenosta. Siirrettävä tieto jaetaan IP-paketeiksi, jotka verkossa toimivat reitittimet ohjaavat oikeisiin paikkoihin paketissa olevien osoitetietojen mukaisesti. IP ei takaa lähettävän datan perillemenoa eikä sitä, että datapaketti saapuu ehjänä vastaanottajalle. IP suojaa ainoastaan datapaketin otsikon, joka kontrolloi paketin kulkua verkossa. Jos otsikosta laskettu tarkistussumma ei vastaanottopisteessä täsmää hylätään lähetetty paketti [8,9].

Jokaiselle asemalle määritellään 32-bittinen IP-osoite, verkko- ja aliverkko-osan pituuden osoittama aliverkkopeite (subnet mask) sekä oletusreititin (default gateway), jota käytetään aliverkon ulkoiseen liikennöintiin. Lähde- ja kohdeosoitteiden sekä aliverkkopeitteen perusteella asema osoittaa samassa aliverkossa olevat paketit suoraan kohdeasemalle ja eri aliverkkoon kuuluvat paketit oletusreitittimelle.

TCP/IP:n kuljetuskerros (TCP) vastaa tiedonsiirrosta päätejärjestelmien välillä. TCP kuljettaa datavuon yhteydellisesti ja varmistettuna. TCP kokoaa verkon linjalta saapuvat IP-paketit oikeaan järjestykseen ja pyytää tarvittaessa lähettämään puuttuvat tai virheelliset tiedot uudestaan. Näin TCP huolehtii datansiirron luotettavuuden säilymisestä lähettäjän ja vastaanottajan välillä. Lisäksi se pyrkii käyttämään hyväksi mahdollisimman hyvin verkon resurssit pakkaamalla niin paljon dataa kuin mahdollista yhteen IP-pakettiin. Samalla TCP yrittää ylläpitää mahdollisimman hyvää tiedonsiirtonopeutta välttämällä verkon kuormitetuimpia osia [9].

Internetin IP-osoitteet suunniteltiin alunperin siten, että verkossa olisi suhteellisen harvalukuinen määrä suurtietokoneita palvelimina (serveri). Nykyisin käytössä olevassa IP-

protokollassa (IPv4) osoitteet ovat 32-bittisiä. 32-bittisessä järjestelmä mahdollistaa noin neljä miljardia erilaista osoitetta (=2^{32}). Noin kaksikymmentä vuotta sitten tämä tuntui niin suurelta osoitejoukolta ettei sen arveltu koskaan loppuvan kesken. Aika on kuitenkin todistamassa tämän vääräksi eikä vähiten langattomasti kommunikoivien laitteiden yleistymisen vuoksi. Nykyisin noin puolet kaikista IP-osoitteista on käytössä. Internetiin liitettävien laitteiden lisääntyessä ennustettua tahtia, ovat kaikki osoitteet varattuja vuonna 2010 eikä enää uusia laitteita voida enää liittää nykyisen järjestelmän puitteissa. Tämän vuoksi ollaan kehittämässä uutta IP-protokollaa, joka sallii suuremman osoitejoukon [8,9].

Uusin IP-protokollaversio on IPv6, jota on kehitetty yli neljä vuotta. Uudessa protokollassa osoitteet ovat 128 bittisiä, jolloin erilaisten osoitteiden määrä kasvaa noin $3.4*10^{29}$ miljardiin. Valtaisan osoitejoukon lisäksi IPv6 mahdollistaa käyttäjän autokonfiguroinnin verkkoon.

5.2 Muut protokollat

IPX/SPX (Internet Packet eXchange/Sequential Packet eXchange)

Novellin kehittämä IPX/SPX-protokollapino on tarkoitettu NetWare-palvelimen ja työasemien väliseen yhteyteen. Verkkokerroksella on käytössä yhteydetön reitittyvä IPX-protokolla. IPX-osoite on 10 tavuinen ja jakautuu 4 tavun pituiseen verkko-osaan ja 6 tavun pituiseen isäntäosaan. Osoitteita ei kontrolloida, vaan käyttäjä voi valita haluamansa osoitteen. Lähettävä ja vastaanottava asema tunnistetaan verkko-, asema- ja socket-numeroilla. Reititysprotokolla etsii reitit kohdeverkkoon ja valitsee lyhyimmän tien. Lähettävän ja vastaanottavan aseman tunnuksina käytetään verkkokortin MAC-osoitteita. Socket-numero puolestaan ilmoittaa lähettävän ja vastaanottavan aseman prosessin, joille annetaan kullekin oma numero. Kuljetuskerroksella käytetään yhteydellistä kuljetuspalvelua, jossa ennen tiedonsiirtoa muodostetaan SPX-virtuaaliyhteys asemien välille. Yhteys pysyy auki, jos tietoa lähetetään säännöllisesti [2].

NetBEUI (NetBIOS Extended User Interface)

NetBEUI on Microsoftin kehittämä yksinkertainen reitittymätön protokolla Windows-työaseman ja LAN Manager/NT-palvelimen väliseen yhteyteen. Protokolla on periaatteessa NetBIOS-emulaattori, joka huolehtii koneiden nimien käsittelystä. Kuljetus- ja verkkokerrosta ei ole toteutettu lainkaan, joten protokollapinossa ei ole verkko-osoitteita. Tämän vuoksi NetBEUI:ta ei voida reitittää. Protokolla tarjoaa palvelut sanomien nimien käsittelyyn, valvontaan ja käyttöön. NetBEUI käyttää yhteydettömiä tietosähkeitä NetBIOS-nimien tarkistamiseen, etsimiseen ja ilmoitukseen. Yhteydellisillä infosanomilla perustetaan istunto ja lähetetään tietoa. Yhteys- ja infosanomat numeroidaan, kuitataan ja kuljetetaan yhteydellisinä DLC -kerroksessa käyttäen LLC-siirtotienohjausta. Siirtoyhteyskerroksessa käytetään MAC-osoitteita [2].

5.3 Protokollien diagnostisointi

Tiedonsiirtovirheet

Onnistuneen tiedonsiirron edellytyksenä on tietoliikenneprotokollan kyky havaita ja korjata lähetyksessä tapahtuneet virheet. Tiedonsiirrossa vastaanottaja havaitsee kolmentyyppisiä virheitä: virheellisesti siirretyt sanomat, puuttuvat ja kahdentuvat sanomat [1, 11].

Virheelliset sanomat havaitaan sisällön perusteella tehtävien tarkistusten avulla. Virheitä syntyy esimerkiksi amplitudin ja vaiheen vääristymistä. Myös kohinan ja linjahäiriöiden aiheuttamat signaalin vääristymät aiheuttavat virheitä sanomiin. Virheellisten sanomien havainnointi tapahtuu tarkisteiden avulla, joita ovat mm. pariteettitarkistus ja polynominen tarkistus eli CRC (Cyclic Redundancy Check).

Puuttuvat sanomat voivat johtua mm. sanoman muistiin siirtävän ohjainlogiikan synkronointivirheestä, häiriöiden aiheuttamista sanoman päättymismerkin tunnistusvirheistä tai linjakatkoksista. Sanomasta voi saapua myös useampia versioita samalle vastanottajalle, jolloin kyseessä on kahdennettu sanoma. Puuttuvat tai kahdennetut sanomat havaitaan protokollaan liitetyllä sanomien järjestysnumeron seurannalla, jonka perusteella vastaanottaja voi päätellä ovatko lähetetyt sanomat saapuneet perille.

Pariteettitarkistus perustuu tietyn bittijoukon 1-bittien määrään, joka asetetaan parilliseksi tai parittomaksi. Tarkistukseen käytetään ylimääräistä pariteettibittiä. Tarkistuksen perustana on todennäköisyys, että kohteena olevasta bittijoukosta vääristyy pariton määrä bittejä. Parillisen bittimäärän vääristyessä virheet jäävät huomaamatta. Pariteettitarkistus on jo väistynyt suurimmaksi osaksi, mutta on käytössä edelleen yksinkertaisissa sovelluksissa.

Polynomitarkistus perustuu tarkistuslukuihin, jotka lasketaan jokaisesta viestistä etukäteen sovitulla tavalla. Vastaanottajan asema tarkistaa sanoman ja jos tarkistusluku poikkeaa lähetetystä viesti on virheellinen.

Tietoliikenteen virheiden korjausmenetelminä käytetään lähinnä kahta tapaa: ARQ (Automatic Repeat ReQuest), jossa virheen havainnoinnin jälkeen pyydetään lähettäjää lähettämään virheellinen tai puuttuva sanoma uudestaan ja FEC (Forward Error Correction), jossa sanoma itsessään sisältää virheellisen tiedon korjaamiseen tarvittavaa tietoa.

ARQ-menetelmässä lähettäjä odottaa kuittausta tietyn ajan, jonka jälkeen sanoma lähetetään uudestaan. Vastaanottaja päättelee järjestysnumeron avulla onko kyseessä jo käsitelty sanoma vai uusi sanoma. Hyväksytty sanoma kuitataan vastaanotetuksi. Menetelmää käytetään mm. TCP-protokollassa. Toinen ARQ-menetelmä on NAK-sanomat (Negative AcKnowledgement. Lähettäjän saadessa NAK-sanoman viimeiseksi lähetetty sanoma lähetetään uudestaan. NAK-sanomaan voidaan liittää järjestysnumero, jolla kerrotaan mikä vastaanotetuista sanomista oli virheellinen. Ensimmäinen tapa aiheuttaa usein tarpeettomia viiveitä ajastetun toimintansa vuoksi ja se onkin TCP/IP-protokollan suurimpia ongelmia. NAK-sanomilla virheistä toipuminen tapahtuu välittömästi, kun virhe havaitaan.

FEC (Forward Error Correction) tarkoittaa kaikkia menetelmiä, jossa vastaanottaja korjaa siirtovirheen sanoman mukana tulevilla tiedoilla. Lähettäjä liittää siirrettävän tiedon mukana

korjausbittejä, joiden perusteella vastaanottaja päättelee onko jokin tietobiteistä tai korjausbiteistä muuttunut. Menetelmä ei kuitenkaan pysty korvaamaan ARQ-menetelmää, koska tietoa voi olla tuhoutunut liian paljon, joten sitä täydennetään esimerkiksi CRC-tarkistuksella [1].

Verkonhallintaprotokolla SNMP [12]

SNMP kehitettiin TCP/IP-protokollaa käyttävien verkkojen verkonhallintajärjestelmäksi. Sittemmin sitä on laajennettu käsittämään myös muut verkkoympäristöt. SNMP sisältää seuraavat osa-alueet:

- hallinta-asema (Management station)
- agentit (Management agents)
- hallintatietokanta (Management information base, MIB)
- varsinainen verkonhallintaprotokolla (Network management protocol) SNMP

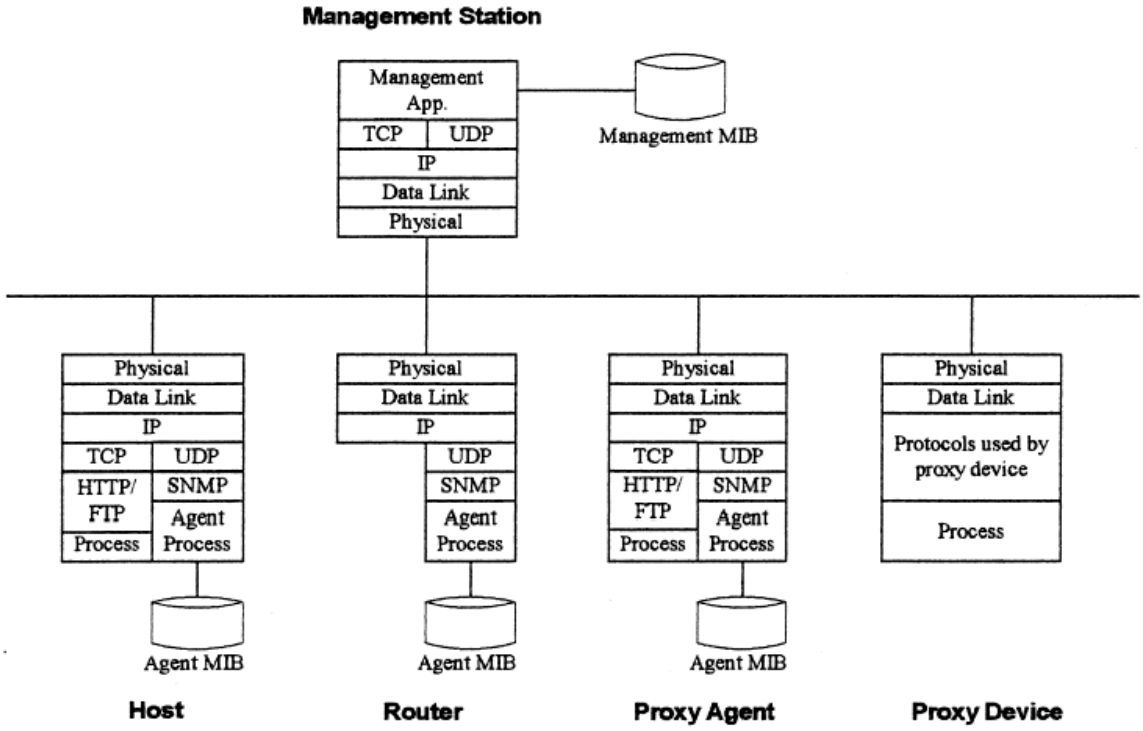
Hallinta-asema on käyttöliittymä ylläpitäjän ja verkonhallintajärjestelmän välillä. Hallinta-asema sisältää erilaisia sovelluksia datan analysointiin ja vioista toipumista varten, ylläpitäjän käyttöliittymän verkon monitorointia ja ohjausta varten, kääntäjän ylläpitäjän komentojen toteuttamiseksi verkon etäpäätteissä ja MIB:stä koostetun informaatiotietokannan kaikista verkon hallittavista kohteista. Agentit vastaavat hallinta-aseman tieto- ja toimintapyyntöihin ja lähettävät tärkeitä tietoja myös automaattisesti. Isäntäkoneet, sillat, reitittimet ja keskittimet voidaan varustaa SNMP:llä, jolloin niitä voidaan ohjata hallinta-asemalta.

Verkohallintaresurssit esitetään SNMP:ssä objekteina. Jokainen objekti on periaatteessa muuttuja, joka esittää hallittavan agentin piirrettä. Näiden objektien kokoelma on hallintatietokanta, MIB. Agenteilla on pääsy hallinta-asemaan MIB:n kautta. Hallinta-asema suorittaa valvontatoiminnon hakemalla MIB:stä objektien arvon. Hallinta asema voi toteuttaa komennon suoraan agentissa tai muuttaa agentin asetuksia muuttamalla haluttujen muuttujien arvoja.

Hallinta-asema ja agentit on kytketty toisiinsa verkonhallintaprotokollan välityksellä. SNMP sisältää kolme avainominaisuutta:

- Get-komennolla hallinta-asema noutaa agentin objektien arvot
- Set-komennolla hallinta-asema asettaa agentin objektien arvon
- Trap-komennolla agentti ilmoittaa hallinta-asemalle merkittävistä tapahtumista

Kuvassa 6 on esitetty SNMP-arkkitehtuuri

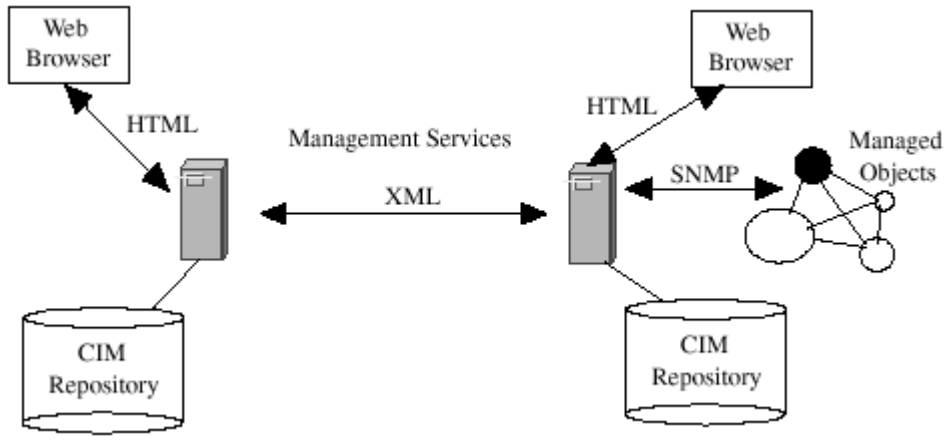


Kuva 6. SNMP:n periaate [17].

SNMP:stä on kehitetty useita versioita mm. SNMPv2 ja SNMPv3, jotka parantavat monia alkuperäisen version ominaisuuksia, esimerkiksi turvallisuusnäkökohtia, joita ensimmäisessä versioissa ei otettu juuri lainkaan huomioon. Tietoverkkojen koon kasvu on otettu huomioon SNMPv2:ta alkaen hajauttamalla verkonhallintaa useiden palvelimien kesken. Toistaiseksi yleisessä käytössä on edelleen versio 2, tosin myös versiota 3 on otettu jonkin verran käyttöön.

RMON kehitettiin laajenevien verkkojen tiedonkeruuongelmia varten. SNMP kerää keskitetysti tiedot kaikilta verkon asemilta. RMON puolestaan on asennettu aliverkkoihin, joissa se kerää tietoa aliverkon asemilta ja käsittelee raaka-datan tilastoiksi. Hallinta-asema lähettää kyselyn tarvittaessa verkon RMON-pisteille, joten hallinta-aseman ei tarvitse kerralla käsitellä yhtä suurta tietomäärää kuin keskitetyssä verkonhallinnassa. RMON pystyy käsittelemään vain alimpien protokollatasojen toimintoja. Tämän vuoksi on kehitetty RMON2, joka voi käsitellä myös protokollapinon ylempiä tasoja. RMON2:n avulla hallintajärjestelmä pystyy määrittämään tietoliikenteen tarkan lähtö- ja vastaanottopaikan.

Viimeisimpänä kehityssuuntauksena on ollut WBEM (Web-based enterprise management), joka käyttää mm. XML-kieltä ja HTTP-protokollaa tiedonsiirtoon asemien välillä (kuva 7). CIM-mallia (Common Information Model) käytetään hallittavien objektien kuvauksena. CIM-malli koodataan XML:n avulla sovellusten väliseen liikenteeseen sopivaksi ja HTTP-protokollaa käytetään hallintatiedonnoutamiseen hallintapalvelimilta hallinta-asemalle.

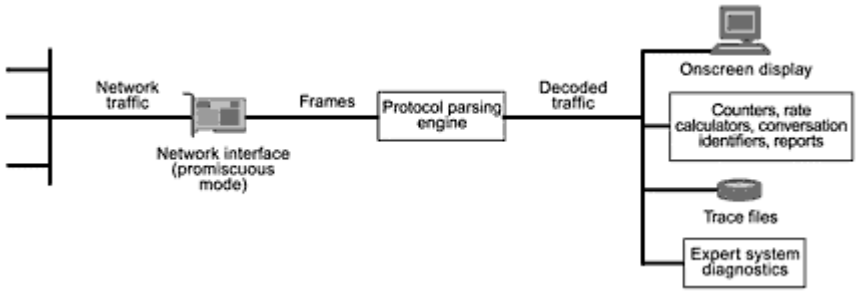


Kuva 7. WBEM-malli [17].

Vianetsintätyökalut

Tietoverkkojen ongelmien ratkaisuun on saatavilla monipuolisia vianetsintätyökaluja. Sähkövikojen etsintään tarkoitettu kaapelitestaaja voi sisältää kehittyneen aikatason heijastusmittarin ja digitaalisen signaaliprosessorin vikatilojen tarkkaan paikantamiseen ja laajan kaistanleveyden suorituskyvyn nopeaan tarkasteluun. Kannettavat vianetsintätyökalut yhdistävät, verkkokorttien, keskittimien ja kaapelintestauksen korkeamman tason protokollatestien kanssa (esim. Ping ja TraceRoute). SNMP-konsoleita on myös integroitu yksittäisiin laitteisiin, Web-palvelimiin ja kannettaviin diagnostiikkalaitteisiin, ja niitä käytetään verkon kokoonpanon ja dokumentaation työkaluina. Protokolla-analysaattoreita puolestaan käytetään kaikkein vaikeimpien ongelmien ratkaisuun.

Protokolla-analysaattori sieppaa kaiken liikenteen verkosta, jäsentää sen verkkoprotokollan sääntöjen mukaan ja näyttää tulokset (kuva 8). Protokolla-analysaattoreita käytetään eniten Ethernet-verkossa, mutta myös muissa verkkoratkaisuissa käytetään vastaavia työkaluja. Analysaattori kaappaa verkkokortin vastaanottamat kehykset ja tallentaa ne suureen RAM-puskuriin. Kaapatusta kehyksestä voidaan etsiä lähettäjän ja vastaanottajan MAC-osoitteet, jonka jälkeen ohjelma etenee protokollapinoa pitkin purkaen joka kerroksesta tarvittavat tiedot mm. verkko-osoitteet. Tämän jälkeen kaapattua liikennettä voidaan analysoida.



Kuva 8. Protokolla-analysaattorin toimintamalli [18].

Analysaattorilla voidaan tutkia pakettien järjestystä ja viiveiden kestoa, sillä ohjelma lisää joko absoluuttisen tai suhteellisen aikakoodin jokaiseen pakettiin. Kaapattua liikennettä voidaan suodattaa olennaisen tiedon etsimiseksi. Ohjelmisto pystyy myös kääntämään heksadesimaalidataa ASCII-tekstiksi. Lisäksi verkkonimet voidaan kääntää numeerisiksi verkko-osoitteiksi. Virhetilojen tunnistamiseen oireiden perusteella käytetään asiantuntijajärjestelmiä.

Kytkentäiset verkot ovat vähentäneet protokolla-analysaattorien mahdollisuuksia diagnostiikkatyökaluna. Analysaattori perustuu verkkokortin kykyyn toimia tilassa, jossa se voi kaapata myös muita kuin sille tarkoitettuja kehyksiä. Tämän vuoksi analysaattorin toiminta rajoittuu Ethernetin törmäysalueelle (tai reitittimeen tai siltaan). Kytkentäisessä Ethernet-verkossa analysaattori ei pysty kaappaamaan liikennettä ilman erityistä kaappausporttia kytkimessä. Usein kuitenkin protokolla-analysaattori on ainoa tapa paikantaa verkossa tapahtuvia virheitä [18].

6 Internet ja Intranet

Internet syntyi jo 1970-luvulla Yhdysvalloissa, mutta varsinaisesti sen laaja käyttöönotto tapahtui 1990-luvun puolivälissä WWW-selaimen keksimisen jälkeen. Internet on maailmanlaajuinen verkkojen verkosto. Internet yhdistää TCP/IP-koneet ja -lähiverkot IP-reitityksellä. Internet kuljettaa peruspalvelujen (Telnet, FTP) lisäksi HTTP- (Hypertext Transfer Protocol), IRC- (Internet Relayed Chat) ja RTP-liikennettä (Real Time Protocol). Tiedonsiirto internetissä perustuu TCP/IP-protokollapinoon, jossa kullakin internetiin liitetyssä/liitettävässä laitteella on oma IP-osoite. TCP/IP-protokollaa käytetään internetin lisäksi myös suljetuissa intraneteissä, jotka ovat yksityisiä tietoverkkoja [2].

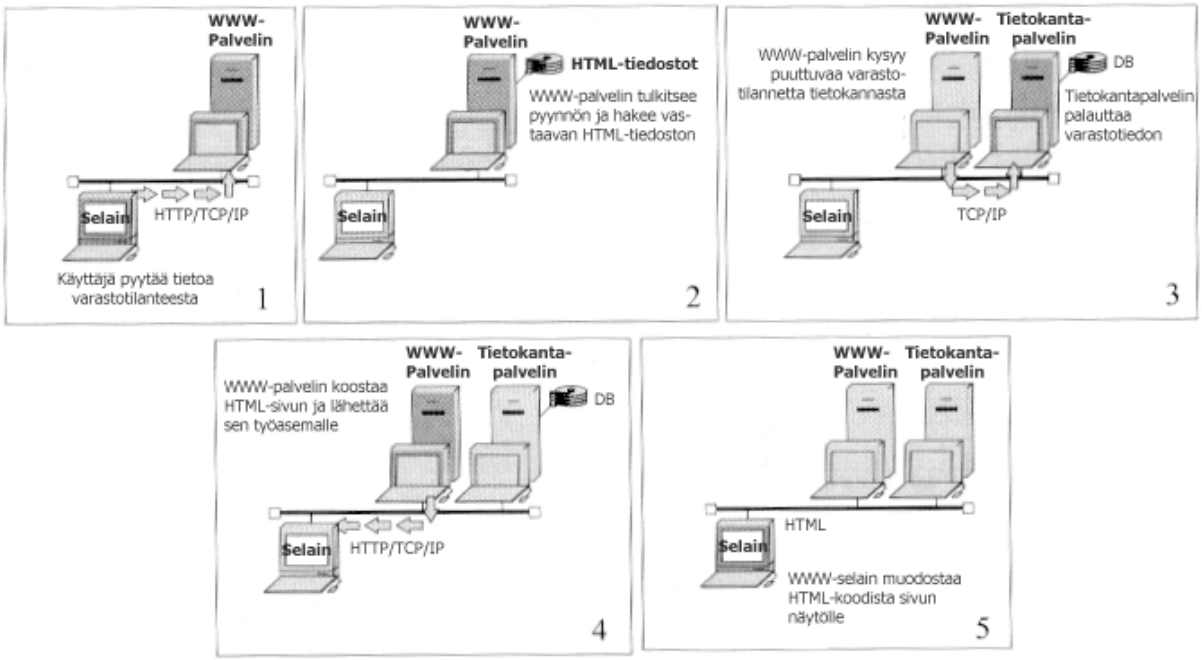
Internet koostuu seuraavista verkkojen ryhmistä [19]:

- runkoverkot, jotka koostuvat suurista verkoista, joilla liitetään pienempiä verkkoja yhteen
- alueelliset verkot, esimerkkinä yliopistojen väliset verkot
- kaupalliset verkot, jotka tarjoavat yhteyden runkoverkkoon tilauksesta ja lisäksi kaupallisten organisaatioiden omistamat verkot sisäiseen käyttöön, joista on myös yhteys internetiin
- paikallisverkot, esimerkkinä yritysten verkot tai kampusverkot.

Useimmiten liikennettä kaupallisten, sotilaallisten ja hallinnon verkkojen sekä muiden verkkojen välillä on rajoitettu.

Intranet-verkot ovat esimerkiksi yrityksen sisäisiä verkkoja, joissa käytetään julkisen internetin protokollia ja ratkaisuja tietojärjestelmien toteutukseen. Intranetin käyttöliittymänä on WWW-selain, jonka avulla käytetään eri sovelluksia, esimerkiksi sähköpostia tai tietokantaratkaisuja. WWW-järjestelmän toiminta on esitetty kuvassa 9. Käyttäjä pyytää tarvitsemaansa tietoa lähettämällä lomakkeen tai valitsemalla linkin WWW-sivulta. Selainohjelma välittää pyynnön WWW-palvelimelle HTTP-protokollana. Palvelin tunnistaa käyttäjän ja tulkitsee toimenpiteen HTML-tiedostoon kohdistuvaksi. Palvelin hakee pyydetyn tiedoston, tarkistaa käyttäjäoikeuden ja suorittaa HTML-koodissa olevan script-ohjelman.

Palvelin saattaa hakea tietoa myös muilta palvelimilta, jonka jälkeen se muodostaa tiedoista HTML-sivun, joka lähetetään työasemalle. Selain pyytää mahdollisia lisätietoja ja muodostaa WWW-sivun, jonka ulkoasu määräytyy selainohjelman ja käyttäjän asetusten mukaan [2].



Kuva 9. WWW-järjestelmä [2].

6.1 Ongelmatilanteet ja diagnostisointi

Viat ja niiden eristäminen

Internetin tietoliikenne perustuu useimmiten client-server-sovelluksiin. Viimeaikoina Internetiin on myös tullut hajautettuja sovelluksia ja palveluja, kuten video- ja audiopalveluja. Verkon dynamiikka (ohimenevät ruuhkat, reitin vaihdokset) vaikuttaa merkittävästi näiden palvelujen suorituskykyyn. Verkon dynamiikka ilmenee näissä sovelluksissa kadonneina tai viivästyneinä lähetyksinä. Nämä viat johtuvat usein reitittimen toiminnasta [20, 21].

Internetissä verkon dynamiikka on havaittavissa sovelluksissa datapakettien viiveen vaihteluna ja pakettien katoamisena. Verkonhallinnan kannalta olisi tärkeää pystyä paikantamaan reititin, jossa vika tapahtuu. Dynamiikka voi johtua ainakin kahdesta syystä. Reitittimen kuorman kasvaessa jonotusaika lisääntyy, mikä johtaa pakettien viiveen vaihteluun. Ohimenevissä ruuhkatilanteissa reititin saattaa "pudottaa" datapaketin, jolloin sovellus havaitsee sen paketin katoamisena. Toinen syy verkkodynamiikkaan on lähettäjän ja vastaanottajan välisen reitin muuttuminen, joka voi johtua esimerkiksi reitittimen tai linkin pettämisestä, reitittimen vääristä asetuksista tai reitittimen epävakaisesta tilasta. Dynaamiset ilmiöt vaikuttavat eri tavalla eri sovelluksiin. Esimerkiksi pitkien tiedostonsiirtojen yhteydessä tapahtuvat satunnaiset paketin katoamiset eivät välttämättä vaikuta juuri lainkaan tiedonsiirtoon. Toisaalta taas esimerkiksi audio- ja videokonferenssipalvelut voivat häiriintyä merkittävästi verkon dynamiikan vuoksi.

Yksi tapa eristää viat on luodata verkkoa vian havaitsemisen jälkeen. Esimerkiksi monilähetyksessä (multicast) traceroute-luotain pystyy selvittämään paketin katoamistiedot viestin reitiltä. Tämän tiedon avulla voidaan paikallistaa paketin häviämisestä vastuussa oleva reititin tai reitittimet. Vianeristysjärjestelmä voi kerätä tietoa yhdestä tai useasta verkon solmupisteestä ja käyttää tätä historiatietoa yhdessä reaktiivisen luotauksen kanssa vikojen eristykseen. Monet kaupalliset verkonhallintaohjelmistot, kuten IBM:n Netview, Hewlett-Packardin Openview, Sun Microsystemsin Solstice ja Cabletron Systemsin Spectrum keräävät keskitetysti tietoa mm. MIB:stä tai sovelluskohtaisista rajapinnoista. Näissä järjestelmissä yksi agentti hallitsee lähiverkkoa tai laitetta. Kaikki edellämainitut käyttävät RMONia mm. Ethernetin, TokenRingin, kytkimien tai keskittimien valvontaan. Kerättyä tietoa käytetään mm. reititinvikojen ja ruuhkaisten linkkien havaitsemiseen. Olemassa olevat järjestelmät eivät kuitenkaan välttämättä pysty eristämään vikoja esimerkiksi audiokonferenssisovelluksissa. Monitorireitittimet eivät pysty riittävästi korreloimaan paketin viiveen vaihtelua reitittimen toiminnan kanssa (reitin vaihdos, jonon muodostuminen). Lisäksi verkon dynamiikka vaikuttaa sovelluksiin monin eri tavoin. Keskusjohtoisesti toimivat verkonhallintajärjestelmät eivät luonnollisesti pysty skaalautumaan internetin kokoon, jossa on satoja tuhansia reitittimiä.

Kestäviä ja skaalautuvia verkonhallinnan menetelmiä ovat esimerkiksi:

1) *Julkaisu-kuuntelu,* jossa jokainen osapuoli julkaisee säännöllisesti yhteenvedon hajautetun tiedonkäsittelyn tilasta. Julkaisu lähetetään kaikille muille osapuolille ja vastaanottajat päivittävät tilaansa näiden yhteenvetojen perusteella. Menetelmä auttaa käsittelemään ryhmädynamiikkaa ja verkkodynamiikkaa.

2) *Empiirinin sopeutuminen,* jossa sovellukset mukauttavat käyttäytymistään verkon havaitun tilan mukaan. Esimerkiksi TCP:n lähetysikkuna mukautuu verkon ruuhkaan hävinneiden pakettien lukumäärän mukaan.

3) *Jaettu oppiminen,* joka liittyy molempiin edellämainittuihin. Skaalaava menetelmä, joka antaa hajautetun tiedonkäsittelyn jokaisen osapuolen oppia muilta osapuolilta joko verkon tilasta tai jostain muusta jaetun sovelluksen näkökohdasta.

Näitä periaatteita voidaan soveltaa erääseen verkonhallinnan menetelmään: verkkokarttojen hajautettuun keräämiseen. Verkkokartta on tietoverkkojen vianhallinnan tärkeä komponentti. Verkkokartalla tarkoitetaan graafista esitystä verkosta, jossa solmupisteet kuvaavat reitittimiä ja linkit kuvaavat lähekkäin olevia reitittimiä. Monet verkonhallintajärjestelmät pystyvät esittämään huomautuksilla varustettuja verkkokarttoja. Ohjelmisto voi liittää reitittimiin huomautuksia esimerkiksi pakettien katoamisen määristä, katkoksista, keskimääräisistä viiveistä, jne. Verkkokarttoja ei kuitenkaan voida suoraan käyttää tunnistamaan sovellusten aiheuittamia virheitä. Tieto virheen tapahtumisesta jossakin reitittimessä ei vielä kerro, mikä sovellus aiheutti vian.

Hajautetussa kartoituksessa käytetään ohjelmia, joita kutsutaan arvioijiksi (surveyor). Yksi tai useampia arvioijia sijoitetaan verkkoon. Jokainen arvioija etsii välittömässä läheisyydessään olevan verkon osan. Arvioijat koordinoivat keskenään, etteivät ne turhaan kartoita samaa verkon osaa uudelleen *(julkaisu-kuuntelu).* Jokainen arvioija määrittelee vaikutuspiirinsä ja kartoittaa sen sisällä olevan verkon alueen. Kartoitettu alue lähetetään myös muille arvioijille.

Vaikutuspiiri voidaan määritellä uudelleen, jos jokin arvioijista pettää. Arvioijat myös laajentavat vaikutuspiiriään tarpeen mukaan, esimerkiksi muiden arvioijien pettäessä *(empiirinen sopeutuminen)* [20].

Virheistä toipuminen

Reitittimien aiheuttama pakettien hävittämien ruuhkasta johtuen voidaan jakaa kahteen tapaukseen: yksittäiseen ja lyhyeen hävikkiin sekä pitempiaikaiseen hävikkiin. Yksittäisestä paketin häviämisestä voidaan toipua välivarastoreitittimien avulla (cache-router). Kun välivarastoreititin välittää luotettavan paketin, se kopioi sen omaan varastoonsa ja liittää pakettiin oman IP-osoitteensa. Kun jokin reititin joutuu ruuhkan vuoksi pudottamaan paketin jonosta, se lähettää paketista löytämäänsä välivarastoreitittimen osoitteeseen "drop"-viestin. Välivarastoreititin tutkii viestin saatuaan varaston ja jos paketti on tallella, lähettää sen uudelleen. Pitempiaikaista hävikkiä varten verkossa on puskuroivia reitittimiä (buffer-router), jossa on enemmän tallennuskapasiteettia kuin välivarastoreitittimissä. Jos välivarastoreititimellä ei ole tallella kadonnutta pakettia, se välittää drop-viestin puskurireititititimelle, joka lähettää kadonneen paketin uudelleen suoraan drop-viestin lähettäneelle reitittimelle. Jos puskurissakaan ei ole tallella kadonnutta pakettia puskuroiva reititin lähettää drop-viestin alkuperäiselle lähettäjälle, joka lähettää uudelleen paketin suoraan drop-viestin lähettäneelle reitittimelle [21].

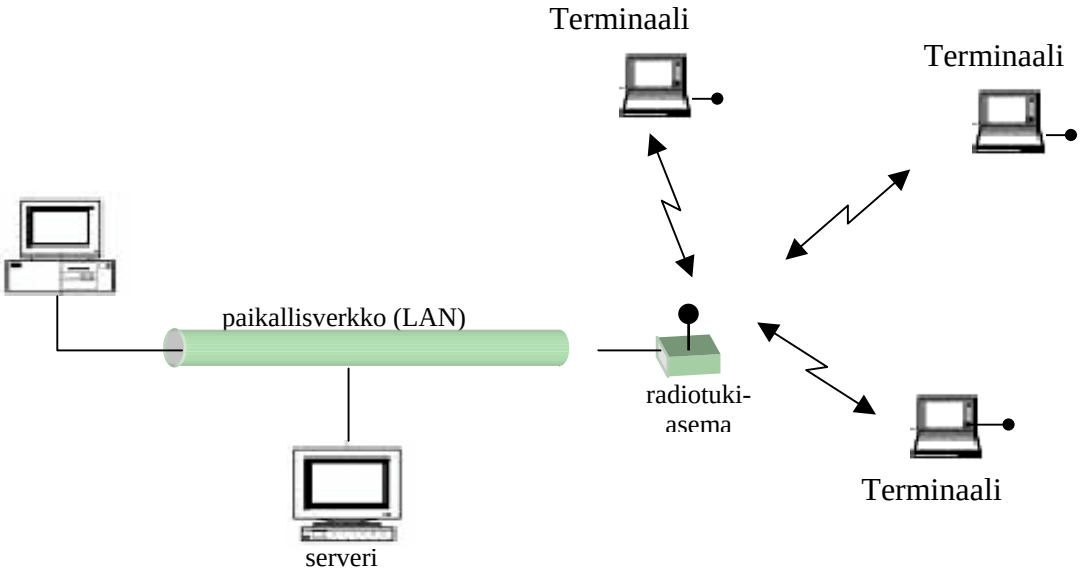
7 Langaton tiedonsiirto

7.1 Langaton lähiverkko

Tavallisissa lähiverkoissa tietoa siirretään kaapeleita pitkin verkkoon kytkettyjen päätelaitteiden ja verkkopalvelimen välillä. Kaapeleiden käyttö rajoittaa verkon joustavuutta, sillä verkkoon kytketyt laitteet pitää olla sekä verkkokaapelin läheisyydessä että fyysisesti kytkettävissä verkkokaapeliin. Tämä rajoittaa laitteiden liikuteltavuutta. Tilanteissa, jossa laitteiden pitää olla joustavasti liikuteltavissa verkon alueella tai jossa laite on kiinni pyörivässä kohteessa, on tarpeellista kytkeä laite langattomasti lähiverkkoon. Langattomassa lähiverkossa (WLAN, Wireless Local Area Network) tiedonsiirto tapahtuu pääasiassa vapailla, viranomaisluvista riippumattomilla radiotaajuuksilla. Langattomien paikallisverkkojen teknologia mahdollistaa laajakaistaisten, nopeiden yhteyksien käytön rajoitetuilla alueilla. Suurimmat tiedonsiirtonopeudet ovat tyypillisesti 2000 kbit/s. Langattomien lähiverkkojen kantavuus on yleensä 50 metristä 200 metriin [5, 6, 7].

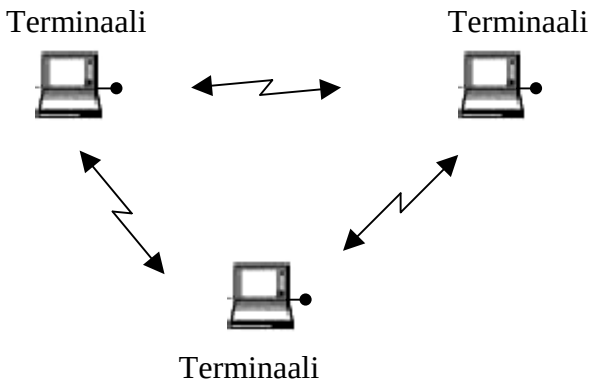
Langattomat lähiverkot voidaan jakaa kahteen perustyyppiin verkkoarkkitehtuurin mukaan. Arkkitehtuureja ovat kiinteään, langalliseen lähiverkkoon radiotukiasemalla liitetty langaton paikallisverkko sekä ad hoc verkko. Tyypillisin tapa toteuttaa langaton paikallisverkko on käyttää näistä ensin mainittua (kuva 10). Verkko on langallisen ja langattoman verkon yhdistelmä, jossa radiotukiasema huolehtii yhteyden ylläpitämisestä radioverkkoon kytkettyjen laitteiden kanssa. Langallisen verkkoliitännän vuoksi verkko voi olla hyvinkin laaja. Langallinen verkko liikennöi verkolle ominaisen liikenneprotokollan mukaisesti. Radioliikenne voidaan jakaa kahteen osaan, liikennöintiin joko langattomasta kiinteään

verkkoon (uplink) tai kiinteästä langattomaan (downlink) päin. Uplink-liikenne tapahtuu sovitun kanavallepääsytekniikan mukaan, jossa tunnistetaan ja rekisteröidään uudet, langattoman yhteyden päässä olevat laitteet. Downlink-liikennöinnissä käytetään tyypillisesti yhteistä kanavaa, jolla tieto siirretään radiotukiasemasta liikkuville pisteille [5,6,7].



Kuva 10. Langaton paikallisverkko liitettynä radiotukiaseman kautta kiinteään paikallisverkkoon (Jari Halme).

Ad-hoc-lähiverkossa kaikki verkon laitteet ovat irrallaan ja käyttävät tiedonsiirrossa ainoastaan langatonta tekniikkaa. Verkon muodostavat spontaanisti kuuluvuusalueella olevat päätelaitteet, jotka kommunikoivat suoraan toistensa kanssa (kuva 11). Yhteys päätelaitteiden välille voi rakentua ilman järjestelmänhallintaa. Tällainen verkkoarkkitehtuuri vaatii tehokasta mukautuvaisuutta, jotta verkon kuuluvuusalueella oleville päätelaitteille voidaan tarjota nopea ja joustava tiedonsiirtopalvelujen tarjonta. Ad-hoc-verkon rajoitteena on pieni kantavuus.



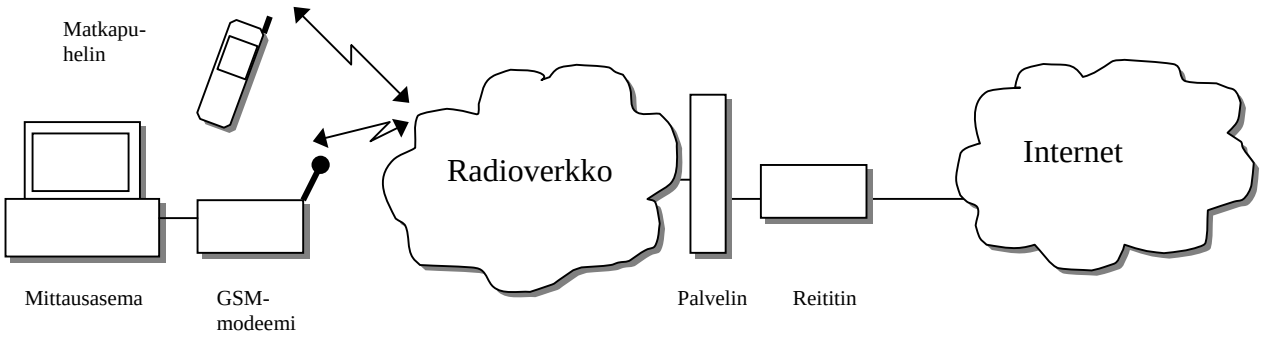
Kuva 11. Ad hoc tyyppinen langaton lähiverkko (Jari Halme).

Langattomien paikallisverkkojen radiolinkit toimivat tyypillisesti 2400 - 2500 MHz:n taajuuskaistalla. Myös 5300 MHz:n ja 5700 MHz:n taajuusalueille on tulossa tuotteita. Suuri

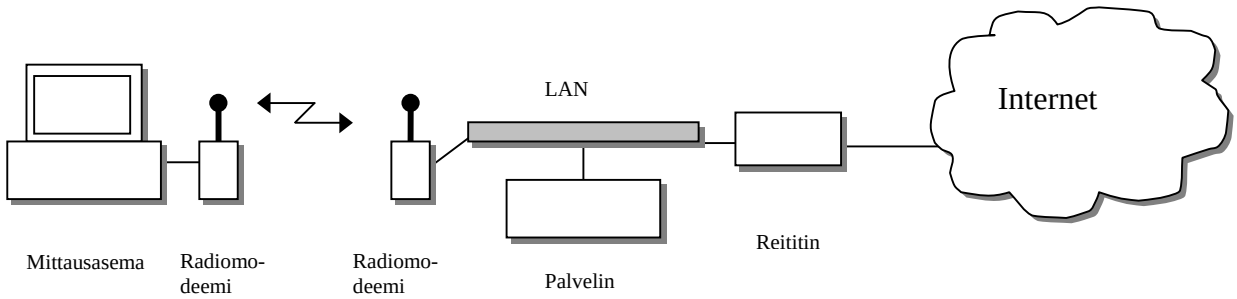
osa tuotteista on toteutettu hajaspektritekniikalla ja ne hyödyntävät joko suorasekvenssi- tai taajuushyppelytekniikkaa. Pääosa markkinoilla olevista tuotteista tukee 1 - 2 Mbit/s ja osa 10 Mbit/s tiedonsiirtonopeutta. Eri laitevalmistajien tuotteet eivät ole täysin yhteensopivia sekavan standardointikäytännön vuoksi. Tämän vuoksi eurooppalaisessa HIPERLAN- (High Performance Radio LAN) ja amerikkalaisessa IEEE 802.11-projekteissa on tehty standardointityötä, jossa tavoitteena on ollut parantaa eri laitevalmistajien ratkaisujen yhteensopivuutta. Standardien myötä WLAN-sovellusten määrän uskotaan kasvavan nopeasti [6,7].

7.2 Langaton Internet

Langaton yhteys internetiin voidaan toteuttaa useilla eri tavoilla [5, 6, 7, 10]. Matkapuhelimilla ja -viestimillä, joissa on datansiirto-ominaisuus, yhteys internetiin saadaan radioverkon kautta ottamalla yhteys internetiin liitetylle palvelimelle, joka reitittää viestin (kuva 12). Lisäksi samaan tapaan voidaan käyttää GSM-modeemeja. Käyttämällä valmistajakohtaisia radiomodeemeja langaton yhteys internetiin tapahtuu kahden tai useamman modeemin välillä, joista vähintään yksi on liitetty paikallisverkon tai suoraan puhelinverkon kautta palvelimelle, joka reitittää yhteyden internetiin (kuva 13).



Kuva 12. Matkapuhelinyhteys internetiin (Jari Halme).



Kuva 13. Radiomodeemiyhteys internetiin (Jari Halme).

Langaton tiedonsiirto internetin yli riippuu sekä langattoman yhteyden että internet-yhteyden nopeudesta. Näistä langaton yhteys on usein paremmin määriteltävissä. Esimerkiksi GSM verkossa nopeus on yleensä 9600 kbit/s tai 14.4kbits/s ja hajaspektritekniikkaan perustuvissa

erillisissä radiomodeemeissa laitteesta riippuen maksimissaan 115.2 kbit/s. Sen sijaan internet-yhteyden vasteaikaa ei voida määrittää tarkasti. On-line -mittauksissa joudutaan tyytymään vain noin 1 - 10 Hz:n nopeuteen. Lisäksi internet-yhteyksissä voi esiintyä yhteyskatkoksia ja dataa saattaa kadota matkalle. Samalla siirrettävä data kannattaa salata. Internet-pohjainen yhteys soveltuu tällä hetkellä parhaiten selainohjelmilla suoritettavaan mittausdatan monitorointiin sekä mittausdataa sisältävien tiedostojen siirtoon [5, 6, 7, 10].

7.3 Langattoman tiedonsiirron ongelmat ja diagnostisointi

Langattoman tiedonsiirron diagnostisointin ja verkonhallinnan periaatteet eivät poikkea merkittävästi kiinteän verkon sovelluksista. Vain tekninen toteutus on luonnollisesti erilainen. Langattomaan tiedonsiirtoon liittyviä erityispiirteitä ja -ongelmia aiheuttavat mm. seuraavat tekijät [21,22]:

- Mobiililaitteisiin liittyy epäluotettavuutta, koska mm. energiansaanti ja toiminta-aika ovat rajoitettuja.
- Mobiililaitteiden tiedonkäsittelyresurssit voivat vaihdella dynaamisesti.
- Verkkoinfrastruktuuri on dynaaminen, joten niiden topologiassa saattaa tapahtua jatkuvia muutoksia, esimerkiksi käyttäjien liikkuessa tai kulkeutuessa tukiasemien katteen ulkopuolelle.
- Langattomassa verkossa saman käyttäjän liittymä verkkoon vaihtelee (roaming)
- Langattomassa verkossa käytetään pääsääntöisesti kapeakaistaisia kapasiteetiltaan rajoitettuja radiolähetyksiä, jotka ovat alttiita häiriöille ja viiveille.
- Langattoman verkon ympäristö on hierarkinen, johon mobiilit päätelaitteet kiinnittyvät määrätyissä pisteissä. Kiinteän verkon hallintaan tarkoitetut järjestelmät eivät pysty käsittelemään "kerrostunutta" verkon rakennetta, koska langattomat verkot esitetään tasaisena (flat).

Langattoman verkon vikatilanne voi johtua yhden tai useamman verkon komponentin pettämisestä. Kriittisiä komponentteja ovat mm. kytkimet, tukiasemat, tietokannat, päätelaitteet ja langattomat linkit. Langattoman lähiverkon yleinen ongelma on radiosignaalin monitie-eteneminen lähetyspisteestä vastaanottopisteeseen. Tällöin eri reittejä tulleiden signaalien interferenssi voi sotkea informaatiota ja laskea oleellisesti verkon hyötysuhdetta. Lähettimien ja vastaanottimien sijainnin hallinnalla ja lähetyskeilojen suuntaamisella voidaan parantaa verkon hyötysuhdetta.

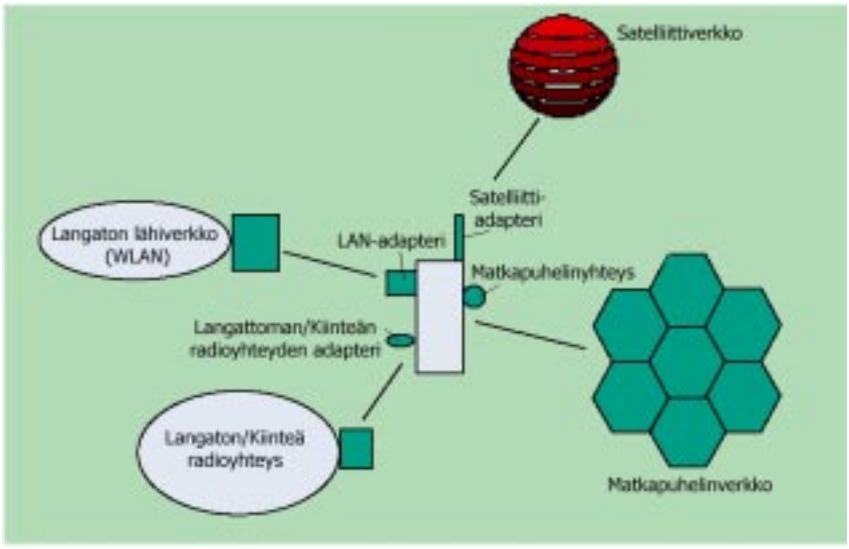
Langattoman verkon selvitymiskykyä vikatilanteesta voidaan parantaa monilla konfiguraatioilla ja arkkitehtuureilla, esimerkiksi Sonet Ring-tekniikalla, monitoimilaitteilla ja peittävillä verkoilla. Tukiasemien paremmalla arkkitehtuurilla voidaan tehostaa selviytymiskykyä parantamalla signaali-kohina-suhdetta, jolloin radiolinkkien vikatilanteet vähenevät [23].

Sonet Ring (Synchronous Optical NETwork Ring)

Rinnakkaisvarmennus on yksi tapa parantaa päästä-päähän-yhteyden (end-to-end-connection) luotettavuutta. Tämä voidaan tehdä käyttämällä vikasietoista Sonet Ringiä kytkentäisen verkon ja useiden tukiasemien linkittämiseen samalla alueella. Rengasmuotoinen verkko selviää yhden kaapelin katkoksesta tai yhden lähetin-vastaanottimen viasta, koska sanomat voidaan lähettää verkkorenkaassa kumpaan suuntaan tahansa.

Monikäyttö/monimoodi-laitteet

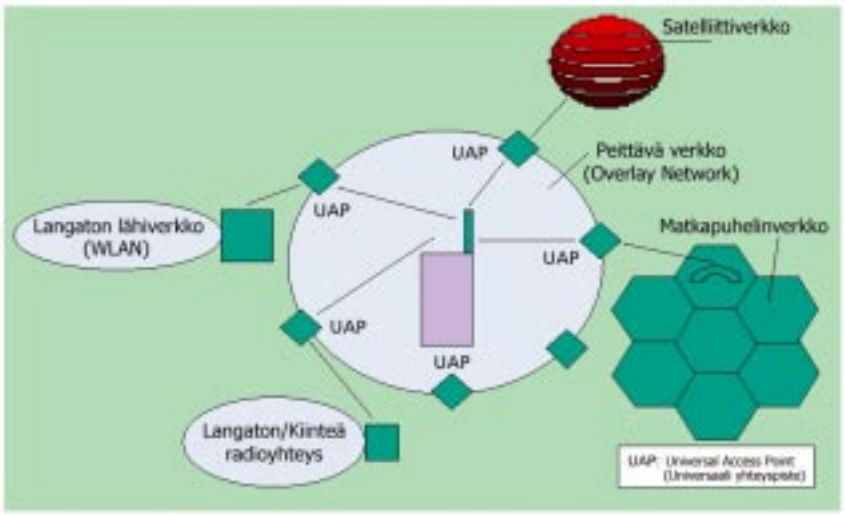
Toinen tapa parantaa verkon toipumista vikatilanteista on käyttää monitoimilaitteita, jossa yhdessä päätelaitteessa on monta liityntätapaa verkkoon, esimerkiksi kaksitoimiset matkapuhelimet (matkapuhelin/satelliittipuhelin). Arkkitehtuuri tarjoaa päällekkäisiä liitäntämahdollisuuksia, joilla varmistetaan langattoman toiminnan peitto verkon, linkin tai kytkimen vikatapauksessa (kuva 14). Jokaiseen päällekkäiseen verkoon on sijoitettu tietokanta, jonka avulla tarkkaillaan verkon olosuhteita sekä käyttäjän paikkaa, päätteen ominaisuuksia ja asetuksia. Tiedon avulla lähetettävät viestit mukautetaan kulloinkin käytössä olevan verkon ominaisuuksien mukaan.



Kuva 14. Monitoimilaitteen käyttö luotettavuuden parantamiseksi [23].

Peittävä verkko (Overlay network)

Käyttämällä peittävää verkkoa luotettavuutta voidaan paranta ja samalla verkon viat voidaan "kätkeä" käyttäjiltä (kuva 15). Peittävässä verkossa käyttäjä ottaa yhteyden universaalin yhteyspisteen kautta (Universal Access Point, UAP), joka valitsee käyttäjälle sopivimman yhteyden useista mahdollisista verkoista saatavuuden, halutun palvelun laadun ja käyttäjän toiveiden perusteella. UAP suorittaa protokollan ja taajuuden käännöksen sekä sisällön mukautuksen [23].



Kuva 15. Peittävän verkon käyttö luotettavuuden parantamiseksi [23].

Langattoman tiedonsiirron Päästä-Päähän (end-to-end) -luotettavuus ja selviytymiskyky

Langattomaan tiedonssirtoon liittyy useimmiten yhteys myös kiinteisiin verkkoihin. Kytkentä koostuu yleensä kiinteiden ja langattomien verkkojen ketjukytkennöistä. Päästä-päähän kytkennän luotettavuus riippuu ketjun heikoimmasta lenkistä, mikä on edelleen useimmiten lähetettävä radiosignaali. Radiosignaalin luotettavuutta on kuitenkin jatkuvasti parannettu. Keinoina on käytetty mm. parempia koodausmenetelmiä ja tukiasemien lisäystä. Taulukossa 1 on esitetty eri komponenttien luotettavuuden ja redundanssin eroja.

Taulukko 1. Päästä-päähän kytkennän komponenttien luotettvuus ja redundanssi [23].

Laite	**Kuvaus**	**Varmennettavuus (redundanssi)**
Yhteyslinkki	Paikallinen silmukka, kierretty parikaapeli, valokuitukaapeli, langaton yhteys	Huono tai olematon. Yksittäisillä käyttäjillä ei lainkaan redundanssia, korkean kapasiteetin linkeillä voi olla vaihtoehtoisia piirejä.
Kytkentäinen verkko	Kytkimien väliset kuituverkot, piirikytkentäiset tai ATM	Korkea. Tyypillisesti linkkien ja kytkimien suuri varmennettavuus yhteyksien nopean palautumisen varmistamiseksi vikatilanteissa
Kytkentäisen verkon ja tukiaseman välinen linkki	Monikanavainen mikroaaltolähetin tai monikanavainen valokuituyhteys	Matala. Lähetystien katkeaminen (radiosignaalin tai kaapelin katkos) aiheuttaa linkin katkoksen. Voivat sisältää nopeasti käynnistettäviä varajärjestelmiä.
Tukiasema	Kytkin ja radiotaajuuden vastaanotin	Matala. Voi sisältää akkuvarmennuksen ja joitkin nopeasti käynnistyviä varaelektroniikkajärjestelmiä
Langaton linkki	Tietyn maantieteellisen alueen kattava radiotaajuustie	Huono tai olematon. Ei varmennettavuutta ellei ole toisiaan peittäviä langattomia verkkoja

Kytkentöjen komponenttien luotettavuus lisää koko verkon luotettavuutta. Yhteys- ja radiolinkeissä olisi mahdollista lisätä kaksoisvarmennusta, mutta näin ei yleensä ole tehty johtuen taloudellisista seikoista ja kaistanlaajuuden rajoituksista [23].

8 Yhteenveto

Tietoverkkojen hallinta on käynyt entistä monimutkaisemmaksi verkkojen koon ja tiedonsiirtonopeuksien kasvaessa. Verkonhallintaan on kehitetty monia menetelmiä, protokollia ja ohjelmistoja. Laajojen verkkojen hallinta on kuitenkin vasta ottamassa ensiaskeleitaan, vaikkakin joitakin ehdotelmia verkonhallinta-arkkitehtuuriksi on esitetty. Reaaliaikaisten sovellusten käyttöönotto on korostanut vianhallinnan merkitystä entisestään. Verkonhallintaa on pyritty automatisoimaan kehittämällä ns. älykkäitä agentteja. Agentit ovat ohjelmia, jotka keräävät tietoa verkon eri pisteistä ja lähettävät nämä tiedot hallinta-asemalle. Agenttien "älykkyyttä" ja automaatioastetta on pyritty kehittämään, jotta ihmisen osuus verkon hallinnassa saataisiin mahdollisimman pieneksi. Pelkkä nykyisten tietoverkkojen laajuus estää usein ihmisen suorittaman tehokkaan verkonhallinnan. Verkonhallintaa ollaan pyritty myös siirtämään keskusjohtoisesta hallinnasta hajautettuun hallintaan. Hajautettujen järjestelmien käyttöönotto Internetin diagnostisoimiseen on vielä alkutekijöissään, mutta todennäköisesti lähi vuosina valvontatekniikat kehittyvät nopeasti.

Kiinteistä verkoista ollaan siirtymässä osittain langattomiin verkkoihin, vaikkakin runkoverkot pysynevät nopeamman tiedonsiirtokapasiteettinsa ansiosta perusverkkoratkaisuna vielä pitkään. Käyttäjän yhteys runkoverkkoihin ja lähiverkkoihin voidaan toteuttaa langattomasti ja näin on jo osittain tehtykin. Internetin nopea ja halpa käyttömahdollisuus joko matkapuhelimen kautta tai kannettavan päätelaitteen (esim. kannettava tietokone tms) on seuraava edistysaskel tiedonsiirrossa. Ratkaisuja on jo tällä hetkellä olemassa, mutta niiden käyttöä ovat toistaiseksi rajoittaneet kalliit yhteydet ja tiedonsiirron hitaus.

TCP/IP ja Ethernet tulevat pysymään tiedonsiirron perusratkaisuina lähiverkoissa ja Internetissä vielä pitkään, tämän takaa nykyinen valtava käyttäjämäärä. On kuitenkin vaikea ennustaa, mitkä ovat tulevaisuuden verkkoratkaisut. Tietotekniikassa on usein käynyt niin, että paras ratkaisu ei olekaan menestynyt, vaan käyttäjät ovat syystä tai toisesta valinneet jonkun muun ratkaisun. Kilpailevia protokollia ja arkkitehtuureja vianhallintaan on niin monta vielä tällä hetkellä, että aika näyttää mikä tai mitkä niistä tulevat laajempaan käyttöön. Esimerkiksi langatonta yhteyttä Internettiin ollaan toteuttamassa useilla kilpailevilla menetelmillä (matkapuhelin vs. kannettavat päätelaitteet). Useat rinnakkaiset ja kilpailevat menetelmät vaikeuttavat entisestään tietoverkkojen kunnonvalvontaa ja diagnostiikkaa. Palvelujen käyttäjien vaatimukset riittävästä palvelutasosta ja palvelujen jatkuva lisääntyminen sekä monimutkaistuminen asettavat erityisiä haasteita tietoverkkojen luotettavuudelle ja sen seurannalle.

Lähdeluettelo

[1] Granlund, K. 1999. Tietoliikenne. Jyväskylä: Teknolit Oy. 352 s.

[2] Puska, M. 1999. Lähiverkkojen tekniikka – Pro Training. Helsinki: Suomen ATK kustannus Oy. 318 s.

[3] Schofield, M. Controller Area Network (CANbus). [viitattu 26.02.2001]
Saatavilla: http://www.omegas.co.uk/CAN/

[4] Uotila, P. 1997. Tietoliikenteen tekniikka - verkot ja protokollat. Helsinki: Suomen ATK-kustannus Oy. 225 s.

[5] RAD Company Online page. [verkkodokumentti] The Wireless LANs Page [viitattu 30.12.1999] Saatavilla: http://www.lifewell.co.il/

[6] Aho, P., Martiskainen, T., [verkkodokumentti] Langaton lähiverkko. Seminaarityö. [viitattu 31.12.1999] Saatavilla: http://www.carelia.scp.fi/

[7] Saaranen, M., Mähönen, P., Langattomat lähiverkot. Multimediaa radioaalloilla. Prosessori maaliskuu 1998. s. 71 -73.

[8] Wikström, K., Nettiliittymä kaikkeen: www.sulautettukone.fi. Prosessori joulukuu 1999. s. 36 - 42.

[9] TCP/IP Online document. [verkkodokumentti] TCP/IP Frequently Asked Questions [viitattu 15.12.1999] Saatavilla: www.itprc.com/tcpipfaq/

[10] Suominen, J., Langattomat mittausjärjestelmät. Teollisuuden internet-pohjaiset mittausjärjestelmät. Dosesoft Oy:n seminaari 2.12.1999, Hyvinkää. Seminaarijulkaisu.

[11] Hood, C.S., Ji, C. 1997. Proactive Network Fault Detection. Proceedings of 16th IEEE Annual Conference on Computer Communications (INFOCOM), vol. 3, 4 – 7 joulukuuta 1997, Kobe, Japani. New Jersey: IEEE. S. 1147 – 1155.

[12] Stallings, W. 1997. Local & Metropolitan Area Networks, 5th ed. New Jersey: Prentice Hall. 605 s.

[13] Aboelela, E., Douligeris, C. 1999. Fuzzy Temporal Reasoning Model for Event Correlation in Network Management. Proceedings of 24th Conference on Local Computer Networks (LCN´99), 18 – 20 lokakuuta, 1999, Lowell, MA, USA. New Jersey: IEEE. S. 150-159

[14] Choi, T., Tang, A. 1995. Enterprise Network Management: LAN Status Monitoring. IEEE International Conference on Communications, vol. 3, 22 – 18 kesäk. 1995, Seattle, WA, USA. New Jersey: IEEE. S. 1448 – 1452.

[15] Rao, M., Yang, Haibin., Yang, Heming. 1998. Integrated distributed intelligent system architecture for incidents monitoring and diagnosis. Computers in Industry, vol. 37, nro. 2, s. 143 – 151.

[16] Lo, C.-C., Chen, S.-H. 1999. A scheduling-based event correlation scheme for fault identification in communications network. Computer Communications, vol. 22, nro. 5. s. 432 – 438.

[17] King, A., Hunt, R. 2000. Protocols and architecture for managing TCP/IP network infrastructures. Computer Communications, vol. 23, nro. 16, s. 1558 – 1572.

[18] Steinke, S. 1999. Protocol analyzers. Network Magazine, June 1999, [viitattu 09.05.2001]
Saatavilla: www.networkmagazine.com/article/NMG20000724S0052

[19] Murhammer, M.W., Atakan, O., Bretz, S., Pugh, L.R., Suzuki, K., Wood, D.W. 1998. TCP/IP Tutorial and Technical Overview. IBM Corporation.. 720 s. [viitattu 09.05.2001]
Saatavilla: www.redbooks.ibm.com/pubs/pdfs/redbooks/gg243376.pdf

[20] Reddy, A., Estrin, D., Govindan, R. 2000. Large-Scale Fault Isolation. IEEE Journal on selected areas in communications, vol. 18, nro. 5. s. 733 – 743.

[21] Ahola, K., Mölsä, J., Valtari, K. 1999. Taktinen Internet. MATINENn raporttisarja A, 4/1999. Helsinki: Maanpuolustuksen tieteellinen neuvottelukunta MATINE. 34 s.

[22] Network Management in a Wireless Environment. [viitattu 09.05.2001]
Saatavilla: www.symbol.com/products/whitepapers/whitepapers_network_mgmt_in_wi.html

[23] Snow, A.P., Varshney, U., Malloy, A.D. 2000. Reliability and survivability of wireless and mobile networks. IEEE Computer Magazine, vol 33(7), July 2000. New Jersey: IEEE. s 49 - 55.