Satakunnan ammattikorkeakoulu

Vesa Lummevaara

SNMP V3 VERKONHALLINTA & CISCOWORKS

Tekniikan Porin yksikkö
Tietotekniikan koulutusohjelma
Tietoliikenteen insinöörityötkinto
2008

SNMP V3 VERKONHALLINTA & CISCOWORKS

Lummevaara, Vesa
Satakunnan Ammattikorkeakoulu
Tietotekniikan koulutusohjelma
Kesäkuu 2008
Mustonen, Arto
UDK: 004.73
Sivumäärä: 85

Asiasanat: SNMP, verkonhallinta, RMON, Ciscoworks, LMS

Tämän opinnäytetyön aiheena oli tutkia SNMP version 3 -verkonhallintaprotokollaa ja sen soveltamista lähiverkossa Ciscoworks -ohjelmistotyökaluilla. Näitä varten koulun tietoliikenteen laboratorioon rakennettiin pieni testilähiverkko, jossa SNMPv3:a ja verkonhallintaohjelmia hyödynnettiin tämän verkon laitteiden hallintaan.

Teoriaosuudessa perehdyttiin SNMP:n arkkitehtuuriin käyden läpi sen toimintaa verkossa ja esiteltiin sen peruselementit. Tässä osuudessa tarkasteltiin myös SNMP:n kehitys ensimmäisestä versiosta nykyisin käytettävään kolmanteen versioon, sekä RMON -tekniikka verkon kokonaisliikenteen valvontaan.

Käytännön osuudessa tutustuttiin Cisco -laitteiden SNMPv3 -komentoihin ja konfigurointiin Ciscoworks -hallintaa varten. Ciscoworks Lan Management Solution -ohjelmien toiminta ja niiden pääpiirteet esiteltiin lyhyesti. Tämän jälkeen tarkasteltiin SNMPv3:n ja sen tietoturvaominaisuuksien hyödyntämistä LMS:n ohjelmilla, kuten hallittavien laitteiden ominaisuuksien ja asetusten noutamista ja muuttamista laitteessa. Myös SNMPv3:n pyyntö-, asetus- ja trap -sanomien rakennetta ja sisältöä purettiin tarkastelua varten.

Saatuihin tuloksiin ja Ciscoworks -pohjaiseen verkonhallintaan oltiin tyytyväisiä. Ciscoworks LMS -ympäristö vaatii sen käyttäjältä pientä perehtymistä sen ohjelmien toimintaan, mutta nämä hallittaessa se antaa käyttäjälleen tehokkaat ja yksityiskohtaista tietoa tarjoavat työkalut niin pienten kuin suurtenkin lähiverkkojen tietoturvalliseen hallintaan. Ciscoworks LMS -ohjelmapakettia voidaankin käyttää verkonhallinnan opetusympäristönä.

NETWORK MANAGEMENT USING SNMP V3 & CISCOWORKS

Lummevaara, Vesa
Satakunta University of Applied Sciences
Degree Programme in Telecommunications
June 2008
Mustonen, Arto
UDC: 004.73
Number of Pages: 85

Key Words: SNMP, network management, RMON, Ciscoworks, LMS

The subject of this thesis was to research network management based on SNMP version 3 and by using the Ciscoworks -software. For reaching these goals a test-LAN was built in the universitys IT-laboratory and the Ciscoworks LMS -software was implemented along with SNMPv3 to manage this LAN and the devices in it.

In the theory part of this thesis the architecture of SNMP was introduced, including the action strategy of SNMP in a network and explaining the basic elements of it. Also the development of SNMP from version 1 to 3 was introduced along with the RMON-protocol. RMON is used for collecting statistics of the total traffic in the LAN.

SNMPv3 configuration commands and syntaxes in Cisco devices were explained in the practical part of this thesis. Ciscoworks Lan Management Solution -applications were introduced along with using these applications for SNMPv3 based network management and implementing its security features. The SNMPv3 message format, Get, Set and Trap packets in the test-LAN were also analysed.

The final results of using Ciscoworks for network management were good. Thus, Ciscoworks LMS -applications require that the administrator familiarizes himself with these tools for effective and secured network management and gains a lot of detailed information of different size LAN's and network devices. The Ciscoworks LMS software is applicable for a network management learning environment.

SISÄLLYS

1 JOHDANTO

Erilaiset tietoverkot tarjoavat erilaisia palveluja ja protokollia, joilla kuljettaa tietoa verkossa. Tänä päivänä tietoverkkojen kehittyessä laajemmiksi niin yrityksissä kuin oppilaitoksissakin tarvitaan palveluja ja protokollia joiden avulla verkkojen ylläpitäjät voivat etsiä verkosta virheitä, valvoa sen resurssien saatavuutta ja kontrolloida sen laitteiden toimintaa. Tätä kutsutaan verkonhallinnaksi.

Simple Network Management Protocol on jo pitkään ollut TCP/IP -pohjaisten verkkojen hallinnan yleiskäsite. SNMP mahdollistaa verkon laitteiden ja näiden objektien sujuvan hallinnan yksinkertaisessa rakenteessa. SNMP:tä on kuitenkin vaivannut 2000 -luvulle saakka yksi suuri ongelma, joka tänä päivänä on tietoliikenteessä hyvin yleisesti esillä ja kahvipöytäkeskustelujen aiheena; nimittäin tietoturvattomuus. Vuonna 2002 ongelmaan saatiin ratkaisu, kun SNMP:n 3. versio toi mukanaan käyttäjien tunnistuksen ja lähetettävän tiedon salauksen. SNMPv3:en perustuu myös tämä opinnäytetyö.

SNMP -verkonhallinta vaatii kuitenkin vähintään yhden hallinta-aseman, jossa on SNMP -sanomia tulkitseva ja niitä lähettävä ohjelmisto. Tällaisia ohjelmia ovat muun muassa Castlerockin SNMPc -hallintaohjelma ja Ciscoworks LMS -ohjelmapaketti.

Tätä opinnäytetyötä tarjottiin minulle syksyllä 2007 ja päätavoitteena oli tutkia SNMPv3:n teoriaa ja sen käyttöönottoa Cisco Systems:n laitteilla Satakunnan ammattikorkeakoulun Porin yksikön tietoliikenteen laboratoriossa. Tähän työhön kuului myös juuri koululle hankitun Ciscoworks Lan Management Solution -ohjelmapaketin käyttöönotto ja sen verkonhallintatyökalujen ominaisuuksien ja toimintojen selvittäminen. LMS -ympäristössä oli tarkoitus soveltaa SNMPv3:a laitteiden hallintaan. Ohessa oli myös ajatus tutkia mahdollisuutta soveltaa Ciscoworks:n SNMPv3 -pohjaista verkonhallintaa oppimisympäristönä koulun

tietoliikenteen laboratoriossa. Koska olin kiinnostunut tutustumaan lähemmin SNMP -verkonhallintaan ja Cisco Systems:n ohjelmistoihin, otin työn innolla vastaan.

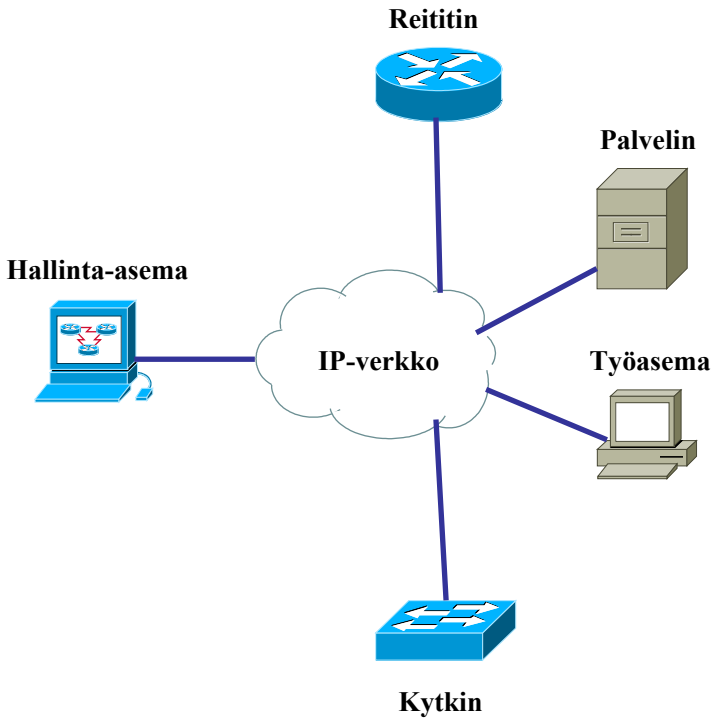
Tämän kirjallisen osuuden aluksi tutustutaan hieman SNMP:n arkkitehtuuriin ja sen kehitykseen vuosien saatossa. Koska RMON -tekniikka on tärkeä osa SNMP:tä ja verkonhallintaa, on se käyty lyhyesti lävitse tässä teoriaosuudessa. Laitteiden konfigurointi -kappaleessa käydään läpi SNMPv3:n asetusten käyttöönotto Ciscon laitteilla. Tässä kappaleessa painotetaan myös niitä komentoja, joita Ciscoworks -ympäristössä tulisi käyttää. Tämän jälkeen tarkastellaan Ciscoworks LMS ja sen sisältämät ohjelmat. Vaikka tässä opinnäytetyössä onkin valotettu näiden ohjelmien käyttöä ja toimintaa, on siitä huolimatta suositeltavaa tukeutua myös LMS -ohjelmiston omaan manuaaliin. Viimeiseksi tarkastellaan SNMPv3 -pohjaista verkonhallintaa Ciscoworks LMS:n ohjelmilla käymällä läpi tärkeimmät SNMPv3:a käyttävät ohjelmat ja niiden työkalut, sekä tutkitaan testiverkosta kaapattujen SNMP -sanomien rakennetta ja sisältöä.

2 SNMP ARKKITEHTUURI

SNMP on IETF:n (Internet Engineering Task Force) määrittelemä OSI -kerrosmallin sovelluskerroksen (Layer 7) verkonhallintaprotokolla verkon eri komponenttien, kuten reitittimien, kytkinten, palvelimien ja työasemien hallintaan (Kuva 2-1). Se koostuu joukosta standardeja, jotka kuvaavat sovellustason toiminnan, tietokannan rakenteen ja dataobjektit. SNMP on suunniteltu käytettäväksi UDP/IP -yhteyden ylitse, ja koska UDP on yhteydetön protokolla, on myös SNMP yhteydetön. SNMP:llä hallittavien laitteiden informaatiosisältöä käsitellään muuttujina (Variables). SNMP on myös nimensä mukaisesti pidetty mahdollisimman yksinkertaisena huolimatta uudempien versioiden tuomista lisäyksistä protokollaoperaatioihin ja arkkitehtuuriin. /1/

SNMP:n ajatus on tarjota verkon järjestelmänvalvojalle kehysmalli, jolla voidaan hallita verkon tapahtumia ja helpottaa vianhakua. Sen avulla voidaan vastata välittömästi laitteiden lähettämiin vikaraportteihin ja tehdä korjaukset etätyöasemalta. Tämä ja hallittavan verkon liikenteen valvonta tuovat kustannustehokkaan ratkaisun. /1/

SNMP:n käyttöön liittyy kolme tärkeää peruskomponenttia; Verkonhallinta-asema (Network Management Station, NMS), hallittavissa kohteissa sijaitsevat agenttitoiminnot (Network Management Agent, NMA) ja hallintatietokanta (Management Information Base, MIB). NMS käyttää eri protokollaoperaatioita ja -sanomia hakeakseen ja asettaakseen tietoa agenttien MIB-tietokannasta. Näitä pdu-komentoja ovat Get, GetNext, GetBulk ja Set. Agenttijärjestelmiin voidaan myös asettaa ”triggerikomentoja”, jotka tietyn ehdon toteutuessa lähettävät hälytyksen tai ilmoituksen NMS:lle. Näitä operaatioita ovat Trap ja Inform. /1/



Kuva 2-1. Tyypillinen SNMP -verkko hallittavine laitteineen.

Seuraavaksi käydään läpi SNMP verkon peruselementit, jotka ovat hallinta-asema (NMS), agentit ja hallintatietokanta MIB. Kuva 2-2 selventää elementtien keskinäisen kommunikoinnin.

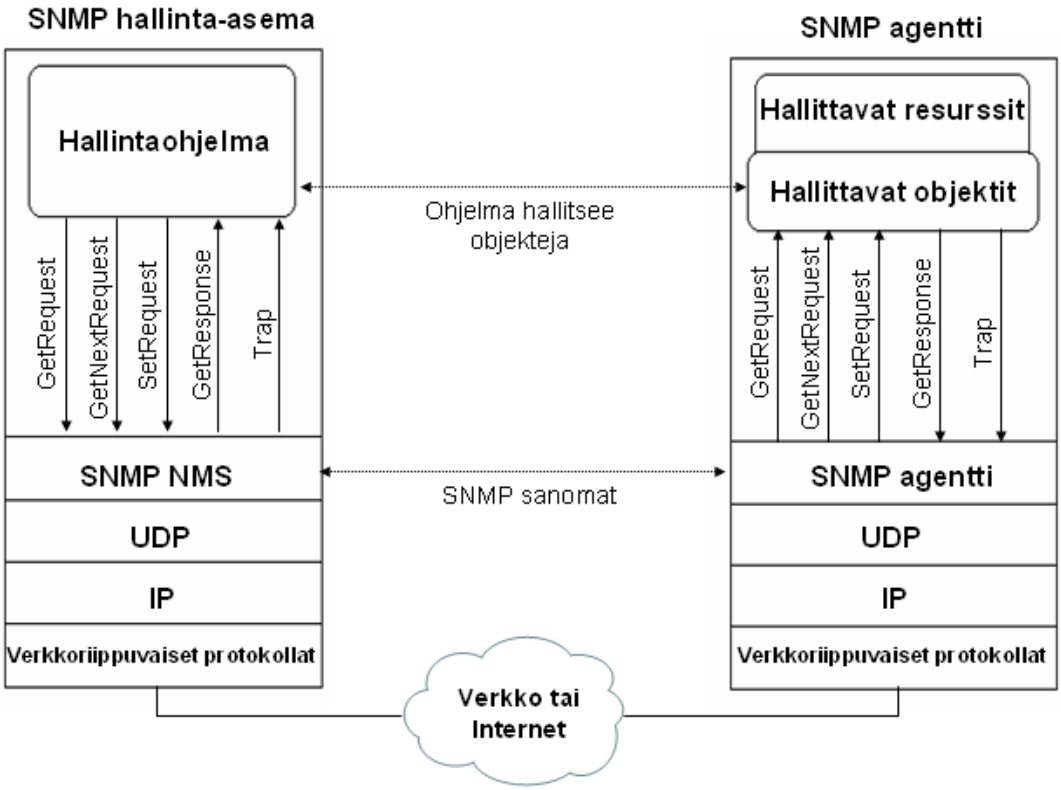
2.1 NMS

Hallinta-asema (usein myös Network Management System tai Console) on tyypillisesti itsenäinen työasema tai palvelin, mutta se voi olla myös jaettu järjestelmä. NMS käyttää verkonhallintaohjelmistoa, joka voi koostua useista hallintatyökaluista. Nämä työkalut tarjoavat järjestelmänvalvojalle rajapinnan verkon objektien hallintaan. NMS:n avulla voidaan monitoroida verkon liikennettä, muuttaa verkon laitteiden asetuksia, hallita vikatilanteista toipumista, ja hakea muuta tietoa verkosta ja sen eri osista. Fyysisenä laitteena NMS on tehokas tietokone suurella keskusmuisti- ja kiintolevykapasiteetilla sekä nopealla prosessorilla varustettuna. NMS käyttää pdu -komentoja, joilla se hakee informaatiota muuttujien muodossa agenttien hallinnoimilta laitteilta. Näistä sanomista kerrotaan lisää seuraavassa kappaleessa. /1/ ja /2/

2.2 Agentit

Agentit ovat hallittavan verkon laitteilla sijaitsevia ohjelmistomoduuleja, jotka huolehtivat kommunikoinnista hallinta-asemien kanssa tarjoten informaatiota hallitsemastaan laitteesta. Agentteja voidaankin pitää SNMP arkkitehtuurissa verkon fyysisinä laitteina. Agentit vastaavat NMS:ien lähettämiin Get -pyyntöihin Response -sanomilla, jotka sisällyttävät pyydetyn informaation arvon. Lähetettävän tiedon agentit säilyttävät lokaalin laitteen puurakenteisessa tietokannassa muuttujina. Tästä tietokannasta käytetään lyhennenimitystä MIB.

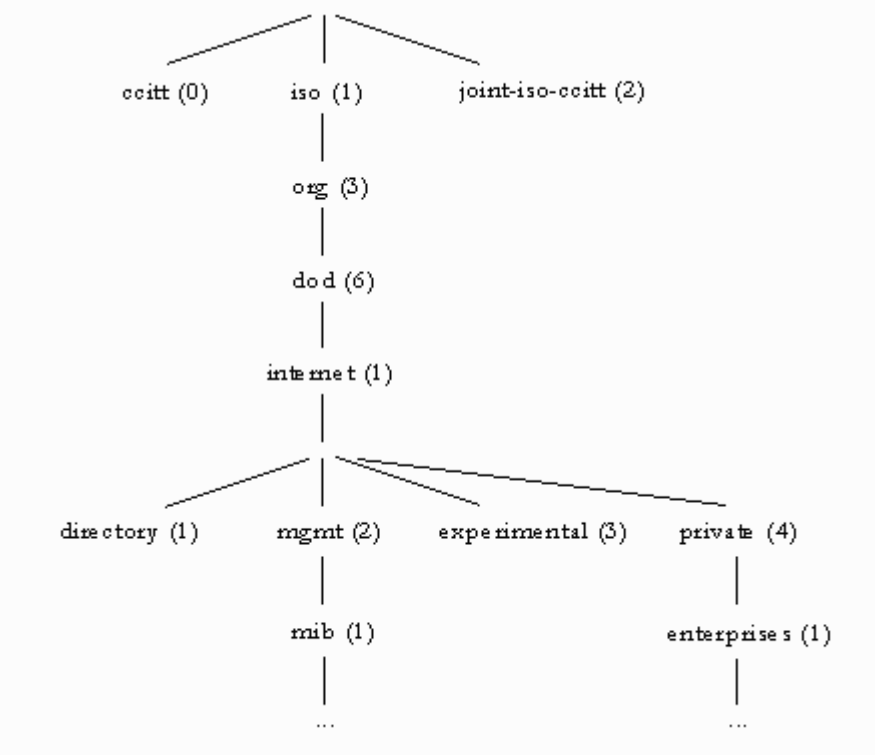
Agentit voivat lähettää myös Trap- ja Inform-pdu -sanomia NMS:lle raportoimaan laitteen tilan muutoksesta ja muista tapahtumista, kuten esimerkiksi reitittimen uudelleen käynnistymisestä ja reititystaulujen päivityksestä, sekä mahdollisista vikatilanteista. /1/ ja /2/



Kuva 2-2. SNMP hallinta-aseman ja agentin välinen kommunikointi.

2.3 MIB

Management Information Base on tietokanta, joka kuvaa hallittavan laitteen datan muuttujina ja muuttujajoukkoina. Tällaista dataa voi olla esimerkiksi kytkimen muistikapasiteetti, ethernet -liitännän MAC-osoite ja liitäntään saapuneiden pakettien lukumäärä. Muuttujat ovat MIB:n puurakenteessa lehtinä ja ne voidaan yksilöllisesti tunnistaa ASN.1 -standardin OID (Object Identifier) -tunnisteilla. OID:t voidaan ajatella puhelinnumeroina, jotka on järjestetty hierarkisesti eri organisaatioiden määrittelemin numeroin luetteloksi. Esimerkki tällaisesta numerosta voisi olla 1.3.6.1 -alkuinen numero, joka on Internet-yhteisön hallitsema ja määritelty RFC 1065 -suosituksessa. 1.3.6.1 on myös oma pieni puu, joka sisällyttää alleen pienempiä puita (solmuja) ja lehtiä (objekteja). OID -tunnisteen lisäksi myös tietokannan muuttujat on nimetty. MIB:n puurakenne määrittelee alleen muuttujajoukot loogisiksi ryhmiksi (Kuva 2-3).



Kuva 2-3. MIB:n puurakenne (Kuva http://www1.ncaa.org).

Yleinen kehysmalli, johon MIB voidaan rakentaa, löytyy suosituksesta RFC 1155, jossa on määritelty SMI (Structure of Management Information). SMI määrittelee

mm. mitä tietotyyppejä voidaan käyttää, kuinka ne esitetään ja nimetään MIB:ssa. Ajatus SMI:n takana on ohjata yksinkertaiseen ja laajennettavaan MIB -tietokantaan. MIB:sta on määritelty myös toinen versio, MIB-II, RFC 1213 -suosituksessa. Tämä tarjoaa laajemman tietokannan lisäten objekteja ja ryhmiä. MIB-II on nykyisin yleisesti käytössä. /1/

3 SNMP:N KEHITYS

SNMP:n kehityksen aloituspiste oli vuonna 1987 määritelty SGMP (Simple Gateway Monitoring Protocol), joka oli suunniteltu suoraluonteiseen reitittimien hallitsemiseen. Kun heräsi tarve yleisempään ja monipuolisempaan verkonhallintaan, päätettiin aloittaa uuden protokollan kehittely SGMP:n pohjalta. Itse SNMP:n kehitys alkoi sen ensimmäisen version (SNMPv1) spesifioinnista RFC 1157 -suosituksessa elokuussa 1988 ja se on toiminut ytimenä SNMP -versioille 2 ja 3. SNMPv2:n kehittely alkoi vuonna 1992, jolloin kaksi työryhmää perustettiin tätä varten. Toinen työryhmä keskittyi tietoturvaominaisuuksien suunnitteluun. Lopullinen käytännön standardi SNMPv2:sta sai nimen SNMPv2c viitaten community string -avaimien käyttöön tietoturvamenetelmänä SNMPv1:n tavoin. Tietoturvaominaisuuksien pois jättäminen suosituksesta johtui laitetoimittajien ja käyttäjien ennakkoluuloista tietoturvamäärittelyihin. Tietoturvaominaisuudet ovat kuitenkin määritelty SNMPv2:lle ja tämä on saanut oman suosituksen, sekä nimityksen SNMPv2u, joka viittaa käyttäjänimi -pohjaiseen (User-based) tunnistukseen. Vuonna 1997 IETF perusti työryhmän SNMPv3:n kehittämiseen, ja tämä versio toi mukanaan kaivatut tietoturvaominaisuudet. Seuraavaksi käydään läpi yksityiskohtaisemmin SNMP:n eri versiot ja niiden ominaisuudet. /1/ ja /2/

3.1 SNMP-versio 1

SNMPv1 aloitti verkonhallinta protokollan uuden sukupolven ja sen ensimmäiset RFC -suositukset ilmestyivät jo vuonna 1988, mutta lopulliseen muotoonsa se pääsi vuonna 1990 RFC 1157 -suosituksella. Tässä suosituksessa esiteltiin malli hallinta-

aseman (NMS) ja hallittavien järjestelmien (agenttien) kommunikoinnista. Lisäksi kaksi dokumenttia, RFC 1055 (SMI) ja RFC 1212 (MIB), määrittelevät hallittavan informaation ja tukevat SNMP -suositusta. /2/

SNMP tarvitsee toimiakseen kuljetuskerrosta (Transport Layer), mutta ei ota kantaa onko se yhteydetön vai yhteydellinen. Useimmat SNMP toteutukset käyttävät TCP/IP -arkkitehtuuria ja yhteydetöntä UDP -protokollaa. UDP -lohkot lähetetään IP -paketteina. UDP -otsikko sisältää lähettäjän ja vastaanottajan porttiosoitteet mahdollistaen sovelluskerroksen protokollien, kuten SNMP:n, kommunikoinnin keskenään. SNMP:lle on asetettu UDP -portit 161 ja 162, joista ensimmäistä agenttisovellus käyttää vastaanottamaan Get-Request, GetNext-Request ja Set-Request -operaatioita. NMS käyttää porttia 162 vastaanottamaan Trap -operaatioita agentilta. NMS ja agentti voivat käyttää operaatioiden lähettämiseen mitä tahansa vapaana olevaa porttia. /1/

Ensimmäinen versio SNMP:stä sisällyttää hallittavien laitteiden objektien käsittelyyn kolmenlaisia protokollaoperaatioita:

- ◊ Get -operaatio: Hallinta-asema pyytää agentilta objektin arvoa.
- ◊ Set -operaatio: Hallinta-asema asettaa agentin objektille arvon.
- ◊ Trap -operaatio: Agentti lähettää ilman pyyntöä hallinta-asemalle objektin arvon.

Get -operaatioita tunnetaan ensimmäisessä SNMP -versiossa kahta tyyppiä; Get ja GetNext. Jälkimmäinen eroaa ensimmäisestä siinä, että se lähettää kysytyn objektin viereisen objektin arvon. Tällä tavoin hallinta-aseman käyttäjä saa selville hallittavan laitteen MIB:n rakenteen dynaamisesti ja kykenee selvittämään tuntemattoman solmun objektit ja niiden arvon. /1/

Kun NMS lähettää agentille Get-Request pdu:n, jossa pyydetään tietyn objektin arvoa, agentti suorittaa arvon haun MIB:sta ja lähettää sen Get-Response pdu:lla NMS:lle. Virheen sattuessa agentti lähettää muuttujan arvon sijaan virheilmoituksen, joka voi olla esim. noSuchName, mikä tarkoittaa, ettei haetulla nimellä löydy OID:tä.

Mikäli suoritetaan useamman arvon haku yhdellä Get-Request pdu:lla ja yksikin näistä tuottaa virheen, palauttaa agentti virheilmoituksen epäonnistuneesta haku-yrityksestä. /1/

Set -operaatiolla voidaan asettaa objektille uusi arvo tai poistaa arvo kokonaan. Tämän pdu:n rakenne on hyvin samanlainen kuin Get-Request operaation, jolla siis pyydetään arvoa MIB:sta. NMS lähettää agentille Set-Request pdu:n, joka sisältää objektin nimen, OID:n ja päivitettävän arvon. Onnistuneen arvon päivityksen jälkeen agentti lähettää vastaukseksi Get-Response pdu:lla päivitetyn objektin tunnisteen ja uuden arvon NMS:lle. Esimerkiksi, jos NMS lähettää agentille seuraavanlaisen operaation; SetRequest (ipRouteMetric1.9.1.2.3 = 9), niin agentti vastaa operaatiolla GetResponse (ipRouteMetric1.9.1.2.3 = 9). Virhetilanteen sattuessa agentti palauttaa virheilmoituksen pdu:lla, joka voi olla samanlainen kuin Get-Request operaatiolla. /1/

SNMP ei tarjoa varsinaista toimintoa komentojen antamiseen agentille. On kuitenkin mahdollista käyttää Set -operaatiota suorittamaan tietty tehtävä agentin hallitsemalle laitteelle. Tiettyjä objekteja voidaankin ajatella komentoina, joiden arvoa muuttamalla Set -operaatiota käyttäen saadaan aikaan tietty toiminto. Tällainen tapaus voisi olla vaikkapa reBoot -objekti MIB:ssä, jonka arvo on oletuksena 0. Kun Set -operaatiota käytetään muuttamaan tämä arvoon 1, käynnistyy tällöin agentin hallitsema laite uudelleen ja objektin arvo palautuu takaisin arvoon 0. /1/

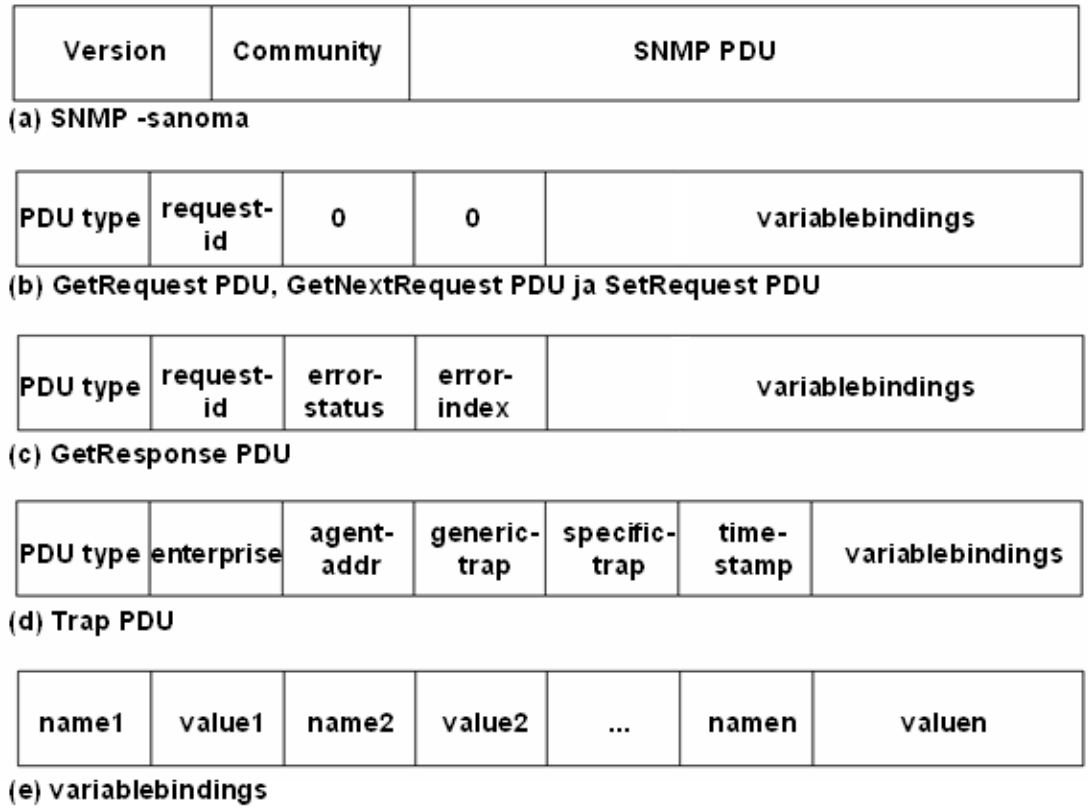
Trap -operaatio eroaa edellisistä operaatioista paitsi rakenteeltaan, kuin myös sillä, että sen lähettää hallittavan laitteen agentti. Trap -pdu lähetetään NMS:lle, kun jokin merkittävä tapahtuma toteutuu agenttijärjestelmässä. Esimerkki tällaisesta tapahtumasta on linkDown -trap-pdu, jolloin agentti ilmoittaa hallinta-asemalle lokaalin laitteen jonkin liitännän olevan alhaalla. Trap -operaatiot eivät saa Response -pdu:ta, kuten muut operaatiot. /1/

SNMP:n ensimmäinen versio kärsii totaalisesta tietoturvattomuudesta. Siinä ei ole minkäänlaista suojattua käyttäjän autentikointia ja tiedon salausta, vaan käyttäjän tunnistus suoritetaan community string -avaimilla, jotka ovat selkokielisiä sanoja ja siten myös helposti hakkerien luettavissa. Community string -avaimet toimivat kuten

salasanat ja niitä käytetään oikeutena lukea tietoa agentin hallitsemalta laitteelta (read-only), tai myös kirjoittamaan siihen tietoa (read-write). Jos siis NMS:n käyttäjällä on käytössään vain read-only community string -avain, voi hän suorittaa ainoastaan Get -kyselyjä. Read-write community string -avain mahdollistaa Set -operaation käytön tiedon kirjoittamiseen agentin laitteelle. Oletuksena kummatkin avaimet ovat selkokielisiä sanoja public ja private, joita on kritisoitu ja luokiteltu yhdeksi suurimmista Internetin tietoturvauhista. SNMPv1:stä käytettäessä onkin syytä vaihtaa oletusavaimet turvallisempiin.

3.1.1 SNMPv1-sanoman rakenne

SNMPv1:ssä NMS:n ja agentin välillä siirrettävien sanomien rakenne sisältää versionumeron osoittaen käytettävän SNMP -version, community -nimen ja yhden viidestä eri pdu:sta. Kuvasta 3-1 voidaan nähdä sanoman perusrakenne, sekä protokollaoperaatioiden sanomarakenne.



Kuva 3-1. SNMPv1 sanomatyypit.

Kuvasta voidaan havaita, että GetRequest-, GetNextRequest- ja SetRequest -protokollaoperaatioilla on sama formaatti kuin GetResponse -operaatiolla. Seuraavaksi käydään läpi sanomien kentät ja niiden merkitys.

- ◊ Version: SNMPv1:a käytettäessä kentän arvo on 1.
- ◊ Community: Community String -avain. Oletuksena joko public tai private riippuen luetaanko vai kirjoitetaanko tietoa laitteelle.
- ◊ Request-id: Yksilöllistää pyyntösanoman.
- ◊ Error-status: Käytetään osoittamaan tapahtunut virhe pyynnön käsittelyn aikana. Arvot tälle ovat noError (0), tooBig (1), noSuchName (2), badValue (3), readOnly (4), sekä genErr (5).
- ◊ Error-index: Kun error-status saa muun arvon kuin 0, tämä kenttä ilmoittaa muuttujan, joka aiheutti virheen. Muuttuja on hallittava objekti.
- ◊ Variablebindings: Lista muuttujista ja niitä vastaavista arvoista. Joissakin tapauksissa, kuten GetRequest -operaatiossa, tämä saa arvon null (0). Variablebinding käyttämällä voidaan yhdistää useita samantyyppisiä pyyntöjä yhteen sanomaan ja saada vastauksena useiden objektien arvot yhdessä vastaussanomassa. Tämä vähentää huomattavasti verkon kuormitusta.
- ◊ Enterprise: Objektityyppi, joka generoi trap -operaation.
- ◊ Agent-addr: Trap:n generoivan objektin osoite.
- ◊ Generic-trap: Geneerinen traptyyppi. Arvot tälle ovat coldStart (0), warmStart (1), linkDown (2), linkup (3), authentication-Failure (4), egpNeighborLoss (5), sekä enterprise-Specific (6).
- ◊ Specific-trap: Spesifinen trap -koodi.
- ◊ Time-stamp: Aikaero SNMP -elementin alustamisen ja trap -operaation generoimisen välillä. /1/

3.2 SNMP-versio 2

SNMP:n versio 2 sai RFC 1441 -suosituksen huhtikuussa 1993 ja se perustuu suurimmaksi osaksi SNMP:n ensimmäiseen versioon. SNMPv2 sai vuoden 1996 alussa myös kaksi laajentavaa suositusta, RFC 1901-1908 (SNMPv2c) ja RFC 1909-1910 (SNMPv2u). SNMPv2c nojaa samaan tietoturvamalliin kuin versio 1 käyttäen

community string -avaimia käyttäjän tunnistukseen. Vaikka SNMPv2c onkin jäänyt virallisesti luonnokseksi, on se kuitenkin saanut laajan hyväksynnän käytännön standardiksi. /2/

SNMPv2 esittelee aiempaan versioon nähden kaksi uutta protokollaoperaatiota, jotka ovat:

- ◊ GetBulk -operaatio: NMS pyytää agentilta kohtuullisen suurta määrää dataa pääasiassa isokokoisista taulukoista.
- ◊ Inform -operaatio: Trap -operaatio, joka saa kuittaussanoman NMS:lta.

GetBulk -operaation variablebindings kentässä annetaan tietty määrä arvoja (N+R). N -arvoihin saakka toimitaan kuten GetNext -operaatiossakin. Sen sijaan kun N -arvot ylittyvät, niin ylittäville objekteille haetaan leksikografisia seuraajia operaatiossa erikseen määrätty määrä. Huomattavaa GetBulk -operaatiossa on, että mikäli pyyntöön vastaava agentti ei voi tarjota arvoa kaikille kysytyille muuttujille, lähettää se osittaisen vastauksen NMS:lle sisältäen arvot vain tietyille muuttujille. /3/

Inform -operaatio vaatii kaksisuuntaisen kommunikoinnin, sillä agentti jää odottamaan hallinta-aseman vastausta perille saapuneesta inform -sanomasta. Agentti toistaa sanomaa kunnes se saa kuittauksen. Tällä tavoin trap -sanomat saavat luotettavuuden. Inform -operaation huonona puolena on verkon liikenteen lisääntyminen vastaussanomien lähetyksestä johtuen, mikä saattaa hidastaa verkon toimintaa. /1/

SNMPv2 tuo myös parannuksia suorituskykyyn, tietoturvaan, luotettavuuteen ja hallinta-asemien väliseen kommunikointiin. SNMPv2 ei itsessään ole yhteensopiva SNMPv1:n kanssa, koska se käyttää eri sanomaformaattia ja protokollaoperaatioita. RFC 1908 määrittelee kuitenkin kaksi mahdollista yhteensopivuusstrategiaa: välittävät agentit ja kaksikieliset hallinta-asemat. /1/ ja /2/

3.2.1 Välittävä agentti

Välittävä agentti (Proxy agent) on SNMPv2 -ominaisuus, joka antaa nimensä mukaisesti agentin välittää informaatiota eteenpäin. Tämä voi tarkoittaa protokollaoperaatioiden kääntämistä ja toimittamista eteenpäin SNMPv1 -agentille tai laitteelle, joka ei käytä SNMP:tä verkonhallintaprotokollana. Ensimmäisessä tapauksessa agentti välittää NMS:lta tulleet Get-, GetNext-, ja Set -operaatiot suoraan SNMPv1 agentille, mutta kääntää GetBulk -operaation GetNext -operaatioksi, jonka vastaanottava agentti osaa tulkita. Trap -operaation välittävä agentti kääntää sen SNMPv2 -trappdu:ksi ja välittää sen NMS:lle. Lisäksi SNMPv2 -agentti voi välittää operaatiopyynnöt toisen sijaintialueen SNMPv2 -agentille. Välittävä agentti ei kuitenkaan prosessoi operaatiopyyntöjä, kuten Get-, GetNext- ja Set-request sanomia, sillä sen ei pidä vaikuttaa hallittavan objektin nimeen tai arvoon, vaan välittää pyyntö hallinta-aseman haluamalle laitteelle. /2/

3.2.2 Kaksikielinen hallinta-asema

Kaksikielinen NMS (Bilingual NMS) tukee sekä SNMPv1-, että SNMPv2 -ympäristöä. NMS tallentaa hallitsemiensa laitteiden agenttien versioinformaation tietokantaansa ja aina kommunikoidessaan laitteen agentin kanssa se tarkistaa käytettävän version. Tällä tavoin hallittavan verkon laitteet voivat käyttää kumpaa protokollaversiota tahansa. /2/

3.2.3 SNMPv2-sanoman rakenne

SNMPv2:n sanomaformaatti ei ole juurikaan erilainen verrattuna ensimmäiseen versioon. GetRequest-, GetNextRequest-, SetRequest-, SNMPv2-Trap-, Response- ja InformRequest -operaatiot ovat PDU -rakenteeltaan samanlaisia. Kuvasta 3-2 voidaan nähdä GetBulkRequest -operaation hieman erilainen rakenne.

PDU type	Request-id	0	0	Variablebindings

(a) GetRequest-, GetNextRequest-, SetRequest-, SNMPv2-Trap- ja InformRequest-PDU

PDU type	Request-id	Error-status	Error-index	Variablebindings

(b) Response-PDU

PDU type	Request-id	Non-repeaters	Max-repetitions	Variablebindings

(c) GetBulkRequest-PDU

Kuva 3-2. SNMPv2 -operaatiot.

GetBulkRequest -operaatiolla on kaksi uutta kenttää, joita ei löydy toisista operaatioista: non-repeaters ja max-repetitions. Non-repeaters -kenttä ilmoittaa variablebindings -listan muuttujien määrän. Max-repetitions -kenttä puolestaan ilmoittaa lopuille variablebindings -listan muuttujille tarvittavien vastaussanomien määrän. Ylempänä mainittu SNMPv2-Trap -operaatio ei poikkea rooliltaan edeltäjästään, mutta käyttää eri sanomaformaattia. SNMPv2-Trap käyttää samaa formaattia kuin muut SNMPv2 -operaatiot, paitsi GetBulkRequest. /1/

3.3 SNMP-versio 3

SNMPv3 määriteltiin RFC 3411-3418 suositukseksi joulukuussa 2002 ja on SNMP -verkonhallintaprotokollan viimeisin versio. IETF on vahvistanut sen täydeksi Internet-standardiksi, joka on RFC -suositusten korkein kypsyystaso. Se perustuu vahvasti SNMPv2u:n arkkitehtuuriin. Versio 3:n vahvin, ja sen tervetullut ominaisuus verrattuna versioihin 1 ja 2, on sen tietoturvallisuus. Tämä mahdollistaa käyttäjän salatun tunnistuksen (autentikoinnin) ja siirrettävän tiedon salauksen hallittavassa verkossa. Tärkeimmät ominaisuudet ovat seuraavat:

- ◊ Sanoman eheys: Takaa ettei pakettiin ole vaikutettu siirron aikana.
- ◊ Autentikointi: Takaa että paketti on oikeasta ja halutusta lähteestä.
- ◊ Salaus: Takaa etteivät ulkopuoliset (esimerkiksi hakkerit) pääse tulkitsemaan paketin sisältöä.

Samalla tuorein versio korvaa community string -avaimet ryhmänimellä (Groupname) ja käyttäjänimellä (Username). Näille ryhmille ja käyttäjille voidaan määritellä omat tietoturvatasot. Käyttäjänimille määritellään tietoturvatasosta riippuen joko autentikointisalasana, salaussalasana tai molemmat.

SNMPv3 esittelee myös mahdollisuuden konfiguroida hallittavia laitteita dynaamisesti. Tämä tapahtuu agentin asetusten vastaavia MIB -objekteja muuttamalla Set -operaatioin. Dynaaminen konfigurointi tukee asetusten lisäämistä, poistoa ja muokkaamista joko lokaalisti tai etäyhteydellä. /4/

3.3.1 Tietoturvamalli ja tasot

SNMPv3:n käyttäjäpohjainen tietoturvamalli (USM) tarjoaa kolme erilaista tietoturvan tasoa, jotka ovat noAuthNoPriv, authNoPriv ja authPriv (Taulukko 1-1). Tietoturvamalli on agentin käyttämä tietoturvastrategia.

- ◊ noAuth: Paketti autentikoidaan vain käyttäjänimen perusteella. Tämä tunnistusmenetelmä on verrattavissa community string -avaimiin.
- ◊ Auth: Paketti autentikoidaan käyttäen joko HMAC MD5- tai SHA-1 menetelmää. Kumpaa tahansa menetelmää käytettäessä määritellään käyttäjälle autentikointisalasana.
- ◊ Priv: Paketti autentikoidaan käyttäen joko HMAC MD5- tai SHA-1 menetelmää ja salaa paketin käyttäen DES, 3DES tai AES menetelmää. Käytettävästä menetelmästä riippumatta käyttäjälle määritellään salaussalasana. /4/

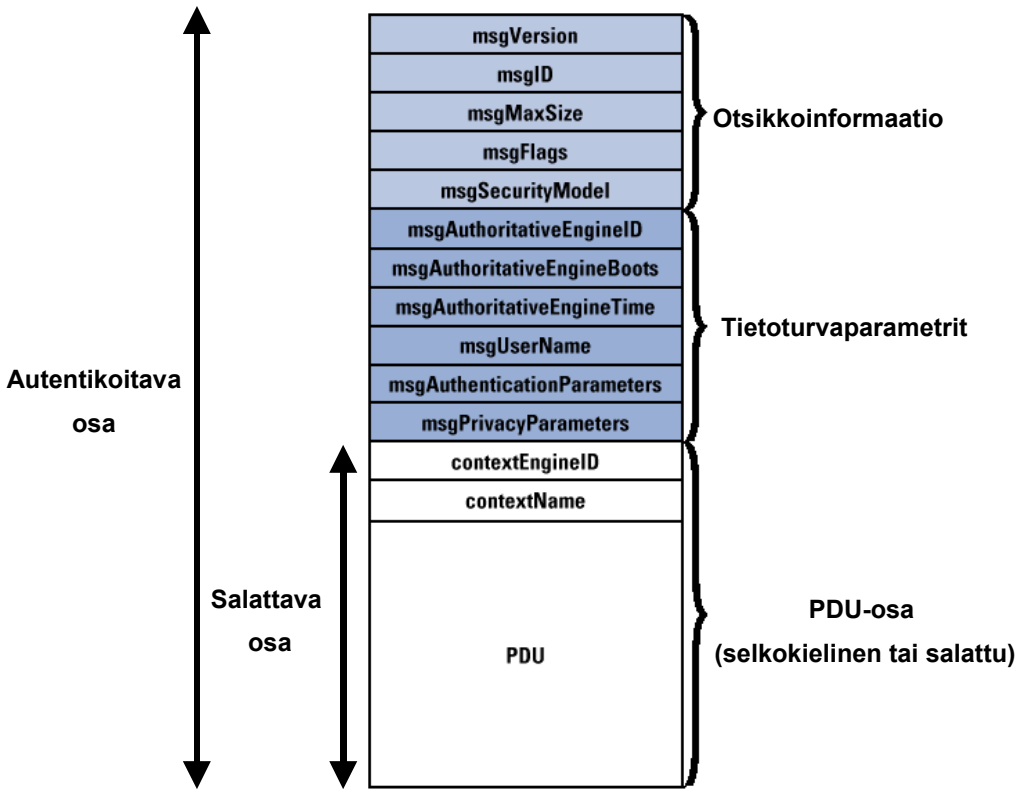
AES:sta (Advanced Encyption Standard) on käytettävissä 128-, 192- ja 256-bittiset salausmenetelmät. Taulukosta 1-1 voidaan nähdä SNMP:n tietoturvamallit ja niiden tasojen kombinaatiot.

Taulukko 1-1. SNMP:n tietoturvamallit ja tasot.

Malli	Taso	Autentikointi	Salaus	Tapahtuma
v1	noAuthNoPriv	Community String	Ei	Autentikointi Community String -avaimilla
v2	noAuthNoPriv	Community String	Ei	Autentikointi Community String -avaimilla
v3	noAuthNoPriv	Käyttäjänimi (Username)	Ei	Autentikointi käyttäjänimellä
	authNoPriv	MD5 / SHA-1	Ei	Käyttää HMAC MD5 ja SHA –algoritmeja autentikointiin
	authPriv	MD5 / SHA-1	DES, 3DES, AES 128-bit, AES 192-bit, AES 256-bit	Käyttää HMAC MD5 ja SHA –algoritmeja autentikointiin ja DES, 3DES, AES 128-bit,192-bit, sekä 256-bit -algoritmeja salaukseen

3.3.2 SNMPv3-sanoman rakenne

Kuvassa 3-3 on esitetty SNMPv3 -sanoman rakenne.



Kuva 3-3. SNMPv3 -sanoman formaatti sisältäen turvamallin kentät.

- ◊ Version: SNMPv3:a käytettäessä kentän arvo on 3.
- ◊ ID: Uniikki tunniste sanoman lähettäjän ja vastaanottajan välillä, joka koordinoi kysely- ja vastaussanomat.
- ◊ Message Size: Lähettäjän tukema sanoman maksimikoko oktetteina.
- ◊ Message Flags: Oktettimerkkijono, joka sisältää kolme lippua vähiten merkitsevinä kolmena bittinä; reportableFlag, privFlag ja authFlag.
- ◊ Security Model: Tunniste, joka kuvaa lähettäjän käyttämän tietoturvamallin ja samalla osoittaa mitä mallia vastaanottajan tulee käyttää.
- ◊ AuthoritativeEngineID: Auktoritatiivisen SNMP -engine:n snmpEngineID, jota SNMP käyttää sanoman vaihdossa. Näin ollen tämä arvo viittaa lähettäjään Trap-, Response- ja Report -sanomissa ja vastaanottajaan Get-, GetNext-, GetBulk-, Set- ja Inform -sanomissa.
- ◊ AuthoritativeEngineBoots: Auktoritatiivisen SNMP -engine:n snmpEngineBoots -arvo, jota SNMP käyttää sanoman vaihdossa. Kenttä saa kokonaislukuarvon väliltä 0 – 2^{31}-1, joka osoittaa SNMP -engine:n alustuskerrat ensimmäisen alustamisen jälkeen.

- ◊ AuthoritativeEngineTime: Auktoritatiivisen SNMP -engine:n snmpEngineTime -arvo, jota SNMP käyttää sanoman vaihdossa. Kenttä saa kokonaislukuarvon väliltä 0 – 2^{31}-1, joka osoittaa ajan sekunneissa viimeisimmästä snmpEngineBoots -objektin alustuksesta.
- ◊ User Name: Käyttäjänimi, jota käytetään sanoman vaihdossa käyttäjän tunnistukseen.
- ◊ AuthenticationParameters: Jos autentikointia ei käytetä tämän sanoman yhteydessä, saa kenttä arvon Null (0). Muussa tapauksessa tämä on autentikointiparametri, joka nykyisen USM -määrittelyn mukaan on sanoman autentikointikoodi (HMAC).
- ◊ PrivacyParameters: Jos salausta ei käytetä tämän sanoman yhteydessä, saa kenttä arvon Null (0). Muussa tapauksessa tämä on salausparametri, joka nykyisen USM -määrittelyn mukaan on arvo, jota käytetään alkuarvona salausalgoritmissa.
- ◊ ContextEngineID: Oktettimerkkijono, joka on uniikki tunniste SNMP-entiteetille.
- ◊ ContextName: Oktettimerkkijono, joka on uniikki tunniste contextEngine:lle.
- ◊ PDU: Data, joka on SNMPv3 sanomamallissa sama kuin SNMPv2 PDU. /1/

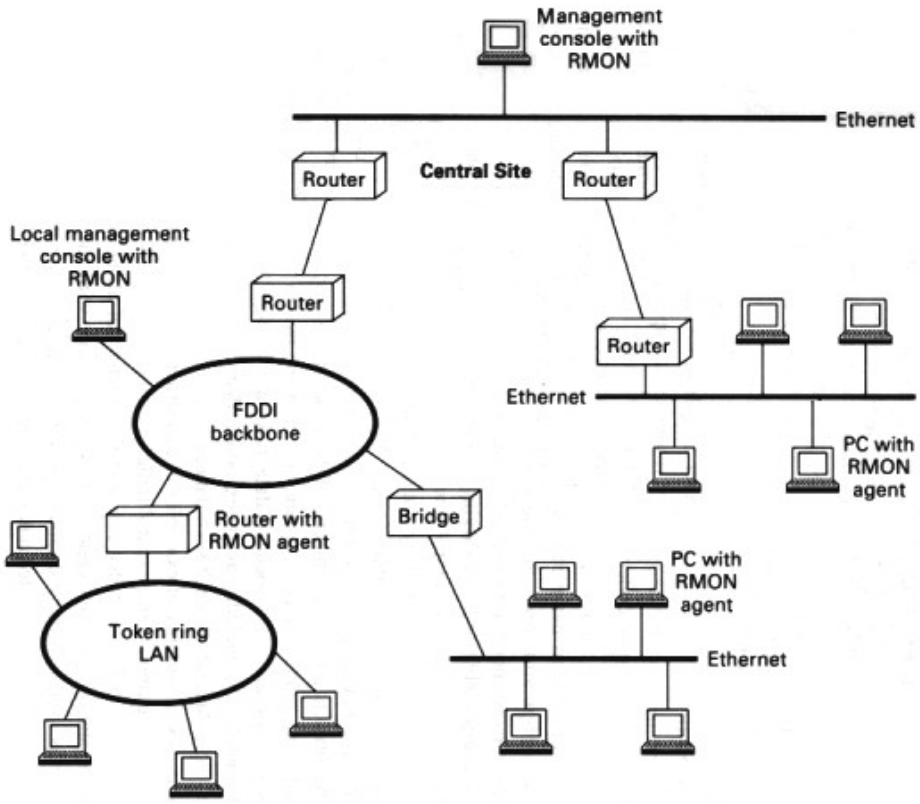
3.4 Remote Network Monitoring (RMON)

Remote Network Monitoring, eli etähallinta, on määriteltynä RFC 1757 suosituksessa. Sen uudempi toteutus löytyy suosituksesta RFC 2021 ja tunnetaan nimellä RMON2. RMON on tärkein lisäys SNMP -standardeihin SMI:n, MIB:n ja SNMP:n lisäksi. Sen avulla saadaan kootusti tiedot lähiverkoissa esiintyvästä datasta RMON-hallinta-asemalle. RMON -standardissa määritellään uusi RMON-MIB, joka täydentää jo olemassa olevaa MIB-II -standardia. Koska MIB-II itsessään ei voi tarjota tietoa kuin sen agentin hallitsemasta lokaalista laitteesta, oli tarpeen kehittää standardi, jolla saataisiin koottua lähiverkon kokonaisliikenne ja valvonta, sekä suorittaa tämä keskitetysti. RMON mahdollistaa koko lähiverkon laitteiden seurannan kuormittamatta liikaa hallinta-asemia, yksittäisiä agentteja ja verkkoa. RMON kuormittaa kuitenkin merkittävästi sitä konetta, johon se on kytketty, sillä tietoa analysoidaan merkittävästi jo sitä kerätessä. Käytännössä RMON toimii siten,

että jokaisessa lähiverkkosegmentissä on oma RMON-agentti, joka välittää kerätyt tiedot RMON-hallinta-asemalle (Kuva 3-4). /1/ ja /3/

RMON toi mukanaan useita etuja, jotka luetellaan seuraavaksi:

- ◊ Yhteydetön toiminta: Siirrettävä tieto säilyy, vaikka yhteys hallinta-aseman ja agentin välillä olisi poikki. Tieto siirretään yhteyden palaamisen jälkeen.
- ◊ Ennakoiva valvonta: Agentti monitoroi verkon toimintaa jatkuvasti ja huomauttaa hallinta-asemaa vian ilmetessä verkossa.
- ◊ Virheiden havainnointi ja raportointi: Agentti monitoroi aktiivisesti verkkoa ja sen resurssien kulutusta etsiäkseen virheitä ja poikkeavia tilanteita. Agentti voi valvoa verkkoa myös passiivisesti ja tunnistaa poikkeuksellisia tapahtumia, kuten ruuhkaantumisen. Tällaisten tapahtumien sattuessa agentti lähettää tiedon hallinta-asemalle.
- ◊ Lisäarvodata: Verkon toimintaa voidaan valvoa suoraan agentissa vapauttaen hallinta-asema tästä vastuusta.
- ◊ Useat hallinta-asemat: Verkkotopologia voi sisällyttää myös useamman RMON-hallinta-aseman. Tämän ansiosta hallintainformaation luotettavuus paranee, voidaan suorittaa eri toimintoja ja taata hallinta useille elementeille. RMON-agentti voi olla yhteydessä useampaan RMON -hallinta-asemaan. /1/ ja /3/



Kuva 3-4. Esimerkki RMON:n käytöstä (Kuva http://www.chapo.co.il).

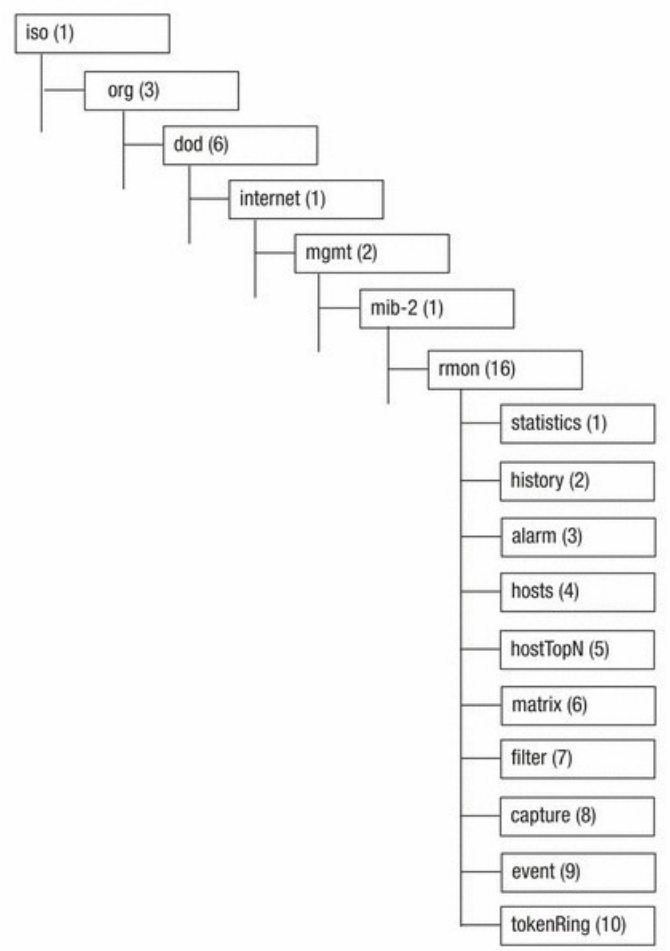
3.4.1 RMON1

RMON1-toiminta perustuu verkkoliikenteen ja sen sisältämien pakettien tarkkailuun OSI -kerrosmallin tasoilla 1 ja 2. Se lukee lähettäjän ja vastaanottajan osoitteet, jolloin se saa selville paketin reitin. RMON1 havaitsee myös virheelliset paketit, kuten väärän kokoiset paketit, jolloin nämä hylätään. /1/ ja /3/

RMON1-MIB sisältää kymmenen erilaista ryhmää. RMON1 tilastoi ja luokittelee verkon tapahtumat eri ryhmien mukaisesti. Ryhmät osoittavat ennalta ne tiedot, joita RMON-agenttien halutaan keräävän. Näiden perusteella verkkoliikenteen analysointia RMON-hallinta-asemassa on pyritty helpottamaan. /3/

Seuraavassa käydään läpi eri ryhmät (Kuva 3-5):

- ◊ Statistics: Ylläpitää tilastotietoja agentin valvomista eri verkonosista, kuten virhe- ja pakettitietoja.
- ◊ History: Tallentaa ajoittain tilastonäytteitä Statistic -ryhmän informaatiosta.
- ◊ Alarm: Toimii yhdessä Event- ryhmän kanssa ja vertaa eri näytteitä sille määriteltyihin raja-arvoihin. Jos hälytyskynnys ylittyy, välitetään tieto RMON-hallinta-asemalle.
- ◊ Host: Seuraa verkon isäntäkoneiden välistä liikennettä valvomalla pakettien lähetys- ja vastaanotto-osoitteita.
- ◊ HostTopN: Muodostaa raportteja isäntäkoneista, joiden verkkoliikenne on vilkasta.
- ◊ Matrix: Näyttää virhe- ja tilastotiedot taulukkomuodossa.
- ◊ Filter: Suotimella voidaan suodattaa pois tiettyjä verkkoliikenteen paketteja.
- ◊ Capture: Tämän avulla voidaan kaapata ne paketit tarkasteltaviksi, jotka ovat läpäisseet suotimen.
- ◊ Event: Luo määrättyjä tapahtumia, jotka ilmoittavat hallinta-asemalle hälyttimien laukeamisesta. Toimii yhdessä Alarm -ryhmän kanssa.
- ◊ Token Ring: Sisältää tilasto- ja konfigurointitietoja Token Ring -verkoista. /1/ ja /3/



Kuva 3-5. RMON1-MIB:n ryhmät (Kuva http://publib.boulder.ibm.com).

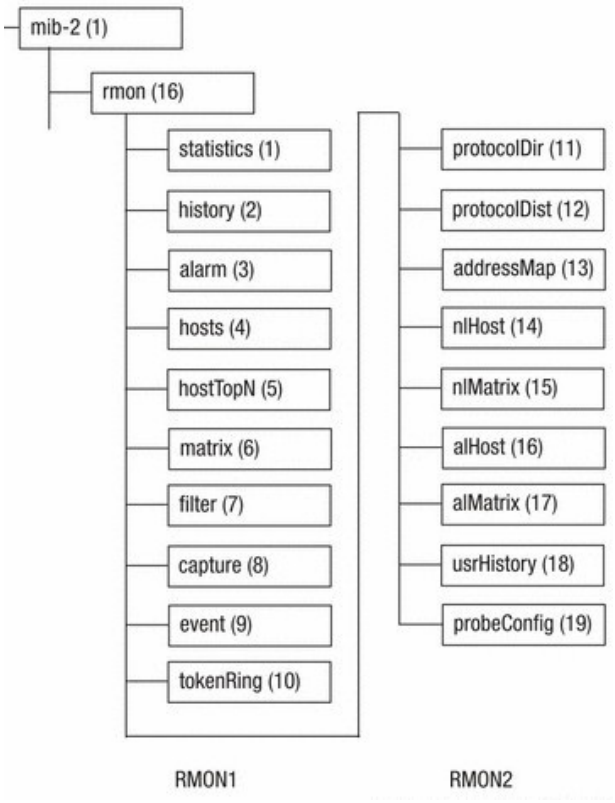
3.4.2 RMON2

RMON protokollan toinen versio tarjoaa mahdollisuuden tarkastella OSI -kerrosmallin kerroksia 3 – 7. Käytännössä tämä tarkoittaa, että RMON-agentti voi monitoroida liikennettä oman verkkosegmenttinsä ulkopuolelta ja nähdä reitittimelle saapuvan liikenteen. RMON-agentti voi myös valvoa ja tallentaa tiettyjen sovellusten aiheuttamaa liikennettä, kuten sähköposti- ja www-liikennettä. /1/ ja /3/

RMON2 sisältää RMON1:n tapaan myös kymmenen ryhmää, joiden tarkoituksena on valvoa OSI -kerrosmallin ylempiä kerroksia. RMON2:n ryhmät ovat lueteltuna seuraavassa (Kuva 3-6):

- ◊ Protocol directory: Sisältää kaikki RMON-agentin käyttämät protokollat.

- ◊ Protocol distribution: Tilastoi jokaisen protokollaliikenteen jakautumisen lähiverkkosegmentissä.
- ◊ Address map: Yhdistää kytkettyjen laitteiden IP -osoitteet näiden MAC -osoitteisiin ja TCP-/UDP -portteihin.
- ◊ Network-layer host: Isäntäkoneiden sisään- ja ulosmenevän liikenteen tilastointi IP -osoitteiden perusteella.
- ◊ Network-layer matrix: Isäntäkoneiden välisen liikenteen tilastointi IP -osoitteiden perusteella.
- ◊ Application-layer host: Isäntäkoneiden sisään- ja ulosmenevän liikenteen tilastointi sovelluskerroksen osoitteiden perusteella
- ◊ Application-layer matrix: Isäntäkoneiden välisen liikenteen tilastointi sovelluskerroksen osoitteiden perusteella.
- ◊ User history collection: Tutkii ajoittain käyttäjän määrittelemät muuttujat ja tilastoi ne perustuen käyttäjän määrittelemiin parametreihin.
- ◊ Probe configuration: Määrittelee RMON-agentin konfigurointi parametrit. /1/ ja /3/



Kuva 3-6: RMON2-MIB:n ryhmät (Kuva http://publib.boulder.ibm.com).

4 LAITTEIDEN KONFIGUROINTI

4.1 Yleistä Ciscon laitteiden konfiguroinnista

Tässä opinnäytetyössä käytettiin Cisco 2800 -sarjan reititintä, sekä 3550 -sarjan Catalyst -kytkintä SNMPv3 -testiverkkoympäristön mallintamiseen. Seuraavassa kappaleessa esitetyt SNMPv3 -laiteasetukset ovat Ciscon reititinlaitteille tarkoitetut perusasetukset, mutta tässä työssä käytettyjen laitteiden kohdalla jouduttiin hieman poikkeamaan näistä suositelluista asetuksista. Niinpä eri laitteita käytettäessä onkin suositeltavaa tarkistaa laitteen valmistajan verkkosivuilta (http://www.cisco.com) laitekohtaiset SNMPv3 -asetukset. Kytkinlaitteille Cisco on antanut omat suositeltavat asetusohjeensa, jotka myös käydään läpi seuraavassa kappaleessa. Cisco 2800- ja Catalyst 3550 -laitteiden opinnäytetyössä käytetyt konfiguraatiot löytyvät myöhemmästä kappaleesta ja kirjan lopun liitteistä 1 ja 2.

4.2 SNMPv3 -asetukset

Agenttisovellusten konfigurointia varten Ciscon laitteet käyttävät **snmp-server** -komentoja. Näitä komentoja käyttämällä hallinta-asema saa yhteyden hallittavaan laitteeseen ja laite voi lähettää hallinta-asemalle hälytys- ja tapahtumasanomia. Cisco IOS SNMPv3 -agentin peruskonfigurointi käsittää seuraavat vaiheet:

- ◊ EngineID: Luodaan SNMP -moottorille tunnistelukujono, jolla laite yksilöidään hallittavassa verkossa.
- ◊ Ryhmänimet (Groupnames): Luodaan käyttäjille ryhmät.
- ◊ Käyttäjät (Users): Luodaan käyttäjätunnukset hallinta-asemien käyttäjille. Käyttäjänimeä tarvitaan otettaessa yhteyttä hallinta-asemalta agenttiin.
- ◊ Isännät (Hosts): Määritellään ilmoitussanomien (trap tai inform) vastaanottajat. Tavallisesti vastaanottavana isäntänä toimii hallinta-asema.

4.2.1 SNMP-server engineID

EngineID -tunniste määritellään agentin hallitsemalle laitteelle, jotta tämän SNMP -prosessi olisi uniikki SNMP -verkossa. Vaikka tätä ei staattisesti määriteltäisikään, luodaan se silti dynaamisesti siinä vaiheessa, jossa luodaan käyttäjänimet. Tällöin engineID generoidaan käyttäen Cisco enterprise -numeroa (1.3.6.1.4.1.9) ja lokaalin laitteen ensimmäisen liitännän MAC -osoitetta. Staattisesti määriteltäessä engineID:n pitää olla vähintään kymmenmerkkinen heksadesimaalijono.

SNMP -moottorille voidaan luoda joko lokaali- tai etätunniste. Etätunniste tulee luoda, kun laite käyttää Inform -ilmoitussanomia. Etätunnistetta käytetään autentikointi- ja salausavainten luontiin. Seuraavaksi käydään läpi engineID:n syntaksi sekä esimerkki engineID -konfiguraatiosta:

Router(config)# **snmp-server engineID** [local *engineid-merkkijono*] | [remote *ip-osoite* udp-port *porttinumero engineid-merkkijono*]

Router(config)# **snmp-server engineID local** 1234567890. /4/

4.2.2 SNMP-server group

Komennolla **snmp-server group** saadaan luotua käyttäjäryhmä, joka sitoo sen sisällä olevat käyttäjät ryhmälle määriteltyyn tietoturvamalliin ja tasoon. Alla on esimerkki tämän komennon syntaksista ja esimerkkikonfiguraatiot:

Router(config)# **snmp-server group** *ryhmän nimi* {v1 | v2c | v3 {auth | noauth | priv}} [read *lukunäkymä*] [write *kirjoitusnäkymä*] [notify *ilmoitusnäkymä*] [access *access-list*]

Router(config)#**snmp-server group** testiryhma **v3 auth**
Router(config)#**snmp-server group** snmpryhma **v3 auth priv**.

Ensimmäisessä esimerkissä luotiin käyttäjäryhmä testiryhmä, jolle asetettiin tietoturvamalli 3 (SNMPv3) ja autentikointimenetelmä ryhmän käyttäjien

todentamiseen. Toisessa esimerkissä otettiin autentikoinnin lisäksi käyttöön pakettien salaus. Tässä tapauksessa kaikkien tähän ryhmään kuuluvien käyttäjien lähettämät SNMPv3 -paketit myös salataan.

Näkymät (Views) yhdistävät hallittavat objektit käyttäjän hallintaoikeuksiin (Access rights). Objektilla voi olla eri hallintaoikeudet jokaisessa näkymässä. /4/

4.2.3 SNMP-server user

Snmp-server user -komennolla luodaan lokaalille laitteelle käyttäjänimi. Hallinta-asema käyttää tätä nimeä ottaakseen SNMP -yhteyden agentin hallitsemaan laitteeseen. Käyttäjänimelle luodaan tietoturvamallista riippuen autentikointisalasana ja salaussalasana sekä määritellään käytettävät autentikointi- ja salausmenetelmät. Alla on komennon syntaksi ja esimerkkejä käyttäjien luonnista:

Router(config)# **snmp-server user** *käyttäjänimi ryhmän nimi* [remote *ip-osoite* [udp-port *porttiosoite*]] {v1 | v2c | v3 [encrypted] [auth {md5 | sha} *autentikointisalasana* [priv des | 3des | aes {128 | 192 | 256} *salaussalasana*]]} [access *access-list*]

Router(config)# **snmp-server user** Pekka testiryhma **v3 auth md5** pekka2salasana
Router(config)# **snmp-server user** Seppo snmpryhma **v3 auth md5** seppo3salasana **priv aes 128** seponsalasana4.

Ensimmäisessä esimerkissä luotiin testiryhma -nimiseen ryhmään käyttäjänimi Pekka, jolle asetettiin MD5 -autentikointi ja autentikointisalasana. Toisessa esimerkissä snmpryhma -nimiseen ryhmään luotiin käyttäjä Seppo, jolle asetettiin MD5 -autentikoinnin lisäksi myös pakettien salaus käyttäen AES 128-bittistä salausta, sekä salaussalasanaa. /4/

4.2.4 SNMP-server host

Snmp-server host -komennolla määritellään ilmoitussanomien (trap tai inform) vastaanottaja. Tavallisesti tämä vastaanottaja on hallinta-asema (NMS). Se voi olla

myös toinen agentti, esimerkiksi välittävän agentin tapauksessa. Seuraavaksi käydään läpi vastaanottavan isännän määrittelyn syntaksi ja esimerkki konfiguraatiosta:

Router(config)# **snmp-server host** *ip-osoite* [traps | informs] [version {1 | 2c | 3 [auth | noauth | priv]}] *community-string* [udp-port *portti*] [*notification-type*]

Router(config)# **snmp-server host** 172.16.10.250 **traps version 3 priv** Seppo.

Esimerkissä määriteltiin trap -sanomien vastaanottajaksi 172.16.10.250 -osoite. Trap -paketit määriteltiin myös autentikoitaviksi ja salattaviksi. Käyttäjänimi komentorivin lopussa toimii salasanana. /4/

4.2.5 SNMP -asetusten tarkastaminen

Laitteelle syötettyjä SNMP -asetuksia voidaan tarkastella erilaisin **show** -komennoin laitteen CLI -tilassa. Käydään seuraavaksi läpi joitakin hyödyllisiä komentoja:

Router# show snmp
Näyttää SNMP -liikenteen statistiikan, kuten muun muassa lähetetyt ja vastaanotetut SNMP -paketit, sekä lähetetyt trap- ja virhesanomat.

Router# show snmp engineid
Näyttää laitteen SNMP -prosessin lokaalin ja etätunnisteen.

Router# show snmp group
Näyttää luotujen ryhmien nimet, tietoturvamallin, sekä luku-, kirjoitus- ja ilmoitusnäkymien tunnisteet.

Router# show snmp user
Näyttää luotujen käyttäjien nimet, niiden ryhmän, käytettävät tietoturvamenetelmät, käyttäjään sidotun engineID:n ja tallennustyypin.

Router# show snmp host
Näyttää määriteltyjen trap- ja inform -sanomien vastaanottajien ip- ja porttiosoitteet, ilmoitussanoman tyypin, käyttäjän ja tietoturvamallin.

Router# show snmp mib
Näyttää tietokannan objektit.

Router# show snmp view
Näyttää SNMP -prosessin näkymät.

Debug -komennoilla saadaan tarkasteltua reaaliajassa laitteella tapahtuvaa sisään- tai ulosmenevää liikennettä, tai muita tapahtumia. Seuraavaksi esitellään muutama hyödyllinen laitteen SNMP -liikenteen seuraamiseen tarkoitettu debug -komento:

Router# debug snmp packets
Näyttää sisään- ja ulosmenevät SNMP -paketit.

Router# debug snmp headers
Näyttää sisään- ja ulosmenevien SNMP -pakettien otsikot.

Router# debug snmp requests
Näyttää laitteelle tulevat pyyntösanomat. /4/ ja /5/

4.2.6 SNMPv3 -asetusten yhteenveto

Tässä kappaleessa käydään yhteenvetona läpi esimerkki Cisco-reitittimen SNMPv3 -asetuksista. Nämä asetukset toimivat pohjana otettaessa laite hallittavaan verkkoon.

Router(config)# snmp-server group snmpgroup v3 priv
Router(config)# snmp-server user snmpuser snmpgroup v3 auth md5 authpassword priv aes 128 encryptpassword
Router(config)# snmp-server enable traps snmp authentication coldstart warmstart linkup linkdown

Router(config)# snmp-server host 172.16.10.250 traps version 3 priv snmpuser. /4/

Edellisen sivun konfiguraatiossa luodaan ensin ryhmä snmpgroup, jolle asetetaan SNMPv3 -tietoturvamalli ja tietoturvatasoksi authPriv. Tähän ryhmään luodaan käyttäjä snmpuser, jolle asetetaan autentikointimenetelmäksi MD5 ja salausmenetelmäksi AES 128-bittinen salaus. Näille turvamenetelmille määriteltiin myös omat salasanat. Kuten voi huomata, tässä esimerkissä ei määritelty erikseen engineID:tä, vaan se generoitiin dynaamisesti käyttäjää luodessa. Laitteen SNMP -prosessille asetettiin myös RFC 1157 -suosituksessa määritellyt SNMP-trap -ilmoitussanomat, authentication, coldstart, warmstart, linkup ja linkdown. Näin ollen agentti lähettää trap -sanoman, kun lokaali laite vastaanottaa epäonnistuneen autentikoinnin, laite uudelleen käynnistyy laitevian vuoksi, laite käynnistetään uudestaan käyttäjän toimesta, tai laitteen jokin liitäntä joko suljetaan tai avataan. SNMPv3 -asetusten lopuksi määritellään vielä trap -sanomien vastaanottajan ip-osoite, joka tässä kuvitteellisessa tapauksessa on hallinta-asema (NMS). Trap -sanomien suojaksi tässä komennossa on määritelty authPriv -tietoturvataso ja salasanana toimii käyttäjänimi.

Kaikkien yllämainittujen komentojen kumoamiseen käytetään **no** -liitettä komennon alussa, kuten esimerkiksi **no snmp-server group snmpgroup v3 priv**, jolloin kyseinen luotu ryhmä poistetaan laitteelta. /4/

Cisco esittelee verkkosivuillaan myös useita muita snmp-server -komentoja, joita ei tässä työssä ole tarpeen käydä läpi. Kuitenkin kaikki SNMPv3 -toiminnan kannalta Ciscoworks -ympäristössä tärkeät CLI -komennot tarkastellaan seuraavassa kappaleessa.

Cisco Catalyst -kytkinten SNMPv3 -asetukset noudattavat pääpiirteittäin samaa kaavaa kuin reititinten konfiguraatiot. Tämän opinnäytetyön puitteissa testatuilla Catalyst 2950-, 2960-, 3550- ja 3560 -kytkimillä ei kuitenkaan ollut mahdollisuutta pakettien salaukseen (authPriv).

4.3 Laitteiden asetukset Ciscoworks -ympäristössä

Cisco määrittelee Ciscoworks -työkaluilla hallittavien laitteiden asetuksille tiettyjä vaatimuksia, jotka käydään läpi tässä kappaleessa. Ciscoworks LAN Management Solution (LMS) on ohjelmistopaketti Cisco -laitteiden hallintaan verkossa. Jotta LMS toimisi halutulla tavalla, on hallittavan verkon laitteet konfiguroitava oikein. Seuraavaksi käydään läpi LMS:n vaatimat laitekonfiguraatiot:

- ◊ Hostname: Jokaisella Cisco IOS -laitteella on oltava isäntänimi, jolla laite tunnistetaan verkossa. Tämä nimi löytyy myös CDP -taulusta. Jos verkossa on kaksi samannimistä laitetta, niin LMS tunnistaa näistä vain toisen. Isäntänimi määritellään Cisco IOS -laitteilla komennolla **hostname** *nimi*.
- ◊ Domain-name: Toimialueen nimi määritellään komennolla **ip domain-name** *nimi*. Tämä nimi vaikuttaa isäntänimeen.
- ◊ SNMPv3: On suositeltavaa ottaa laitteilla tämä versio käyttöön sen tietoturva ominaisuuksien vuoksi. Tähän pätevät edellisissä kappaleissa kerrotut komennot. On kuitenkin LMS:n kannalta suositeltavaa asettaa ryhmiä luotaessa näille sekä luku- että kirjoitusnäkymät (readview ja writeview). Seuraavaksi on tästä esimerkki: **snmp-server group snmpgroup v3 priv read campus write campus**. Lisäksi LMS:n Resource Manager Essentials (RME) -ohjelmaa käytettäessä voidaan laitteella suorittaa komento **snmp-server system-shutdown**, jolloin sallitaan RME:n resetoida laite tarvittaessa.
- ◊ Telnet / SSH: RME:n avulla voidaan suorittaa laitteen konfigurointia ottamalla laitteeseen Telnet- tai SSH -yhteys. Tätä varten laitteelle pitää asettaa VTY -liitännät salasanalla suojattuna.
- ◊ Cisco Discovery Protocol: LMS:n Campus Manager (CM) -ohjelma käyttää CDP:tä etsiäkseen Cisco -laitteita verkosta. CDP:n käyttöönotto sallii CM:n hakea informaatiota naapurilaitteista ja lähettää SNMP -kyselyitä näille laitteille. CM voi löytää verkkotopologian ainoastaan kun CDP on otettu käyttöön. Cisco IOS -laitteilla CDP asetetaan päälle globaalisti komennolla **cdp run** ja liitännässä komennolla **cdp enable**. /6/

5 CISCOWORKS LAN MANAGEMENT SOLUTION

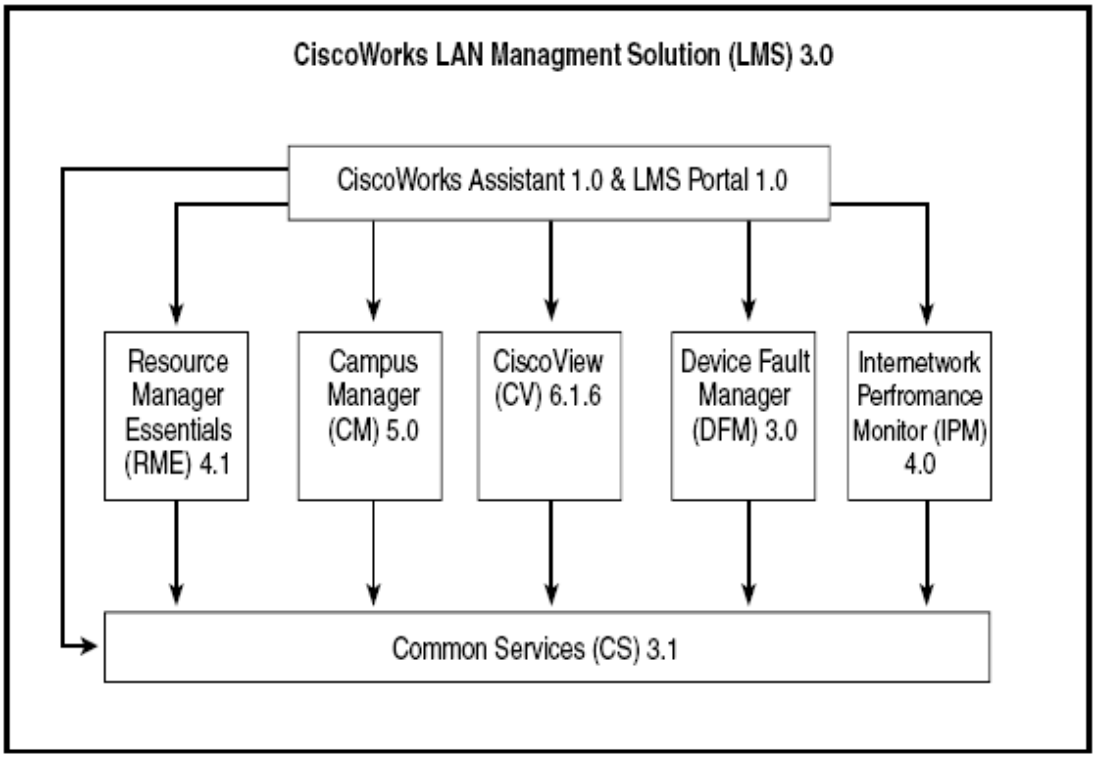
5.1 Yleistä Ciscoworks Lan Management Solution:sta

Tämän opinnäytetyön käytännön osuuden tarkoituksena oli ottaa käyttöön Ciscoworks LMS -työkalu testiverkossa ja soveltaa siinä SNMPv3:a verkonhallintaan. LMS on osa Ciscoworks -ohjelmistopakettia ja se sisältää tarvittavat ohjelmat niin pienten kuin suurtenkin lähiverkkojen hallintaan. Ohjelmilla voidaan konfiguroida, monitoroida ja hallita vikatilanteet maksimissaan 5000:llä laitteella, kun käytetään yhtä LMS -palvelinta. Kahdella palvelimella laitteita voi olla hallittavana jopa 10 000. LMS tukee myös jopa 250 000:ta isäntäkonetta.

Lan Management Solution -ohjelmapakettiin kuuluu seuraavat ohjelmat (Kuva 5-1):

- ◊ Ciscoworks Common Services: Tarjoaa joukon yhteisiä ohjelmapalveluita kaikille LMS:n ohjelmille.
- ◊ Resource Manager Essentials: Hallitsee laitteiden sisältöä, muutoksia, asetustiedostoja, syslog -analyysejä ja ohjelmakuvia. Lisäksi jäljittää ja valvoo laitteita, jotka ovat verkon toiminnan kannalta kriittisiä.
- ◊ Campus Manager: Luo kuvan hallittavan verkon topologiasta, paikantaa ja näyttää verkon käyttäjät ja isännät, sekä hallitsee virtuaalilähiverkot (VLANs). CM voi lisäksi jäljittää ja näyttää kehys- ja pakettiliikenteen verkossa sekä linkkityypit.
- ◊ CiscoView: Voidaan hallita laitteiden asetuksia ja valvoa niiden liitännöissä kulkevaa liikennettä laitteen graafisen etupaneelin avulla.
- ◊ Device Fault Manager: Hallitsee verkon laitteiden vikaantumistilanteita reaaliajassa, ylläpitää virhelokia ja vastaanottaa e-mail-, trap- ja syslog -ilmoituksia.

- ◊ Internetwork Performance Monitor: Seuloo ennakoivasti laajaverkkojen vastausaikoja, viiveenvaihtelua ja käytettävyyttä.
- ◊ Ciscoworks LMS Portal: LMS:n aloitussivu, joka kokoaa kaikkien ohjelmien tärkeimmät toiminnot saman paneelin alle. Tarjoaa mahdollisuuden siirtyä nopeasti ohjelmasta toiseen. Portaalin tietoja voidaan kustomoida käyttäjän haluamaan muotoon ja sen sisältöä voidaan lisätä tai karsia.
- ◊ Ciscoworks Assistant: Avustaa LMS -palvelimen käyttöönotossa opastaen tarvittavien tietojen syöttämisessä ja laitteiden haussa. Assistant avustaa myös virheenseulontatiedon keräämisessä.
- ◊ Integration Utility: Tuki kolmannen osapuolen hallinta-asemille. /7/



Kuva 5-1. Ciscoworks LMS -ohjelmien hierarkia.

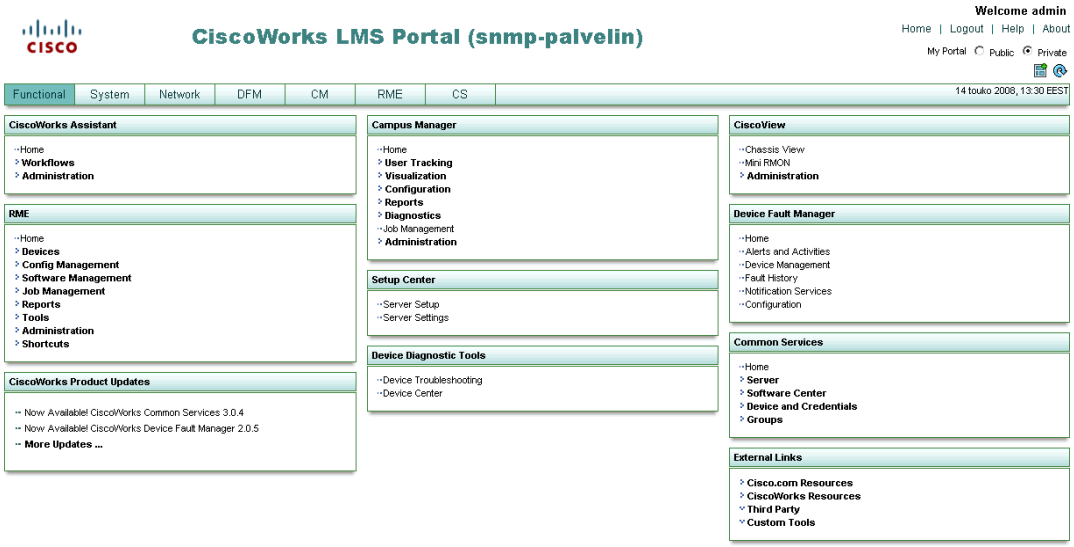
Tässä opinnäytetyössä otettiin Ciscoworks LMS:n asennuksen yhteydessä käyttöön yllä olevista ohjelmista muut, paitsi Internetwork Performance Monitor ja Integration Utility, koska näillä ei nähty olevan tarkoitusta tämän työn tavoitteen kannalta katsottuna. Lisäksi LMS päivitettiin uusimpaan 3.01 -versioon (aiempi 3.0), jotta saataisiin LMS:n ohjelmille tuki pakettien salaukseen. Päivityksestä huolimatta Device Fault Manager ei kuitenkaan tue pakettien salausta. Cisco on ilmoittanut että

tämä tullaan mahdollisesti korjaamaan tulevissa päivityksissä. 3.01 -päivitys tuo muun muassa Common Serviceen mahdollisuuden laitteiden löytämiseksi (device discovery). Tämä käyttää hyväkseen CDP:tä ja aiemmin tämä ominaisuus oli vain Campus Manager -ohjelman kautta käytettävissä. /8/

5.2 Ciscoworks LMS:n peruskäyttö ja toiminnot

Ciscoworks LMS voidaan käynnistää joko kaksoisnapsauttamalla hiirellä sen kuvaketta Windows -työpöydällä tai avaamalla selain ja ottamalla sen kautta yhteys osoitteeseen http://*localhost*:1741. Localhost on lokaalin koneen nimi, joka tässä opinnäytetyössä on *snmp-palvelin*. Mikäli SSL on käytössä, niin porttiosoite on 443 ja koko osoite muotoa https://*localhost*:443. /7/

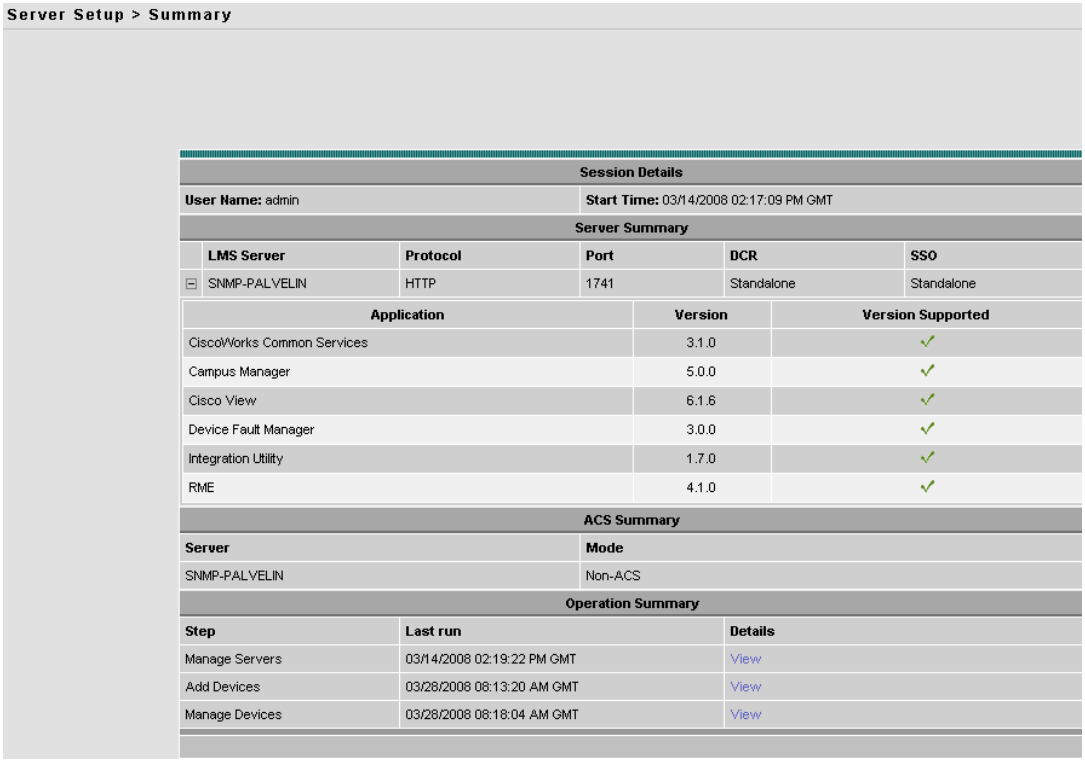
Kun yhteys palvelimeen on muodostettu, ja siihen on kirjauduttu joko järjestelmänvalvojan tai tavallisilla käyttäjätunnuksilla, aukeaa LMS Portal -aloitussivu (Kuva 5-2 ja Liite 3). Portal on linkkisivu muihin LMS:n ohjelmiin ja se on käyttäjän kustomoitavissa siinä esitettävän informaation suhteen. Portal tarjoaa statistiikkaa ja yksityiskohtaista informaatiota asennetuista ohjelmista. Se tarjoaa myös nopean navigoinnin usein käytettyihin toimintoihin. Kaikkiin LMS:n ohjelmiin voidaan siirtyä joko ohjelman nimeä tai sen paneelissa olevaa Home -linkkiä klikkaamalla. Tällöin aukeaa ohjelman oma kotisivu, josta pääsee käsiksi ohjelman kaikkiin toimintoihin. /7/



Kuva 5-2. Ciscoworks LMS Portal.

5.2.1 Ciscoworks Assistant

Assistant -ohjelma tarjoaa työjärjestyksen palvelimen asetuksille (server setup) ja laitteiden ongelmaselvitykseen (device troubleshooting). Ensimmäiseksi mainittu työjärjestys onkin hyvä suorittaa heti ensimmäisen LMS:ään kirjautumisen jälkeen (Kuva 5-3). Tässä vahvistetaan palvelimen nimi ja pääkäyttäjän kirjautumistunnukset, etsitään laitteita verkosta, lisätään ne halutuille LMS:n ohjelmille ja annetaan halutessa oletustiedot näiden laitteiden hallintaan. Samoin voidaan asettaa palvelin Access Control Server -tilaan. ACS voidaan ottaa käyttöön LMS -palvelimella, mikäli verkossa ei jo ole AAA -palvelinta ja halutaan varmistaa pääkäyttäjien autenttisuus. /7/ Tässä opinnäytetyössä ei otettu tätä ominaisuutta käyttöön.



Kuva 5-3. Ciscoworks Assistant ja Server Setup -työkalu.

Palvelimen asetusprosessissa löydetyille laitteille voidaan määritellä oletustiedot (default credentials), joilla voidaan hallita näitä laitteita. Oletustietoihin voidaan syöttää laitteelle vaadittavat kirjautumistunnukset (standard credentials), SNMP -asetukset (SNMP credentials), kuten tietoturvamalli- ja taso, käyttäjänimi, salasanat ja käytettävät autentikointi- ja salausmenetelmät sekä http -asetukset (http settings).

Kun työjärjestyksen kaikki vaiheet on käyty lävitse, näyttää Assistant yhteenvedon määritellyistä asetuksista. Nämä saadaan hyväksyttyä painamalla Finish -painiketta.

5.2.2 Common Services

Tämän ohjelman kautta voidaan hallita kaikkien ohjelmien yhteisiä toimintoja, kuten laitteiden lisääminen manuaalisesti ja niiden oletustietojen asettamista. Tämän mahdollistaa Device and Credentials, johon voi navigoida myös Portalin kautta. CS tarjoaa myös mahdollisuuden käyttäjien etuoikeuksien määrittelyyn, SSL -salauksen käyttöön asiakasselaimen ja hallittavan palvelimen välillä, SMTP -asetusten

määrittelyyn ilmoitusten vastaanottamiseen sähköpostin muodossa, sekä Cisco.com -tietojen määrittelyyn laiteprofiilien (device packages) ja ohjelmakuvien (software images) latausta varten. /7/

5.2.3 Resource Manager Essentials

RME:n ominaisuuksiin kuuluu verkon kaikkien Cisco -laitteiden hallinta. Se tarjoaa eri toimintoihin seuraavanlaisia työkaluja:

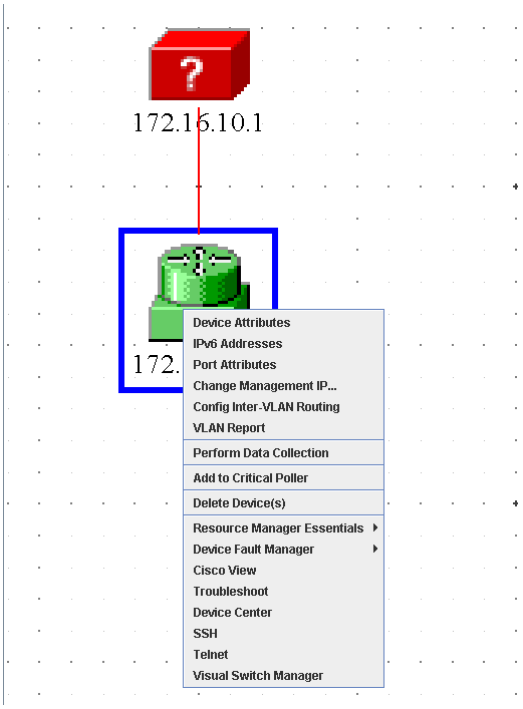
- ◊ Devices: Näyttää inventaarion verkon laitteista. Laitteita voidaan tarkastella erilaisissa ryhmissä, kuten tietyn ohjelman mukaan ryhmiteltynä ja käyttäjän määrittelemissä ryhmissä.
- ◊ Config Management: Voidaan tarkastella laitteiden konfiguraatioita ja config editor:n avulla muokata niitä. Config editor näyttää laitteen asetukset puurakenteena ja sen lehtiä klikkaamalla voidaan muuttaa laitteen asetuksia.
- ◊ Software Management: Ohjelmakuvien hallintatyökalu. Ohjelmakuvia voidaan ladata verkosta, laitteilta ja tiedostojärjestelmistä. Tämän jälkeen niitä voidaan jakaa verkon laitteiden kesken.
- ◊ Job Management: Hallitsee työprosesseja. Käyttäjä voi pysäyttää ja poistaa näitä prosesseja. Prosessit on luokiteltu Job ID:n mukaan.
- ◊ Reports: Tämän avulla voidaan luoda raportteja liittyen esimerkiksi tiettyyn protokollaan tai työprosessiin. Voidaan myös arkistoida raportteja.
- ◊ Tools: Työkaluja automaattisten toimintojen luomiseen laitteiden asetuksiin ja syslog -ilmoituksiin liittyen.
- ◊ Administration: Antaa lukuisia säätömahdollisuuksia muun muassa raporteissa näytettävään informaatioon, työprosessien aikataulutukseen, laitehallinnan asetuksiin, syslog -ilmoitusten varmuuskopiointiin ja inventaarion objektien luokitteluun.
- ◊ Shortcuts: Raportteja sekä yhteenvetoja laitteista ja asetuksista.

5.2.4 Device Fault Manager

DFM mahdollistaa verkon laitteiden vianhallinnan ja vikaraporttien tarkastelun. DFM vastaanottaa trap- syslog- ja email -ilmoituksia verkon laitteilta. Näihin tietoihin päästään käsiksi Alert and Activities -linkin kautta. Notification Services -välilehdellä päästään luomaan ilmoitusryhmiä. Device Management tarjoaa yksityiskohtaista tietoa laitteen asetuksista, järjestelmästä ja tapahtumista. Fault History antaa käyttäjän selata halutulta aikaväliltä hälytyksiä ja tapahtumia. Configuration välilehti antaa käyttäjän muuttaa jonon prioriteettejä liikenteen mukaan ja asettaa kyselyparametreja (polling parameters), sekä hallintakynnyksiä (managing tresholds). SNMP:n trap -sanomista ja niiden tarkastelusta kerrotaan myöhemmässä kappaleessa. /7/

5.2.5 Campus Manager

CM:n yksi mielenkiintoisimmista toiminnoista on sen Visualization -linkin alta paljastuva Topology Services -työkalu (Kuva 5-4), joka käynnistää Javalla toteutetun visuaalisen hallintatyökalun. Tällä työkalulla voidaan silmäillä topologiakuvaa hallittavasta verkosta, sekä hakea ja muuttaa tietoja näistä laitteista. Vaikka työkalu tuntuu hieman karulta, on se kuitenkin erittäin käyttökelpoinen myös kehys- ja paketti -liikenteen tarkasteluun. Laitteet on lisäksi jaettu niiden ominaisuuksien mukaan erilaisiin ryhmiin, kuten PoE -laitteisiin ja käyttäjän omiin ryhmiin. /7/



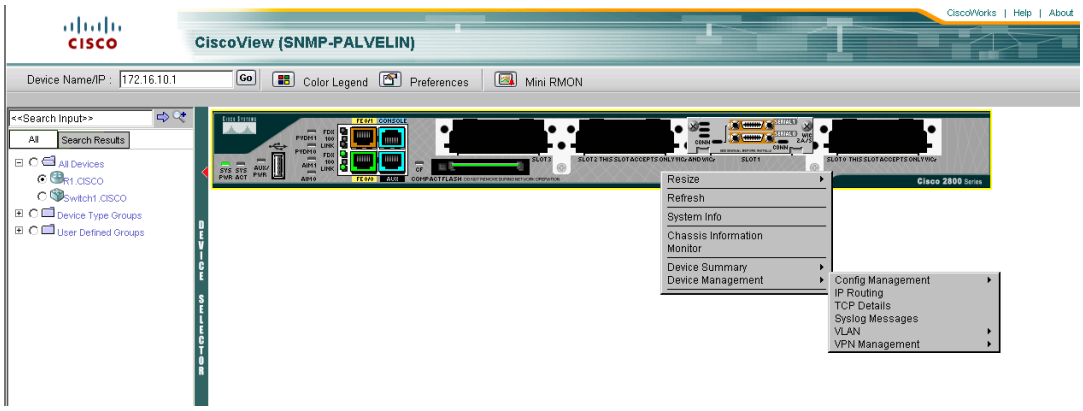
Kuva 5-4. Topology Services.

Configuration -linkin alta löytyy mahdollisuus VLAN:n, PVLAN:n ja Trunk -yhteyksien määrittelyyn ja konfigurointiin. VLAN Port Assignment:lla voidaan lisätä kytkinten portteja muihin jo luotuihin virtuaalilähiverkkoihin.

Diagnostics auttaa käyttäjää reittien hahmottamisessa. Path Analysis -työkalu antaa käyttäjän valita joko data- tai puhepakettien seuraamisen lähdeosoitteesta kohdeosoitteeseen. Onnistuneen reitinjäljityksen jälkeen ohjelma piirtää verkkotason (layer 3) kuvan reitistä ja sen solmukohdista. Sivun muilla välilehdillä voidaan tarkastella paketin reittiä raportin ja taulukon muodossa, sekä virheraportteja.

5.2.6 CiscoView

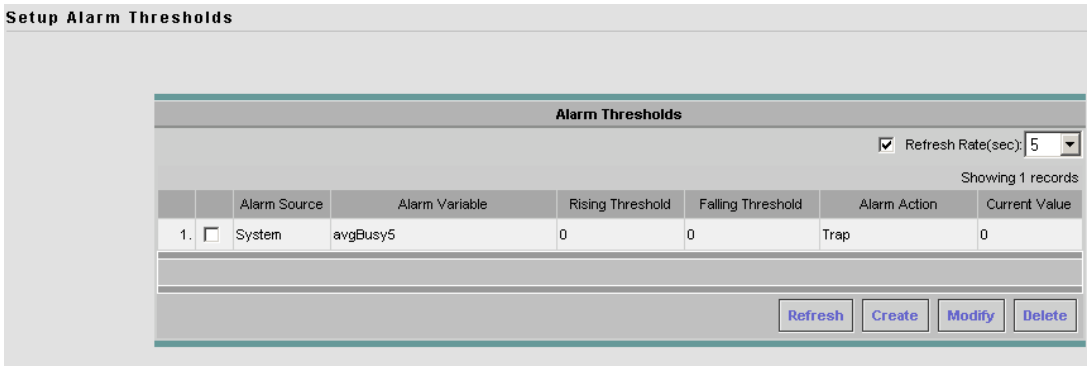
CV on graafinen SNMP -pohjainen laitehallintatyökalu, joka tarjoaa reaaliaikaista kuvaa Cisco -laitteiden etupaneelista (Kuva 5-5). CV:llä voidaan sulkea ja avata laitteen liitäntöjä, tarkkailla niissä virtaavaa liikennettä, katsoa laitteen järjestelmätietoja ja laitteesta riippuen muuttaa sen asetuksia. /7/



Kuva 5-5. CiscoView ja reitittimen profiili.

CiscoView:ssä on oletuksena laiteprofiileja (device packages) hyvin monelle kytkin- ja reititinmallille. Tässä opinnäytetyössä käytetylle 2800 -sarjan reitittimelle ei kuitenkaan laiteprofiilia löytynyt, joten se jouduttiin lataamaan erikseen cisco.com:sta. Tämä laiteprofiili sallii hyvin rajatun reitittimen konfiguroinnin verrattuna 3550 -sarjan kytkimen konfigurointimahdollisuuksiin.

CV sisältää myös Mini-RMON hallintaohjelman, jolla voidaan tarkkailla hallittavan verkon kokonaisliikennettä, havaita verkossa vallitsevat ongelmatilanteet ja sitä kautta parantaa verkon suorituskykyä (Kuva 5-6). /7/ Mini-RMON:lla voidaan asettaa hälytyskynnyksiä (alarm tresholds), joiden ylityttyä ohjelma ilmoittaa käyttäjälle hälytyskynnyksessä määritellyn ehdon toteutumisesta, joka voi olla esimerkiksi laitteen tiettyyn liitäntään saapunut liian suuri paketti.



Kuva 5-6. Mini-RMON ja hälytyskynnysten asetukset.

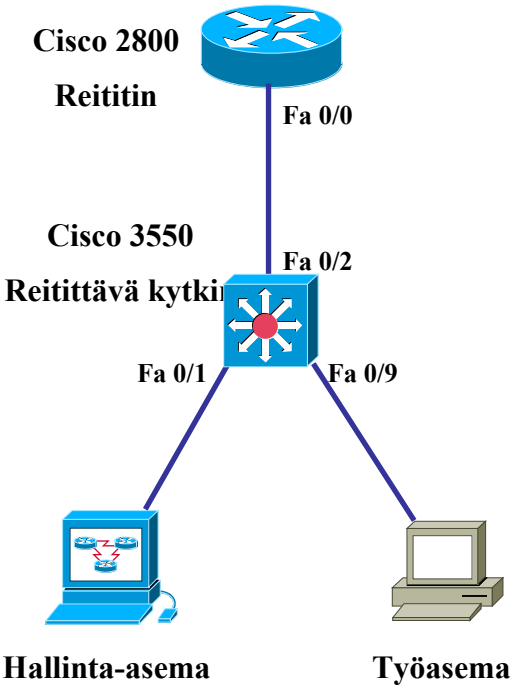
5.2.7 Muut LMS:n toiminnot ja ominaisuudet

Seuraavaksi käydään läpi muita LMS:n toimintoja ja ominaisuuksia:

- ◊ Setup Center: Palvelimen asetukset. Server Setup tarjoaa saman kuin Assistant ja se on hyvä suorittaa aina uuden asennuksen jälkeen. Server Settings kuuluu Common Services -ohjelmaan ja antaa käyttäjän muokata vapaammin palvelimen asetuksia. Asetukset on jaettu viiteen välilehteen, jotka ovat System Settings, Security Settings, Data Collection Settings, Data Collection Schedule ja Data Purge Settings.
- ◊ Device Diagnostic Tools: Device Troubleshooting ja Device Center auttavat laitteiden vianetsinnässä. Device Center tarjoaa useita työkaluja vian etsimiseen ja rajaamiseen. Täältä käyttäjä voi pingata, ottaa telnet yhteyden laitteelle, jäljittää reitin laitteelle, testata SNMP -yhteyden, tarkkailla eri raportteja ja muokata laitteen asetuksia. Device Troubleshooting on Assistant -ohjelmaan kuuluva työkalu, joka suorittaa automaattisesti tietyn joukon testejä, joiden tulokset esitetään käyttäjälle raporttina.
- ◊ Device and Credential Repository: DCR on tallennuspaikka kaikille verkon laitetiedoille joita hallintaohjelmat käyttävät. DCR auttaa useita ohjelmia jakamalla luettelon hallittavista laitteista näiden kesken. Ohjelmat voivat lukea ja kirjoittaa tietoja laiteluetteloon. DCR mahdollistaa myös laitteiden lisäämisen muista lähteistä, kuten kolmannen osapuolen hallinta-asemilta, sekä laitetietojen siirtämisen muihin lähteisiin. /7/

6 SNMPV3:N KÄYTTÖ CISCOWORKSISSA

Tässä kappaleessa käydään läpi SNMPv3 -asetusten käyttöönotto Ciscoworks LMS -ympäristössä. SNMPv3 -asetusten testaamista varten ja moniulotteisemman kuvan saamiseksi rakennettiin opinnäytetyön suorittamista varten pieni testiverkko, jonka topologian voi nähdä kuvasta 6-1.

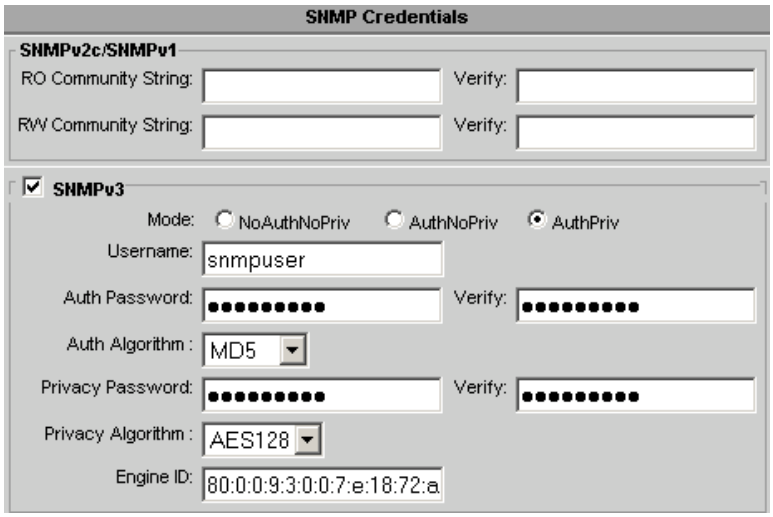


Kuva 6-1. Laboratorion testiverkko.

Testiverkon laitteilla sovellettiin 3:nessa kappaleessa selostettuja komentoja. Työssä käytettiin myös yhtä työasemaa tarkkailemaan kytkimen ensimmäiseen porttiin (Fa 0/1) tulevaa ja lähtevää liikennettä käyttäen Ethereal -ohjelmaa.

6.1 SNMPv3:n käyttöönotto LMS:ssä

Laitteiden SNMPv3 -asetusten määrittely voidaan Ciscoworks LMS:ssä suorittaa joko Server Setup -työkalun tai Common Services -ohjelman avulla. /7/ Jälkimmäisessä toimitaan valitsemalla Device Credentials -linkin alta Device Management -työkalu. Tällöin avautuu sivu joka esittelee laiteluettelon, josta käyttäjä valitsee laitteen, tai laitteet, joiden asetuksia halutaan muuttaa. Nämä tiedot tallentuvat DCR -tietokantaan. Edit Device Credentials -valinnan kautta käyttäjälle avautuu sivu asetusten määrittelyä varten, josta löytyy myös SNMP -asetuksia varten oma välilehti. Kaikkia tietoja ei tarvitse tällä sivustolla täyttää, vaan esimerkiksi pelkkien SNMP -asetusten määrittely riittää. Kuvasta 6-2 voidaan nähdä SNMP credentials -ikkuna, jossa määriteltynä SNMPv3 -asetukset.



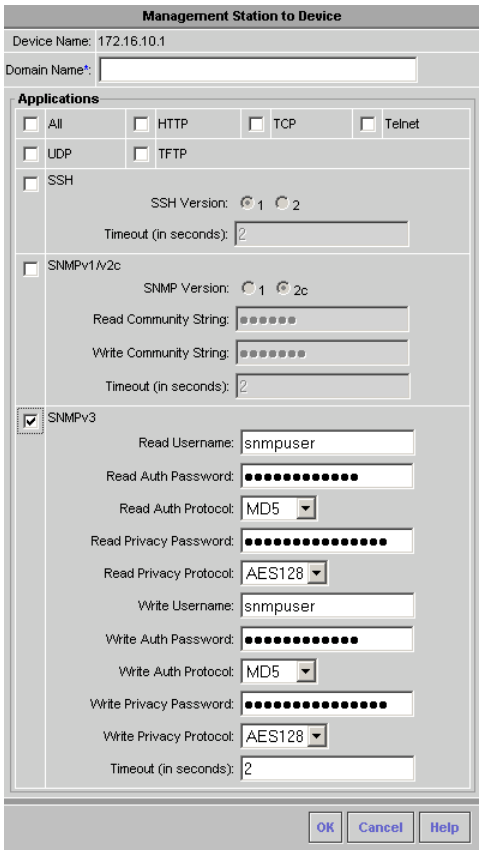
Kuva 6-2. SNMPv3 -asetukset autentikointi- ja salausmäärittelyillä.

Jos laitteella ei haluta käytettävän salausta, valitaan AuthNoPriv -asetus käyttöön. Mikäli kumpaakaan tietoturvamenetelmää ei haluta käyttää, otetaan NoAuthNoPriv -valinta käyttöön. Tätä valintaa ei kuitenkaan suositella, koska tällöin verkonhallinnassa ei ole minkäänlaista tietoturvaa. Engine ID:n määrittely ei ole pakollinen toimenpide, vaan käyttäjätunnuksen ja salasanojen avulla ohjelma hakee kyseisen käyttäjän moottoritunnisteen ja lisää sen dynaamisesti tähän kenttään.

Kun tarvittavat asetukset ovat syötetty, valitaan lopuksi Finish, jolloin määritellyt asetukset tulevat käyttöön. Tämä ei kuitenkaan välttämättä tapahdu heti, vaan voi kestää useamman sekunnin.

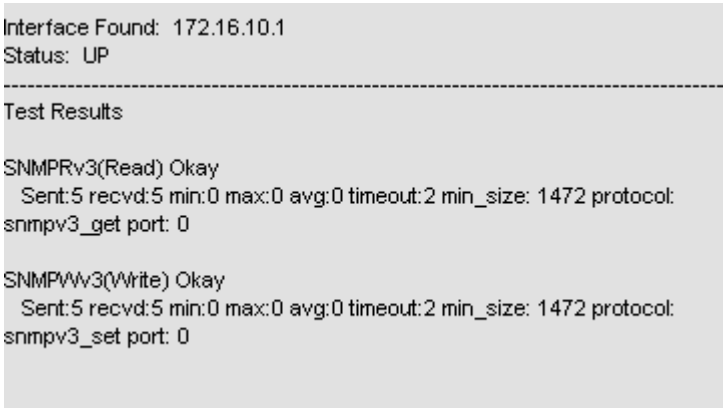
6.1.1 SNMPv3 -asetusten testaaminen

Portal -sivun Device Diagnostic Tools -paneelin alta löytyy Device Center, joka tarjoaa monipuoliset toiminnot eri protokollakerrosten testaamiseen ja vikojen rajaamiseen. Sivulta aukeavasta laiteluettelosta valitaan haluttu laite testausta varten, jolloin ruudun keskelle aukeaa joukko paneeleita. Tools -paneelin alta löytyy Management Station to Device -työkalu, joka on ensisijainen apuväline laitteiden SNMP -asetusten toiminnan testaamiseen (Kuva 6-3).



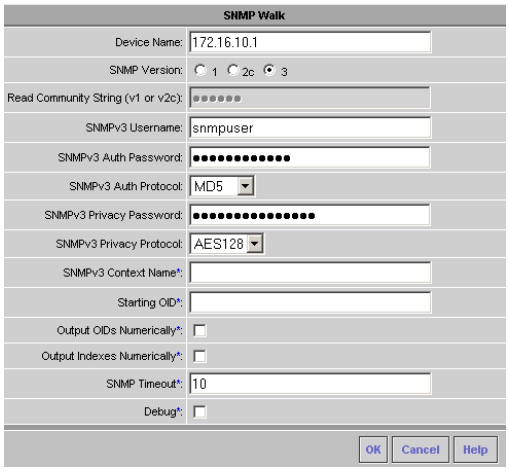
Kuva 6-3. Management Station to Device.

Tässä ikkunassa tulee valita juuri ne SNMP -asetukset, jotka määriteltiin laitteelle aiemmin Device Management -työkalulla. Tietojen syöttämisen jälkeen aloitetaan testi painamalla OK. Tällöin ohjelma testaa käyttäjän luku- ja kirjoitusoikeuksia laitteelle (Kuva 6-4).



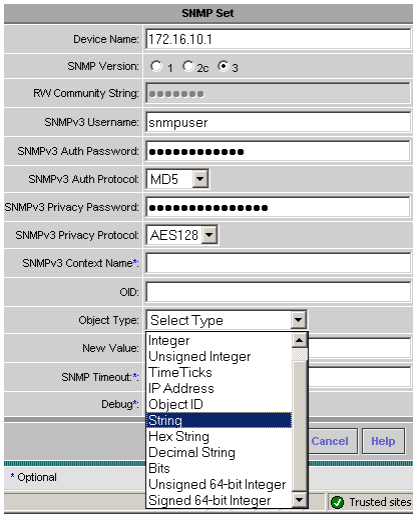
Kuva 6-4. Onnistunut SNMPv3 -testi.

Device Center:n toiminnoista löytyy lisäksi erilliset työkalut SNMP -Set ja Walk -toimintojen suorittamiseen. Jälkimmäisellä voidaan hakea laitteen MIB -tietokannasta objektien arvoja syöttämällä OID -tunnuksen tai alkuosan siitä sille varattuun kenttään, jolloin hakua rajataan (Kuva 6-5). Jos OID -tunnusta ei syötetä, haetaan laitteen MIB:n kaikkien objektien kaikki arvot.



Kuva 6-5 SNMP Walk -työkalu.

SNMP Set -työkalu antaa käyttäjän muuttaa laitteen MIB -tietokannan objektien arvoja. Käyttäjän tulee määritellä SNMP -käyttäjäasetusten lisäksi muutettavan objektin OID -tunnus, objektin tyyppi ja uusi arvo (Kuva 6-6).



Kuva 6-6. SNMP Set -työkalu.

Mikäli laitteiden SNMP -asetusten kanssa on sattunut virhe, päästään näitä asetuksia muuttamaan nopeasti Edit Device Credentials -linkin kautta, joka löytyy myös Device Centerin Tools -paneelista. Tässä paneelissa on myös linkkejä muihin ohjelmiin ja työkaluihin.

6.2 SNMPv3 -pohjainen hallinta LMS -ympäristössä

Ciscoworks LMS:n käytössä SNMP on hyvin vahvasti läsnä. Ohjelmat, jotka käyttävät SNMP:tä verkon laitteiden kanssa kommunikoidessaan, ovat Common Services, Resource Manager Essentials, Campus Manager, Device Fault Manager, CiscoView ja Internetwork Performance Monitor. Näistä ohjelmista CS ja DFM käyttävät UDP -porttia 162 vastaanottamaan trap -sanomia laitteilta. Lisäksi kaikki muut ohjelmat DFM:ää lukuun ottamatta tukevat molempia tietoturvamenetelmiä, kun taas DFM käyttää vain autentikointia. /7/

Viimeisimmässä LMS:n päivityksessä Common Services, aiemmin pelkän Campus Managerin lisäksi, antaa mahdollisuuden käyttää SNMP:tä löytääkseen laitteita hallittavasta verkosta. /8/ Tämä tapahtuu Device Discoveryn avulla, jolloin määritellyillä SNMP -asetuksilla ohjelma hakee laitteen tiedot Get -operaatioilla ja tallentaa ne DCR -laiteluetteloon muidenkin ohjelmien käytettäväksi. Kyseinen työkalu löytyy CS:n Device and Credentials -linkin alta.

6.2.1 Campus Manager ja Topology Services

CM:n Visualization -linkin alta löytyvällä Java -pohjaisella Topology Services -ohjelmalla luodaan SNMP:tä käyttäen hallittavasta verkosta topologiakuva. Tämän kuvan esittämiä laitteita voidaan käsitellä tarkemmin klikkaamalla hiiren oikeaa nappia laitteen ikonin kohdalla, jolloin avautuu valikko, josta voidaan valita tarkasteltaviksi laitteen attribuutit, IPv6 -osoitteet, porttien attribuutit ja VLAN -raportit. Lisäksi se mahdollistaa hallintaosoitteen vaihdon, virtuaalilähiverkkojen välisen konfiguroinnin, tietojen keräyksen, laitteen poiston DCR:stä ja kriittisten laitteiden kyselyn. Viimeisin huolehtii tärkeiden laitteiden usein tapahtuvasta tilan kyselystä. Tavallisesti koko hallittava verkko tarkastetaan kahden tunnin välein

suoritettavilla kyselyillä. Kun otetaan tietyillä laitteilla käyttöön Critical Polling, suoritetaan näille laitteille tilakysely viiden minuutin välein.

Yllämainittujen kysely- ja asetustoimenpiteiden lisäksi valikko tarjoaa muun muassa linkit SSH:n, Telnetin, RME:n, DFM:n ja CiscoView:n käyttöön.

6.2.2 Default Fault Manager ja Trap -sanomat

DFM:n tärkein ominaisuus SNMP:n kannalta on sen kyky vastaanottaa trap -sanomia. Kuten aiemmin on mainittu, DFM on ohjelma joka vastaanottaa paitsi laitteiden lähettämiä ilmoitus- ja virhesanomia, myös antaa käyttäjälle työkalut erityyppisten virhetilanteiden havainnoinnin määrittelyyn eri konfiguraatioin ja kynnyksin. DFM pitää yllä virhetilastoa, joka helpottaa tulevissa virhetilanteissa ja osoittaa hallittavan verkon ongelmakohdat. /7/

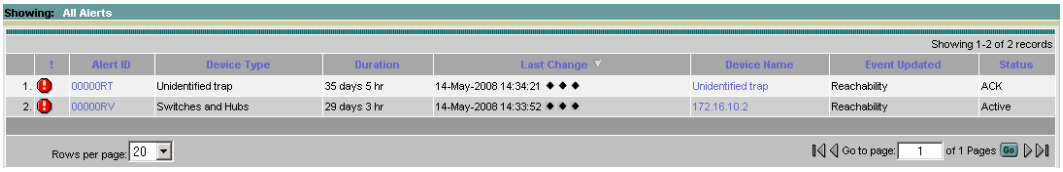
DFM vastaanottaa trap -sanomia UDP -porttiin 162, mutta jos tämä ei tilapäisesti ole käytössä, niin vastaanottavana porttina toimii portti 9000. DFM voi käyttää samaa DCR -laiteluetteloa kuin muut ohjelmat, mutta tällöin pitää ottaa huomioon laitteiden salausasetukset käytettäessä SNMPv3:a. Koska DFM ei tue pakettien salausta, tulee siihen liitettävien laitteiden tietoturvatason olla authNoPriv. Muutoin DFM lisää laitteen tuntemattomien laitteiden ryhmään aiheuttaen virheilmoituksen ”SNMPv3 is not supported.”. Virheilmoituksen aiheuttaa myös noAuthNoPriv -tietoturvataso viestillä ”Missing SNMPv3 authentication password.”. /7/

DFM voi toimia myös trap -sanomien välittäjänä muille hallinta-asemille. DFM ei koske trap -sanomaan millään lailla, vaan vastaanottaa laitteen agentin lähettämän trap -sanoman UDP porttiin 162 ja lähettää mielivaltaisesta portista sen edelleen toisen hallinta-aseman porttiin 162. /7/

Mikäli DFM:n trap -sanomien vastaanottavaa porttia halutaan muuttaa, tämä voidaan tehdä valitsemalla Configuration, edelleen Other Configurations ja tämän alta SNMP Trap Receiving. Syöttämällä kenttään Receiving Port uuden porttinumeron ja

hyväksymällä tämä Apply -painikkeella, ottaa DFM uuden portin käyttöön vastaanottamaan trap -sanomia. /7/

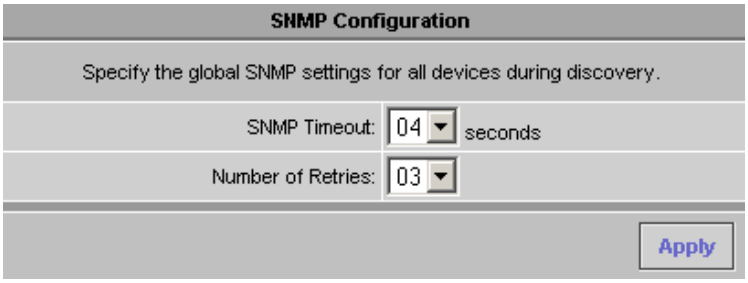
Trap -sanomien tarkasteluun pääsee navigoimalla Alerts and Activities -sivulle, josta oletuksena näkee kaikki virheilmoitukset. Jokaisen laitteen kaikki aiheuttamat virheet on järjestetty niiden jokaisen viimeisimmän kuittaamattoman virheilmoituksen alle. Klikkaamalla laitteen nimeä avautuu laitteen kaikki virheet ja tapahtumat näyttävä taulukko. Virheet ja muut ilmoitukset voidaan kuitata, jolloin DFM olettaa kyseisen hälytyksen aiheuttaneen vian korjaantuneen. Kun laitteen agentti lähettää trap -sanoman DFM:lle, kirjaa tämä sen kyseisen laitteen Alert -taulukkoon (Kuva 6-7).



Kuva 6-7. Alerts and Activities -hälytystaulu.

Trap -sanomien näkyvyyttä DFM:ssä testattiin tämän opinnäytetyön testiverkossa asettamalla laitteet lähettämään trap -sanomia, kun esimerkiksi konfiguraatioita muutetaan, liitäntöjä avataan tai suljetaan ja kun laite käynnistetään uudelleen. Nämä testit onnistuivat ja trap -sanomat olivat luettavissa hälytystaulukosta.

Jotta DFM olisi perillä laitteiden jatkuvasta toiminnasta, suorittaa se säännöllisiä SNMP -kyselyitä joilla se varmistaa laitteen läsnäolon hallittavassa verkossa. Device Management -välilehden SNMP Config -painikkeen alta käyttäjä pääsee muokkaamaan näiden kyselyiden aikavälejä ja epäonnistuneen kyselyn sattuessa toistettavien kyselyiden lukumäärää (Kuva 6-8).

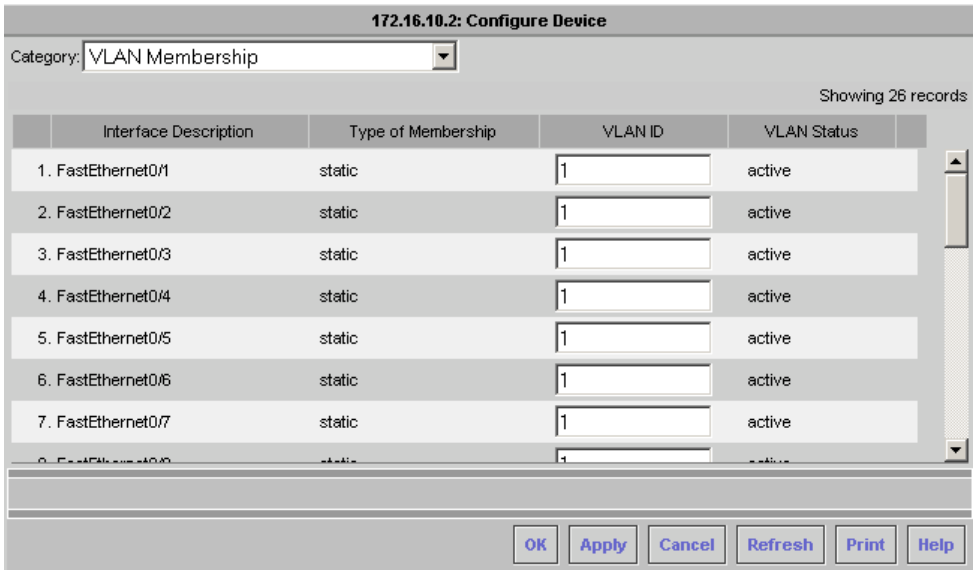


Kuva 6-8. SNMP Configuration -valikko.

6.2.3 CiscoView ja SNMPv3

CiscoView käyttää SNMP:tä laitetietojen hakuun ja asetusten muuttamiseen. Kun CiscoView:n laiteluettelosta valitaan haluttu laite tarkasteltavaksi, lähettää CV suuren määrän Get-, GetNext- ja GetBulk -pyyntösanomia hakeakseen tietoa laitteesta ja virittääkseen laitteen profiilikuvan vastaamaan oikean, fyysisen laitteen etupaneelia.

Kun profiilikuvaa klikataan hiiren oikealla napilla, saadaan esiin laitteen hallintavalikko, josta löytyy laitteen device package:sta riippuen toimintoja laitteen liitännöissä kulkevan liikennemäärän seurantaan, laitteen järjestelmätietojen esittämiseen, laitteen asetusten konfigurointiin Config Editor -työkalulla, sekä reititysten-, VPN:n ja VLAN:n hallintaan. Laitteen asetuksia muutettaessa, kuten esimerkiksi luotaessa kytkimelle uusi virtuaalilähiverkko (VLAN), lähettää CiscoView kyseisen laitteen agentille Set -operaation, joka sisältää uuden VLAN:n määrittelyyn tarvittavat objektit arvoineen yhdessä OID -tunnusten kanssa (Kuva 6-9).



Kuva 6-9. VLAN -jäsenyyksien määrittely CiscoView:ssa.

Testiverkon Ethereal -työasemalla tehdyistä SNMPv3 -sanomajäljityksistä voitiin havaita verkon reitittimen SNMP -pakettien täysi tietoturvataso pakettien salauksen vuoksi, jolloin näiden pakettien sisältöä ei voitu tulkita (Liitteet 4 ja 5). Sen sijaan

kytkimelle osoitettujen SNMP -pakettien sisältöä voitiin lukea, koska tässä verkossa käytetty Cisco 3550 -sarjan kytkin tuki vain autentikointimenetelmää (Liitteet 6 ja 7).

6.3 SNMPv3 -sanomat testiverkossa

Tämän opinnäytetyön yksi tavoite SNMPv3:n käyttämisen Ciscoworks:ssa ohella oli tutkia SNMPv3 -sanomaliikennettä testiverkossa. SNMPv3 -sanomia tähystettiin verkon Ethereal -työasemalta, joka siis toimi verkon liikenteen ”nuuhkijana” kytkimen Fa 0/9 -portissa.

6.3.1 GetRequest -sanomat

CiscoView -ohjelmaa käyttäen testiverkon Cisco 2800 -sarjan reitittimeltä tarkkailtiin Monitor -työkalulla laitteen prosessorin kuormitusta, käytetyn muistin määrää ja muistin puskurointiprosenttia. Koska reitittimellä oli käytössään SNMPv3 authPriv -tietoturvataso, ei GetRequest-, eikä myöskään reitittimeltä lähtevän GetResponse -sanoman sisältöä näin ollen voida tulkita. Seuraavaksi katsotaan salatusta GetRequest -sanomasta esimerkki:

Simple Network Management Protocol
- Version: 3 (3)
- Message Global Header
  - Message Global Header Length: 16
  - Message ID: 341
  - Message Max Size: 1024
  - **Flags: 0x07**
    - **.... .1.. = Reportable: Set**
    - **.... ..1. = Encrypted: Set**
    - **.... ...1 = Authenticated: Set**
  - Message Security Model: USM
- Message Security Parameters
  - Message Security Parameters Length: 61
  - Authoritative Engine ID: 800000090300001AA140D3B0

1... .... = Engine ID Conformance: RFC3411 (SNMPv3)
Engine Enterprise ID: cisco (9)
Engine ID Format: MAC address (3)
Engine Boots: 5
Engine Time: 1791
User Name: snmpuser
Authentication Parameter: 5A5103844E6A3DC9D3373799
Privacy Parameter: 000000051D40B893
Encrypted PDU (274 bytes)

SNMPv3 -sanomaosan kohdasta Flags voidaan havaita että sanoma vaatii vastaanottajalta kuittauksen (GetResponse), ja että autentikointi ja salaus ovat käytössä. Lisäksi sanomasta voidaan nähdä käyttäjätunnus ja todeta varsinaisen informaatiosisällön olevan salattu (encrypted).

Cisco 3550 -sarjan kytkimellä suoritettiin samaista Monitor -työkalua käyttäen laitteen sisään- ja ulosmenevän liikenteen valvonta. Koska kytkimellä oli käytössä SNMPv3 autNoPriv -tietoturvataso, voidaan GetRequest- ja GetResponse -sanomien sisältöä lukea testiverkon työaseman kaappaamista paketeista joista on esitettynä seuraavaksi GetRequest -sanoma:

Simple Network Management Protocol
Version: 3 (3)
Message Global Header
Message Global Header Length: 16
Message ID: 613
Message Max Size: 1024
Flags: 0x05
.... .1.. = Reportable: Set
.... ..0. = Encrypted: Not set
....1 = Authenticated: Set
Engine Boots: 9
Engine Time: 9977
User Name: snmpuser

Authentication Parameter: 57F3346F8F3B14945D420336

Privacy Parameter:

Context Name:

PDU type: GET (0)

Request Id: 0x00000265

Error Status: NO ERROR (0)

Error Index: 0

Object identifier 1: 1.3.6.1.4.1.9.9.48.1.1.1.6.1 (SNMPv2-SMI::enterprises.9.9.48.1.1.1.6.1)

Value: NULL

Object identifier 2: 1.3.6.1.4.1.9.9.48.1.1.1.5.1 (SNMPv2-SMI::enterprises.9.9.48.1.1.1.5.1)

Kuten sanoman Flags -osasta voidaan huomata, ei paketti ole salattu ja informatiivinen osa sanoman lopussa on luettavissa. Huomioitavaa on myös pyynnössä kysyttävien objektien OID -tunnusten näkyminen.

Reitittimen ja kytkimen yllä olevat sanomaesimerkit ovat kokonaisuudessaan tarkasteltavissa liitteissä 4 ja 6.

6.3.2 SetRequest -sanomat

SetRequest -operaatiota sovellettiin luomalla reitittimelle uusi VLAN, joka määriteltiin CiscoView -ohjelman avulla. Uusi virtuaalilähiverkko sai nimekseen *testivlan*
ja sai VLAN ID:n 6. Samanniminen ja saman VLAN ID:n omaava virtuaalilähiverkko luotiin myös kytkimelle käyttäen CiscoView -ohjelmaa. Seuraavaksi on esitettynä kytkimen SetRequest -sanoman informaatiosisältö:

PDU type: SET (3)

Request Id: 0x000003ee

Error Status: NO ERROR (0)

Error Index: 0

Object identifier 1: 1.3.6.1.4.1.9.9.46.1.4.2.1.11.1.6 (SNMPv2-SMI::enterprises.9.9.46.1.4.2.1.11.1.6)
Value: INTEGER: 4
Object identifier 2: 1.3.6.1.4.1.9.9.46.1.4.2.1.2.1.6 (SNMPv2-SMI::enterprises.9.9.46.1.4.2.1.2.1.6)
Value: INTEGER: 1
Object identifier 3: 1.3.6.1.4.1.9.9.46.1.4.2.1.3.1.6 (SNMPv2-SMI::enterprises.9.9.46.1.4.2.1.3.1.6)
Value: INTEGER: 1
Object identifier 4: 1.3.6.1.4.1.9.9.46.1.4.2.1.4.1.6 (SNMPv2-SMI::enterprises.9.9.46.1.4.2.1.4.1.6)
Value: STRING: **"testivlan"**
Object identifier 5: 1.3.6.1.4.1.9.9.46.1.4.2.1.5.1.6 (SNMPv2-SMI::enterprises.9.9.46.1.4.2.1.5.1.6)
Value: INTEGER: 1500
Object identifier 6: 1.3.6.1.4.1.9.9.46.1.4.2.1.6.1.6 (SNMPv2-SMI::enterprises.9.9.46.1.4.2.1.6.1.6)
Value: Hex-STRING: 00 01 86 A6

Yllä olevasta esimerkistä voidaan havaita sanoman variablebindings -kentän sisältämät objektien OID -tunnukset ja niille pyydetyt uudet arvot. Tästä voidaan myös selvästi erottaa luodun VLAN:n nimi.

Reitittimelle ja kytkimelle osoitetut kokonaiset SetRequest -sanomat ovat tarkasteltavissa liitteissä 5 ja 7.

6.3.3 Trap -sanomat

Trap -sanoman lähettäminen aiheutettiin testiverkossa sulkemalla CiscoView -ohjelmaa käyttäen kytkimen reitittimelle johtava liitäntä (Fa 0/2). Kytkin oli konfiguroitu lähettämään trap -sanoma kun sen jokin liitäntä suljetaan. Seuraavaksi tarkastellaan PDU -osaa tästä trap -sanomasta:

Context Name:
PDU type: TRAP-V2 (7)
Request Id: 0x00000002
Error Status: NO ERROR (0)
Error Index: 0
Object identifier 1: 1.3.6.1.2.1.1.3.0 (SNMPv2-MIB::sysUpTime.0)
Value: Wrong Type (should be Timeticks): INTEGER: 2144259
Object identifier 2: 1.3.6.1.6.3.1.1.4.1.0 (SNMPv2-MIB::snmpTrapOID.0)
Value: OID: **IF-MIB::linkDown**
Object identifier 3: 1.3.6.1.2.1.2.2.1.1.2 (IF-MIB::ifIndex.2)
Value: INTEGER: 2
Object identifier 4: 1.3.6.1.2.1.2.2.1.2.2 (IF-MIB::ifDescr.2)
Value: STRING: **FastEthernet0/2**
Object identifier 5: 1.3.6.1.2.1.2.2.1.3.2 (IF-MIB::ifType.2)
Value: INTEGER: ethernetCsmacd(6)
Object identifier 6: 1.3.6.1.4.1.9.2.2.1.1.20.2 (SNMPv2-SMI::enterprises.9.2.2.1.1.20.2)
Value: STRING: **"administratively down"**

Informaatiosisällöstä voidaan havaita muun muassa mihin MIB:n objektiin kyseinen trap -sanoma kohdistuu, mikä on liitännän kuvaus ja sen tila.

Yllä oleva trap -sanoma löytyy kokonaisuudessaan liitteestä 8.

7 YHTEENVETO

Ciscoworks Lan Management Solution on monipuolinen verkonhallinnan ohjelmistopaketti, joka mahdollistaa Cisco Systems:n laitteiden monipuolisen kontrolloinnin ja valvonnan verkossa. Ohjelmisto vaatii kuitenkin käyttäjältään jonkin verran perehtymistä sen ympäristöön ja eri ohjelmien toimintaan ennen täyden hyödyn saavuttamista. Koska Ciscoworks LMS soveltuu käytettäväksi vain Ciscon

laitteiden kanssa, ei sitä voida käyttää yhdessä muiden laitetoimittajien tuotteiden kanssa.

Tämän opinnäytetyön päätavoite oli ottaa Ciscoworks LMS -ohjelmistossa käyttöön SNMP -verkonhallintaprotokollan 3. versio ja todeta sen toiminta koulun tietoliikenteen laboratorioon rakennetussa testiverkossa. Tämän verkon molemmat laitteet konfiguroitiin ottamaan käyttöön SNMPv3 -asetukset ja lähettämään ilmoitussanomia Ciscoworks LMS hallinta-asemalle. Näiden laitteiden hallinta onnistui tyydyttävin tuloksin. Pientä hämmennystä aiheutti kuitenkin LMS:n eri ohjelmien samankaltaiset toiminnot ja ohjelmiston ajoittainen hidas toiminta. Osa ohjelmiston ongelmista saatiin ratkottua päivittämällä LMS 3.0 -versio 3.0.1 -versioon. On kuitenkin todettava, että SNMPv3 -pohjainen hallinta LMS:n ohjelmilla oli pääsääntöisesti toimivaa ja tehokasta.

SNMPv3:n valintaan hallintaprotokollana vaikuttivat erityisesti sen tietoturvaominaisuudet, joiden vaikutusta pystyttiin havainnoimaan testiverkossa SNMP -liikennettä tarkkailleen työaseman avulla. Salattujen SNMP -sanomien informaatiosisältöä ei kyetty lukemaan, toisin kuin salaamattomien sanomien, joiden sisältöä ja käsiteltäviä objekteja kyettiin tunnistamaan.

Tämän opinnäytetyön lopputuloksena voidaan todeta, että SNMPv3 on erittäin suositeltava hallintaprotokolla niin pieniin kuin suuriinkin yritysten verkkoihin erityisesti sen tietoturvallisuuden vuoksi. Ciscoworks tarjoaa erittäin tehokkaat työkalut Cisco -laitepohjaiseen verkonhallintaan, mutta vaativat käyttäjältä tietoa ja osaamista. Ciscoworks LMS -ohjelmisto soveltuu käytettäväksi verkonhallinnan opetusympäristönä.

LÄHTEET

1. Stallings, W. SNMP, SNMPv2, SNMPv3, and RMON 1 and RMON2. Reading (Mass.): Addison-Wesley, 2000. [Viitattu 21.5.2008].

2. Wikipedia verkkotietosanakirja. Simple Network Management Protocol [verkkodokumentti]. [Viitattu 21.5.2008]. Saatavissa http://en.wikipedia.org/wiki/SNMP

3. Ruuska, T & Halme, P. Seminaari: Verkonhallinta [verkkodokumentti]. Lappeenrannan teknillinen yliopisto, 2006. [Viitattu 21.5.2008]. Saatavissa: http://www.it.lut.fi/kurssit/0506/Ti5316800/seminaarit/Verkonhallinta_Tomi_Ruuska_Pasi_Halme_seminaari.pdf

4. Cisco Network Academy. CCNP: Implementing Secure Converged Wide-area Network v5.02. [verkkodokumentti]. [Viitattu 21.5.2008]. Saatavissa: http://cisco.netacad.net

5. Cisco Systems. SNMPv3 IOS -commands Guide [verkkodokumentti]. [Viitattu 21.5.2008]. Saatavissa: http://www.cisco.com/en/US/docs/ios/12_0t/12_0t3/feature/guide/Snmp3.html

6. Cisco Systems. Ciscoworks LMS Deployment Guide 3.0 [verkkodokumentti]. [Viitattu 21.5.2008]. Saatavissa: http://www.cisco.com/en/US/prod/collateral/netmgtsw/ps6504/ps6528/ps2425/ps7196/prod_white_paper0900aecd80695cad.pdf

7. Cisco Systems. Installing and Getting Started With Ciscoworks LMS [verkkodokumentti]. [Viitattu 21.5.2008]. Saatavissa: http://www.ciscosystems.com/en/US/docs/net_mgmt/ciscoworks_lan_management_solution/3.0/install/guide/lmsig30.pdf

8. Cisco Systems. Readme for Ciscoworks LMS 3.0 December 2007 Update on Windows [verkkodokumentti]. [Viitattu 21.5.2008]. Saatavissa: http://www.ciscosystems.com/en/US/docs/net_mgmt/ciscoworks_lan_management_solution/3.0.1/readme/windows/guide/lms3_0_dec_2007_update_win.pdf

LIITELUETTELO

```
R1#sh run
Building configuration...

Current configuration : 1265 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
ip cef
!
!
ip domain name CISCO
!
!
voice-card 0
!
!
interface FastEthernet0/0
 ip address 172.16.10.1 255.255.255.0
 duplex auto
```

```
speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/1/0
 no ip address
 shutdown
 no fair-queue
 clock rate 125000
!
interface Serial0/1/1
 no ip address
 shutdown
 clock rate 125000
!
router eigrp 100
 network 172.16.0.0
 auto-summary
!
!
!
ip http server
no ip http secure-server
!
snmp-server group snmpgroup v3 priv write v1default notify *tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFF0F
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps eigrp
```

```
snmp-server enable traps config
snmp-server enable traps frame-relay multilink bundle-mismatch
snmp-server host 172.16.10.250 version 3 priv snmpuser
!
!
control-plane
!
!
line con 0
 password cisco
 login
line aux 0
line vty 0 4
 password cisco
 login
!
scheduler allocate 20000 1000
end


R1#sh snmp group
groupname: ILMI                        security model:v1
readview : *ilmi                       writeview: *ilmi
notifyview: <no notifyview specified>
row status: active

groupname: ILMI                        security model:v2c
readview : *ilmi                       writeview: *ilmi
notifyview: <no notifyview specified>
row status: active

groupname: snmpgroup                   security model:v3 priv
```

readview : v1default writeview: v1default
notifyview: *tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.F
row status: active

R1#sh snmp user
User name: snmpuser
Engine ID: 80000009030000070E1872A0
storage-type: nonvolatile active
Authentication Protocol: MD5
Privacy Protocol: AES128
Group-name: snmpgroup

R1#sh snmp engineid
Local SNMP engineID: 80000009030000070E1872A0
Remote Engine ID IP-addr Port

R1#sh snmp host
Notification host: 172.16.10.250 udp-port: 162 type: trap
user: snmpuser security model: v3 priv

```
Switch1#sh run
Building configuration...

Current configuration : 1987 bytes
!
version 12.1
no service single-slot-reload-enable
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Switch1
!
!
ip subnet-zero
ip domain-name CISCO
!
!
spanning-tree extend system-id
!
!
interface FastEthernet0/1
 no ip address
!
interface FastEthernet0/2
 no ip address
!
interface FastEthernet0/3
 no ip address
!
.
```

```
.
.
!
interface FastEthernet0/24
 no ip address
!
interface GigabitEthernet0/1
 no ip address
!
interface GigabitEthernet0/2
 no ip address
!
interface Vlan1
 ip address 172.16.10.2 255.255.255.0
!
ip classless
ip http server
!
!
snmp-server engineID local 8000000903000011BBBE2C81
snmp-server group snmpgroup v3 auth write v1default notify *tv.FFFFFFFF.FFFFFFFF
snmp-server contact CheckThisForSnmpset
snmp-server enable traps snmp authentication warmstart linkdown linkup coldstart
snmp-server host 172.16.10.250 version 3 auth snmpuser
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
```

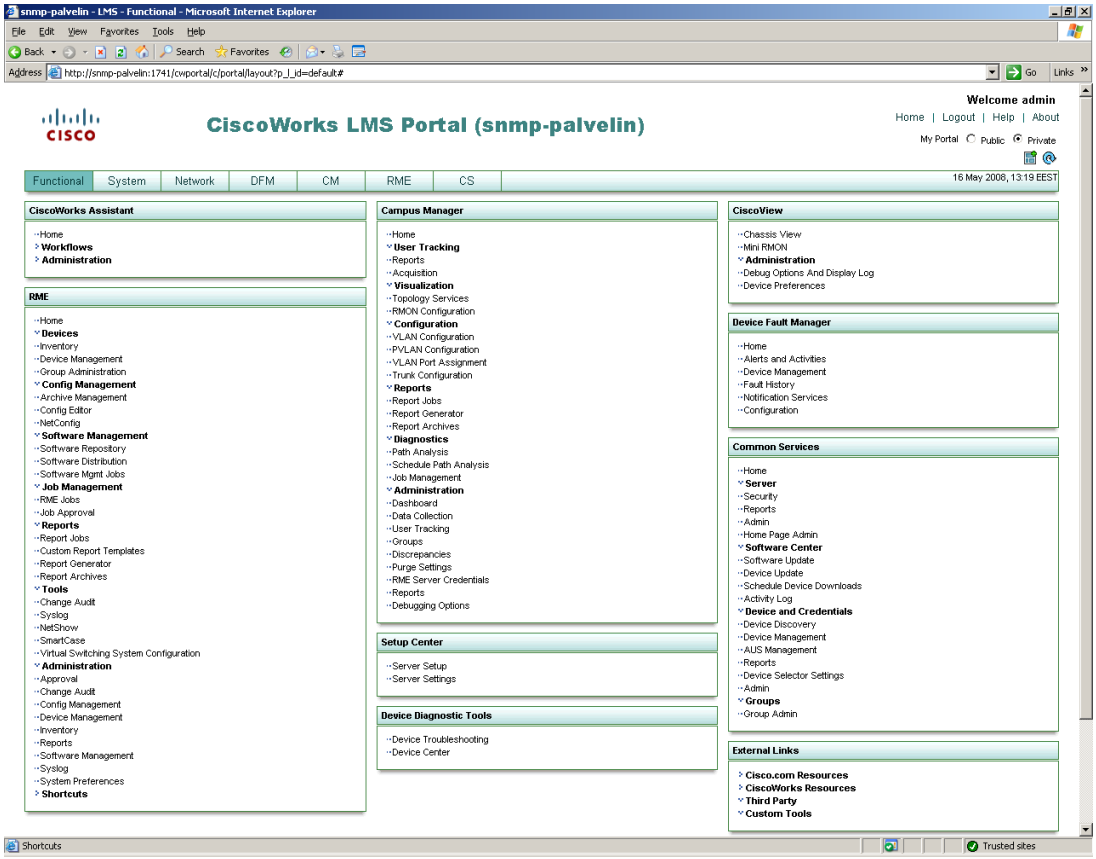
```
line vty 5 15
 login
!
!
monitor session 1 source interface Fa0/1
monitor session 1 destination interface Fa0/9
end

Switch1#sh snmp group
groupname: snmpgroup                  security model:v3 auth
readview :v1default                   writeview: v1default
notifyview: *tv.FFFFFFFF.FFFFFFFF
row status: active

Switch1#sh snmp user
User name: snmpuser
Engine ID: 8000000903000011BBBE2C81
storage-type: nonvolatile
Rowstatus: active
Authentication Protocol: MD5
Group-name: snmpgroup

Switch1#sh snmp engineid
Local SNMP engineID: 8000000903000011BBBE2C81
Remote Engine ID          IP-addr    Port

Switch1#sh snmp host
Notification host: 172.16.10.250        udp-port: 162   type: trap
user: snmpuser  security model: v3 auth
traps: FFFFFFFF.FFFFFFFF
```


snmp-palvelin - LMS - Functional - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://snmp-palvelin:1741/cwportal/c/portal/layout?p_l_id=default#
Go Links
CISCO
CiscoWorks LMS Portal (snmp-palvelin)
Welcome admin
Home | Logout | Help | About
My Portal Public Private
Functional System Network DFM CM RME CS
15 May 2008, 13:19 EEST
CiscoWorks Assistant
Home
Workflows
Administration
RME
Home
Devices
Inventory
Device Management
Group Administration
Config Management
Archive Management
Config Editor
NetConfig
Software Management
Software Repository
Software Distribution
Software Mgmt Jobs
Job Management
RME Jobs
Job Approval
Reports
Report Jobs
Custom Report Templates
Report Generator
Report Archives
Tools
Change Audit
Syslog
NetShow
SmartCase
Virtual Switching System Configuration
Administration
Approval
Change Audit
Config Management
Device Management
Inventory
Reports
Software Management
Syslog
System Preferences
Shortcuts
Campus Manager
Home
User Tracking
Reports
Acquisition
Visualization
Topology Services
RMON Configuration
Configuration
VLAN Configuration
PVLAN Configuration
VLAN Port Assignment
Trunk Configuration
Reports
Report Jobs
Report Generator
Report Archives
Diagnostics
Path Analysis
Schedule Path Analysis
Job Management
Administration
Dashboard
Data Collection
User Tracking
Groups
Discrepancies
Purge Settings
RME Server Credentials
Reports
Debugging Options
Setup Center
Server Setup
Server Settings
Device Diagnostic Tools
Device Troubleshooting
Device Center
CiscoView
Chassis View
Mini RMON
Administration
Debug Options And Display Log
Device Preferences
Device Fault Manager
Home
Alerts and Activities
Device Management
Fault History
Notification Services
Configuration
Common Services
Home
Server
Security
Reports
Admin
Home Page Admin
Software Center
Software Update
Device Update
Schedule Device Downloads
Activity Log
Device and Credentials
Device Discovery
Device Management
AUS Management
Reports
Device Selector Settings
Admin
Groups
Group Admin
External Links
Cisco.com Resources
CiscoWorks Resources
Third Party
Custom Tools
Shortcuts
Trusted sites

Salattu GetRequest -sanoma hallinta-asemalta reitittimelle:

No.	Time	Source	Destination	Protocol	Info
9	6.720553	172.16.10.250	172.16.10.1	SNMP	Encrypted PDU

Frame 9 (404 bytes on wire, 404 bytes captured)
Ethernet II, Src: Dell_8b:91:38 (00:13:72:8b:91:38), Dst: 00:1a:a1:40:d3:b0 (00:1a:a1:40:d3:b0)
Internet Protocol, Src: 172.16.10.250 (172.16.10.250), Dst: 172.16.10.1 (172.16.10.1)
User Datagram Protocol, Src Port: 1050 (1050), Dst Port: snmp (161)
    Source port: 1050 (1050)
    Destination port: snmp (161)
    Length: 370
    Checksum: 0x01cd [correct]
Simple Network Management Protocol
    Version: 3 (3)
    Message Global Header
        Message Global Header Length: 16
        Message ID: 341
        Message Max Size: 1024
        Flags: 0x07
            .... .1.. = Reportable: Set
            .... ..1. = Encrypted: Set
            ....1 = Authenticated: Set
        Message Security Model: USM
    Message Security Parameters
        Message Security Parameters Length: 61
        Authoritative Engine ID: 800000090300001AA140D3B0
            1... .... = Engine ID Conformance: RFC3411 (SNMPv3)
            Engine Enterprise ID: cisco (9)
            Engine ID Format: MAC address (3)

Engine Boots: 5
Engine Time: 1791
User Name: snmpuser
Authentication Parameter: 5A5103844E6A3DC9D3373799
Privacy Parameter: 000000051D40B893
Encrypted PDU (274 bytes)

Salaamaton GetRequest -sanoma hallinta-asemalta reitittimelle:

No. Time Source Destination Protocol Info
10 3.733214 172.16.10.250 172.16.10.1 SNMP GET SNMPv2-SMI::enterprises.9.9.48.1.1.1.6.1 SNMPv2-SMI::enterprises.9.9.48.1.1.1.5.1 SNMPv2-SMI::enterprises.9.2.1.46.0 SNMPv2-SMI::enterprises.9.2.1.66.0 SNMPv2-SMI::enterprises.9.2.1.18.0 SNMPv2-SMI::enterprises.9.2.1.26.0 SNMPv2-SMI::enterprises.9.2.1.34.0 SNMPv2-SMI::enterprises.9.2.1.42.0 SNMPv2-MIB::sysUpTime.0

Frame 10 (308 bytes on wire, 308 bytes captured)
Ethernet II, Src: Dell_8b:91:38 (00:13:72:8b:91:38), Dst: Cisco_18:72:a0 (00:07:0e:18:72:a0)
Internet Protocol, Src: 172.16.10.250 (172.16.10.250), Dst: 172.16.10.1 (172.16.10.1)
User Datagram Protocol, Src Port: 1057 (1057), Dst Port: snmp (161)
Source port: 1057 (1057)
Destination port: snmp (161)
Length: 274
Checksum: 0x519e [correct]
Simple Network Management Protocol
Version: 3 (3)
Message Global Header
Message Global Header Length: 16
Message ID: 613

Message Max Size: 1024
    Flags: 0x05
      .... .1.. = Reportable: Set
      .... ..0. = Encrypted: Not set
      ....1 = Authenticated: Set
    Message Security Model: USM
  Message Security Parameters
    Message Security Parameters Length: 53
    Authoritative Engine ID: 80000009030000070E1872A0
      1... .... = Engine ID Conformance: RFC3411 (SNMPv3)
      Engine Enterprise ID: cisco (9)
      Engine ID Format: MAC address (3)
    Engine Boots: 9
    Engine Time: 9977
    User Name: snmpuser
    Authentication Parameter: 57F3346F8F3B14945D420336
    Privacy Parameter:
  Context Engine ID: 80000009030000070E1872A0
    1... .... = Engine ID Conformance: RFC3411 (SNMPv3)
    Engine Enterprise ID: cisco (9)
    Engine ID Format: MAC address (3)
  Context Name:
  PDU type: GET (0)
  Request Id: 0x00000265
  Error Status: NO ERROR (0)
  Error Index: 0
    Object identifier 1: 1.3.6.1.4.1.9.9.48.1.1.1.6.1 (SNMPv2-SMI::enterprises.9.9.48.1.1.1.6.1)
  Value: NULL

Object identifier 2: 1.3.6.1.4.1.9.9.48.1.1.1.5.1 (SNMPv2-SMI::enterprises.9.9.48.1.1.1.5.1)

Value: NULL

Object identifier 3: 1.3.6.1.4.1.9.2.1.46.0 (SNMPv2-SMI::enterprises.9.2.1.46.0)

Value: NULL

Object identifier 4: 1.3.6.1.4.1.9.2.1.66.0 (SNMPv2-SMI::enterprises.9.2.1.66.0)

Value: NULL

Object identifier 5: 1.3.6.1.4.1.9.2.1.18.0 (SNMPv2-SMI::enterprises.9.2.1.18.0)

Value: NULL

Object identifier 6: 1.3.6.1.4.1.9.2.1.26.0 (SNMPv2-SMI::enterprises.9.2.1.26.0)

Value: NULL

Object identifier 7: 1.3.6.1.4.1.9.2.1.34.0 (SNMPv2-SMI::enterprises.9.2.1.34.0)

Value: NULL

Object identifier 8: 1.3.6.1.4.1.9.2.1.42.0 (SNMPv2-SMI::enterprises.9.2.1.42.0)

Value: NULL

Object identifier 9: 1.3.6.1.2.1.1.3.0 (SNMPv2-MIB::sysUpTime.0)

Value: NULL

Salattu SetRequest -sanoma hallinta-asemalta reitittimelle:

No.	Time	Source	Destination	Protocol	Info
21	4.370374	172.16.10.250	172.16.10.1	SNMP	Encrypted PDU

Frame 21 (207 bytes on wire, 207 bytes captured)
Ethernet II, Src: Dell_8b:91:38 (00:13:72:8b:91:38), Dst: 00:1a:a1:40:d3:b0 (00:1a:a1:40:d3:b0)
Internet Protocol, Src: 172.16.10.250 (172.16.10.250), Dst: 172.16.10.1 (172.16.10.1)
User Datagram Protocol, Src Port: 1050 (1050), Dst Port: snmp (161)
    Source port: 1050 (1050)
    Destination port: snmp (161)
    Length: 173
    Checksum: 0x8a85 [correct]
Simple Network Management Protocol
    Version: 3 (3)
    Message Global Header
        Message Global Header Length: 16
        Message ID: 484
        Message Max Size: 1024
        Flags: 0x07
            .... .1.. = Reportable: Set
            .... ..1. = Encrypted: Set
            ....1 = Authenticated: Set
        Message Security Model: USM
    Message Security Parameters
        Message Security Parameters Length: 61
        Authoritative Engine ID: 800000090300001AA140D3B0
            1... .... = Engine ID Conformance: RFC3411 (SNMPv3)
            Engine Enterprise ID: cisco (9)
            Engine ID Format: MAC address (3)

Engine Boots: 5
Engine Time: 2407
User Name: snmpuser
Authentication Parameter: 1AA253655333F608D9E1E153
Privacy Parameter: 000000051D40B906
Encrypted PDU (77 bytes)

Salaamaton SetRequest -sanoma hallinta-asemalta reitittimelle:

No. Time Source Destination Protocol Info
8 2.831839 172.16.10.250 172.16.10.1 SNMP SET SNMPv2-SMI::enterprises.9.9.46.1.4.2.1.11.1.6 SNMPv2-SMI::enterprises.9.9.46.1.4.2.1.2.1.6 SNMPv2-SMI::enterprises.9.9.46.1.4.2.1.3.1.6 SNMPv2-SMI::enterprises.9.9.46.1.4.2.1.4.1.6 SNMPv2-SMI::enterprises.9.9.46.1.4.2.1.5.1.6 SNMPv2-SMI::enterprises.9.9.46.1.4.2.1.12.1.6 SNMPv2-SMI::enterprises.9.9.46.1.4.2.1.13.1.6

Frame 8 (337 bytes on wire, 337 bytes captured)
Ethernet II, Src: Dell_8b:91:38 (00:13:72:8b:91:38), Dst: Cisco_18:72:a0 (00:07:0e:18:72:a0)
Internet Protocol, Src: 172.16.10.250 (172.16.10.250), Dst: 172.16.10.1 (172.16.10.1)
User Datagram Protocol, Src Port: 1057 (1057), Dst Port: snmp (161)
Source port: 1057 (1057)
Destination port: snmp (161)
Length: 303
Checksum: 0x67b6 [correct]
Simple Network Management Protocol
Version: 3 (3)
Message Global Header
Message Global Header Length: 16
Message ID: 697

Message Max Size: 1024
Flags: 0x05
.... .1.. = Reportable: Set
.... ..0. = Encrypted: Not set
....1 = Authenticated: Set
Message Security Model: USM
Message Security Parameters
Message Security Parameters Length: 53
Authoritative Engine ID: 80000009030000070E1872A0
1... .... = Engine ID Conformance: RFC3411 (SNMPv3)
Engine Enterprise ID: cisco (9)
Engine ID Format: MAC address (3)
Engine Boots: 9
Engine Time: 10316
User Name: snmpuser
Authentication Parameter: AE4AB1EE5057EFADE773659E
Privacy Parameter:
Context Engine ID: 80000009030000070E1872A0
1... .... = Engine ID Conformance: RFC3411 (SNMPv3)
Engine Enterprise ID: cisco (9)
Engine ID Format: MAC address (3)
Context Name:
PDU type: SET (3)
Request Id: 0x000002b9
Error Status: NO ERROR (0)
Error Index: 0
Object identifier 1: 1.3.6.1.4.1.9.9.46.1.4.2.1.11.1.6 (SNMPv2-SMI::enterprises.9.9.46.1.4.2.1.11.1.6)
Value: INTEGER: 4
Object identifier 2: 1.3.6.1.4.1.9.9.46.1.4.2.1.2.1.6 (SNMPv2-SMI::enterprises.9.9.46.1.4.2.1.2.1.6)

Value: INTEGER: 1

Object identifier 3: 1.3.6.1.4.1.9.9.46.1.4.2.1.3.1.6 (SNMPv2-SMI::enterprises.9.9.46.1.4.2.1.3.1.6)

Value: INTEGER: 1

Object identifier 4: 1.3.6.1.4.1.9.9.46.1.4.2.1.4.1.6 (SNMPv2-SMI::enterprises.9.9.46.1.4.2.1.4.1.6)

Value: STRING: "testivlan"

Object identifier 5: 1.3.6.1.4.1.9.9.46.1.4.2.1.5.1.6 (SNMPv2-SMI::enterprises.9.9.46.1.4.2.1.5.1.6)

Value: INTEGER: 1500

Object identifier 6: 1.3.6.1.4.1.9.9.46.1.4.2.1.12.1.6 (SNMPv2-SMI::enterprises.9.9.46.1.4.2.1.12.1.6)

Value: INTEGER: 0

Object identifier 7: 1.3.6.1.4.1.9.9.46.1.4.2.1.13.1.6 (SNMPv2-SMI::enterprises.9.9.46.1.4.2.1.13.1.6)

Value: INTEGER: 0

GetRequest -sanoma hallinta-asemalta kytkimelle:

No. Time Source Destination Protocol Info
12 3.981159 172.16.10.250 172.16.10.2 SNMP GET SNMPv2-MIB::sysDescr.0 SNMPv2-MIB::sysUpTime.0

Frame 12 (188 bytes on wire, 188 bytes captured)
Ethernet II, Src: Dell_8b:91:38 (00:13:72:8b:91:38), Dst: Cisco_9f:a7:00 (00:0b:fd:9f:a7:00)
Internet Protocol, Src: 172.16.10.250 (172.16.10.250), Dst: 172.16.10.2 (172.16.10.2)
User Datagram Protocol, Src Port: 1050 (1050), Dst Port: snmp (161)
    Source port: 1050 (1050)
    Destination port: snmp (161)
    Length: 154
    Checksum: 0x37fb [correct]
Simple Network Management Protocol
    Version: 3 (3)
    Message Global Header
        Message Global Header Length: 16
        Message ID: 662
        Message Max Size: 1024
        Flags: 0x05
            .... .1.. = Reportable: Set
            .... ..0. = Encrypted: Not set
            ....1 = Authenticated: Set
        Message Security Model: USM
    Message Security Parameters
        Message Security Parameters Length: 53
        Authoritative Engine ID: 800000090300000BFD9FA701
            1... .... = Engine ID Conformance: RFC3411 (SNMPv3)
            Engine Enterprise ID: cisco (9)

Engine ID Format: MAC address (3)
    Engine Boots: 3
    Engine Time: 2968
    User Name: snmpuser
    Authentication Parameter: 05D71C401DE059AD51F2727C
    Privacy Parameter:
Context Engine ID: 800000090300000BFD9FA701
    1... .... = Engine ID Conformance: RFC3411 (SNMPv3)
    Engine Enterprise ID: cisco (9)
    Engine ID Format: MAC address (3)
Context Name:
PDU type: GET (0)
Request Id: 0x00000296
Error Status: NO ERROR (0)
Error Index: 0
Object identifier 1: 1.3.6.1.2.1.1.1.0 (SNMPv2-MIB::sysDescr.0)
Value: NULL
Object identifier 2: 1.3.6.1.2.1.1.3.0 (SNMPv2-MIB::sysUpTime.0)
Value: NULL

SetRequest -sanoma hallinta-asemalta kytkimelle:

No. Time Source Destination Protocol Info
12 3.997754 172.16.10.250 172.16.10.2 SNMP SET SNMPv2-SMI::enterprises.9.9.46.1.4.2.1.11.1.6 SNMPv2-SMI::enterprises.9.9.46.1.4.2.1.2.1.6 SNMPv2-SMI::enterprises.9.9.46.1.4.2.1.3.1.6 SNMPv2-SMI::enterprises.9.9.46.1.4.2.1.4.1.6 SNMPv2-SMI::enterprises.9.9.46.1.4.2.1.5.1.6 SNMPv2-SMI::enterprises.9.9.46.1.4.2.1.6.1.6

Frame 12 (316 bytes on wire, 316 bytes captured)
Ethernet II, Src: Dell_8b:91:38 (00:13:72:8b:91:38), Dst: Cisco_9f:a7:00 (00:0b:fd:9f:a7:00)
Internet Protocol, Src: 172.16.10.250 (172.16.10.250), Dst: 172.16.10.2 (172.16.10.2)
User Datagram Protocol, Src Port: 1050 (1050), Dst Port: snmp (161)
    Source port: 1050 (1050)
    Destination port: snmp (161)
    Length: 282
    Checksum: 0xc257 [correct]
Simple Network Management Protocol
    Version: 3 (3)
    Message Global Header
        Message Global Header Length: 16
        Message ID: 1006
        Message Max Size: 1024
        Flags: 0x05
            .... .1.. = Reportable: Set
            .... ..0. = Encrypted: Not set
            ....1 = Authenticated: Set
        Message Security Model: USM
    Message Security Parameters
        Message Security Parameters Length: 53

Authoritative Engine ID: 800000090300000BFD9FA701
1... .... = Engine ID Conformance: RFC3411 (SNMPv3)
Engine Enterprise ID: cisco (9)
Engine ID Format: MAC address (3)
Engine Boots: 3
Engine Time: 3729
User Name: snmpuser
Authentication Parameter: 0DFBA7F06DA139D5C3C0A769
Privacy Parameter:
Context Engine ID: 800000090300000BFD9FA701
1... .... = Engine ID Conformance: RFC3411 (SNMPv3)
Engine Enterprise ID: cisco (9)
Engine ID Format: MAC address (3)
Context Name:
PDU type: SET (3)
Request Id: 0x000003ee
Error Status: NO ERROR (0)
Error Index: 0
Object identifier 1: 1.3.6.1.4.1.9.9.46.1.4.2.1.11.1.6 (SNMPv2-SMI::enterprises.9.9.46.1.4.2.1.11.1.6)
Value: INTEGER: 4
Object identifier 2: 1.3.6.1.4.1.9.9.46.1.4.2.1.2.1.6 (SNMPv2-SMI::enterprises.9.9.46.1.4.2.1.2.1.6)
Value: INTEGER: 1
Object identifier 3: 1.3.6.1.4.1.9.9.46.1.4.2.1.3.1.6 (SNMPv2-SMI::enterprises.9.9.46.1.4.2.1.3.1.6)
Value: INTEGER: 1
Object identifier 4: 1.3.6.1.4.1.9.9.46.1.4.2.1.4.1.6 (SNMPv2-SMI::enterprises.9.9.46.1.4.2.1.4.1.6)
Value: STRING: "testivlan"
Object identifier 5: 1.3.6.1.4.1.9.9.46.1.4.2.1.5.1.6 (SNMPv2-SMI::enterprises.9.9.46.1.4.2.1.5.1.6)

Value: INTEGER: 1500

Object identifier 6: 1.3.6.1.4.1.9.9.46.1.4.2.1.6.1.6 (SNMPv2-SMI::enterprises.9.9.46.1.4.2.1.6.1.6)

Value: Hex-STRING: 00 01 86 A6

Kytkimeltä hallinta-asemalle lähetetty Trap -sanoma:

No. Time Source Destination Protocol Info
1 0.000000 172.16.10.2 172.16.10.250 SNMP TRAP-V2 SNMPv2-MIB::sysUpTime.0 SNMPv2-MIB::snmpTrapOID.0 IF-MIB::ifIndex.2 IF-MIB::ifDescr.2 IF-MIB::ifType.2 SNMPv2-SMI::enterprises.9.2.2.1.1.20.2

Frame 1 (294 bytes on wire, 294 bytes captured)
Ethernet II, Src: Cisco_be:2c:80 (00:11:bb:be:2c:80), Dst: Dell_8b:91:38 (00:13:72:8b:91:38)
Internet Protocol, Src: 172.16.10.2 (172.16.10.2), Dst: 172.16.10.250 (172.16.10.250)
User Datagram Protocol, Src Port: 51786 (51786), Dst Port: snmptrap (162)
    Source port: 51786 (51786)
    Destination port: snmptrap (162)
    Length: 260
    Checksum: 0xcbd4 [correct]
Simple Network Management Protocol
    Version: 3 (3)
    Message Global Header
        Message Global Header Length: 13
        Message ID: 28
        Message Max Size: 1500
        Flags: 0x01
            .... .0.. = Reportable: Not set
            .... ..0. = Encrypted: Not set
            ....1 = Authenticated: Set
        Message Security Model: USM
    Message Security Parameters
        Message Security Parameters Length: 49
        Authoritative Engine ID: 8000009030000011BBBE2C81
            1... .... = Engine ID Conformance: RFC3411 (SNMPv3)

Engine Enterprise ID: cisco (9)

Engine ID Format: MAC address (3)

Engine Boots: 4

Engine Time: 21442

User Name: snmpuser

Authentication Parameter: 79B76EA5D8F863E2C55231C3

Privacy Parameter:

Context Engine ID: 8000000903000011BBBE2C81

1... .... = Engine ID Conformance: RFC3411 (SNMPv3)

Engine Enterprise ID: cisco (9)

Engine ID Format: MAC address (3)

Context Name:

PDU type: TRAP-V2 (7)

Request Id: 0x00000002

Error Status: NO ERROR (0)

Error Index: 0

Object identifier 1: 1.3.6.1.2.1.1.3.0 (SNMPv2-MIB::sysUpTime.0)

Value: Wrong Type (should be Timeticks): INTEGER: 2144259

Object identifier 2: 1.3.6.1.6.3.1.1.4.1.0 (SNMPv2-MIB::snmpTrapOID.0)

Value: OID: IF-MIB::linkDown

Object identifier 3: 1.3.6.1.2.1.2.2.1.1.2 (IF-MIB::ifIndex.2)

Value: INTEGER: 2

Object identifier 4: 1.3.6.1.2.1.2.2.1.2.2 (IF-MIB::ifDescr.2)

Value: STRING: FastEthernet0/2

Object identifier 5: 1.3.6.1.2.1.2.2.1.3.2 (IF-MIB::ifType.2)

Value: INTEGER: ethernetCsmacd(6)

Object identifier 6: 1.3.6.1.4.1.9.2.2.1.1.20.2 (SNMPv2-SMI::enterprises.9.2.2.1.1.20.2)

Value: STRING: "administratively down"

Reitittimeltä hallinta-asemalle lähetetty Trap -sanoma:

No.	Time	Source	Destination	Protocol	Info
1	0.000000	172.16.10.1	172.16.10.250	SNMP	Encrypted PDU

Frame 1 (264 bytes on wire, 264 bytes captured)
Ethernet II, Src: Cisco_18:72:a0 (00:07:0e:18:72:a0), Dst: Dell_8b:91:38 (00:13:72:8b:91:38)
Internet Protocol, Src: 172.16.10.1 (172.16.10.1), Dst: 172.16.10.250 (172.16.10.250)
User Datagram Protocol, Src Port: 57491 (57491), Dst Port: snmptrap (162)
    Source port: 57491 (57491)
    Destination port: snmptrap (162)
    Length: 230
    Checksum: 0x3e93 [correct]
Simple Network Management Protocol
    Version: 3 (3)
    Message Global Header
        Message Global Header Length: 13
        Message ID: 75
        Message Max Size: 1500
        Flags: 0x03
            .... .0.. = Reportable: Not set
            .... ..1. = Encrypted: Set
            ....1 = Authenticated: Set
        Message Security Model: USM
    Message Security Parameters
        Message Security Parameters Length: 57
        Authoritative Engine ID: 80000009030000070E1872A0
            1... .... = Engine ID Conformance: RFC3411 (SNMPv3)
            Engine Enterprise ID: cisco (9)
            Engine ID Format: MAC address (3)

Engine Boots: 8

Engine Time: 19540

User Name: snmpuser

Authentication Parameter: 34FF77B69918B1F35C91A227

Privacy Parameter: E2279E7EAF20CFAE

Encrypted PDU (142 bytes)

LYHENTEET

3DES	Triple-Data Encryption Standard
AES	Advanced Encryption Standard
ASN.1	Abstract Syntax Notation One
CLI	Command Line Interface
DES	Data Encryption Standard
HMAC	Hash-based Message Authentication Code
IETF	Internet Engineering Task Force
IP	Internet Protocol
MD5	Message-Digest 5
MIB	Management Information Base
NMA	Network Management Agent
NMS	Network Management Station
OSI	Open Systems Interconnection
PDU	Protocol Data Unit
PoE	Power over Ethernet
RFC	Request for Comments
SHA	Secure Hash Algorithm
SMI	Structure of Management Information
SNMP	Simple Network Management Protocol
TCP	Transport Control Protocol
UDP	User Datagram Protocol
USM	User-based Security Model