Kalle Lonka

Fingridin tietoliikenneverkon hallintajärjestelmän uusiminen

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikka

Insinöörityö

28.11.2016

Metropolia

Tekijä(t) Otsikko Sivumäärä Aika	Kalle Lonka Fingridin tietoliikenneverkon hallintajärjestelmän uusiminen 47 sivua 28.11.2016
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoverkot / Tietoliikenne
Ohjaaja(t)	Tietoliikennepäällikkö Ari Silfverberg Lehtori Marko Uusitalo

Tässä insinöörityössä tutkitaan, mitä kaikkea tulisi ottaa huomioon, kun lähdetään hankkimaan uuttaa tietoliikenneverkon hallintaan ja valvontaan tarkoitettua verkonhallintajärjestelmää.

Aluksi perehdytään, mitä verkonhallinta on yleisellä tasolla. Tämän jälkeen käydään läpi, mitä kaikkia eri komponentteja verkonhallintajärjestelmä voi pitää sisällään sekä tutustutaan muutamaan yleisesti käytettyyn verkonhallinnan protokollaan.

Työssä kerrotaan, mitä eri tiedonsiirtotekniikoita Fingrid Oyj:llä on käytössään, ja lopuksi selitetään, millainen on nykyinen Fingridin verkonhallintajärjestelmä sekä mitä ominaisuuksia se pitää sisällään.

Käytännön osuudessa määritellään Fingrid Oyj:n ominaisuuksien vaatimukset uutta verkonhallintajärjestelmää varten.

Avainsanat	Verkonhallintajärjestelmä, Verkonhallinta, SNMP,PDH, SDH, MPLS, NMS10, Q1

Author(s) Title Number of Pages Date	Kalle Lonka Replacement of the Fingrid's communication network management system 47 pages 28 November 2016
Degree	Bachelor of Engineering
Degree Programme	Information technology
Specialisation option	Telecommunications
Instructor(s)	Telecommunication Manager Ari Silfverberg Senior Lecturer Marko Uusitalo

This thesis covers what should be taken into account when starting to acquire a new network management system. The study starts by introducing network management. Next it goes through different components a network management system can include, as well as a couple of commonly used network management protocols.

In addition, the study presents the different communication techniques Fingrid Oyj has in use, and finally describes the current network management system and its specialties within.

The practical part of the study defines Fingrid Oyj's feature requirements for a new network management system.

Keywords	Network management system, Network management, SNMP, PDH, SDH, MPLS, NMS10, Q1

Sisällys

Alkulause

Tämä insinöörityö tehtiin Fingrid Oyj:lle. Haluan kiittää kaikkia työssä mukana olleita.

Helsinki 28.11.2016

Kalle Lonka

Lyhenteet

ADM	Add/drop multiplexer. Syöttö-pudotus multiplekserillä pystytään pudottomaan tulevasta ylemmän tason signaalista tai syöttämään lähtevään ylemmän tason signaaliin alemman tason signaaleja.
ADX	Active digital cross Connect. Aktiivinen ristikytkentälaite on kehittyneempi versio DXC:stä.
ATM	Asynchronous Transfer Mode. Asynkroninen tiedonsiirtotapa.
AU	Administrative Unit. AU-osoitin on hallintayksikkö STM-kehyksessä.
AUG	Administrative Unit Group. Hallintayksiköistä muodostettu ryhmä.
CLI	Command line interface. Komentorivi.
CMIP	Common Management Information Protocol. OSI-protokolla verkonhallintaan.
CMOT	CMIP over TCP/IP. Alkuperäinen standardi, mitä oli tarkoitus käyttää TCP/IP-verkkojen hallintaprotokollana.
DES	Data Encryption Standard. Tiedon salaukseen tarkoitettu protokolla.
DXC	Digital Cross-Connect. Synkronisella ristikytkentälaitteella yhdistetään virtuaalikontteja.
FCAPS	ISO:n määrittelemä malli verkonhallintaa varten.
FE	Functional Entity. Yksikkö, joka on itsenäinen osa valvottavaa laitetta.
HEMS	High-level Entity-Management. Vanha verkonhallintaprotokollakokeilu.

IETF	Internet Engineering Task Force. Organisaatio, joka standardoi internet-protokollia.
ISO	International Organization for Standardization. Kansainvälinen standardoimisjärjestö.
ITU-T	Telecommunication Standardization Sector of the International Telecommunication Union. Kansainvälinen televiestintäliitto, jonka päätehtäviin kuuluu mm. standardointi.
LER	Label Edge Router. MPLS-verkossa toimiva reunareititin.
LSP	Label Switched Pad. MPLS-verkossa määritetty reitti.
LSR	Label Switching Router. MPLS-verkossa toimiva runkoreititin.
MIB	Management Information Base. Hierarkkinen tietokanta verkonhallinnassa.
MPLS	Multiprotocol Label Switching. Monia eri protokollia tukeva leimakytkentäinen protokolla.
MSOH	Multiplexer Section Overhead. Multipleksointiväliotsikko STM-kehyslukituksessa.
NE	Network Element. Verkossa oleva laite.
NM	Node Manageri. Erillinen ohjelmisto, jolla nodeja eli laitteita pystytään konfiguroimaan. Esimerkiksi Nokian Macro STE.
NMS10	Nokian kehittämä verkonhallintajärjestelmä.
Node	Verkon solmu eli verkossa sijaitseva laite.
OSI	Open Systems Interconnection. Kuvaa tiedonsiirtoprotokollien yhdistelmää seitsemässä kerroksessa.

PCM	Pulse Code Modulation. Tekniikka, jolla analoginen signaali koodataan digitaaliseen muotoon.
PDH	Plesiochronous Digital Hierarchy. Tiedonsiirtotekniiikka.
PDU	Packet Data Unit. Yhteyskäytännön viesti.
POH	Parh Overhead. Ensimmäinen osa reittiotsikkoa STM-kehyslukituksessa.
Q1	Nokian kehittämä protokolla.
RMON	Remote Network Monitoring. SNMP:n laajennus, jonka on tarkoitus suorittaa etävalvontaa.
RSOH	Regenator Section Overhead. Toistinväliotsikko STM-kehyslukituksessa.
SDH	Synchronous Digital Hierarchy. Tiedonsiirtotekniiikka.
SNMP	Simple Network Management Protocol. Verkonhallintaa varten standardoitu protokolla.
SMI	Structure Management Information. MIB:issä käytetty tietorakenne.
SOH	STM-kehyksessä oleva otsikkoalue.
SONET	Synchronous Optical Network. SONET on määritellyt synkronisen tiedonsiirtotavan ja sen perusnopeudet. SDH perustuu tähän standardiin.
STM	Synchronous Transport Module. Synkroninen siirtokehys, johon SDH perustuu.
TCP	Transmission Control Protocol. Tietoliikenneprotokolla.
TDM	Time Division Multiplexing. Aikajakokanavointi.

TU	Tributary Unit. TU-osoitin on aliyksikkö STM-kehyksessä.
UDP	User Datagram Protocol. Yhteydetön tiedonsiirtokäytäntö.
USM	User-based Security Model. SNMPv3 käyttää USM:ää viestien salaukseen ja autentikointiin.
VACM	View-based Access Control Model. SNMPv3 käyttää VACM-tekniikkaa siihen, kuka pääsee muokkaamaan MIB-tietokantaa.

1 Johdanto

Nykyisin tietoliikenneverkot ovat usein maantieteellisesti laajoja ja niihin on kytkettyinä satoja, ellei jopa tuhansia erilaisia, usein myös eri valmistajien laitteita. Tämäntyyppisten verkkojen hallinta käsin on lähes mahdotonta tai vaatisi ainakin erittäin suuria resursseja. Tästä syystä verkkojen hallintaan tarvitaan automatisoituja verkonhallintajärjestelmiä.

Tässä insinöörityössä tutkitaan, mitä kaikkea tulisi ottaa huomioon, kun lähdetään hankkimaan uutta tietoliikenneverkkojen hallintaan ja valvontaan tarkoitettua verkonhallintajärjestelmää. Aluksi perehdytään, mitä verkonhallinta on yleisellä tasolla, jonka jälkeen käydään läpi, mitä kaikkia eri komponentteja verkonhallintajärjestelmä voi pitää sisällään, sekä tutustutaan muutamiin yleisesti käytettyihin verkonhallinnan protokolliin.

Työssä kerrotaan, mitä eri tiedonsiirtotekniikoita Fingrid Oyj:llä on käytössään. Lopuksi selitetään, millainen on nykyinen Fingridin verkonhallintajärjestelmä sekä mitä ominaisuuksia se pitää sisällään.

Lopuksi määritellään yleisellä tasolla Fingrid Oyj:n vaatimukset uutta verkonhallintajärjestelmää varten ja näiden perusteella laaditaan tarjouspyynnöt etukäteen valituille yrityksille, jotka pystyvät tarjoamaan nämä vaatimukset täyttävän verkonhallintajärjestelmän. Verkonhallintajärjestelmän hankinta on käynnistymässä tämän työn aikana.

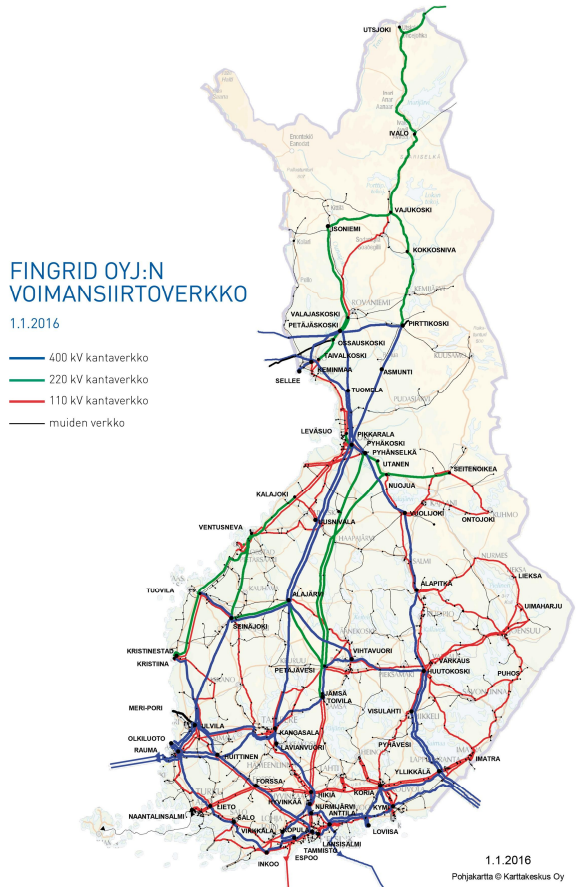
2 Verkonhallinta ja valvonta

2.1 Yhtiön esittely

Fingrid Oyj on Suomen kantaverkkoyhtiö, joka vastaa sähkönsiirrosta kantaverkossa. Kantaverkko on koko maanlaajuinen ja näin ollen keskeinen osa Suomen sähköjärjestelmää. Kantaverkkoon on liittyneenä pääosin kaikki suuret sähköntuottajat, huomattavat sähkönkuluttujat kuten tehtaat sekä alueellisten sähköyhtiöiden jakeluverkot.

Fingridin kantaverkko on myös osa yhteispohjoismaista sähköjärjestelmää, joka on kytketty Keski-Euroopan järjestelmään tasavirtayhteyksin. Lisäksi Suomesta on tasavirtayhteydet Venäjälle ja Viroon.

Kantaverkkoon kuuluu 400, 220 ja 110 kilovoltin voimajohtoja yli 14 000 kilometriä sekä yli sata sähköasemaa.



Kuva 1. Fingrid Oyj:n voimansiirtoverkko (1).

2.2 Verkonhallinnan määrittely

Nykyisin hajautetut järjestelmät sekä tietoliikenneverkot ovat huomattavasti suurempia ja monimutkaisempia kuin esimerkiksi 40 vuotta sitten. Tämäntyyppisissä verkoissa voi olla paljon eri laitevalmistajien laitteita, ja laitteiden kappalemäärät voivat nousta satoihin jopa tuhansiin, jolloin manuaalisesti tehtävä verkonvalvonta on mahdotonta tai ainakin erittäin hankalaa toteuttaa. Näiden verkkojen hallinta vaatii käyttöönsä erilaisia automatisoituja verkonhallintajärjestelmiä. (2.).

Verkonhallinta on myös erittäin tärkeää yritysten liiketoiminnan kannalta, koska tietoliikenneverkon toimimattomuus voi aiheuttaa suuria ongelmia esimerkiksi tiedon siirrossa ja tämä mahdollisesti aiheuttaa suuria taloudellisia menetyksiä yrityksille. Kuitenkin verkonhallintaan tehtävien investointien täytyy olla liiketoiminnan kannalta suhteessa siitä saatavaan hyötyyn. (2.)

Verkonhallinnan tarkoituksena on vähentää vian havaitsemiseen ja vikatilanteissa vian korjaamiseen tarvittavaa aikaa sekä parhaimmillaan ehkäistä vikatilanteet kokonaan antamalla järjestelmän ylläpitäjälle reaaliaikaista tietoa tietoliikenneverkon tilasta.

Kansainvälisen standardointiliitto ISO:n (International Organization for Standardization) FCAPS-mallin määrittelemät avainalueet verkonhallinnassa ovat vikojen hallinta (Fault Management), kokoonpanon hallinta (Configuration Management), käytön hallinta (Accounting Management), suorituskyvyn hallinta (Performance Management) ja turvallisuuden hallinta (Security Management). (2.)

2.3 Vikojen hallinta

Vikojen hallinnalla (Fault Management) tarkoitetaan sitä, että pystytään havaitsemaan vikaantuneet laitteet verkossa ja paikallistamaan, missä päin verkkoa ne sijaitsevat. Vikaantuneet laitteet täytyy eristää verkosta, niin etteivät ne aiheuta ongelmia koko verkon toimintaan. Tämän jälkeen pyritään selvittämään mistä vika on johtunut ja tarvittaessa vaihtamaan vikaantuneet laitteet ja tekemään konfiguroinnit uudelleen, jotta verkko saadaan palautettua alkuperäiseen tilaansa. (2.)

Vikojen hallinta parantaa huomattavasti verkon luotettavuutta, koska parhaimmillaan verkon ylläpitäjä pystyy reagoimaan vikatilanteisiin ja korjaamaan ne ennen kuin verkkoon tulee suurempia katkoja. Tämä voidaan toteuttaa ottamalla verkosta erilaisia lokitiedostoja, hälytyksiä ja tilastoja. Nämä toiminnot, eivät kuitenkaan saa viedä liikaa verkon suorituskykyä. (2.)

Verkko olisi kuitenkin hyvä rakentaa käyttämällä kahdennettuja komponentteja tai ainakin niin, että vaihtoehtoisia tietoliikennereittejä olisi aina käytettävissä. Tällä tavoin vikojen vaikutukset ja kesto voidaan minimoida. (2.)

2.4 Kokoonpanon hallinta

Kokoonpanon hallinnan (Configuration Management) tärkeimpänä tehtävänä on ajaa tarpeen vaatiessa verkko, tai jokin sen osista, hallitusti alas ja käynnistää uudestaan. Tehtävään sisältyy myös laitteiden välisten riippuvuuksien, ohjelmistoversioiden ja konfiguraatiotietojen ylläpitäminen, lisääminen sekä päivittäminen. Laitteista saadut tiedot auttavat huomattavasti, kun halutaan muuttaa verkon loogista rakennetta tai tehdä verkon uudelleen konfigurointia. (2.)

Laajoissa verkoissa on hyvä tietää, mitä laitteita niihin on kytketty ja mitä ne pitävät sisällään, jolloin vikatilanteiden selvittäminen helpottuu. Esimerkiksi voi tulla tilanteita, että verkkoon kytketyillä laitteilla on eri ohjelmistoversioita, jolloin laitteet eivät välttämättä

keskustele keskenään. Tämän tyyppisessä tilanteessa on hyvä tietää, mitä ohjelmistoversiota laitteet sisältävät, jotta voitaisiin päivittää ohjelmistoversiot toisiaan tukeviksi. (2.)

2.5 Käytön hallinta

Käytön hallinnalla (Accounting Management) on tarkoitus saada tietoa verkon todellisesta resurssien ja palvelujen käytöstä. Ylläpitäjän on kyettävä määrittelemään tieto siitä, mitä tietoa kerätään, mistä sitä kerätään ja kuinka usein tieto kerätään. Tällöin pystytään havaitsemaan laitteet, jotka käyttävät turhaan resursseja, tai päinvastoin laitteet, jotka tarvitsevat lisää resursseja. Tällöin pystytään jakamaan resursseja sinne päin verkkoa missä niitä todellisuudessa tarvitaan lisää. Käytönhallinnasta saadaan myös tukea, kun suunnitellaan verkon laajennusta. Laajennusta tehtäessä pitää tuntea riittävän tarkasti, mitä yhteyksiä ja palveluita on käytössä ja mihin kapasiteettia tai uusia yhteyksiä tarvitaan lisää. (2.)

2.6 Suorituskyvyn hallinta

Suorituskyvyn hallinnan (Performance Management) tehtävänä on kerätä ja analysoida tietoa verkon suorituskyvystä. Se muodostuu kahdesta osa-alueesta, jotka ovat valvonta (monitoring) ja hallinta (controlling). Valvonnalla tarkoitetaan verkon liikenteen tarkkailua ja hallinnalla on tarkoitus tarjota välineet verkon asetusten konfigurointia varten, jotta verkon suorituskyky saadaan mahdollisimman tehokkaaksi. Hallinnan tehtävä on osittain sama kuin kokoonpanon hallinnan tehtävä, mutta se on enemmän hienosäätöä kuin kokoonpanon hallinnassa. (3, s. 310.)

Suorituskyvyn hallinnalla ylläpitäjä saa erittäin tärkeitä tietoja verkon tilasta, kuten mitkä ovat keskimääräiset ja huonoimmat vasteajat, mikä on sen hetkinen verkon palvelujen luotettavuus ja kuinka paljon verkossa on törmäyksiä suhteessa koko liikennemäärään. Näitä voidaan verrata aikaisempiin tilastoihin, jotta olisi helpompi tehdä ennaltaehkäiseviä toimenpiteitä ennen kuin verkon suorituskyky heikkenee. Nämä tiedot helpottavat laajan verkon suunnittelua, hallintaa ja ylläpitoa. Suorituskyvyn hallinta keskittyykin juuri

enemmän itse laitteiden ja verkon suorituskykyyn kuin palveluiden käytön seurantaan. (2.)

2.7 Turvallisuuden hallinta

Turvallisuuden hallinta (Security Management) on verkkoon ja siihen liitettyjen laitteiden pääsyjen seurantaa, kontrollointia sekä pääsyä siihen tietoon, jota on kerätty verkon laitteesta osana verkonhallintaa. Yksi tärkeimmistä osista turvallisuuden hallinnassa ovat erilaiset lokeihin kerätyt tiedot. Käytännössä turvallisuuden hallinta onkin suurelta osalta lokien keräämistä, tallennusta ja analysointia. (2.)

2.8 Tärkeitä osa-alueita verkonhallinnassa

Dokumentointi on erittäin tärkeää laajassa verkossa, jotta tiedetään, mitä hallitaan ja minkälainen on verkon looginen ja fyysinen rakenne. Siksi hyvä dokumentointi onkin edellytys kaikelle hallinnalle. (3, s.311.)

Raportoinnilla saadaan tietoa, jota verkossa tapahtuu ja miten tapahtumat ovat kehittyneet. Raportoinnilla saadaan tietoa verkon tapahtumista, vikatilanteista, laitteista ja kapasiteetin käytöstä. (3, s.311.)

Huolto tarkoittaa kaikkia ennakoivia korjaustoimenpiteitä, joita vian ja kokoonpanon hallinnan tuloksena on syntynyt. (3, s.311.)

2.9 Verkon valvonta

ISO:n määrittelemät verkonhallinnan avainalueet voidaan jakaa kahteen ryhmään: verkon valvontaan ja verkon hallintaan. Verkon valvontaa voidaan sanoa verkon lukuprosessiksi, missä on tarkoitus tarkkailla verkon tilaa, sen konfiguraatioita ja analysoida niitä. Verkon hallinta on taas verkon kirjoitusprosessi, missä on tarkoitus ylläpitää verkon laitteiden ja komponenttien konfiguraatioita. (2.)

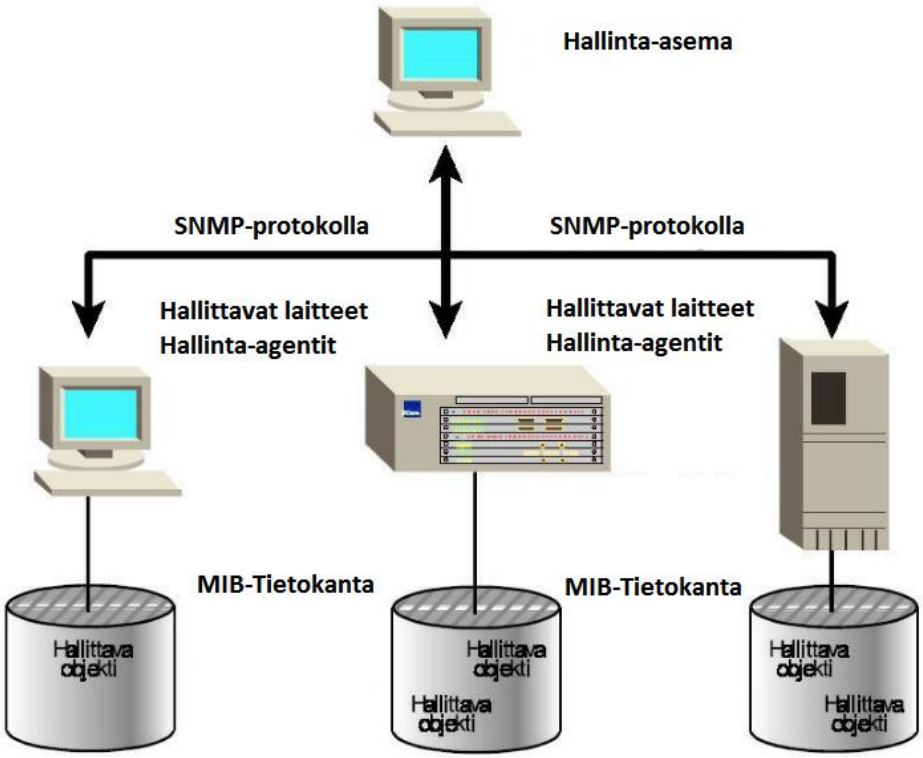
Kuva 2. Verkonhallinnan avainalueiden karkea jako valvontaan ja hallintaan (2, Muokattu).

Yhdessä verkon hallinta ja verkon valvonta muodostavat prosessin, jota kutsutaan verkonhallinnaksi. Ohjelmistoa ja laitteita, millä tämä prosessi toteutetaan, kutsutaan verkonhallintajärjestelmäksi. Verkonhallintajärjestelmä on joukko integroituja sovelluksia ja laitteita, jolla hallinta ja valvonta suoritetaan. Seuraavassa luvussa käydään läpi verkonhallinnan arkkitehtuuria sekä sen komponentteja. (2.)

3 Verkonhallintajärjestelmän komponentit

3.1 Arkkitehtuuri

Yleisellä tasolla verkonhallintaan kuuluu hallinta-asema, jossa on verkonhallinnan sovellus ja tieto hallittavasti laitteista, jotka vastaavasti sisältävät hallinta-agentin ja hallinta-tietokannan. Hallinta-agentti kerää tiedot hallittavan laitteen tietokannasta ja lähettää ne eteenpäin hallinta-asemalle käyttäen esimerkiksi SNMP-protokollaa (Simple Network Management Protocol). Agentti voi toimia myös niin sanotussa proxy-tilassa. Tämä proxy-tila selitetään jäljempänä. Näistä komponenteista muodostuu kokonaisuus, jota kutsutaan verkonhallintajärjestelmäksi. Kaikki edellä mainitut komponentit käydään läpi yksi kerrallaan seuraavissa luvuissa. (3, s.312.)



Kuva 3. Verkonhallinnan arkkitehtuuri yleisellä tasolla. (7, Muokattu).

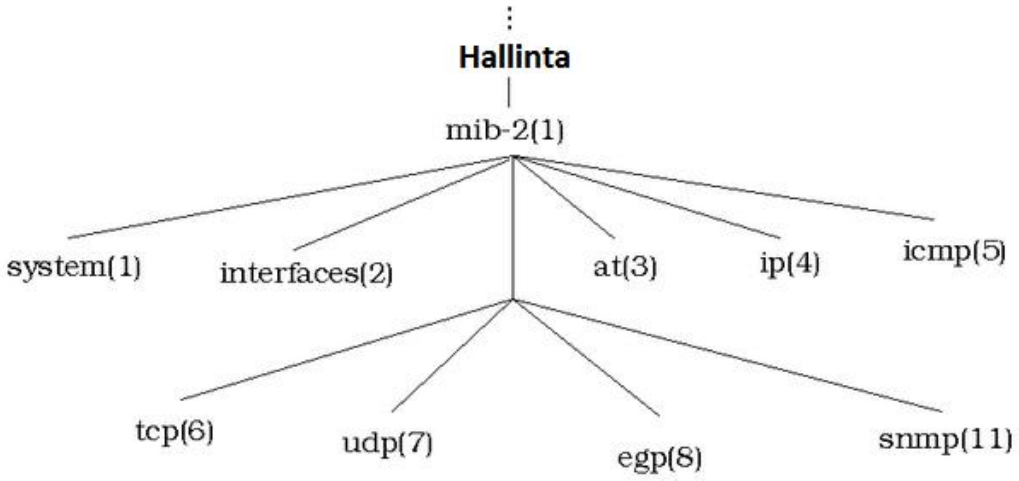
Verkonhallintajärjestelmän tarkoituksena on tehdä kyselyitä verkon eri laitteilla ja palveluille ja varastoida kyselyihin saadut vastaukset. Järjestelmän tarkoitus on myös välittää ennalta määrättyjen hälytyksien tiedot ylläpitäjälle. Verkonhallintajärjestelmän on myös

mahdollista konfiguroida verkkoa uudestaan. Verkonhallinta-aseman ja valvottavien laitteiden väliseen kommunikointiin tarvitaan kaksisuuntainen verkonhallintaprotokolla. (2.)

3.2 MIB

MIB (Management Information Base) on hierarkkinen tietokanta, johon agentti kerää ja ylläpitää tietoa. MIB-tietokantaa voidaan myös kutsua MIB-taulukoksi. Hallinta-aseman pyytäessä tietoa agentilta agentti kerää ne tietokannasta ja lähettää vastauksena hallinta-asemalle tiedot kannasta. Tietokanta sisältää niin standardisoituja kuin myös toimittajakohtaisia MIB-objekteja. Objektit voidaan määritellä keräämään erilaisia tietoja kuten vastaanotettujen ja lähetettyjen pakettien määrää tai tietoa laitteen tilasta. (3, s. 315.)

MIB-tietokanta on rakenteeltaan puumainen. Puun yläosan objektien ominaisuudet on ISO:n määrittelemiä ja taas alemman osan objektit ovat muiden organisaatioiden ja laitevalmistajien määrittelemiä. Puun ylempi taso käsittelee esimerkiksi sellaisia objekteja kuin laitteita (systems), verkkoliitäntöjen liikennettä (interfaces), pakettien tilastoja (IP), TCP-liikennetilastoja ja SNMP-liikennetilastoja. (3, s. 315.)



Kuva 4. MIB:in rakenne yleisellä tasolla (3).

3.3 SMI

SMI (Structure Management Information) on MIB:iin määritetty tietorakenne, mikä kuvaa MIB:in puurakennetta. Se tarjoaa työkalut uusien objektien luomiseen sekä tunnistamiseen. Objektit voivat sisältää kokonaislukuarvoja, verkko-osoitteita, laskureita, mittausarvoja, aikaleimoja tai taulukoita. SMI määrittelee myös hierarkkisen nimirakenteen, jolla hallittavat objektit tunnistetaan. Objektit ovat annettuja nimiä ja sijainteja hierarkkisessa rakenteessa, joilla helpotetaan objektien tunnistamista. SMI:iin kautta voidaan myös määritellä muiden organisaatioiden omia objekteja, jotka hallintajärjestelmä pystyy tunnistamaan. SMI on erittäin tärkeä osa MIB-tietokantaa, koska se määrittää, miten jokin tietokannan osa tulisi olla määritelty. Ilman SMI:tä tietokanta olisi hyödytön. (3, s.316.)

3.4 Agentti

Agentin tarkoitus on kerätä verkonhallinnan tietoa sen hallitsemalta verkkosegmentin alueelta ja tallentaa ne tietokantaan. Agentti vastaa hallinta-aseman tekemiin kyselyihin sekä lähettää sille ennalta määritettyjä huomautus- ja hälytysviestejä tapahtumista. Agentti toimii hallittavissa laitteissa. (7.)

Agentti voi myös toimia proxy-tilassa. Tämän toiminnan avulla laajoissa ja monimutkaisissa verkoissa pystytään välittämään tietoa agentilta toiselle hallinta-asemalle asti, vaikka käytössä olisi eri standardeja. Proxy-tilassa oleva agentti siis välittää ja muuntaa muiden agenttien viestit hallinta-aseman ymmärtämään muotoon. Proxy-toiminnallisuutta hyödynnetään myös verkkoliikenteen minimoimiseksi rakentamalla verkonhallinta hierarkkiseksi. Tämän tyyppisessä tapauksessa hallinta-asema joutuu kommunikoimaan vain muutaman agentin kanssa, jotka keräävät tiedot taas niiden alla sijaitsevilta verkon solmuilta eli nodeilta. (7.)

3.5 Hallinta-asema

Agentin ja hallinta-aseman välillä tapahtuva kommunikointi hoidetaan verkonhallintaprotokollan avulla. Seuraavassa luvussa käydään läpi yleisimmin verkonhallinnassa käytetty SNMP-protokolla ja sen toiminta. (3, s.314-315.)

Hallinta-asema, joka sisältää verkonhallintaohjelmiston, on siis se komponentti verkonhallintajärjestelmässä, jonka täytyy hallita verkonhallintaan liittyvä kokonaisuus. Verkonhallintaohjelmiston täytyy pystyä haettujen ja saatujen tietojen perusteella luomaan topologinen kartta verkosta, reaaliaikainen näkymä verkon laitteista ja yhteyksistä, tekemään erilaisia raportteja verkosta, käsittelemään historiatietoja ja tarvittaessa jopa lähettämään sähköposti tai tekstiviesti ylläpitäjälle verkon kriittisestä häiriöstä. (3, s.314-315.)

4 Simple Network Management Protocol - SNMP

4.1 SNMP-protokollan esittely

SNMP on yleisimmin käytetty verkonhallintaprotokolla, joka suunniteltiin alun perin käytettäväksi TCP/IP-verkkojen (Transmission Control Protocol / Internet Protocol) hallintaan. SNMP-termillä viitataan yleensä kokonaiseen joukkoon verkonhallintastandardeja. Siihen kuuluvat itse protokolla SNMP sekä edellisessä luvussa esitetyt hallintatietokanta MIB ja siihen kuuluva tietorakenne SMI. SNMP sisältyy OSI-mallin (Open Systems Interconnection) seitsemännelle eli sovelluskerrokselle. SNMP on yhteydetön hallintaprotokolla. Tämä tekee siitä tehokkaan, koska se pystyy toimimaan helposti kuormitetussa verkossa. (2, 3 s.314.)

TCP/IP-malli	OSI-malli
Sovelluskerros	Sovelluskerros
	Esitystapakerros
	Istuntokerros
Kuljetuskerros	Kuljetuskerros
Verkkokerros	Verkkokerros
Peruskerros	Siirtoyhteyskerros
	Fyysinen kerros

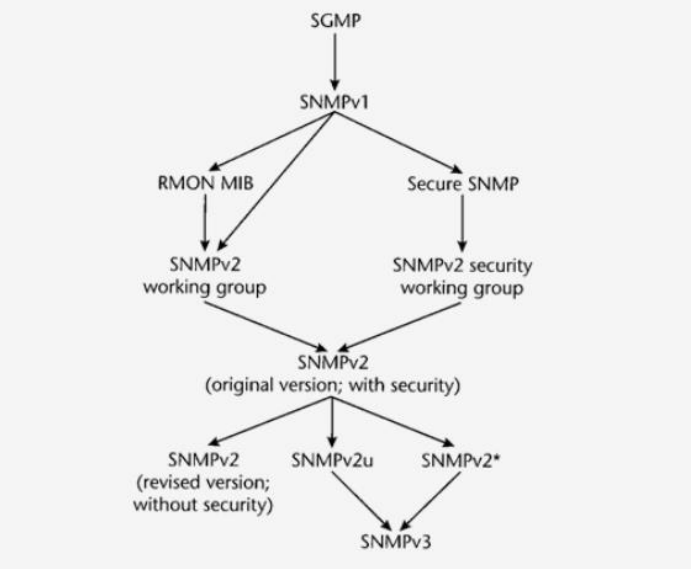
Kuva 5. TCP/IP-mallin ja OSI-mallin kerrokset (8).

4.2 SNMP:n historia

Internet alkoi kasvamaan eksponentiaalisesti 1980-luvun loppupuolella, silloin alettiin suunnittelemaan yleispätevää verkonhallintaprotokollaa. Vaihtoehtoja oli monia, mutta kolme niistä nousivat esille ylitse muiden: HEMS (High-level Entity-Management System), SNMP ja CMIP (Common Management Information Protocol) over TCP/IP eli CMOT. Alkuperäinen suunnitelma oli vuonna 1988, jolloin SNMP valitaan väliaikaiseksi ratkaisuksi ja CMOT olisi pitkän tähtäimen ratkaisu. Perusteluna näihin päätöksiin oli, että OSI-protokollat tulisivat syrjäyttämään TCP- ja IP-protokollat eikä siihen perustavia

ratkaisuja kannattaisi kehittää. SNMP kehittyi kuitenkin nopeasti ja syrjäytti muut olemassa olevat verkonhallintaprotokollat ja vuonna 1989 siitä tuli jo de facto-standardi, jonka päälle monet laitevalmistajat olivat jo toteuttaneet järjestelmiään. Toukokuussa 1990 SNMP:sta tuli Internet-standardi. (2.)

SNMP:ssä huomattiin kuitenkin puutteita, joista yksi tärkeimmistä ominaisuuksista oli turvallisuus. Tämän takia sitä alettiin kehittämään kahdessa eri ryhmässä vuonna 1992. Toinen ryhmä keskittyi turvallisuusominaisuuksin kehittämiseen sekä määrittelyyn ja toinen ryhmä kaikkeen. Vuonna 1993 julkaistiin standardiehdotus uudesta SNMP:sta eli SNMPv2 ja vuonna 1994 tämä hyväksyttiin uudeksi standardiksi. (2.)



Kuva 6. SNMP:n versiohistoria (7).

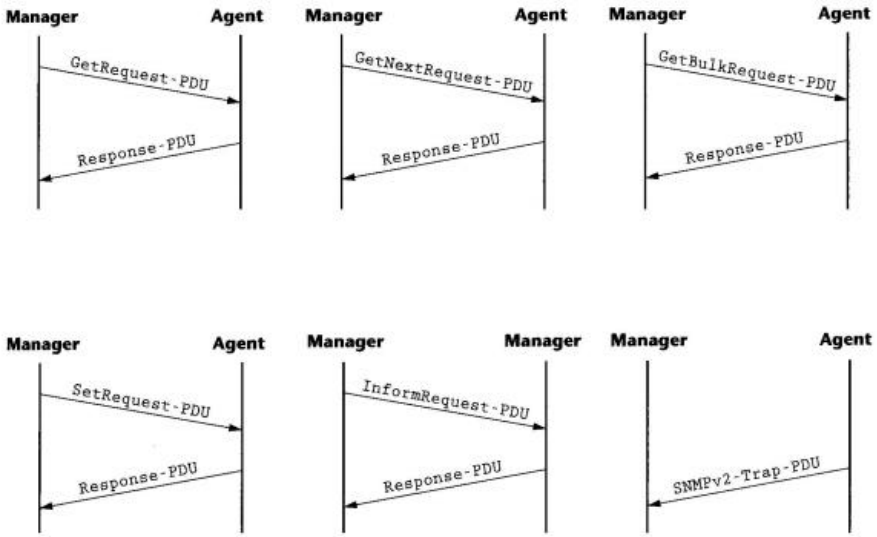
4.3 SNMP versio 3

Nykyisin käytössä oleva SNMPv3 hyväksyttiin Internet-standardiksi maaliskuussa 2002. SNMPv3 korjattiin edellisten versioiden tietoturva-aukkoja, ja näin se pystyi tarjoamaan entistä turvallisemman toiminnallisuuden, joka on erittäin tärkeää verkonhallinnassa. SNMPv3 käyttää USM-tekniikkaa (User-based Security Model) viestien salaukseen ja autentikointiin. VACM-tekniikan (View-based Access Control Model) avulla voidaan määritellä, ketkä pääsevät näkemään ja muuttamaan MIB-tietokantaa. (4; 5.)

SNMPv3-ylläpitäjä voi luoda käyttäjille henkilökohtaisia tunnuksia ja määritellä agentin tietoihin tarkemmat tietoturvaan vaikuttavat parametrit, kuten autentikointi, yksityisyys-protokolla ja avaintunnukset. Ylläpitäjä voi myös määritellä oikeudet MIB-tietokantaan. Suurimpana muutoksena on, että viestien salaamiseen ja käyttäjätunnuksiin liittyvät salasanat lähetetään salattuna käyttämällä DES-salausta (Data Encryption Standard) selväkielisten versioiden sijasta. SNMPv3 antaa lisäksi ylläpitäjälle mahdollisuuden päivittää laitekokoonpanot automaattisesti. (6; s. 240-242.)

4.4 SNMP-viestinvälitys ja operaatiot

SNMP:n viestinvälitys on toteutettu mahdollisimman yksinkertaiseksi verkonhallintajärjestelmän hallinta-aseman (Manager) ja hallittavien laitteiden (Agent) välillä UDP-protokollaa (User Datagram Protocol) hyödyntäen. UDP on tilaton protokolla, jolloin varsinaisesti yhteyttä ei tarvita laitteiden välillä, eikä se tällöin rasita verkkoa. Viestin välitys perustuukin vain muutamiin yksinkertaisiin viesteihin, joita ovat GetRequest, GetNextRequest, GetBulkRequest, SetRequest, InformRequest, SNMPv2-Trap ja Response. Kuvassa 7 on esitetty näiden viestien vaihto. (7.)



Kuva 7. Kuvassa on esitetty Managerin ja Agentin välinen viestinvaihto (7).

GetRequestin viestissä hallinta-asema pyytää agentilta PDU (Packet Data Unit) variable-bindings-kentässä määriteltyjen objektien arvoa. Jos agentti ei pysty toimittamaan objektin arvoa takaisin, niin se palauttaa vastausviestin virheilmoituksen kanssa. Esimerkiksi syinä voi olla, että hallinta-asemalla ei ole oikeuksia tähän tietoon, eikä tietoa ole olemassa, sitä ei ole määritelty MIB:ssä tai paluuviestin UDP-paketin koko ylittyy ja se joudutaan hylkäämään ja muodostamaan uudestaan. (7.)

GetNextRequestin viestissä hallinta-asema pyytää agentilta variable-bindings-kentässä määriteltyjen objektien tietoa. Tässä viestissä käydään MIB:in puurakenne systemaattisesti läpi sekä dynaamiset taulukot objekti objektilta. (7.)

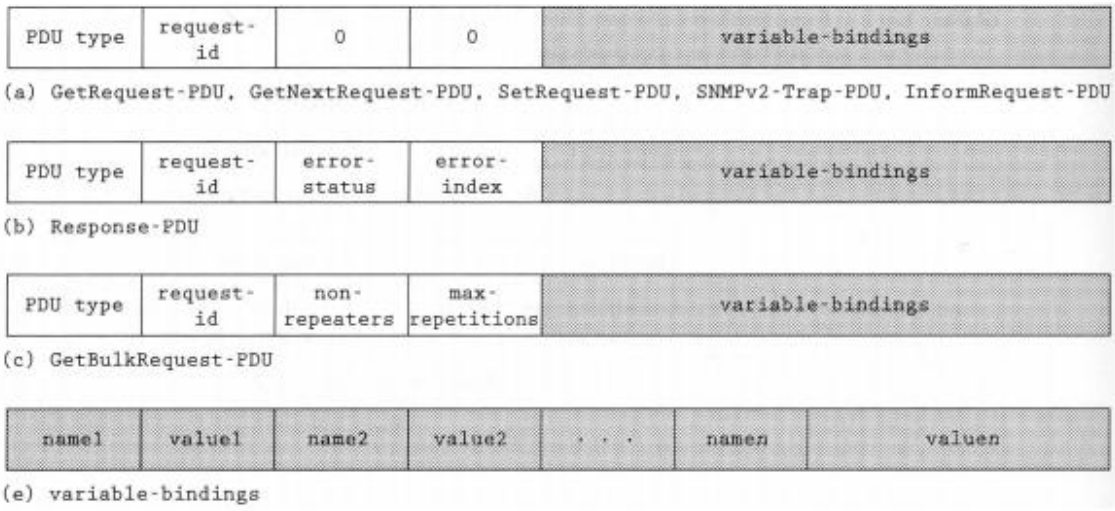
GetBulkRequest viesti on hyvin samanlainen kuin GetNextRequest. Erona on se, että pystytään pyytämään mahdollisimman suuri määrä tietoa vastausviestissä, mutta niin ettei UDP-paketin kokorajoitus ylity. (7.)

SetRequest viestillä hallinta-asema voi lähettää pyynnön objektin muuttamista varten. Vastausviestinä agentti lähettää objektin nimen sekä objektille asetetun uuden arvon. Näin hallinta-asema pystyy tarkistamaan, että agentti on suorittanut muutoksen oikein. (7.)

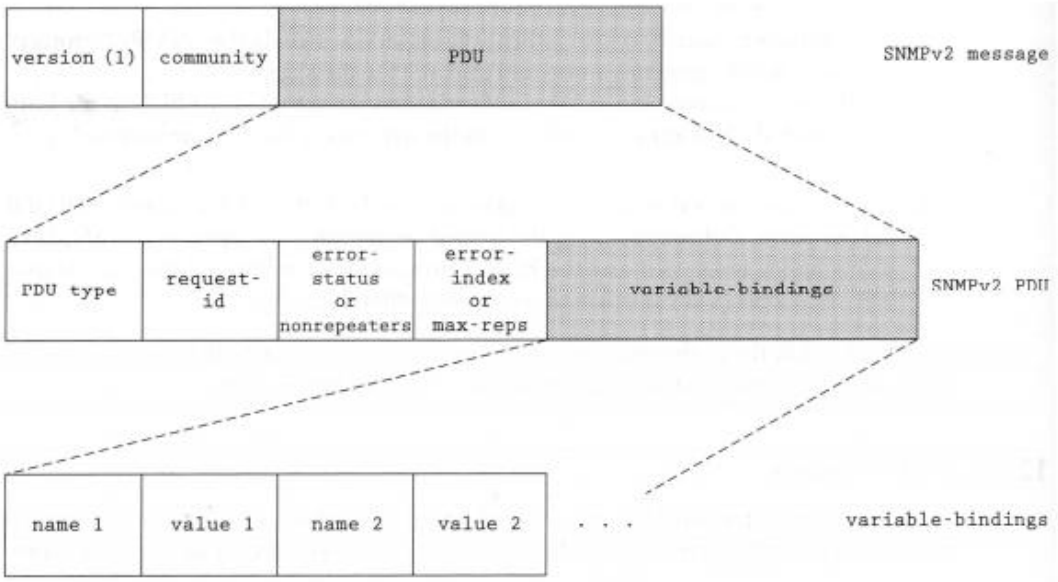
Response on vastausviesti, jolla agentti vastaa kaikkiin edellisiin viesteihin. Sen sisältö riippuu kysytystä tiedosta. (7.)

SNMPv2-Trap on ainoa viestityyppi, jossa kommunikaation aloittaa agentti. Agentille voidaan siis määrittää ehtoja, joiden täyttyessä se lähettää hallinta-asemalle ilmoituksen. Esimerkiksi on voitu määrittää, että kun jossain laitteessa on yli 3 virhesekuntia niin agentti lähettää tiedon hallinta-asemalle. Ainut ongelma tässä viestissä on, että hallinta-asema ei ilmoita agentille viestin saapumisesta perille. (7.)

InformRequest viesti on tarkoitettu kahden hallinta-aseman väliseen tiedonvaihtoon. Toinen hallinta-asema voi esimerkiksi lähettää viestin, kun se haluaa välittää tietoa toisessa hallinta-asemassa pyörivälle applikaatiolle. Tätä tarvitaan hierarkkisesti rakennetuissa hallintaympäristöissä. (7.)



Kuva 8. SNMPv3:n käyttämät eri viestityyppien paketti-informaatio (7).



Kuva 9. SNMPv3-viestin rakenne (7).

5 Remote Network Monitoring - RMON

5.1 Yleistä RMON:sta

Internet Engineering Task Force eli IETF kehitti RMON:in (Remote Network Monitoring) vuonna 1995 korvaamaan SNMP:n puutteita. Molemmat SNMP ja RMON käyttävät tiedonkeruuseen agentteja, jotka keräävät tietonsa MIB-tietokantaan. SNMP:n ja RMON:n suurin ero onkin, että kun SNMP-hallinta-aseman pitää koko ajan tehdä kyselyitä agenteille, niin RMON:n ei tarvitse sitä tehdä. RMON:issa voidaan kerättyä tietoa käydä tarkastelemassa myöhemmin historiaan perustuen. Tämä edesauttaa sitä, ettei tiedon kerääminen ruuhkauta verkkoa, vaan kaikki kerätty tieto voidaan lähettää kokonaisuutena hallinta-asemalle. (3, s.316-320.)

RMON voidaan sijoittaa melkein mihin tahansa laitteeseen verkossa. Osa valmistajista toteuttaa RMON-ominaisuuden laitteisiinsa, mutta on myös saatavina erillisiä verkkosegmenttiin liitettäviä RMON-agentteja. Tavallisimmin RMON sijoitetaan verkon kriittiseen kohtaan, josta sillä voi seurata verkon kuormitusta, sanomakokoja, virhetilanteita ja asemien tietoliikennekäyttäytymistä. (3, s.316-320.)

Verkon hallinta-aseman ei tarvitse jatkuvasti tutkia keruuyksiköitä. Agentti lähettää hälytyksen vasta, kun sille ennalta määritetty vikakynnys ylittyy tai alittuu. SNMP:n rooliksi jää tässä tapauksessa välittää vain tieto RMON-keruuyksikön ja hallinta-aseman välillä. (3, s.316-320.)

5.2 RMON MIB

RMON MIB on kehitetty niin, että sitä käytetään yhdessä SNMP:n kanssa. Jos hallinta-aseman käyttäjä huomaa jotain epänormaalia verkossa, voi hän siirtyä tutkimaan ongelmaa tarkemmalla tasolla. RMON sisältää seuraavat standardoidut hallintaryhmät, jotka puolestaan voivat sisältää alaryhmiä. (3, s.316-320.)

Statistics-ryhmä kerää nimensä mukaansa tilastotietoja kehys- ja tavumääristä, kehyskoista, virheellisistä kehyksistä jne. RMON MIB:iin on määritetty viisi virhelaskuria, jotka ovat Runts eli alimittaiset kehykset, Oversize eli ylipitkät kehykset, Fragments eli vioittuneet kehykset, CRC- sekä Jabber-virheet.

History-ryhmä kerää dataa tapahtumahistoriasta, jota voidaan käyttää myöhemmin. Hallinta-aseman käyttäjä voi määritellä näytteenottovälit sekä mittausajan. Samanaikaisesti voi olla käytössä useampia näytteenottotaajuuksia.

Alarms-ryhmä seuraa erilaisia laskureita ja muodostaa niistä hälytyksiä, kun ennalta määritetyt hälytysehdot toteutuvat. Hälytykset lähetetään Trap-viesteinä, jolloin niitä lähtee vain yksi kappale virhettä kohdin. Hälytys tarvitsee toimiakseen Filters- ja Events-ryhmän, joille määritellään hälytysobjekti sekä hälytyksen jatkokäsittely.

Hosts-ryhmän tehtävä on kerätä tietoa verkon MAC-osoitteista, niiden esiintymisjärjestyksestä. Ryhmä tallentaa myös kaikkien asemien kehyskoot, liikennetyypit, kehysten tulosuunnat ja virhetilanteet.

HosTopN-ryhmä kerää tilastoja annettujen mittausperusteiden pohjalta (pakettimäärä, tavut, virheet, törmäykset jne.) eniten kuormittaneista MAC-osoitteista.

Traffic Matrix-ryhmä kerää tilastoa MAC-osoitteiden keskinäisestä liikenteestä.

Filters- eli suodatin-ryhmän kautta ohjataan kehysten keräystä.

Packet Capturen-ryhmään kerätään kehyksiä. RMON voi kerätä useita erilaisia kehyksiä puskureihinsa samanaikaisesti.

Events-ryhmä ohjaa hälytysrajan toteuttaneet tapahtumat joko omaan lokitiedostoon tai SNMP:n käynnistämiseen.

5.3 RMON MIB versio 2

RMON:in ensimmäisen versio mahdollisti alempien OSI-mallin kerrosten seuraamisen eli fyysisen- ja siirtoyhteys-kerroksen. Jos siis ylemmillä kerroksen tasoilla oli jotain ongelmia, ne täytyi hoitaa muilla työkaluilla. Tämän takia kehitettiin RMON MIB 2, joka valmistui vuonna 1997. Sitä ei siis kehitetty korvaamaan RMON-versio 1 vaan täydentämään sitä niin, että se pystyisi seuraamaan myös ylempiä OSI-mallin kerroksia. RMON MIB versio 2 lisäsi standardiin seuraavat hallintaryhmät: (13).

ProtocolDir eli protokolla hakemisto on lista protokollista, joita laitteet tukevat.

ProtocolDist avulla nähdään liikennetilastot kaikista käytetyistä protokollista.

AddressMap sisältää tiedot verkkokerroksen IP-osoitteista MAC-osoitteisiin.

Network-layer Hosts on verkkokerroksen liikeanalyysi laitteittain.

Network-layer matrix sisältää taas verkkokerroksen liikennetilastot laitepareittain.

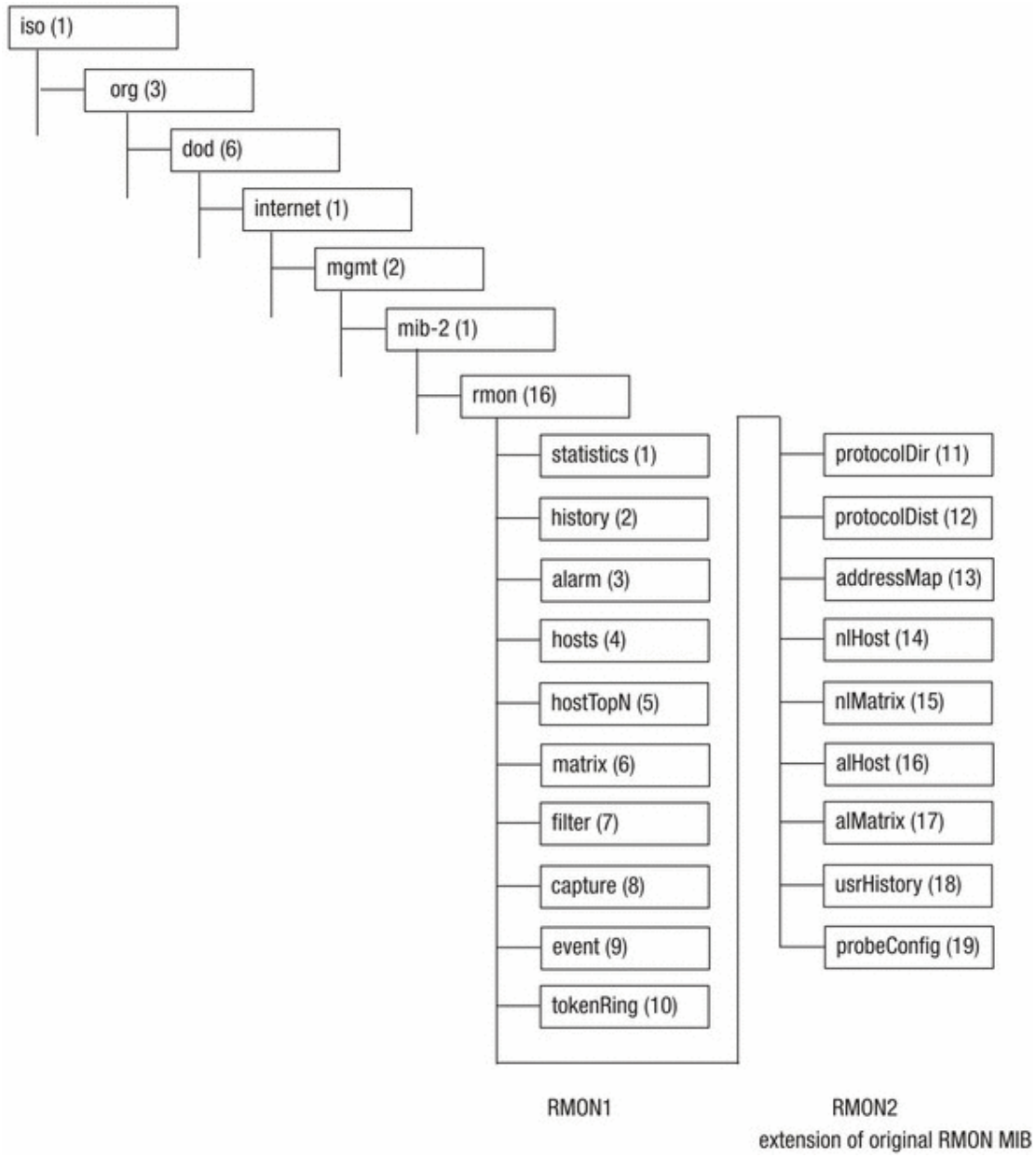
Application-layer Host sisältää ohjelmistokerroksen laitteiden liikennetilastot ohjelmistoprotokollittain laitekohtaisesti.

Application-layer matrix sisältää ohjelmistokerroksen liikennetilastot laitepareittain.

User historysta saadaan ajoittaisia näytteitä käyttäjien määrittelemistä muuttujista.

ProbeConfigista pystytään konfiguroimaan laitteita etänä (13).

RMOB MIB ja RMON MIB versio 2 standardiin kuuluvat hallintaryhmät ovat esitetty kuvassa 10.



Kuva 10. RMON:in hallintaryhmät (14.)

6 Fingrid Oyj:ssä käytetyt tiedonsiirtotekniikat

6.1 Yleistä digitaaliset siirtojärjestelmät

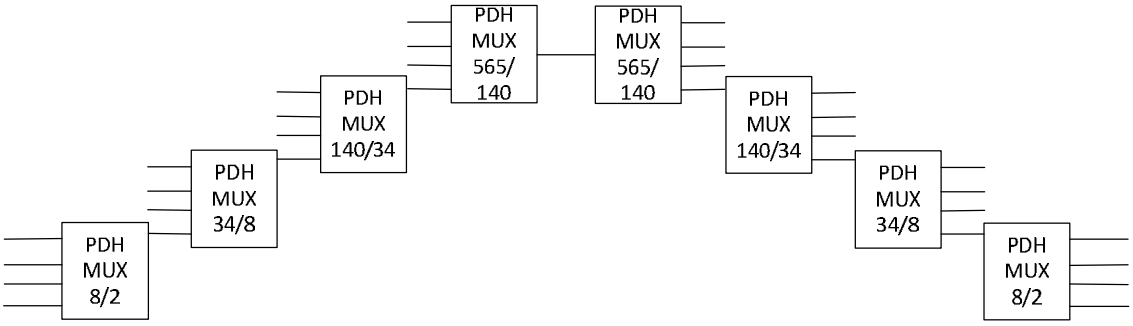
Digitaaliset siirtojärjestelmät jaetaan plesiokronisiin PDH- (Plesiochronous Digital Hierarchy) ja synkronisiin SDH- (Synchronous Digital Hierarchy) järjestelmiin. Plesiokroninen tarkoittaa "melkein synkronista" järjestelmää. PDH-tekniikka on kehitetty 1970-luvun alussa ja SDH-tekniikka taas 1980-luvun lopussa.

PDH-nimitys on tullut SDH-järjestelmien syntymisen myötä. PDH tunnettiin ennen nimellä PCM (Pulse Code Modulation). Molemmat PDH ja SDH perustuvat TDM-tekniikkaan (Time Division Multiplexing), mikä tarkoittaa aikajakokanavointia. Siinä signaalit jaetaan eri aikaväleille. (9.)

6.2 PDH-tekniikka

PDH-järjestelmien siirtolaitteessa 64 kbit/s kanavat niputetaan 2 Mbit/s kehyksiin synkronisesti. Neljä 2 Mbit/s kanavaa kanavoidaan edelleen 8 Mbit/s siirtotasolle niin, että 8 Mbit/s kehys sisältää täyteinformaatiota, jolloin 2 ja 8 Mbit/s signaalien ei tarvitse olla synkronissa keskenään. (9.)

Tämä tarkoittaa, että PDH:ssa multipleksointi tapahtuu neljän signaalin ryhmissä eli siinä on mahdollista pakata 4 alemman tason yhteyttä yhteen ylemmän tason yhteyteen. PDH on standardisoitu digitaalinen hierarkia, missä eri bittivirtoja kanavoidaan nopeammiksi bittivirroiksi. Euroopassa käytettyjä nopeuksia ovat 2, 8, 34, 140 ja jopa 565 Mbit/s. Kuvasta 11 on havainnollistettu, kuinka PDH:ssa joudutaan menemään askel kerrallaan eteenpäin. (9.)



Kuva 11. PDH-verkon yleiskuva.

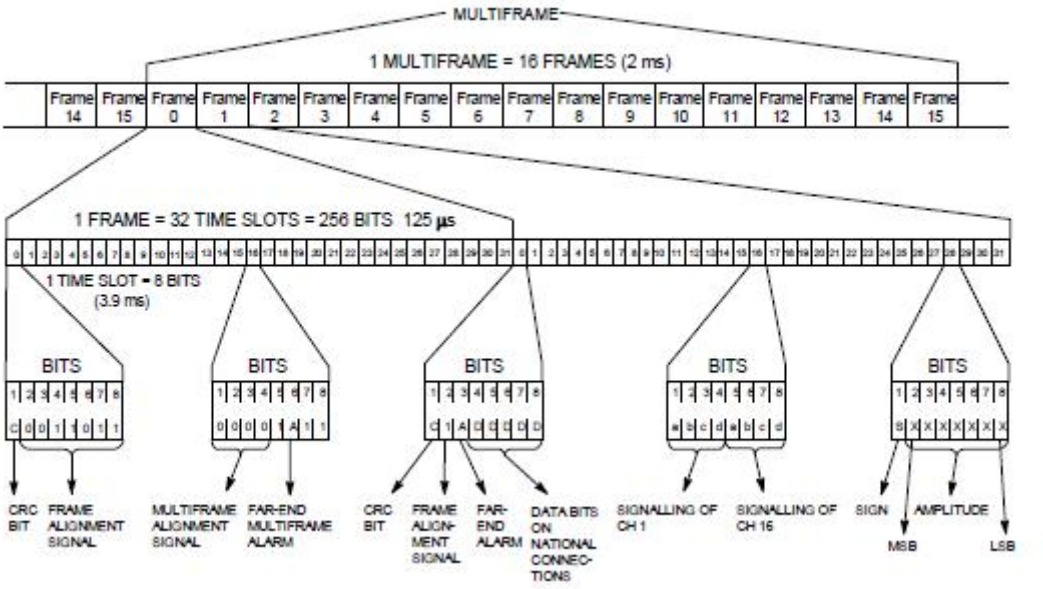
Plesiokroninen PDH:n nimessä tarkoitti siis "melkein synkronista", ja se tulee siitä, että synkronointi tapahtuu vain 2 Mbit/s signaalin tasolle asti, ja ylemmän tason laitteet käyvät omalla kellollaan. Näin ollen alemman tason signaaleja ei voida helposti purkaa ilman, että purettaisiin ylemmän tason signaaleja ensin. Kuvasta 11 huomataan hyvin, kuinka tarvitaan jokaisen tason laite ennen kuin saadaan E1-yhteys. (9.)

Tämän lisäksi PDH-laitteiden optisia liitäntöjä ja hallintaa ei ole standardisoitu, ja se vaihtelee eri valmistajien välillä, mikä vaikeuttaa huomattavasti PDH-verkkojen valvontaa ja hallintaa. SDH-verkot korvaavat tai ovat korvaamassa PDH-verkon, ja jäljelle jäävät vain PDH-verkon 2 Mbit/s kanavointilaitteet. Näin on tapahtumassa myös Fingridissä. (9.)

6.2.1 TDM-aikajakokanavointi

Aikajakokanavoinnissa yhden kehyksen eli framen pituus on 125 µs. Kehys sisältää 32 aikaväliä, mitkä numeroidaan 0 - 31 ja jokainen niistä on 8 bittiä. Puhekanaville tarkoitetut aikavälit ovat 1 - 15 ja 17 - 31. Euroopassa puheen koodaus on 8000 näytettä sekunnissa, ja jokainen näyte on 8 bittiä, josta saadaan 64 kbit/s. (10.)

Synkronointiaikaväli 0 käytetään esimerkiksi sisäiseen tiedonsiirtoon yli 2 Mbit/s yhteyksien kehyslukitukseen, hälytyksiin sekä valvontaan. Merkinantoaikaväli on 16 eli siinä kohtaa siirretään signalointi tieto. Koko kehys sisältää 256 bittiä. Kun se toistetaan 8000 kertaa sekunnissa, niin saadaan multipleksoitua signaalin siirtonopeus, joka on 2048 kbit/s. (10.)



Kuva 12. 2 Mbit/s kehyskuva (10).

6.2.2 Aikaväli TS0

TS0-aikavälin bitit 2 - 8 korvataan kehyksen kehyslukitus-sanalla 0011011 joka toisessa kehyksessä. Kehyslukitus-sana menetetään, jos siinä on kolme peräkkäistä virhettä, kun se otetaan vastaan. Kehyslukitus menetetään myös, jos aikavälin TS0 bitti B2 virheilee muissa kehyksissä kolme kertaa peräkkäin. Kehyslukitus otetaan talteen vasta siinä kohtaan, kun siinä ei ole virheilyä, TS0-bitti B2 on seuraavassa kehyksessä 1 ja vastaanotettu signaali TS0:ssa on virheetön. (10.)

	<---------- Time slot TS0 bits ---------->							
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Time slot TS0 containing the frame alignment signal	CRC moni-toring	0	0	1	1	0	1	1
		<---------- Frame alignment signal ---------->						
Time slot TS0 not containing frame alignment signal	CRC moni-toring	1	Far-end alarm	<----	Internal system data transfer	---------->		

Kuva 13. Kehyslukitusaikavälin TS0-bittien käyttö (10).

Aikavälissä TS0 käytetään CRC-tarkistusta kehyslukituksen varmistamista sekä siirtovirheiden tarkkailua varten. Yhteyden lähetys ja vastaanottopäässä täytyy olla samanlaiset siirtorekisteriketjut, jotta lähetys olisi todennäköisesti virheetön. (10.)

Matemaattisesti CRC-tarkistus on menetelmä, jossa bittijono muokataan sellaiseen muotoon, että se on jaollinen tietyllä polynomilla. Kun vastaanottopäässä se jaetaan samalla polynomilla ja saadaan jakojäännös 0, on vastaanotto virheetön. (10.)

BER (Bit error rate) -koodivirheiden määrästä voidaan päätellä todennäköisen hälytyksen syy. BER 10^-5 antaa esimerkiksi hälytyksen B, mikä on huomautus huonontuneesta signaalista. BER 10^-3 antaa hälytyksen A, mikä voi esimerkiksi tarkoittaa signaali on katkaisurajan kriteerien alapuolella tai sitä ei ole ollenkaan. Tällöin lähetetään linjalle AIS-signaali (Alarm indication signal). (10.)

TS0-bittejä 5 - 8 käytetään Q1-väylien tai muiden hallintaväylien välittämiseen verkonvalvonnan tarpeisiin. Valvontaväylän nopeus on tässä tapauksessa 300 - 2400 bit/s.

6.3 SDH-tekniikka

SDH-tekniikkaa kehitettiin verkkokapasiteetin tarpeen myötä. SDH perustuu SONET-standardiin (Synchronous Optical Network), joka on kehitetty Yhdysvalloissa. Yhdysvalloissa käytetyt PDH kehysrakenteet ovat erilaisia kuin Euroopassa. SONET:issa on määritellyt synkronisen tiedonsiirtotavan ja sen perusnopeudet. Euroopassa sekä lähes kaikkialla muualla maailmassa on käytössä ITU-T:n määrittelemät SDH:n standardit. (9.)

SDH:n standardoinnin G.707 tarkoituksena oli saada optiset tiedonsiirtoyhteydet yhteensopiviksi. Verkonhallinta, valvonta ja huolto piti saada hoidettua myös SDH:N avulla ja samalla saatiin minimoitua laitteiden määrää verkossa. Standardin avulla oli myös tarkoitus saada verkko soveltumaan erilaisiin tarkoituksiin esimerkiksi alueverkkoihin, runkoverkkoihin, ATM-verkkoihin (Asynchronous Transfer Mode) tai IP-verkkoihin.

SDH perustuu synkronisiin siirtokehyksiin STM-N (Synchronous transport module). SDH:lle on määritelty nopeuksia lähes 10Gbit/s asti. SDH:n määritellyt nopeudet näkyvät taulukossa 1.

Taulukko 1. SDH:n määritellyt nopeudet.

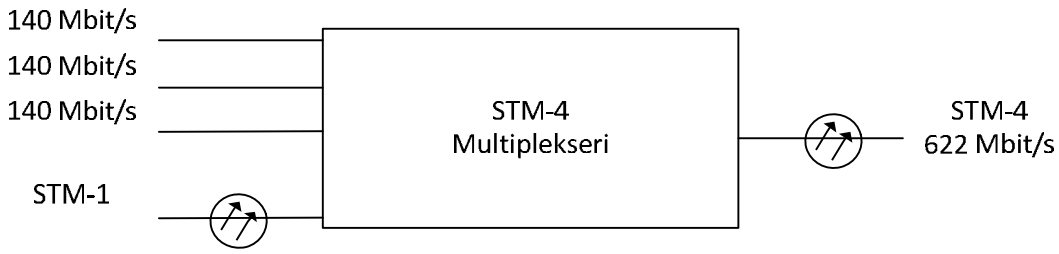
STM-N	Siirtonopeus Mbit/s
STM-1	155,52
STM-4	622,08
STM-16	2488,32
STM-64	9953,28

6.3.1 SDH:n kanavointi- ja ristikytkentälaitteet

SDH-multiplekserit tuovat huomattavia säästöjä laitteistokustannuksiin perinteiseen PDH-tekniikkaan verrattuna sekä mahdollistavat ristikytkennät purkamatta kehyksiä.

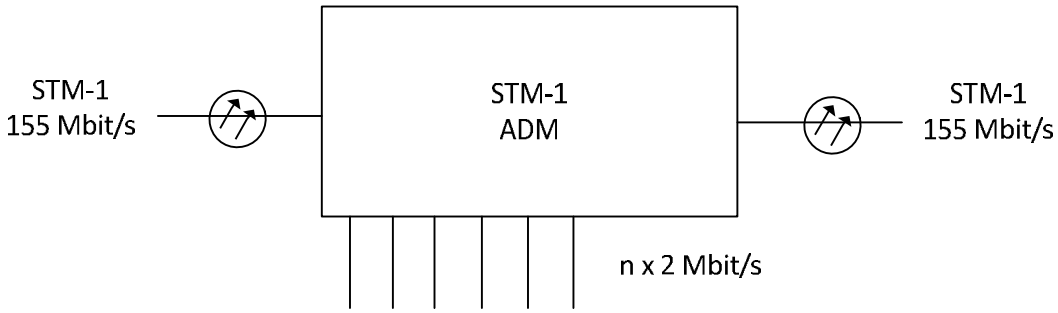
Kuva 14. E1 signaalin kanavoiminen yhteen STM-1 signaaliin (9, muokattu).

STM-1 päätemultiplekserillä pystytään kanavoimaan 63 kappaletta E1-signaaleja STM-1-signaaliin. Esimerkiksi 2 Mbit/s signaali voidaan synkronisesti kytkeä suoraan 155 Mbit/s järjestelmään, joka mahdollistaa sen ettei kaikkia siirtonopeuksia tarvitse purkaa signaalin kytkemistä varten. Päätemultiplekseriä käytetään nimensä mukaisesti päästä päähän-yhteyksiin. (9.)



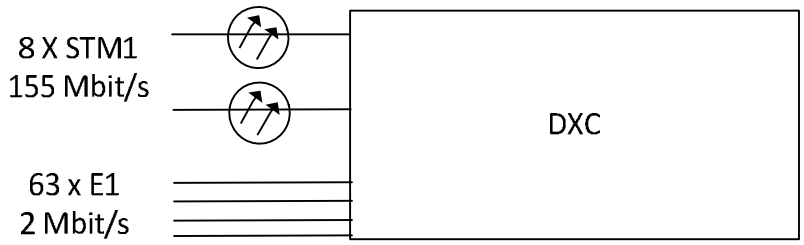
Kuva 15. STM-4-multiplekserin kanavointi (9, muokattu).

Vastaavasti taas STM-4 multiplekserillä pystytään kanavoimaan neljää 140 Mbit/s tai STM-1-signaalia (155 Mbit/s) yhteen STM-4 signaaliin (622 Mbit/s). Tätä tekniikkaa hyödyntämällä voidaan kanavointi tehdä aina STM-64-signaaliin asti. (9.)



Kuva 16. STM1-ADM-multiplekserin toiminta.(9, muokattu)

Syöttö-pudotus-multiplekserillä ADM (Add/drop multiplexer) STM-1-versiossa pystytään poimimaan tulevasta STM-1 signaalista 126 kappaletta E1-signaaleja demultipleksoimatta tai päättämättä sitä. Vastaavasti voidaan lähtevään signaalin lisätä E1-signaaleja sen verran, mitä paikkoja on vapaina. ADM voidaan varustaa myös muilla alikanavaliitännöillä. (9.)



Kuva 17. DXC-ristikytkentälaitteen toiminta.(9, muokattu)

Synkronisella DXC (Digital Cross-Connect) ristikytkentälaitteella pystytään yhdistämään virtuaalikontteja ja yhdistämään ne haluttuun liitäntään. Esimerkiksi voidaan kytkeä 2-140 Mbit/s signaaleja ja STM1-signaaleja STM-1 signaalien välillä. (9; 11.)

ADX (Active digital cross connect) on aktiivinen ristikytkentälaite, joka on kehittyneempi versio DXC:stä. Esimerkiksi ADX voi sisältää Add/drop-kanavointilaitteen, jossa on 63 kappaletta E1-liitäntöjä, STM-1-liitäntä ja sisältää vielä digitaalisen E1-liitäntöjen ristikytkennän. (12.)

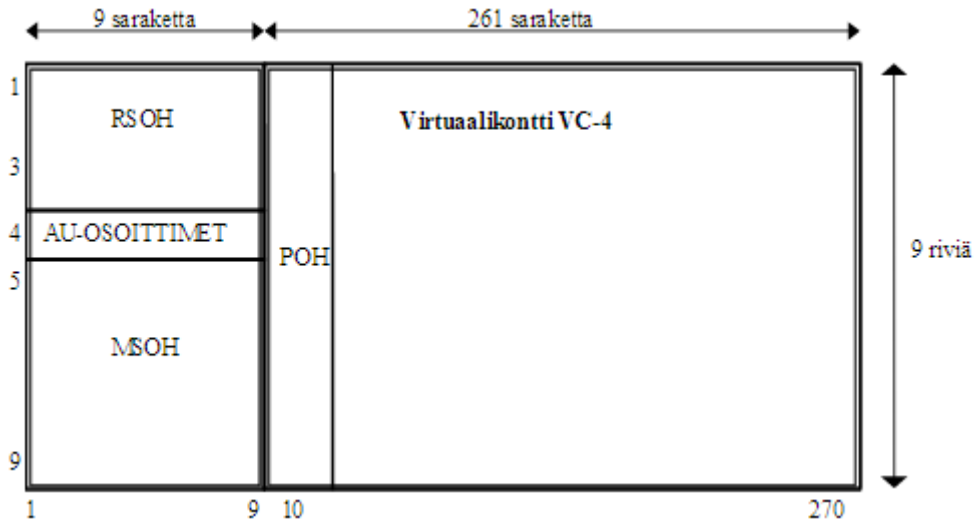
6.3.2 STM-1-kehysrakenne

Kuvassa 18 on esitetty STM-1-kehyksen rakenne. STM-1-kehyksen siirtonopeus on 155,52 Mbit/s, ja sen rakenne muodostuu 270 pystysarakkeesta ja 9 vaakarivistä, jotka sisältävät yhden tavun eli 8 bittiä. Kehyksen bittimäärä tulee seuraavalla laskukaavalla. (12.)

270 pystysaraketta * 9 vaakariviä * 8 bittiä = 19 440 bittiä

Kehys luetaan vasemmalta oikealla ja ylhäältä alas 8000 kertaa sekunnissa, joka on sama kuin 64 kbit/s-kanavan näytteenottotajuus. Näin ollen yhden kehyksen ajaksi saadaan 125µs, mistä voidaan laskea bittinopeus. (12.)

19 440 bittiä / 125µs = 155,52 Mbit/s



Kuva 18. STM-1-kehyksen rakenne (12).

Kehyksessä yhdeksän ensimmäistä saraketta muodostavat otsikkoalueen, SOH. Tämän alueen tavuja voidaan käyttää esimerkiksi juuri verkonhallinnassa. Siirto-otsikon kolme ylintä riviä muodostavat toistinlaitevälin otsikon RSOH. Neljännellä rivillä on AU-pointterit. Viisi alinta riviä muodostavat multipleksointilaitevälin otsikon MSOH. Lopuksi jäävät 261 saraketta muodostavat virtuaalikontin VC-4, ja se jakaantuu kahteen osaan. Ensimmäisessä osassa on reittiotsikko POH (Path Overhead) ja toisessa osassa hyötykuorma C-4 (12).

6.3.3 STM-1-kehyksen otsikot

STM-kehyksestä löytyy reittiotsikko POH, multipleksointilaitevälin otsikko MSOH ja toistinlaitevälin otsikko RSOH niin kuin edellä mainittiin. Näitä otsikoita käytetään verkon valvonnassa ja ylläpidossa. (12.)

Kuva 19. STM-1-otsikko rakenne (12).

Reittiotsikko POH:ta käytetään laadun tarkkailemiseen sekä siitä saadaan selville käytetyn kontin tyyppi. J1-tavua käytetään lähettämään yhteensä 16 tai 64 tavun viesti kerrallaan. Jokaisella reitillä on oma viestinsä. Viesti tukee jatkuvaa testausta minkä tahansa reitin pisteen ja lähteen välillä. B3 on virheentarkistustavu reittivirheitä varten. C2-tavusta saadaan selville, mikä on kontin rakenne. G1-tavun avulla pystytään lähettämään tila- ja suorituskykymonitorointi informaatiota vastaanottavan pään päätelaitteelta lähettävälle laitteelle. F2 on huoltokanava operaattoreiden päätelaitteiden välille. H4-tavulla tehdään monikehys-vaiheosoitus TU-kuormalle. F3-tavu on sama kuin F2, mutta sen käyttö on riippuvainen virtuaalikonteista. K3-tavulla voidaan tehdä automaattinen reititys VC-4-poluille. N1-tavu on Tandem-yhteyden monitorointia varten. (12.)

Reittiotsikko MSOH:n kautta kulkee tietoa pariteetin tarkastamisesta, varareitityksestä sekä siinä on data- että äänikanava ja siihen kuuluvat myös irtonaisesti AU-pointterit. B2 on virheentarkistustavu, jota käytetään virheiden monitorointiin. K1-tavun kaikkia bittejä sekä K2-tavun bittejä 1-5 käytetään automaattiseen varmistuskytkentään. D4-D12 ovat datakanavatavuja, jotka muodostavat 567 kbit/s datakanavan. Niitä voidaan käyttää datan siirtoon tai verkonhallintaan. S1-tavu ilmoittaa synkronoinnin statuksen, mikä näyttää käytetyn kellolähteen tyypin. M1 on kaukopään virhehälytystavu. E2-tavua sanotaan

huoltopuhelintavuksi ja sitä voidaan käyttää puhelinkommunikointiin multipleksereiden välillä. (12.)

Toistinlaitevälin otsikko RSOH:n tehtävänä on kehyksen kohdistaminen, mutta siinä on myös erilaisia kanavia datalle ja puheelle sekä pariteettitarkistus. A1- ja A2- tavut ovat kehystahdistustavuja, jotka aloittavat jokaisen STM-1-kehyksen. Niiden sisältö on 11110110 00101000. J0 on 16 perättäistä lähetettyä jäljitystavua, jotka muodostavat toistinlaitevälin jäljitysviestin eli se varmistaa, että viesti tulee oikeasta paikasta. B1-virheentarkitustavua käytetään bittivirheiden monitorointiin. E1 on huoltopuhelintavu, jota käytetään puhekommunikointiin toistinten välillä. F1 on käyttäjälle suunnattu vapaana oleva tavu, jota voidaan käyttää tilapäisille data- ja puheyhteyksille. D1-D3-datakanavatavut (DCCM) muodostavat yhteensä 192 kbit/s datakanavan, jota käytetään käyttäjän datan siirtoon esimerkiksi VOIP (Voice over IP) tai verkonhallintaan. (12.)

6.3.4 STM-1 kehyksen rakentaminen

Kehyksen rakentaminen aloitetaan kehystämällä alijärjestelmäsignaali, josta muodostuu kontti C (container). SDH-verkoissa varsinainen tiedonsiirto tapahtuu juuri kontissa. Konttiin lisäämällä reittiotsikko POH siitä muodostuu virtuaalikontti VC, joka on kehyksen tärkein yksikkö. Koko tapahtumaketjua, jossa alijärjestelmäsignaali pakataan virtuaalikonttiin, sanotaan mapitukseksi. (12.)

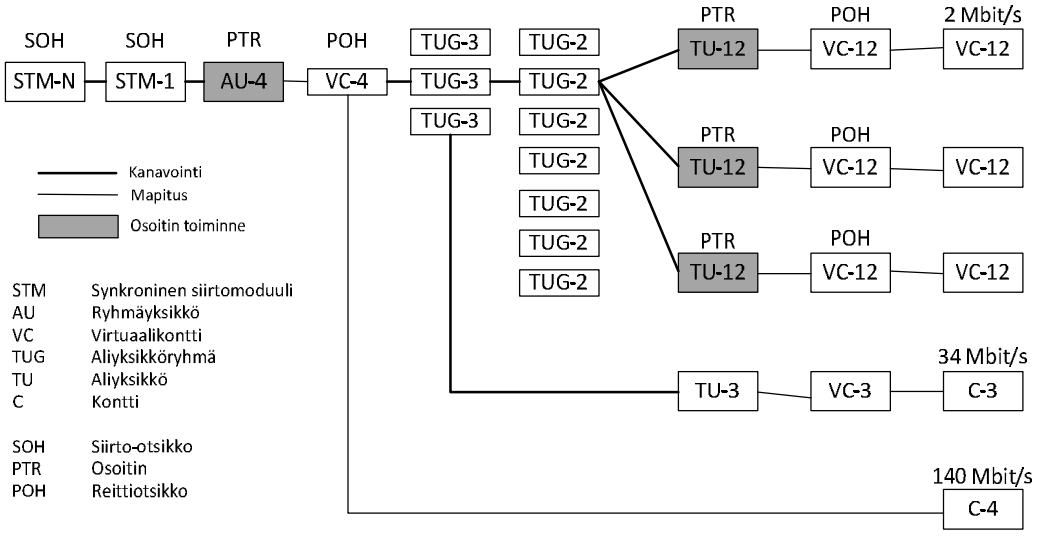
Seuraavaksi tehdään virtuaalikontin sijainnin määritys TU-osoittimeen ennen multipleksointia ylempään virtuaalikonttiin. Virtuaalikontti ja TU-osoite muodostavat aliyksikön TU:n (Tributary Unit). (12.)

Seuraavaksi multipleksoidaan useista aliyksiköistä aliyksikköryhmä TUG. Tämän jälkeen määritellään AU-4-osoittimeen VC-4:n sijainti suhteessa STM-1-kehykseen. Virtuaalikontti ja AU-4-osoitin muodostavat AU-4-hallintayksikön (Administrative Unit). AU-4-osoitin on aina kiinteässä paikassa STM-kehyksessä. (12.)

VC-4:n sijainti sen sijaan suhteessa STM-kehykseen on kelluva ja pystyy liukumaan STM-kehykseen nähden. Tästä seuraa, että yksi VC-4 voi sijaita kahdessa peräkkäisessä STM-1-kehyksessä. Alemman tason virtuaalikontit voivat tehdä saman VC-4:n sisällä. Ennen STM-1-kehyksen sijoittamista muodostetaan hallintayksikköjen ryhmä AUG

(Administrative Unit Group), joka on suoraan multipleksoitavissa vastaavan kokoiseen STM-kehykseen. (12.)

Lopuksi muodostetaan STM-1-kehys lisäämällä AUG:n multipleksointilaitevälin otsikko MSOH (Multiplexer Section Overhead) ja toistinlaitevälin otsikko RSOH (Regenator Section Overhead). Tämän jälkeen voidaan vielä STM-1 multipleksoida korkeamman tason STM-n kehyksiksi. (12.)



Kuva 20. STM-1-otsikko rakenne (12).

6.4 Multi Protocol Label Switching - MPLS

6.4.1 MPLS:n historia

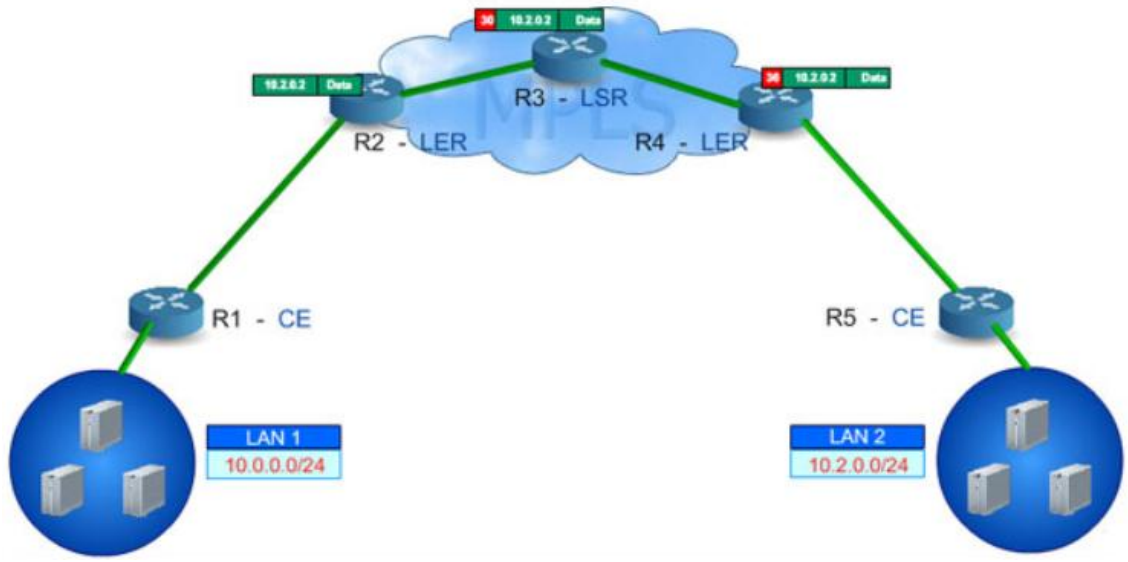
IETF muodosti vuonna 1997 työryhmän määrittelemään MPLS-standardia (Multi Protocol Label Switching). Tämän tarkoituksena oli ratkaista IP-protokollan skaalautumisongelmat ATM-verkkoja käyttäessä ja myös nopeuttaa huomattavasti tiedonsiirtonopeuksia. MPLS:ää määritettiin tukemaan kaikkia eri teknologioita, kuten Sonet, Frame Relayta, ATM:ää, Ethernetiä, PPP:tä (Point to Point Protocol) jne. MPLS on nimensä mukaisesti monia eri protokollia tukeva leimakytkentäinen protokolla, joka toimii OSI-mallin kerroksilla 2 ja 3. (14.)

6.4.2 MPLS:n toiminta

MPLS-verkon reunareititin tai sisääntuloreititin liittää leiman IP-pakettiin sen saapuessa kohdeverkosta ja lähettää paketin eteenpäin. Leimoissa on tietoa, jonka avulla jokainen reititin MPLS-verkossa tietää, miten paketti pitää käsitellä ja mihin se pitää välittää. Jokainen reititin verkossa tietää jo etukäteen kyseisten leimojen seuraavan reitin ja näin ollen sen ei tarvitse perinteiseen tapaan käydä tutkimassa vastaanottajan taulukkoa. Tämä nopeuttaa huomattavasti tiedonsiirtoa ja mahdollistaa suuremmat tiedonsiirtonopeudet. Kun paketti saavuttaa ulospääsyreitittimen, niin leima poistetaan ja IP-paketti välitetään kohdeverkkoon. (14.)

MPLS-verkossa kaikki reitit on määritelty etukäteen ja kaikissa paketeissa on tieto siitä ,mihin ne ovat menossa seuraavaksi. Näistä reiteistä käytetään nimeä LSP Label Switched Paths. Pakettien saapuessa ja poistuessa MPLS-verkosta täytyy reunareitittimien ymmärtää kohdeverkkojen protokollia sekä reititystietoja. (14.)

LSP- tai MPLS-tunneleista saadaan monenlaista etua ja hyötyä. Paketit kulkevat valmiiksi määritettyjä reittejä pitkin MPLS-verkossa, mikä siis nopeuttaa tiedonsiirtoa. Ainoastaan MPLS-tunnelin päästä pystytään syöttämään dataa, joka varmistaa datan eheyden. MPLS:ssä on hyvä skaalautuvuus eri IP-verkkojen välillä. (14.)



Kuva 21. Yksinkertaisen MPLS-verkon arkkitehtuuri (15).

6.4.3 MPLS:n elementit

MPLS-verkko sisältää kahden tyyppisiä reitittimiä, ja ne ovat reunareitittimet Label Edge Router (LER) sekä runkoreitittimet Label Switching Routers (LSR). Reunareitittimien tehtävä on lisätä FEC (Forward Equivalence Class) eli edelleenreititysluokka IP-pakettiin sen saapuessa MPLS-verkkoon. FEC-luokka muodostetaan jonkun yhteisen tekijän perusteella. Esimerkiksi paketit, jotka kulkevat samaa LSP:tä eli polkua pitkin tai kuuluvat samalle asiakkaalle, saavat yhteisen FEC-luokan. Samassa FEC-luokassa olevat paketit kulkevat samaa reittiä pitkin. MPLS-kirjallisuudessa on reunareitittimetkin voitu vielä erotella Ingress Label Edge Router ja Egress Label Edge Router eli sisäänpääsy- sekä ulospääsy-reunareittimet. LSR eli runkoreitittimen tehtäväksi jää välittää paketteja leimojen perusteella eteenpäin MPLS-verkossa. (14.)

6.4.4 MPLS:n tunniste

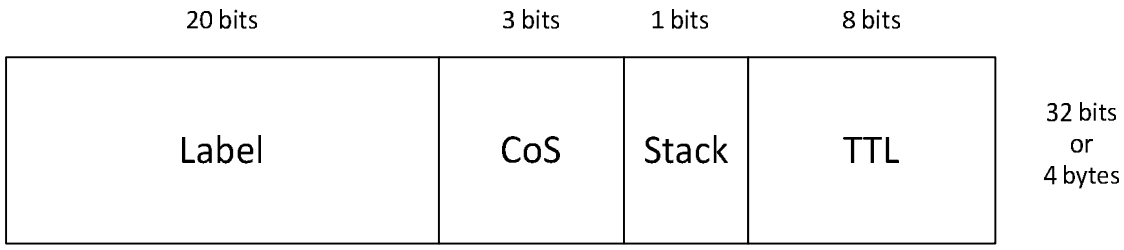
MPLS:n tunniste on 32 bittiä pitkä ja sisältää seuraavat kentät:

Leima (Label 20 bittiä) osiossa määritellään FEC-luokitus, jonka jälkeen annetaan leiman arvo. Näitä tietoja käytetään paketin lähettämiseen eteenpäin. (14.)

CoS (Class of Service 3 bittiä) tunnetaan myös nimellä TC (Traffic class) tai EXP. CoS:n perusteella LSR:t ja LER:t tietävät, mihin jonoon kukin paketti kuuluu. (14.)

Stack bitti kertoo, missä kohdassa hierarkiaa leima sijaitsee. MPLS-verkossa kulkevalla IP-paketilla voi olla siis useita päällekkäisiä leimoja. (14.)

TTL (Time-to-live) kertoo nimensä mukaisesti paketin elinajan MPLS-verkossa. TTL-arvo vähenee aina yhdellä, kun paketti siirtyy seuraavalle reititinlaitteelle. Jos arvo tippuu nollaan, paketti hylätään kokonaan. TTL:n avulla voidaan ehkäistä reitityssilmukoiden muodostumista sekä sen avulla voidaan jäljittää paketteja. LER:t muodostavat TTL:n MPLS-verkon reunalla sekä myös poistavat sen. (14.)

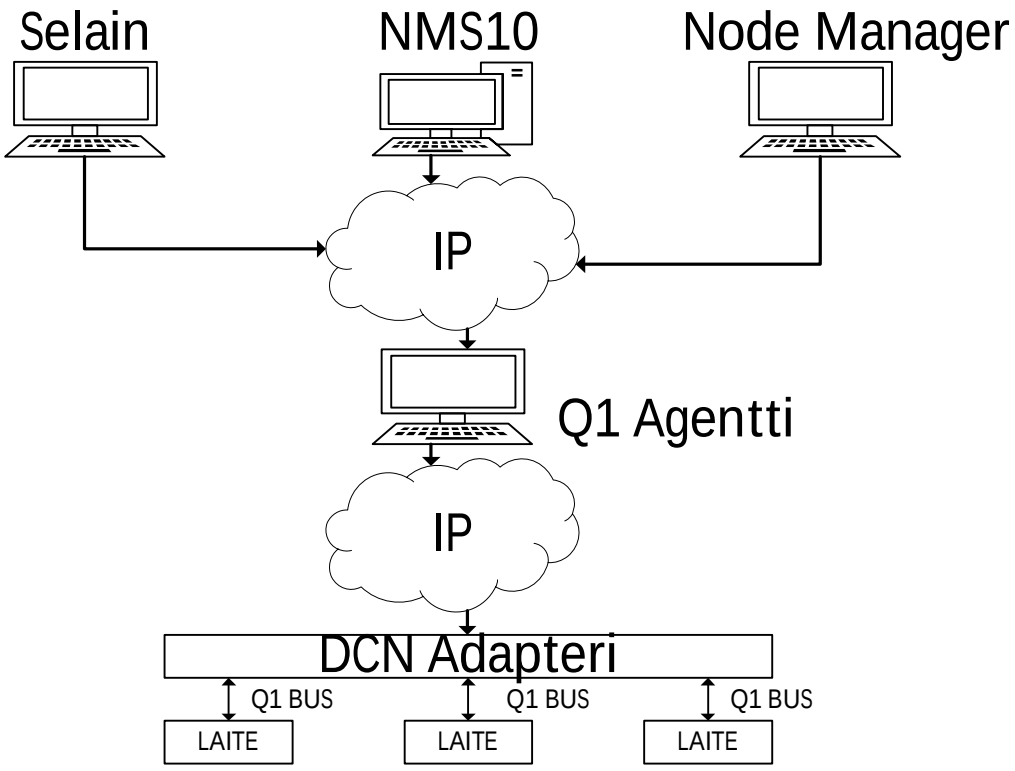


Kuva 22. MPLS:n tunniste.

7 Fingridin tietoliikenneverkon nykyinen hallintajärjestelmä NMS10

7.1 Yleistä

NMS10 on Nokian kehittämä graafinen verkonhallintajärjestelmä, joka on rakennettu HP OpenView'n päälle. NMS10:n ensisijainen tehtävä on kerätä hälytyksiä ja suorituskyvyn tietoja verkossa olevilta laitteilta Q1-agenttien avulla. Q1-agentti lähettää keräämiään tietoja eteenpäin SNMP:n välityksellä hallinta-asemalle, mikä näyttää ne järjestelmän ylläpitäjälle. Agenttien ja verkon laitteiden välillä on NMS10-järjestelmässä DCN-adaptereita, jotka hoitavat pollauksen Q1-protokollan avulla. Itse verkon laitteiden konfigurointia tehdään erillisillä Node Managereilla. Q1-pipe-protokolla mahdollistaa tämän konfigurointitoiminnon. (15; 17.)



Kuva 23. NMS10-Arkkitehtuuri (16, muokattu).

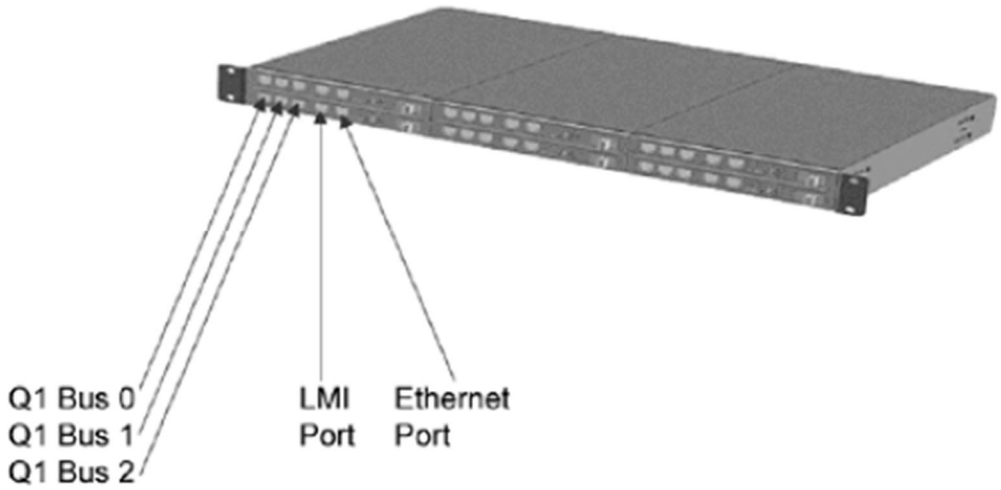
7.2 Q1-Agentin ominaisuudet

Q1-agentin ansiosta pystytään lisäämään, katsomaan, muokkaamaan ja poistamaan Q1-väyliä, laitteita, laitteiden tyyppejä, asemia ja managereita. Q1 tukee vianhallintaa,

suorituskyvynhallintaa, varaston hallintaa, kokoonpanon hallintaa sekä verkon testausta. Q1-agentti välittää tietonsa verkonhallinta-asemalle ja laitteiden päivityksistä myös Node Managerille. Q1-agentin avulla pystytään käynnistämään ja sulkemaan väyliä sekä pystytään skannaamaan verkkoa ja konfiguroimaan agenttien asetuksia. Q1-agentteilla pystytään myös luomaan ja palauttamaan varmuuskopioita. Q1-agentti tukee myös hälytyksien suodatusta. (16.)

7.3 DCN-adapteri

Q1-agentin ja DCN-adapterin avulla verkkoon voidaan lisätä Nokian laitteiden sekä hallintajärjestelmän lisäksi myös kolmannen osapuolen hallintajärjestelmiä. DCN-adapterin ja laitteiden välillä käytetään Nokian Q1-protokollaa. (16.)



Kuva 24. 6 kappaletta DCN-adaptereita kiinni yhdessä telineessä (16, muokattu).

DCN-adapterista löytyy viisi fyysistä liitäntä, jotka ovat seuraavat:

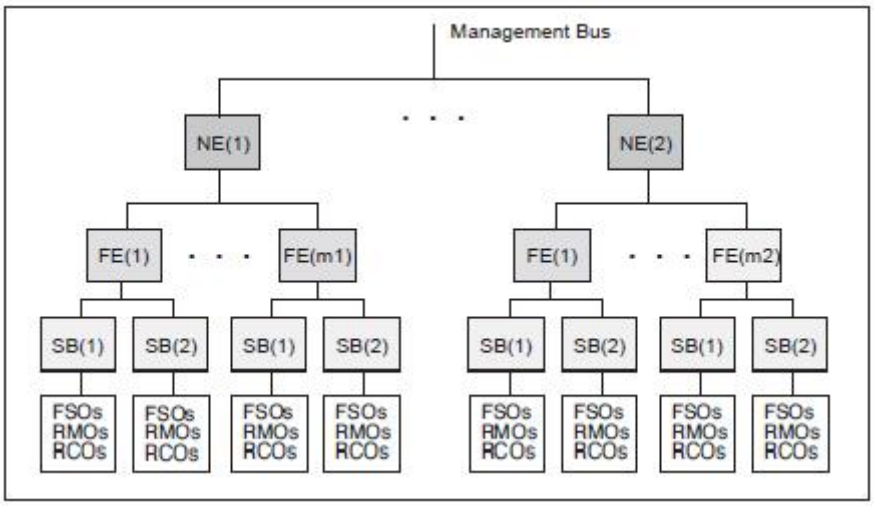
Ethernet-liitännän kautta adapteri voi liittyä suoraan paikalliseen hallintaverkkoon tai vaihtoehtoisesti silta tai reititin voi tarjota ethernet-liitännän Q1-agentille. Liitäntä on standardoitu 10Base-T, joka toimii half duplexina 10 Mbit/s nopeudella. Liitännän fyysinen rajapinta on RJ-45. (17.)

LMI (Local management interface) on paikalliseen hallintaan tarkoitettu liitäntä, jonka kautta voidaan konfiguroida adapteria CLI:n (Command line interface) avulla. Sitä käytetään esimerkiksi, kun määritellään laitteille IP-osoitteet. Liitäntä on V.24-sarjaliitin 9600 bits/s nopeudella. Liitännän fyysinen rajapinta on RJ-45. (17.)

DCN-adapterista löytyy vielä näiden liitäntöjen lisäksi 3 kappaletta Q1-väyliä. Niiden avulla voidaan ottaa suojattu yhteys verkon laitteisiin. Yksi Q1-väylä voi tukea parhaimmillaan, jopa 200 verkon laitetta yhtä aikaa. Kaikki Q1-väylät ovat erillisiä toisistaan ja niihin liitettäviin laitteisiin pitää määritellä yksilöllinen Q1-osoite. Tämä suojattu yhteys löytyy DCN-adaptereitten versioista C4.0/C4.1 alkaen. Liitännän fyysinen rajapinta RJ-45 ja sarjaliitäntä nopeus on 300 - 19200 bit/s. (17.)

7.4 Q1-protokolla

Nokian Q1-protokolla on SNMP:tä vastaava protokolla. Q1-protokolla on kehitetty versio Nokian TMS-protokollasta. Q1-protokollaa käytetään Q1-agentin ja laitteiden välisessä kommunikaatiossa. (18.)



Kuva 25. Laitteiden sisäinen hierarkia (18).

Laitteiden sisäinen hierarkia on jaettu neljään eri osaan, jotka ovat Network Element (NE), Functional Entity (FE), Supervision Block (SB). SB sisältää vielä kolme erillistä objektia. Objektit ovat Fault Supervision Object (FSO), Remote Measurement Object (RMO) ja Remote Control Object (RCO). Hierarkia toimii siten, että yksi NE voi sisältää

useamman FE:n. Yksi FE vois sisältää useamman SB:N ja yksi SB voi sisältää taas useampia objekteja. NE:t, FE:t ja SB:t tunnistetaan käyttämällä numerointia, joka voi vaihdella kokoonpanon mukaan. Objektien koodit ja niiden merkitykset löytyvät Nokian TMS dokumentaatiosta. (18.)

Network Element (NE) on verkkoelementti eli laite, joka välittää tietoa eteenpäin adapterille ja on kytkettynä Q1-väylään. Jokaisella laitteelle määritetään oma osoite, jolloin samaan Q1-väylään pystytään kytkemään useita laitteita. Osoitteet ovat 6-bittisiä. (18.)

Functional Entity (FE) on yksikkö, joka on yleisesti itsenäinen osa valvottavasta laitteesta. Esimerkiksi FE voi olla multiplekseri tai yksi terminaali toistimesta, jossa on kahdeksan terminaalia. SB:t antavat FE:lle hälytystietoja, jotka on määritelty seuraavasti: A hälytys on kiireellinen, B hälytys on laskennallinen, C on muistutushälytys ja D palvelu-hälytys. (18.)

Supervision Block (SB) -valvontalohko sisältää objektiryhmät FSO, RMO JA RCO. Yleisesti ottaen SB on erillinen osa valvottavaa laitetta, mutta ei anna erillistä hälytystä luokituksesta. Yksi FE on jaettu useaan eri SB:hen, jotta vianvalvonta, mittaus sekä kontrollointi voitaisiin erotella SB-numeroilla. Tämä tehdään sen takia, että yksi ja sama koodi voidaan käyttää vain kerran SB:ssä. SB:t on numeroitu heksalukuna ja numeroiden ei tarvitse olla peräkkäisiä. (18.)

FSO on vianvalvontaobjekti SB:ssä. FSO aktivoi vikakoodin vian sattuessa. Se aktivoi vikakoodin esimerkiksi silloin, kun jonkun ennalta määritellyn parametrin arvo ylittyy tai alittuu. FSO kertoo vikakoodin ja sen, missä SB:ssä vika on havaittu. (18.)

RMO on kaukomittausobjekti SB:ssä, ja se yksilöidään etämittauskoodilla Remote Measurement Code (RMC). Mittauskoodia käytetään yksilöimään eri mittaustoiminnot yhdessä SB:ssä. Jokaisella mittauskoodilla on omat mittausmenetelmänsä. Yleisemmin mittauskoodeja käytetään, kun mitataan bittivirheitä tai virtalähteen jännitteitä. Sama mittauskoodi voi sijaita vain yhdessä SB:ssä kerrallaan. Esimerkiksi, jos valvottavassa laitteessa olisi 3 virtajännitevirhettä ja 1 bittivirhe, niin kaikki 3 virtajännitevirhettä olisi oltava eri SB:ssä ja 1 bittivirhe voisi taas sijaita missä tahansa kolmesta SB:stä. RMO kertoo siis mittauskoodin sekä sen, missä SB:ssä se sijaitsee. (18.)

RCO on kauko-ohjausobjeti SB:ssä ja yksilöidään kauko-ohjauskoodilla Remote Control Code (RCC). Koodeja käytetään yleisesti ottaen kontrolloimaan takaisinkytkentöjä (loop-back) sekä suojausten tilaa laitteissa. Koodit toimivat samalla periaatteella kuin RMO:n esimerkissä on kerrottu. (18.)

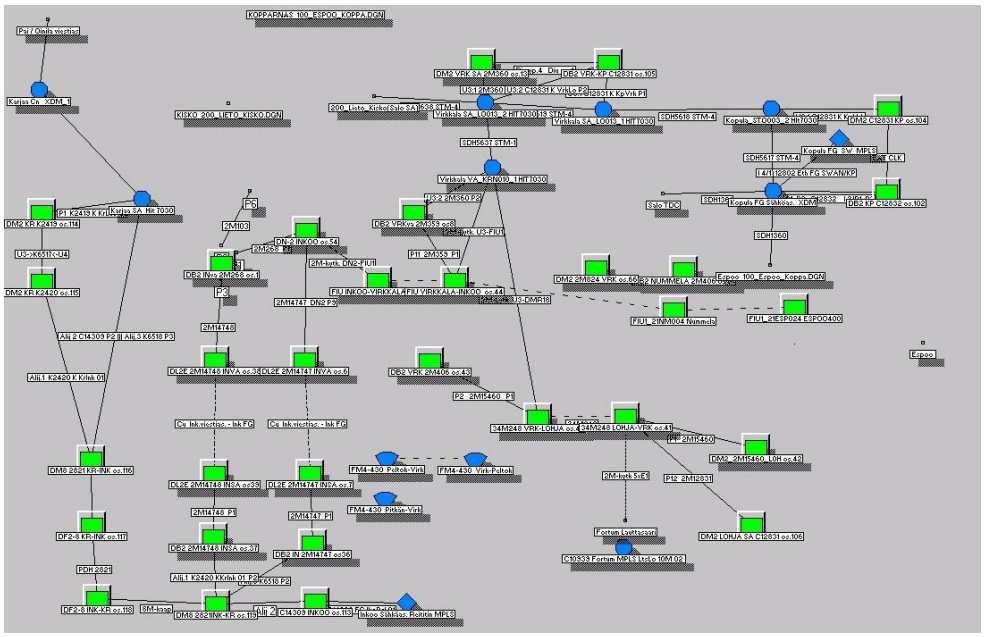
7.5 Q1 Pipe-protokolla

Q1 pipe-protokolla toimii TCP/IP-yhteyksien yli ja sillä on tarkoitus ottaa yhteys Clientiin. Esimerkiksi Node Managerit sekä suojauksenviestiyhteyslaitteet (SVY), kuten Nokian TPS64, kytketään käyttämällä Q1 pipe-protokollaa. Palvelin hyväksyy yleensä yhteydet porttiin 27500. (19.)

Palvelimen täytyy tukea useampia samanaikaisia TCP/IP-yhteyksiä, ainakin yhden yhteyden jokaista Q1-väylää kohden sekä yhden paikallista hallintaa varten. Esimerkiksi jos palvelin tarjoaa neljä kappaletta Q1-väyliä, sen täytyy tukea vähintään 5 TCP-yhteyttä samanaikaisesti. Riippuen sisäisistä resursseista palvelimella on mahdollisuus tukea myös enemmän samanaikaisia yhteyksiä. (19.)

7.6 Yhteenveto

Järjestelmää käyttävän henkilön mukaan NMS10-järjestelmässä on paljon hyviä puolia, mutta se on vanha lisensoitu järjestelmä, joka alkaa olla elinkaarensa loppupuolella. Ohjelmiston tuki on lopetettu, jonka takia siihen ei ole enää lisenssejä saatavilla. Järjestelmä on suunniteltu Windows NT-ympäristöön, josta johtuen siinä on tiettyjä rajoituksia. Esimerkiksi ohjelmisto ei tue moniprosessoriympäristöä. Nykyisin ohjelmistoa ajetaan Windows XP:n päällä, mikä aiheuttaa myös ongelmia mm. hitautta.



Kuva 26. NMS10-näkymä.

Verkkolaitteet sekä verkon topologia määritellään käsin NMS10-järjestelmään. NMS10 ei pysty näyttämään 64 kbit/s reittejä päästä päähän, vaan ne täytyy seurata käsin. Hälytyksen sattuessa verkkotopologia kuvasta ei pysty suoraan sanomaan, mistä hälytys johtuu, vaan se joudutaan tutkimaan käsin. Mitä enemmän verkossa on laitteita, sitä vaikeammiksi vian etsintä muuttuu. Solmuissa käytetyt objektit ovat kiinteitä eikä objekteja pysty järjestelmään lisäämään. NMS10-käyttöliittymästä näkee hälytystapahtumia taaksepäin 2 miljoonaa kappaletta. Hälytysten tallentaminen levylle on erittäin vaikeaa. Helpottavia tekijöitä olisi, jos 64 kbit/s yhteyksistä nähtäisiin reittinäkymä, sekä niitä pystyttäisiin nimeämään.

Mielestäni olisi hyvä, jos 64 kbit/s reitityksen tekeminen onnistuisi järjestelmässä automaattisesti ja pystyisi tekemään myös verkonvalvonnan tarpeita varten 1 - 4 bitin yhteyksiä aikavälin TS0 bitteihin 5 - 8. Tämän tulisi tapahtua kuitenkin siten, että ensin järjestelmä ehdottaisi reititystä ja lopullisen hyväksynnän antaisi käyttäjä.

8 Fingridin uusi verkonhallintajärjestelmä

8.1 Projektin taustat

Fingrid Oyj:n tietoliikenneverkkoa käytetään kaukokäyttöyhteyksiin (RTU), suojauksenviestiyhteyksiin (SVY) sekä laajakaistayhteyksiin (SWAN). Verkossa on käytössä tällä hetkellä luvussa 7 kuvatut PDH-, SDH- sekä MPLS-tekniikat.

Tämän projektin tarkoituksena on lähteä hankkimaan Fingrid Oyj:lle uutta verkonhallintajärjestelmää korvaamaan vanha NMS10-hallintajärjestelmä. Uuden verkonhallintajärjestelmän avulla on tarkoitus saada kaikki tietoliikennelaitteet sekä suojauksenviestiyhteyslaitteet reaaliaikaiseen valvontaan. Tällä hetkellä suojauksenviestiyhteyslaitteista saadaan ainoastaan kosketintietoon perustuva hälytys käytönvalvonnan ala-aseman laitteilta (RTU). Uuden verkonhallintajärjestelmän täytyy pystyä luomaan visuaalinen kuva verkon tilasta, laitteista ja yhteyksistä. Sen täytyy pystyä jakamaan reaaliaikaista tietoa kaikille sidosryhmille, tekemään verkon reititys sekä hoitamaan tietoliikennepalveluiden seuranta ja raportointi. Tarkoitus on myös, että suojaus- ja viestiyhteyksien dokumentaatio löytyy jatkossa verkonhallintajärjestelmästä.

Näillä toiminnoilla saadaan tarkka kuva verkosta ja sen toiminnasta sekä verkon laitteista. Tämä nopeuttaa reagointia vikatilanteissa, helpottaa verkon uudelleen konfigurointia ja parantaa huomattavasti turvallisuutta. Turvallisuutta parantaa myös se, että verkonhallintajärjestelmä tulee Fingridin omaan omistukseen ja se asennetaan yrityksen omiin tiloihin. Vanha NMS10-järjestelmä sijaitsee nykyisen palveluntoimittajan tiloissa. Tämän lisäksi pystytään tekemään helposti myös ennakoivia huoltotoimenpiteitä. Dokumentaation automatisoinnin tarkoituksena on vähentää huomattavasti dokumentaation tekemiseen tarvittavaa työmäärää. Järjestelmällä otetaan yksi askel lähemmäksi digitalisaatiota.

8.2 Verkonhallintajärjestelmän määrittely

8.2.1 Reititysominaisuudet

Uuden verkonhallintajärjestelmän täytyy pystyä luomaan sekä näyttämään 64 kbit/s yhteyksiä päästä päähän. Järjestelmän tulee pystyä lukemaan yhteyksiä koskevat tiedot

nykyisin käytössä olevista Nokian Dynanet-, DNWP:n Connection Master- sekä Coriantin SDH-laitteista. Liityntäkorttien asetukset pitää pystyä määrittelemään samassa yhteydessä, kun luodaan 64 kbit/s reittiä.

DNWP:n Connection Masterilla sekä Coriantin SDH-laitteilla täytyy pystyä luomaan myös päästä päähän-reittejä VC12/3/4, EoS (Ethernet over SDH) sekä EoS LCAS. Ethernet-liitynnän parametrit täytyy pystyä määrittelemään yhteyttä luodessa.

Verkonhallinnan täytyy pystyä näyttämään fyysisiä reittejä päästä päähän kaikkien valvottavien laitteiden läpi.

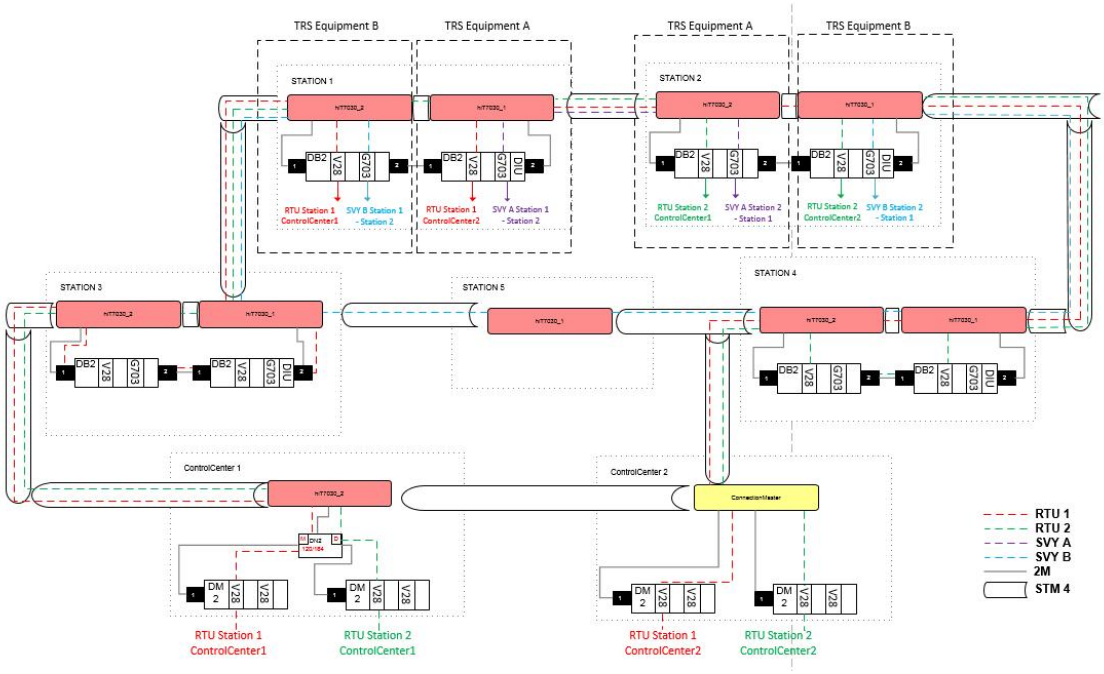
Reittejä/päätepisteitä täytyy pystyä muokkaamaan luomatta palvelua uudelleen. Palvelulla pitää pystyä olemaan erilaiset päätepisteet (esimerkiksi V.28 ja 2M).

64 kbit/s yhteyksien reitityksissä tulee ottaa huomioon, että toisiaan varmentavat yhteydet eivät kulje saman laitteen tai aseman tai kuitukaapelin läpi. Tällä saadaan varmistettua, että kahdennus on toimiva. Toisiaan varmentavat yhteydet on pystyttävä näyttämään samaan aikaan kartalla. Verkonhallintajärjestelmän tulisi pystyä tekemään 1 - 4 bitin yhteyksiä aikavälin TS0 bitteihin 5 - 8 Q1-verkonvalvontaa varten.

Verkonhallintajärjestelmän tulee pystyä näyttämään myös yhteydet, joissa ei ole päätepistettä tai päätepisteitä niin sanottuina haamuyhteyksinä.

Yhteydet on oltava varattavissa muokkausta varten. Järjestelmän tulee pystyä hakemaan verkosta olemassa oleva reititystieto ja ottamaan hallintaan käyttäjän määrittelemät reitit ykset.

Verkonhallintajärjestelmässä on pystyttävä muokkaamaan palveluita, asiakkaita, yhteystyyppejä (esimerkiksi RTU, SVY, SWAN) sekä reittejä.



Kuva 27. Suojauksenviesti- ja kaukokäyttöyhteyden reititys.

8.2.2 Ylläpitäjän ominaisuudet

Ylläpitäjällä täytyy olla mahdollisuus määrittää oikeudet käyttäjille eri laitteisiin ja järjestelmän toiminallisuuksiin. Esimerkiksi oikeustasoja voisi olla ylläpitäjä, muokkaaja sekä pelkkä katselija.

Suojauksenviestiyhteyslaitteilla pitää olla omat oikeutensa. Ylläpitäjän täytyy pystyä myös määrittämään käyttäjille oikeudet eri näkymiin.

Verkonhallintajärjestelmässä täytyy olla mahdollisuus varmuuskopiointiin sekä palautus varmuuskopioinnista koskien Dynanetin ja Connection Masterin asetuksia ja ristikytkentöjä.

Käyttäjien tekemistä tapahtumista pitää kerätä lokit, joita ylläpitäjä hallinnoi.

8.2.3 Verkkonäkymät

Verkonhallintajärjestelmän täytyy pystyä näyttämään erilaisia näkymiä. Esimerkiksi kun kartalla näkyvää asemaa klikataan päästään alemmalle tasolle, jossa näkyvät aseman laitteet sekä reititykset.

Asemille sekä laitteille täytyy pystyä määrittämään X- ja Y-koordinaatit. Näytettävän karttapohjan täytyy olla käyttäjän itse määriteltävissä.

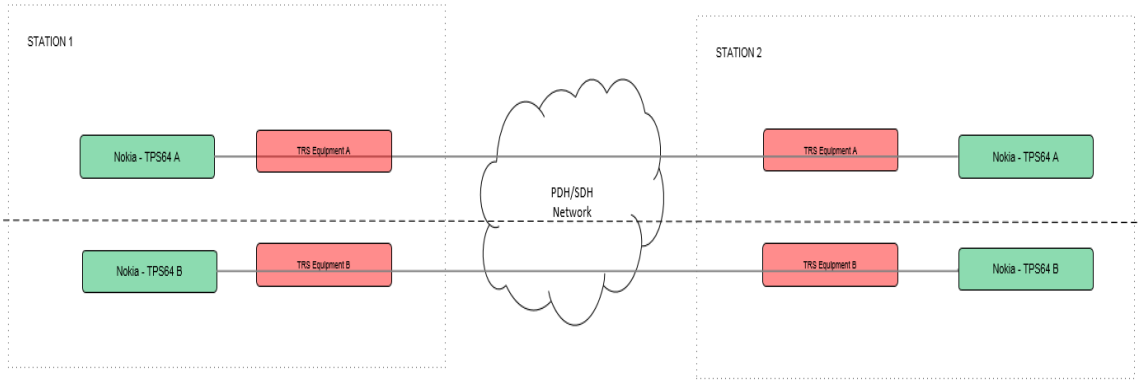
Sähköasemalla voi olla erikseen 400 kV:n ja 110kV:n asema, jolloin ne täytyy näyttää näkymässä erillisenä kohteina saman näkymän sisällä. Lisäksi mainituissa kohteissa olevat yksittäiset laitteet ja kohteiden väliset linkit täytyy näkyä.

Suunnittelunäkymässä tulee näkyä kaikki laitteet ja verkot. Tämä tarkoittaa sitä, että näkymässä näytetään olemassa olevat laitteet ja verkot, mutta myös suunnitellut verkot sekä laitteet. Olemassa olevan verkon sekä suunnitellun laajennuksen täytyy selvästi erottua toisistaan esimerkiksi värejä käyttämällä.

Verkkoon pitää pystyä lisäämään uusia laitetyyppejä myös virtuaalisia, jotta yhteydet voi kuvata mahdollisimman selkeästi. Objektit täytyy pystyä määrittämään järjestelmään itse tai ylläpitäjän toimesta.

Laitteissa, laitteiden välisissä yhteyksissä sekä asemissa täytyy näkyä sen hetkinen tilanne. Esimerkiksi hälytyksen sattuessa linkki välkyttäisi punaista tai keltaista valoa hälytyksen luokituksen mukaan. Välkyttäminen tarkoittaisi samalla, että hälytystä ei ole vielä kuitattu.

Suojauksenviestiyhteyksiä sekä synkronointia varten täytyy olla omat näkymänsä. Synkronointinäkymä päivitetään hälytyksistä. Esimerkiksi järjestelmään täytyy antaa synkronointihälytys, kun laitetta normaalisti synkronoiva 2 Mbit/s-yhteys menee poikki. Käyttäjän täytyy pystyä määrittelemään järjestelmä siten, että synkronoinnin tila käydään läpi automaattisesti.

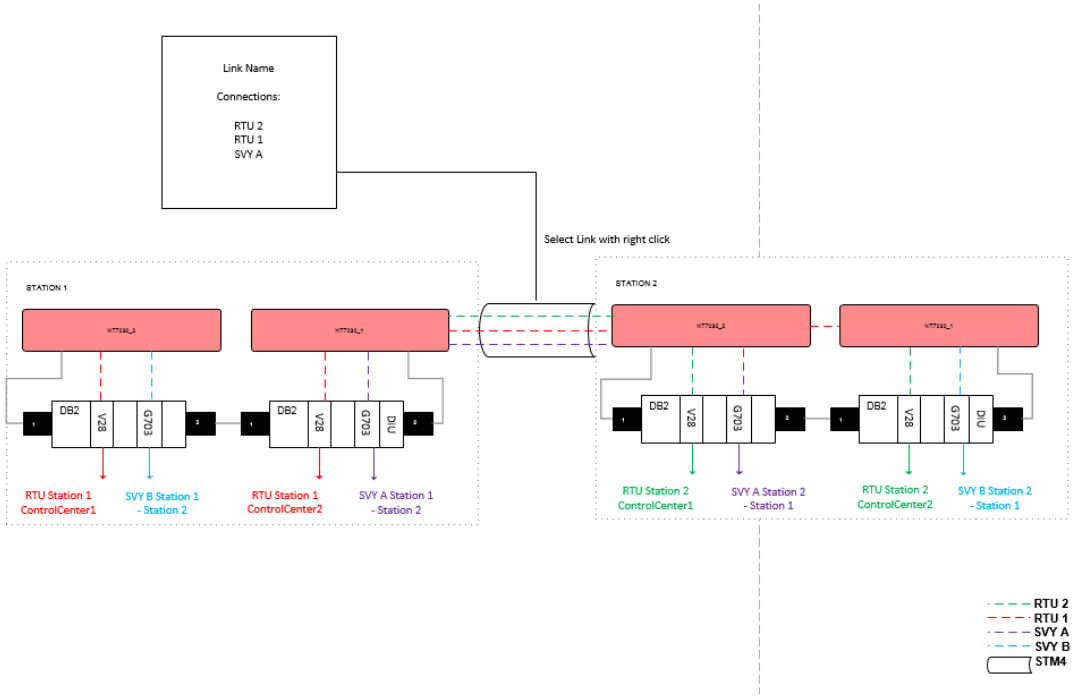


Kuva 28. Suojauksenviestiyhteyden näkymä.

Suojauksenviestiyhteyslaitteille tulee olla erillinen näkymä tapahtumalokia varten. Tapahtumalokista tulee näkyä niin nykyiset kuin aikaisemmat tapahtumat. Tapahtumahistoriassa täytyy olla tarkennettu haku, jossa pystytään hakemaan tapahtumia eri parametrien avulla suodatettuna. Tämä on erityisen tärkeää suojauksenviestiyhteyslaitteille.

Yhteyksistä täytyy näkyä sen tyyppi. Esimerkiksi onko se kupari-, optinen-, radiolinkki-, radiomodeemi- vai satelliittiyhteys. Käyttäjän pitää pystyä määrittämään nämä linkkityypit. Esimerkiksi kupari voisi olla musta viiva ja radiolinkki musta katkoviiva jne.

Asemiin, laitteisiin, yhteyksiin ja hälytyksiin tulisi pystyä lisäämään huomioita kommenttiteksteillä.



Kuva 29. Linkin näkymä.

8.2.4 Hälytykset

Käyttäjän täytyy pystyä määrittelemään useampia hälytysnäkymiä ja muokkaamaan niitä halutun näköiseksi esimerkiksi erilaisilla suodatuksilla. Hälytysnäkymässä täytyy pystyä

valitsemaan niin nykyiset kuin aikaisemmat hälytykset sekä käyttäjän määrittelemän aikavälin mukaan. Hälytyksiä olisi hyvä pystyä suodattamaan esimerkiksi Q1-väylä- sekä solmutasolla.

Asemille, linkeille, palveluille, kaukokäytön- ja suojauksenviestiyhteyksille sekä reitittimille ja muille lähiverkkolaitteille tulee olla omat hälytysnäkymät. Asemanäkymään täytyy pystyä lisäämään asemakohtainen hälytyslista.

Järjestelmän täytyy pystyä näyttämään hälytykset hierarkian mukaan eli mistä vika on lähtöisin, jotta vika olisi mahdollisimman helppo jäljittää. Esimerkiksi jos STM-16 on poikki, pystyttäisiin lähtemään purkamaan hälytyksiä ylhäältä alaspäin.

8.2.5 Raportit

Verkonhallintajärjestelmän pitää pystyä luomaan suorituskyvynraportteja järjestelmästä (kaukokäyttöyhteydet ja suojauksenviestiyhteyksistä), palveluista, laitteista ja yhteyksistä. Suojaus- ja kaukokäyttöyhteyksien käytettävyysraporteissa täytyy olla tieto sekä yksittäisten yhteyksien käytettävyydestä, että koko järjestelmän käytettävyydestä.

Järjestelmän pitää pystyä luomaan raportteja laitteista, jotka eivät ole hallinnan alla ollenkaan sekä 64 kbit/s yhteyksistä, joissa on vain yksi päätepiste tai päätepistettä ei ole ollenkaan.

Verkonhallintajärjestelmän pitäisi myös pystyä luomaan raportti verkossa olevista laitteista (malli, versio) ja määristä.

8.2.6 Tuki

Verkonhallintajärjestelmästä täytyy olla mahdollisuus saada 24 tuntia vuorokaudessa oleva tuki niin kauan, kun järjestelmä on kunnolla käyttöön otettu ja asiantuntijat hallitsevat järjestelmän. Sen jälkeen pitää olla 8 tuntia 5 päivää viikossa oleva tuki. Tämän lisäksi järjestelmästä täytyy saada kattava koulutus, käyttäjädokumentaatio sekä käyttöönotto-ohjeet.

8.2.7 Lisäominaisuudet

Verkonhallintajärjestelmään olisi hyvä pystyä integroimaan nykyinen Fingridin omaisuudenhallintajärjestelmä.

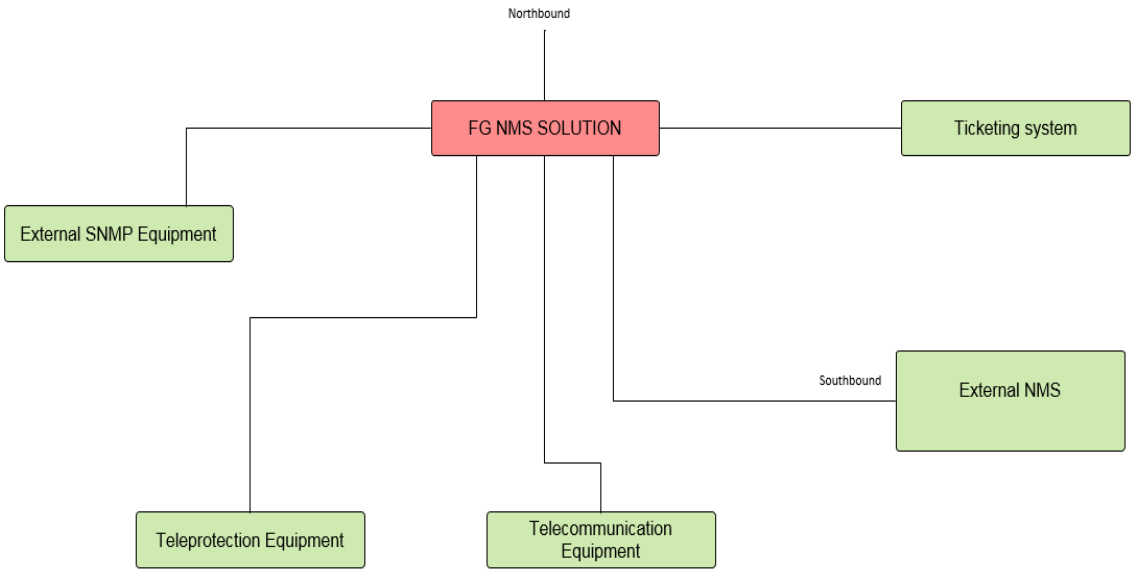
Järjestelmässä pitäisi pystyä siirtämään olemassa olevasta Q1-serveriltä laitteiden tiedot, kuten hw- ja sw-versiot, valvontaväylät, osoitteet, laitetyypit ja asematiedot.

Northboundliitynnän avulla pitäisi pystyä välittämään palveluiden hälytykset ylemmän tason valvontajärjestelmään.

Verkonhallintajärjestelmään olisi hyvä pystyä ottamaan vastaan Southbound SNMP trappeja useammasta järjestelmästä. Esimerkiksi pystyttäisiin samaan kolmannen osapuolen NMS-järjestelmästä tietoja, kuten MPLS (palveluista) tai satelliittien tai kaukokäyttöyhteyksien verkonhallintajärjestelmästä.

Verkonhallintajärjestelmän olisi hyvä pystyä valvomaan IP-pohjaisten laitteiden porttien, virtalähteiden ja tuulettimien tilaa.

Järjestelmän tulee olla täysin kahdennettu, jotta järjestelmän luotettavuus ja käytettävyys on riittävä.



Kuva 30. Verkonhallintajärjestelmään liitettävät laitteet sekä järjestelmät.

9 Yhteenveto

Insinöörityössä tutkittiin ja opittiin ymmärtämään, mitä kaikkia etuja verkonhallintajärjestelmällä on tarkoitus saada. Hallinnan ja valvonnan tarkoitus on helpottaa huomattavasti verkkoa operoivan työntekijöiden työtä sekä pienentää työmäärää tarjoamalla kaikki se tieto ja dokumentaatio verkosta, jonka avulla verkkoa pystytään helposti muokkaamaan sekä nopeasti selvittämään verkossa syntyneet vikatilanteet.

Verkonhallintajärjestelmiä on kehitetty monenlaiseen eri käyttöön. Isoissa yrityksissä, joissa on käytössä paljon erilaisia tekniikoita ja protokollia, tarvitaan rinnakkaisia verkonhallintajärjestelmiä. Ihannetilanteessa kuitenkin nämä kaikki verkonhallintajärjestelmät pystytään integroimaan yhteen järjestelmään siten, että yhdellä järjestelmällä pystyttäisiin monitoroimaan muita järjestelmiä ainakin osittain.

Yksinkertaisuudessaan verkonhallinnan arkkitehtuuri ja siihen kuuluvat komponentit ovat hyvin selkeitä. Kuitenkin laajoissa verkoissa, missä on paljon eri laitevalmistajien laitteita, tekniikoita ja useita protokollia vaatii erittäin paljon asiantuntemusta ottaa tarvittavat asiat huomioon verkonhallintajärjestelmässä.

Verkonhallinnassa yleisimmin käytössä oleva protokolla on SNMP, mihin työssäkin perehdyttiin, mutta variaatioita on monenlaisia ja muitakin protokollia on käytössä. Suurimpana ongelma tässä tulee vastaan useiden protokollien yhdistäminen samaan järjestelmään.

Projektissa tutustuttiin valittujen tarjoajien olemassa oleviin verkonhallintajärjestelmiin ja niiden ominaisuuksiin. Käytännön osuudessa määriteltiin Fingrid Oyj:n verkonhallintajärjestelmän vaatimukset ja tarvittavat ominaisuudet. Näitä vaatimuksia käytettiin Fingridin tarjouspyynnön teknisessä osassa. Hankinnan osuus ei ehtinyt mukaan tähän työhön. Hankintaa tullaan jatkamaan tämän työn pohjalta, yhteistyössä Fingridin asiantuntijoiden kanssa.

Tätä työtä jatketaan myös käytännön asioiden osalta, kuten miten verkonhallintajärjestelmä pystytään liittämään olemassa olevaan verkkoon sekä minne päin verkkoa asiakaskoneet sekä palvelimet sijoitetaan. Palvelimia, asiakaskoneita ja näyttöjä hankittaessa tulee ottaa huomioon järjestelmän niiltä vaatimat ominaisuudet.

Lähteet

1 Fingrid. Verkkodokumentti. <http://www.fingrid.fi/fi/Sivut/default.aspx>. Luettu 30.9.2016.

2 Hautaniemi, Mika. 1994. Diplomityö. Verkkodokumentti. <http://www.net-lab.tkk.fi/julkaisut/tyot/diplomityot/611/verkonhallinta.html>. Luettu 7.10.2016.

3 Jaakohuhta, Hannu. 2005. Lähiverkot – Ethernet. Helsinki: Edita.

4 Chapple, Mike. Verkkodokumentti. <http://searchsecurity.techtarget.com/tip/Introduction-to-SNMPv3s-security-functionality>. Luettu 10.10.2016.

5 2014. Verkkodokumentti. <https://www.juniper.net/documentation/en_US/junos14.2/topics/concept/snmp-v3-overview-junos-nm.html>. Luettu 25.10.2016

6 Simoneau, Paul. 1999. SNMP Network Management. McGraw-Hill.

7 Happonen, Ari. 2005. SNMP raportti. Verkkodokumentti. <http://www.it.lut.fi/kurssit/04-05/010626000/linux-tyot/SNMP_Raportti_Ari_Happonen.pdf>. Luettu 27.10.2016.

8 Wikipedia. 2016. TCP/IP-malli ja OSI-malli. Verkkodokumentti. <https://fi.wikipedia.org/wiki/TCP/IP-viitemalli>. Luettu 28.10.2016.

9 Fingridin sisäinen tietoliikenne kurssi. 2008.

10 Nokia. DN2 Functional description.

11 Tutustuminen SDH-tekniikkaan. Verkkodokumentti. <http://www.com-lab.hut.fi/opetus/141/SDH_labra.pdf>. Luettu 29.10.2016

12 RMON2.2016. Verkkodokumentti.<http://www.ciscopress.com/articles/article.asp?p=1073230&seqNum=4>. Luettu 31.10.2016

13 IBM.RMON2. Verkkodokumentti. <http://www.ibm.com/support/knowledgecenter/SSTFXA_6.3.0/com.ibm.netcool_ssm_4.0.1.doc/rg/reference/appRMON2_overview_r.html.>. Luettu 01.11.2016

14 MPLS info. 2009. Verkkodokumentti. <http://mplsinfo.org/index.html>. Luettu 5.11.2016.

15 Nokia. NMS/10 SR C6.1 Product Overview.

16 Nokia Siemens Network. Q1 Agent C4.0 and DCN Adapter C4.0/C4.1 Product Overview.

17 Nokia Siemens Network. DCN Adapter C4.1 User Guide.

18 Nokia. TMS4 Transmission management system. Nokia TMS protocol Description.

19 Nokia. Nokia Q1 Management Pipe Protocol. Protocol Specification