KYMENLAAKSON AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma / Tietoverkkotekniikka

Ville Leppänen
Tomi Tähti

VERKONHALLINTAOHJELMISTO SUORITUSKYVYN VALVONTAA VARTEN

Opinnäytetyö 2013

TIIVISTELMÄ

KYMENLAAKSON AMMATTIKORKEAKOULU
Tietotekniikka

LEPPÄNEN, VILLE
TÄHTI, TOMI

Verkonhallintaohjelmisto suorituskyvyn valvontaa varten
Opinnäytetyö — 60 sivua + 4 liitesivua
Työn ohjaaja — Yliopettaja Martti Kettunen
Toimeksiantaja — Nuuka Solutions
Maaliskuu 2013
Avainsanat — Verkonvalvonta, SNMP, Nagios, verkonhallinta, IP SLA

Opinnäytetyön aiheena oli asentaa ja määritellä avoimen lähdekoodin Nagios-verkonvalvontaohjelmisto. Nagioksen avulla oli tarkoitus valvoa Nuuka Solutionsin verkossa olevia 3G-reitittimiä, niiden resursseja ja yhteyksien suorituskykyä. Nagiokseen oli tavoitteena määrittää valvottavat kohteet sekä palvelut, joille annettiin raja-arvot ongelmatilanteiden tunnistamista varten. Jos raja-arvot saavutettaisiin, Nagios täytyi saada lähettämään sähköpostilla hälytysviesti. Käytännön osuuden lisäksi oli tarkoitus selvittää laajasti aiheeseen liittyvää teoriaa.

Opinnäytetyötä varten saatiin VPN-tunnukset, joiden avulla avattiin yhteys opinnäytetyön kohteena olevaan verkkoon. VPN-yhteyden kautta päästiin määrittelemään Linux-konetta ja sinne asennettiin VNC-palvelin sekä graafinen työpöytäkäyttöliittymä, jotta työpöytänäkymä saatiin etähallintaan. Nagioksen normaali asennus suoritettiin hyödyntämällä virallista asennusohjetta ja dokumentaatiota. Asennuksen jälkeen tarvitut määritykset sekä lisäosien asennukset tehtiin omatoimisesti. Palomuurin sääntöihin sallittiin HTTP-liikenne, jotta saatiin Nagioksen Web-käyttöliittymä näkymään suoraan verkkoselaimen kautta VPN-yhteyden ollessa avoinna.

Työ eteni suunnitelman mukaan aina Nagios-verkonvalvontaohjelmiston määrityksiin ja lisäosien asennukseen asti. Valitettavasti aikataulun kireyden ja ulkoisten syiden tähden kohteena oleviin valvottaviin laitteisiin ei saatu yhteyttä, joten varsinaiset testitulokset jäivät saamatta. Paikallisten testien perusteella kaiken pitäisi kuitenkin toimia halutulla tavalla, jos yhteydet valvottaviin laitteisiin saataisiin toimimaan.

ABSTRACT

KYMENLAAKSON AMMATTIKORKEAKOULU
University of Applied Sciences
Information technology

LEPPÄNEN, VILLE
TÄHTI, TOMI

Network management system for monitoring performance
Bachelor's Thesis
60 pages + 4 pages of appendices
Supervisor
Martti Kettunen, Principal Lecturer
Commissioned by
Nuuka Solutions
March 2013
Keywords
Network monitoring, SNMP, Nagios,
network management, IP SLA

The subject of the study was to install and configure an open source network monitoring program called Nagios. The goal was to monitor the resources of two Cisco routers in the network of Nuuka Solutions with Nagios. In addition, another goal was to monitor the performance of Nuuka Solutions' network by using IP SLA. The service and hosts needed to be defined in order to monitor them successfully. The thresholds also needed to be configured for detecting issues and problems. When these issues or problems were detected, Nagios needed to be set to send automatic notification emails. The final goal was to include extensive theory.

VPN-credentials were given for the thesis to establish a connection into the network that was supposed to be monitored. The configuration of the Linux-system and Nagios was done through the VPN-connection. A VNC-server and a graphical user interface were installed to get a remote connection with the desktop view. Nagios was installed by following the official guidelines and documentation. The required configurations and plug-ins were added and defined manually after the installation. To allow access to the web-interface of Nagios through a normal web-browser, the HTTP-traffic was allowed in the firewall configuration.

The work went on as planned to a point where the plug-ins were installed and the configurations were made. Regrettably because of a tight schedule and various obstacles, no test results were obtained as the devices that were supposed to be monitored were not provided.

SISÄLLYS

KÄSITTEET

Cisco IOS	Internetwork Operating System *on Ciscon verkkolaitteiden käyttöjärjestelmä*
CGI	Computer-Generated Imagery *on tietokonegrafiikan sovellus, jolla luodaan tai rikastutetaan kuvia esimerkiksi videopeleissä tai elokuvissa*
DHCP	Dynamic Host Configuration Protocol *on verkkoprotokolla, joka jakaa IP-osoitteita automaattisesti lähiverkon laitteille*
DLSw+	Data-Link Switching *on Ciscon paranneltu versio DLSw-tunnelointiprotokollasta, joka mahdollistaa muiden kuin IP-pohjaisten protokollien tunneloinnin IP-protokollan päällä*
DNS	Domain Name System *eli hierarkisesti toimiva nimipalvelinjärjestelmä tietokoneille, palveluille ja muille verkkoresursseille, joka IP-osoitteet verkkonimiksi ja toisin päin*
Ethernet	*Yleisesti käytetty pakettikytkentäinen lähiverkkotekniikka (IEEE 802.3)*
FTP	File Transfer Protocol *eli tiedonsiirtoprotokolla, jota käytetään ohjelmistotiedostojen ja datan siirtämiseen tietoverkossa*
Full-Duplex	FDX, s*allii kommunikaation molempiin suuntiin samanaikaisesti*
HTTP	Hypertext Transfer Protocol *eli WWW-liikenteessä käytetty tiedonsiirtoprotokolla*
ICMP	Internet Control Message Protocol *on kontrolliprotokolla, jolla lähetetään viestejä koneesta toiseen*
IP	Internet Protocol, *toimittaa pakettikytkentäisessä internet-verkossa tietoliikennepaketit perille kohteisiinsa*
IP SLA	Internet Protocol Service Level Agreement *on Ciscon kehittämä tietoverkkojen suorituskyvyn monitorointiohjelmisto*

MAC Media Access Control *on siirtokerroksen protokolla*

MD5 Message-Digest algorithm 5 *on laajasti käytetty kryptografinen tarkistusfunktio 128-bittisellä tarkistusarvolla*

MIB Management Information Base, *Joukko muuttujia (tietokanta), joita SNMP-agentin sisältävä järjestelmä ylläpitää. Verkonhallitsijat voivat hakea näiden muuttujien arvot ja muuttaa niitä*

MOS Mean Opinion Score *on menetelmä, jolla mitataan VoIP:n laatua*

NMS Network Management System *on fyysisten laitteiden ja ohjelmistojen yhdistelmä, jota käytetään tietokone- tai tietoverkkojen monitorointiin ja hallintaan*

OID ObjectID *on objektitunnus, jonka avulla viitataan haluttuihin MIB:hin*

OSI Open Systems Interconnection Reference Model, *ISO:n seitsemän kerroksinen malli*

RMON Remote Network Monitoring *eli IP-verkkojen suorituskyvyn mittausprotokolla*

RRD Round-Robin Database *on erityinen varastointijärjestelmä, joka sallii suuren tiedon määrän tallentamisen aikajaksolta*

RTTMON Round Trip Time Monitoring *on Ciscon MIB:iin liittyvä objektiryhmä, joka sisältää verkon monitorointiin käytetyt objektit*

SNA Systems Network Architecture *on täydellinen protokollapino tietokoneiden ja niiden resurssien yhdistämiseen*

SNMP Simple Network Management Protocol, *verkonhallinnassa ja valvonnassa käytettävä protokolla*

TCP Transmission Control Protocol *on protokolla, joka kuljettaa dataa verkkolaitteelta toiselle*

Timestamp	Aikaleima *merkitään laitteen toimesta pakettiin sen saapuessa ja lähtiessä*
Trap	*Ilmoitus tai hälytys verkon aktiivisten osien kuten reitittimien tai siltojen välillä, kun havaitaan ennalta määritetyn tapahtumaraja-arvon ylitys*
UDP	User Datagram Protocol *on yhteydetön protokolla, joka mahdollistaa tiedostojen siirron ilman laitteiden välistä yhteyttä*
VoIP	Voice over Internet Protocol *tarkoittaa puheluiden muodostamista IP-protokollan avulla*
VPN	Virtual Private Network *on tapa jolla voidaan muodostaa julkisen verkon yli näennäisesti yksi yksityinen verkko*

JOHDANTO

Nykypäivänä yhä useammat yritykset tarjoavat tai ylläpitävät palveluita verkossa. Varsinkin suuremmissa yrityksissä verkkotopologiat sekä laitemäärät voivat kasvaa suuriksi ja monimutkaisiksi, minkä vuoksi keskitetty verkonvalvonta ja -hallinta ovat erittäin tärkeitä osa-alueita verkon toimivuuden ja ylläpidon kannalta.

Opinnäytetyö jakautui alun perin Nagios-verkonvalvontaan sekä verkon suorituskyvyn monitorointiin IP SLA:n avulla. Työn edistyessä opinnäytetyöaiheet päätettiin yhdistää opinnäytetöiden aihealueiden päällekkäisyyksien vuoksi.

Nuuka Solutions hyödyntää toiminnassaan 3G-yhteyksiä, joiden toiminnan valvominen on erittäin olennainen osa toimivaa verkkoa. Tämän vuoksi opinnäytetyön tarkoituksena on saada avoimen lähdekoodin Nagios-verkonvalvontaohjelmisto monitoroimaan laiteresursseja sekä IP SLA:n avulla 3G-yhteyksien tilaa ja suorituskykyä.

Opinnäytetyön tavoitteena on saada verkonvalvonta toimintakuntoon siten, että sen avulla voidaan monitoroida perustason palveluita, laiteresursseja sekä yhteyksien toimivuutta. Tällä tavoin saadaan myös rakennettua vankka perusta verkonvalvonnan laajentamiselle ja kehittämiselle.

1 VERKONHALLINTA

Verkonhallinnan osa-alueisiin kuuluu vikatilanteiden, käytön, kokoonpanon, suorituskyvyn sekä turvallisuuden hallinta. Näiden lisäksi löytyy myös muita painopisteitä, kuten dokumentointi ja raportointi.

1.1 Yleistä verkonhallinnasta

Nykyään verkon palvelevuuden merkitys on kasvanut erittäin suureksi ja tärkeää käyttäjille on verkon hallittavuus mahdollisimman hyvin ja kohtuullisilla kustannuksilla. Hallinnan painopisteiden perustuminen useimmiten kokemuksien kautta saatuihin havaintoihin ja niiden perusteella tehtyihin painopisteiden säätöihin, verkonhallinta voi olla monimutkainen ratkaistava. Mahdollinen käytäntöjenhallinta luo erityisiä haasteita verkonhallinnan kannalta. (Jaakohuhta 2005, 309)

Verkon haltijan tehtäviin kuuluu palvelinten ja niiden asiakkaiden välisten yhteyksien ylläpitäminen, siirtokapasiteetin riittävyydestä huolehtiminen sekä yhteyksien luotettavuuden ja turvallisuuden varmistaminen. Tähän tehtävään vaaditaan kyky havaita kaapelointijärjestelmien, aktiivilaitteiden sekä tietokoneiden liityntälaitteiden vikatilanteet. Keskisuurissa ja suurissa organisaatioissa niiden havaitseminen edellyttää keskitettyyn hallintaan siirtymistä. SNMP-protokollaan perustuvat verkonhallintaohjelmat yhdessä Telnet- tai www-pohjaisten laitteiston laitehallintaohjelmien kanssa ovat yleisimpiä hallinnassa käytettyjä työkaluja. (Hakala ja Vainio 2005, 322)

1.2 Verkonhallinnan osa-alueet

ITU-T:n verkonhallintastandardi X.700 määrittelee verkonhallinnan yleisiksi osa-alueiksi seuraavat:

- Vikatilanteiden hallinta (Fault Management), joka kattaa vikojen havaitsemisen, eristämisen ja epätavallisten sekä poikkeavien operaatioiden korjaaminen OSI-ympäristössä. Vikojen seurauksena avoimet järjestelmät epäonnistuvat saavuttamaan toiminnalliset päämääränsä. Viat voivat olla pysyviä tai ohimeneviä. Viat tulevat esille erinäisinä tapahtumina, kuten esimerkiksi virheinä tai virheilmoituksina avoimen järjestelmän operaatiossa. Virheiden havaitseminen

mahdollistaa vikojen tunnistamisen. Vikatilanteiden hallinta sisältää funktioita ja toimintatapoja

- ylläpitämään ja tutkimaan virhelokeja
- hyväksymään ja toimimaan virhehavaintojen tai -ilmoitusten ilmaantuessa
- jäljittämään ja tunnistamaan vikoja
- suorittamaan diagnostiikkatestien sarjoja ja
- korjaamaan vikoja. (ITU-T, standardi X.700)

- Käytön hallinta (Accounting Management), joka mahdollistaa OSI-ympäristön resurssien käytön hallinnan sekä kulutuksen. Käytön hallinta sisältää funktioita ja toimintatapoja
  - tiedottamaan käyttäjää resurssien kulutuksesta
  - mahdollistamaan rajoituksien asettamisen ja tariffiaikataulujen liittämisen resursseihin ja
  - mahdollistamaan kulutuksien yhdistämisen, jossa useisiin resursseihin vedotaan annetun kommunikaatiopäämäärän saavuttamiseksi. (ITU-T, standardi X.700)

- Kokoonpanon hallinta (Configuration Management), joka tunnistaa, omaa määräysvaltaa ja kerää sekä toimittaa dataa avoimille järjestelmille yhteenliitettyjen palveluiden valmistelemisen, alustamisen, käynnistämisen, sulkemisen sekä jatkuvan toiminnan varmistamisen vuoksi. Kokoonpanon hallinta sisältää funktioita ja toimintatapoja
  - avoimen järjestelmän rutiinioperaatioiden suoritusparametrien asettamiselle
  - nimen liittämiselle hallinnoiduille objekteille ja objektiryhmille

- hallinnoitujen objektien alustamiselle ja sulkemiselle
- informaation keräämiselle avoimen järjestelmän nykyisestä tilasta
- avoimen järjestelmän merkittävien tilan muutoksien ilmoittamiselle ja
- avoimen järjestelmän kokoonpanon muuttamiselle. (ITU-T, standardi X.700)

- Suorituskyvyn hallinta (Performance Management), joka sallii resurssien käyttäytymisen OSI-ympäristössä sekä kommunikaatioaktiviteettien tehokkuuden arvioimisen. Suorituskyvyn hallinta sisältää funktioita ja toimintatapoja
  - tilastollisen tiedon keräämiseen
  - järjestelmän tilahistorian lokien ylläpitämiseen ja tutkimiseen
  - järjestelmän suorituskyvyn päättelemiseen keinotekoisissa sekä luonnollisissa tiloissa ja
  - järjestelmän operaatioiden toimintatilojen muuttamiseen. (ITU-T, standardi X.700)
- Turvallisuuden hallinta (Security Management), jonka tarkoituksena on tukea tietoturvakäytäntöjä käyttämällä funktioita ja toimintatapoja, joihin kuuluu
  - tietoturvapalveluiden ja -mekanismien luonti, poisto sekä hallinta
  - tietoturvan kannalta tärkeän informaation jakaminen ja
  - tietoturvan kannalta tärkeiden tapahtumien reportointi. (ITU-T, standardi X.700)

1.3 Verkonhallinnan muut painopisteet

Verkonhallinnan osa-alueiden lisäksi painopisteinä ovat dokumentointi, raportointi, politiikan hallinta, huolto, ylläpidon hallinta sekä palveluiden hallinta. Edellämainittujen lisäksi voidaan mukaan ottaa myös teknologisen kehityksen hallinta. (Jaakohuhta 2005, 311)

Dokumentointi (documentation) on välttämätöntä kaikelle hallinnalle. Varsinkin suuremmissa verkoissa on ilman dokumentointia erittäin vaikeaa, ellei jopa mahdotonta, saada selville mitä kuuluu hallinnan piiriin ja miltä verkon looginen sekä fyysinen rakenne näyttää. (Jaakohuhta 2005, 311)

Raportointi (report) on merkittävässä roolissa, kun halutaan saada tietoa verkon tilasta, tapahtumista ja niiden kehityksestä verkossa. Raportoinnin tarkoituksena on muodostaa yhteenvetotietoa erinäisistä tapahtumista, vikatilanteista, laitteista ja kapasiteetin käytöstä. (Jaakohuhta 2005, 311)

Käytäntöjen hallinta (policy management) varmistaa verkkokapasiteetin saatavuuden organisaation toiminnan kannalta tärkeille sovelluksille. Organisaatio itse päättää etuoikeutetun aseman ansaitsevat sovellukset. (Jaakohuhta 2005, 311)

Ylläpidon hallinnalla (maintenance management) tarkoitetaan kaikkia niitä menettelyitä, joiden avulla verkon keskeisten komponenttien jatkuva toimintavarmuus ja käytettävyys voidaan taata. Esimerkkinä ovat päivystys ja palvelusopimukset. Ylläpidon hallinnan piiriin kuuluu myös viallisten komponenttien korvaaminen siten, että samalla taloudellisten menetysten riski pyritään pitämään vähäisenä. Esimerkkinä ovat varalaitteet ja varaosat. (Jaakohuhta 2005, 311)

Palveluiden hallinnalla (services management) pyritään palveluiden käytettävyyden ja luotettavan ympäristön varmistamiseen. Luotettavalla ympäristöllä tarkoitetaan sitä, että palveluun oikeutetuille käyttäjille taataan palveluiden saatavuus myös järjestelmän vikaantumisenkin sattuessa. (Jaakohuhta 2005, 311)

Teknologisen kehityksen hallinta (migration management) huolehtii verkon rakennusvaiheen kasvavien vaatimusten asettamien kehitystarpeiden huomioonottamisen. Jos jokainen teknologinen uudistus verkossa aiheuttaisi suunnittelemattomia uusintainves-

tointeja, se tulisi olemaan organisaation kannalta erittäin kallista. (Jaakohuhta 2005, 311)

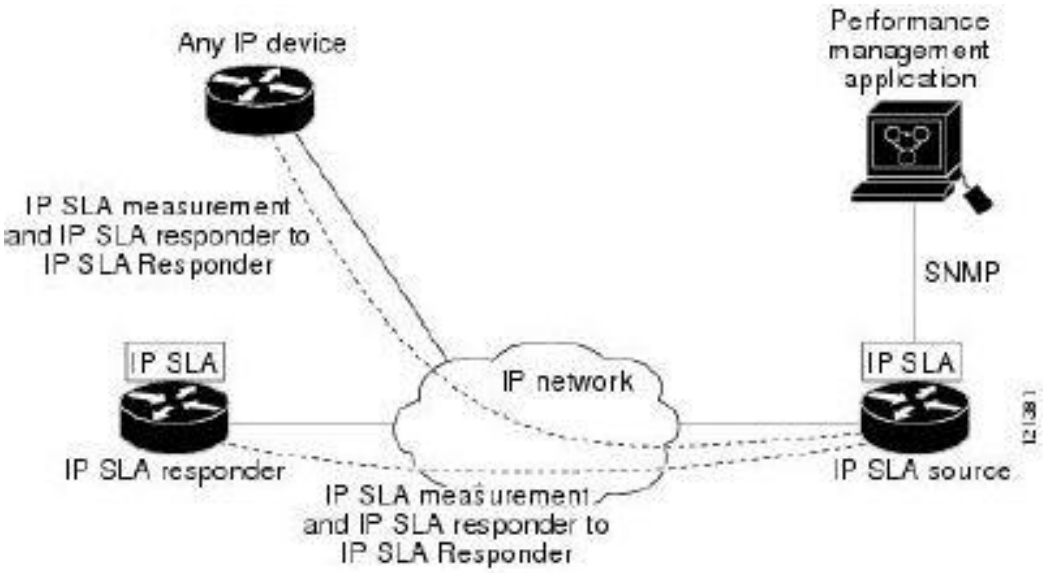
2 IP SLA -TEKNIIKKA

IP SLA on suorituskyvyn monitorointiin tarkoitettu ohjelmisto, mikä löytyy lähes kaikista Ciscon IOS -pohjaisista reitittimistä ja kytkimistä. IP SLA hyödyntää aktiivista liikenteen monitorointia luomalla ja analysoimalla liikennettä mitatakseen suorituskykyä, joko Ciscon laitteiden välillä tai Ciscon laitteesta johonkin IP-protokollaa käyttävään laitteeseen. (IP SLAs Configuration Guide, 2)

Mitattua tietoa voidaan käyttää hyväksi esimerkiksi vianhaussa. IP SLA -operaatioilla voidaan mitata lähes kaikkia suorituskykyparametreja sekä yhdensuuntaisia että edestakaisia. Niillä voidaan mitata myös verkkopalveluiden saatavuutta ja palvelimien vasteaikoja. (IP SLAs Configuration Guide, 2)

2.1 IP SLA -operaation toimintamalli

Alapuolella olevassa kuvassa on esitetty IP SLA -operaatio. IP SLA -laite lähettää paketin kohdelaitteelle. Kohdelaitteen vastaanotettua paketin se lähettää takaisin lähdelaitteelle aikaleimatiedon, mistä voidaan laskea suorituskykyparametrien arvot riippuen mittausoperaatiosta. (IP SLAs Configuration Guide, 4)



Kuva 1 IP SLA operaatio (IP SLAs Configuration Guide, 4)

Verkon suorituskyvyn mittaamiseksi IP SLA:lla täytyy tehdä seuraavat vaiheet:

- Käynnistetään IP SLA Responder -palvelu kohdelaitteeseen, jos mittausoperaatio sitä vaatii.
- Määritetään haluttu mittausoperaatio.
- Määritetään mittausoperaatiolle halutut asetukset.
- Määritetään raja-arvot, jos niitä halutaan käyttää.
- Jaksotetaan mittausoperaatio tai ryhmä mittausoperaatioita tekemään mittaukset halutuin aikavälein.
- Tarkastetaan mittaustulokset Ciscon laitteen komentoriviltä tai keräämällä tiedot laitteen MIB:eistä SNMP-protokollaa hyödyntävän verkonvalvontasovelluksen avulla. (IP SLAs Configuration Guide, 5)

2.2 IP SLA Responder

IP SLA Responder -palvelu löytyy Ciscon reitinlaitteista, minkä avulla voidaan ennakoida ja vastata IP SLA -kyselypaketteihin. Sekä lähde- että kohdelaitteena on oltava Ciscon laite, kun mittauksessa on IP SLA Responder -palvelu päällä. Palvelu mahdollistaa tarkat mittaukset Timestamp-viestien avulla. Näiden viestien avulla voidaan mitata yhdensuuntaista pakettien hävikkiä, latenssia ja pakettien välistä viiveen vaihtelua. (Cisco IOS IP Service Level Agreements User Guide, 14)

Palvelu tarjoaa suuren edun ICMP-pohjaisissa mittauksissa, koska lisästatistiikkaa ei ole saatavilla ICMP-ympäristössä. Palvelu käyttää myös patentoitua IP SLA Control -protokollaa (ohjausprotokolla), joka mahdollistaa sen, että Responder-palvelu kuuntelee tiettyä porttia ja kykenee vastaamaan kyselyyn. (IP SLAs Configuration Guide, 5)

IP SLA Responder kuuntelee tiettyä porttia IP SLA -mittausoperaation lähettämien ohjausprotokollaviestien varalta. Vastaanotettuaan kyseisen viestin Responder käynnistää ja ottaa käyttöön tietyn UDP tai TCP -portin tietyksi ajaksi. Tänä aikana Responder hyväksyy pyynnöt ja vastaa niihin. Responder sulkee kyseisen portin vastattuaan IP SLA -pakettiin tai kun määritetty aika loppuu. Tietoturvan lisäämiseksi ohjausviesteihin voidaan ottaa käyttöön MD5 -autentikointi.(IP SLAs Configuration Guide, 5)

Kaikki IP SLA -mittausoperaatiot eivät vaadi Responder-palvelun käynnistämistä kohdelaitteeseen. Mikäli kohdelaitteessa on mittaukseen valittu palvelu, kuten HTTP tai Telnet valmiiksi käynnissä, niin Responder-palvelua ei tarvita. Koska Responder tukee vain Ciscon laitteita, niin muihin laitteisiin tehdyissä IP SLA -mittausoperaatioissa voidaan käyttää vain niille natiiveja palveluita ja protokollia.(IP SLAs Configuration Guide, 6)

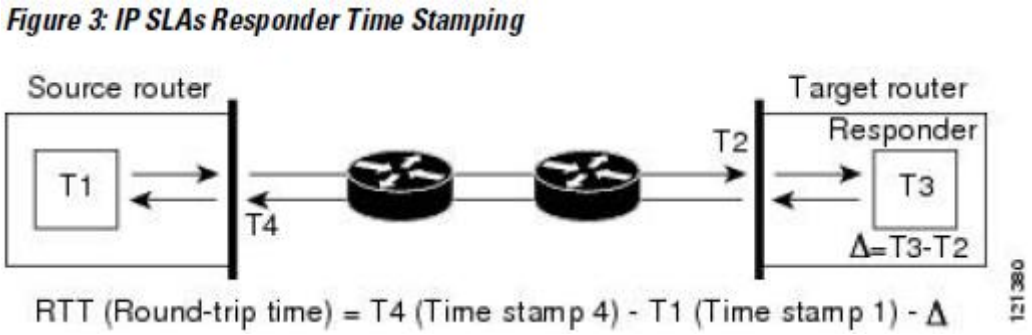
2.2.1 IP SLA:n vastausajan laskeminen

Reitittimellä voi kestää kymmeniä millisekunteja prosessoida saapuvia paketteja muista korkean prioriteetin prosesseista johtuen. Tämä viive vaikuttaa vasteaikoihin, koska vastaus testipaketteihin voi joutua odottamaan prosessoimista. Tässä tapauksessa vasteajat eivät kuvaa tarkasti verkon viiveitä. Mikäli Responder-palvelu on käytössä, niin IP SLA minimoi prosessointiviiveet lähde- sekä kohdereitittimessä mitatakseen aidot

edestakaiset viiveajat. IP SLA:n testipaketit käyttävät aikaleimoja minimoidakseen prosessointiviiveitä. (IP SLAs Configuration Guide, 6)

IP SLA Responder -palvelun ollessa käytössä prosessointiaika saadaan eliminoitua antamalla kohdelaitteelle lupa liittää aikaleimat pakettiin sen saapuessa ja lähtiessä laitteesta. Kun verkossa on paljon liikennettä, niin ICMP ping-testi näyttää usein pitkän ja epätarkan vasteajan kun taas IP SLA:n testi näyttää tarkan vasteajan johtuen Responder-palvelun aikaleimaoperaatiosta. (IP SLAs Configuration Guide, 6)

Alla oleva kuva esittää Responder-palvelun toimintaa. Edestakaisen viiveen laskemiseksi otetaan neljä aikaleimaa. Kohdereitittimessä, jossa on Responder-palvelu käynnissä, aikaleima 2 (TS2) vähennetään aikaleima 3:sta (TS3), jotta saadaan laskettua testipaketin prosessointiaika, joka esitetään kuvassa deltana. Tämä delta-arvo vähennetään edestakaisesta kokonaisviiveestä. Vastaavanlainen operaatio tehdään myös lähdereitittimessä. (IP SLAs Configuration Guide, 6)



Kuva 2. Prosessointiajan eliminointi kohdelaitteessa tehtävän Responder-operaation avulla. (IP SLAs Configuration Guide, 6)

Kahden aikaleiman lisähyötynä voidaan myös jäljittää yksisuuntaista viivettä, yksisuuntaista pakettien välistä viivettä sekä yksisuuntaista pakettihävikkiä. Nämä tiedot ovat erittäin tärkeitä, koska suuri osa verkon käyttäytymisestä on asynkronista. Mikäli halutaan tehdä yksisuuntaisia mittauksia, niin NTP-yhteyskäytäntö pitää olla määritettynä sekä lähde- että kohdereitittimessä, koska molemmat laitteet tarvitsevat täsmälleen synkronoidun kellonajan. (IP SLAs Configuration Guide, 6)

2.3 Mittausoperaatiot

Seuraavassa esitellään mittausoperaatiota, joita Ciscon laiteilla voidaan suorittaa. UDP-mittausoperaatiot käsitellään omana lukuna, koska kaikki operaatiot käyttävät mittauksissa UDP-protokollaa. Myös ICMP-mittausoperaatiot käsitellään omana lukunaan. HTTP, TCP Connect, FTP, DHCP, DNS sekä DLSw+ käsitellään samassa luvussa, sillä ne ovat alemman tason mittausoperaatioita.

2.3.1 UDP-mittausoperaatiot

UDP Jitter -operaatio kehitettiin alun perin määrittämään verkon soveltuvuutta reaaliaikaisille sovelluksille. Se toimii luomalla synteettistä UDP-liikennettä. Esimerkiksi paketteja lähetetään peräkkäin lähdelaitteelta kohdelaitteelle 10ms välein. Jos verkko toimii ihanteellisesti kohdelaite vastaanottaa paketit samoin väliajoin, jolloin viiveen vaihtelun arvo on nolla. Paketit voivat kuitenkin saapua eri väliajoin kuin ne oli lähetetty. Tästä syntyy pakettien välistä viiveen vaihtelua eli jitteriä. (IP SLAs Configuration Guide, 12)

UDP Jitter -operaatiolla voidaan mitata monia muitakin suorituskykyyn liittyviä parametreja, kuten meno- ja paluureittien yksisuuntaista pakettien välistä viiveen vaihtelua, pakettien hävikkiä, viivettä ja koko reitin edestakaista viivettä. (IP SLAs Configuration Guide, 12)

UDP Jitter -operaation määrityksessä käyttäjä valitsee lähetettävien UDP-pakettien määrän, pakettien koon, kuinka tiheällä aikavälillä lähetetään ja kuinka usein kyseinen operaatio suoritetaan. Oletuksena lähetetään kymmenen pakettia, joiden koko on kymmenen tavua, pakettien välinen viive on kymmenen millisekuntia ja tämä operaatio toistetaan 60 sekunnin välein. (IP SLAs Configuration Guide, 12)

UDP Jitter for VoIP -operaatio toimii muuten samalla periaatteella kuin UDP Jitter -operaatio, mutta siihen on lisätty valmiuksia palauttamaan MOS (Mean Opinion Score) ja ICPIF (Calculated Planning Impairment Factor) tuloksia, jotka kuvaavat VoIP-liikenteen laatua. UDP Jitter for VoIP -operaation määrityksessä käyttäjä valitsee käytettävän koodekin, jotta MOS ja ICPIF tulokset saadaan kerättyä. Lähetettävien UDP-pakettien määrän (n), pakettien koon (s), kuinka tiheällä aikavälillä lähetetään (t) ja kuinka usein kyseinen operaatio suoritetaan (f) määräytyvät käytettävästä koodekista.

Käyttäjällä on kuitenkin mahdollisuus muuttaa kyseisiä arvoja, jos on tarvetta. Alla olevasta kuvasta näkee koodekkikohtaiset oletusparametriarvot. (IP SLAs Configuration Guide, 28)

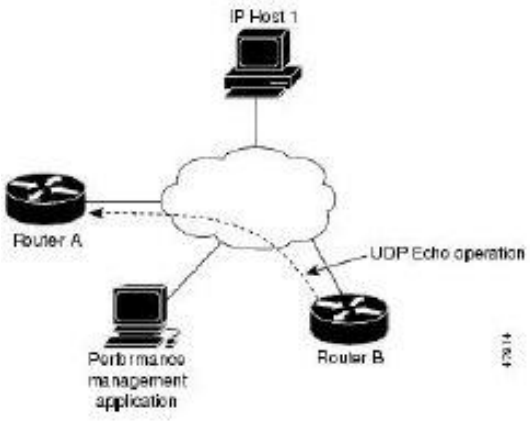
Table 5: Default VoIP UDP Jitter Operation Parameters by Codec

Codec	Default Request Size (Packet Payload) (s)	Default Interval Between Packets (t)	Default Number of Packets (n)	Frequency of Probe Operations (f)
G.711 mu-Law (g711ulaw)	160 + 12 RTP bytes	20 ms	1000	Once every 1 minute
G.711 A-Law (g711alaw)	160 + 12 RTP bytes	20 ms	1000	Once every 1 minute
G.729A (g729a)	20 + 12 RTP bytes	20 ms	1000	Once every 1 minute

Kuva 3. Koodekkien oletusparametrit. (IP SLAs Configuration Guide, 29)

Käyttäjä pystyy monitoroimaan kyseessä olevan operaation tuloksia, joko laitteen komentoriviltä tai keräämällä tiedot laitteen RTTMON-MIB:eistä SNMP -protokollaa hyödyntävän verkonvalvontasovelluksen avulla. (Cisco IOS IP Service Level Agreements User Guide, 22)

UDP Echo -operaatiolla mitataan UDP-liikenteen edestakaista vasteaikaa ja saatavuutta Ciscon laitteen ja minkä tahansa IP-laitteen väliltä. Alapuolella olevassa kuvassa reititin A on määritetty kohdelaitteeksi, johon on laitettu IP SLA Responder -palvelu käyntiin. Reititin B on määritetty lähdelaitteeksi, johon on laitettu UDP Echo -operaatio käyntiin. (IP SLAs Configuration Guide, 146)



Kuva 4. UDP Echo -operaatio. (IP SLAs Configuration Guide, 146)

Lähdelaite lähettää UDP Echo -kyselyn kohdelaitteelle, joka vastaanotettua paketin lähettää UDP Echo -vastauksen takaisin lähdelaitteelle, johon kuluva aika lasketaan mittaustuloksen muodostamiseksi. IP SLA Responder -palvelun ollessa käynnissä saadaan tarkempi tulos, koska kohdelaite on asetettu vastaamaan kyselyihin. Tässä esimerkissä molemmat käytetyt laitteet ovat Ciscon laitteita. IP SLA Responder -palvelua ei voida määrittää muihin kuin Ciscon laitteisiin. IP SLA Responder -palvelu ei ole pakollinen mittauksen suorituksessa, koska kohdelaitteena voi olla mikä tahansa IP-laite. (IP SLAs Configuration Guide, 146)

2.3.2 ICMP-mittausoperaatiot

ICMP Jitter -operaatio tuottaa ICMP-paketteja Ciscon laitteen ja minkä tahansa muun IP-laitteen välille, jotta operaatio saa kerättyä suorituskykyyn liittyviä tietoja. Kohdelaitteena voi olla esimerkiksi palvelin tai tietokone, kunhan laite tukee ICMP-protokollaa. Tällä operaatiolla voidaan mitata yksisuuntaista latenssia, edestakaista viivettä, pakettien välisen viiveen vaihtelua, pakettihävikkiä, peräkkäisten pakettien hävikkiä ja pakettien saapumisjärjestystä. Mittaustuloksia voidaan monitoroida Ciscon laitteiden komentoriviltä, myös SNMP:llä huomio- ja järjestelmäviestejä hyödyntäen voidaan monitoroida rajakynnyksen ylittymistä ennakoivasti. Operaatio ei vaadi IP SLA Responder -palvelun käynnistämistä kohdelaitteeseen. (IP SLAs Configuration Guide, 98)

ICMP Jitter -operaatio käyttää kahta ICMP Timestamp -viestiä, jotka ovat ICMP Timestamp -kysely ja ICMP Timestamp -vastaus. Näiden viestien avulla operaatio kerää

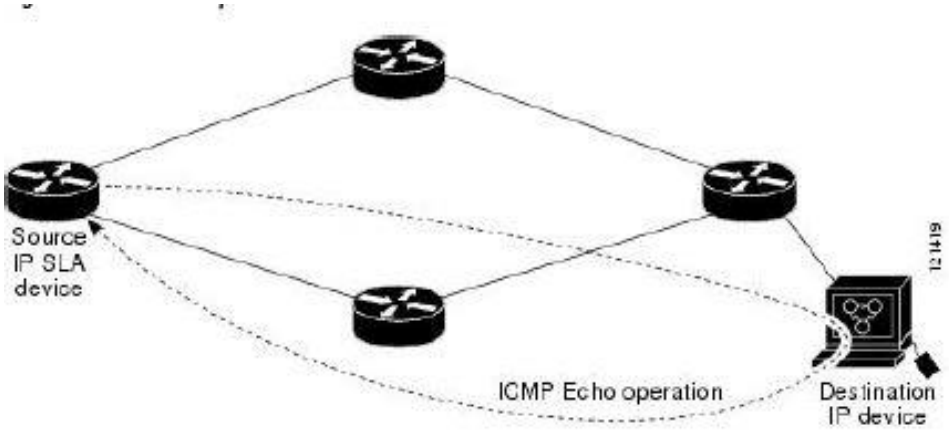
tarvittavat tiedot pakettien hävikin, pakettien välisen viiveen ja latenssin määrittämiseksi. Operaatio lähettää käyttäjän valitseman määrän kyselypaketteja verkkoon. kyselypaketin saapuessa takaisin se on liitetty vastauspakettiin, johon on lisätty kolmas Timestamp-saapumisviesti. Jokainen verkosta palannut paketti sisältää kolme Timestamp-viestiä. Nämä aikaleimaviestit ovat lähetys (originate), vastaanotto sekä vastaus (reply). Näiden tietojen perusteella pystytään laskemaan edestakaisia mittauksia. Jokainen ICMP -paketti sisältää järjestysnumeron otsikossa, jota käytetään laskemaan pakettien määrää ja väärässä järjestyksessä saapuneita paketteja. (IP SLAs Configuration Guide, 98)

ICMP Path Jitter -operaatio pystyy näyttämään pakettien välisten viiveen vaihteluiden, pakettihävikkien sekä viiveen mittauksien statistiikat IP-verkossa. Operaatio toimii eritavalla kuin standardi UDP Jitter -operaatio, jolla pystytään määrittämään yksisuuntaisia ja edestakaisia mittauksia. ICMP Path Jitter -operaatiolla voidaan täydentää UDP Jitter -operaatiota. Esimerkiksi UDP Jitter -operaation keräämät tulokset voivat sisältää odottamattomia arvoja viiveissä ja pakettien välisissä viiveiden vaihteluissa, jolloin ICMP Path Jitter -operaatiota voidaan käyttää hyväksi verkon vianhaussa, kuten ruuhkautuneen verkonosan etsimisessä. (Musardo 2010, 34)

ICMP Path Jitter -operaatio selvittää ensin verkonpolun lähdelaitteelta kohdelaitteelle Traceroute-ominaisuudella. Tämän jälkeen ICMP Echojen avulla mitataan vasteajat, pakettihävikit sekä likimääräiset pakettien väliset viiveet jokaisen verkon linkin välillä. Arvot ovat vain likimääräisiä, koska ICMP mittaa vain edestakaisia arvoja. Tällä operaatiolla ei ole tukea RTTMON-MIB:ssä, joten tulosten nouto voidaan tehdä ainoastaan laitteen komentoriviltä. (IP SLAs Configuration Guide, 211)

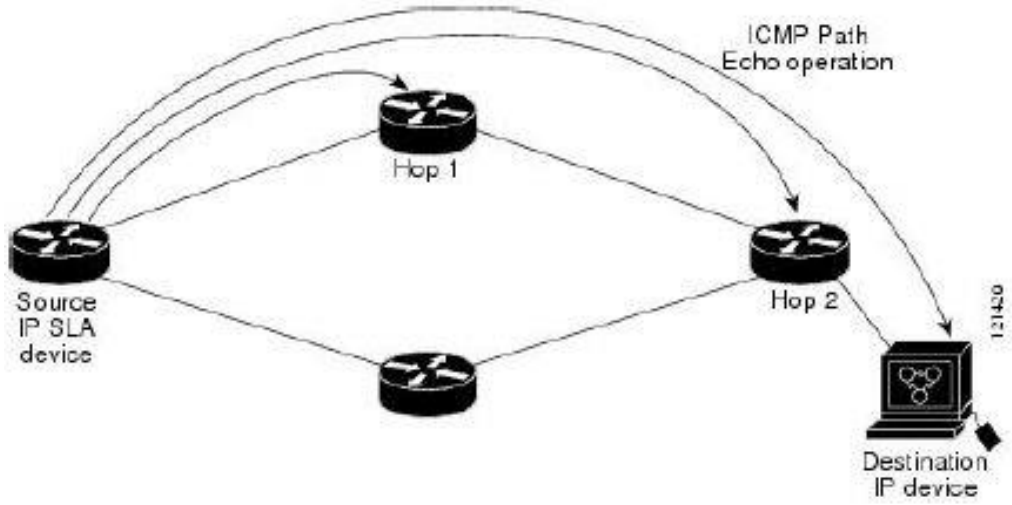
ICMP Echo -operaatiolla mitataan vasteaikaa päästä päähän Ciscon laitteen ja minkä tahansa IP-laitteen välillä käyttäen ICMP Echo kyselyviestiä ja ICMP Echo vastausviestiä. Vasteaika määritetään laskemalla yhteen aika, joka kuluu kyselyviestin lähettämiseen ja vastauksen saamiseen kohdelaitteelta. (Cisco IOS IP Service Level Agreements User Guide, 23)

Alla olevassa kuvassa ICMP Echo -operaatio käyttää pingiä mitatakseen IP SLA -lähdelaitteen ja kohdelaitteen välisen vasteajan. (IP SLAs Configuration Guide, 186)



Kuva 5. ICMP Echo -operaatio (IP SLAs Configuration Guide, 186)

ICMP Path Echo - operaatio mittaa päästä päähän ja hyppy kerrallaan vasteajat Ciscon laitteen ja minkä tahansa laitteiden välillä, jotka käyttävät IP-protokollaa. Tämä Operaatio on hyödyllinen verkon saatavuuden mittaamisessa ja vianhaussa. Operaatio kerää tiedot hyppy kerrallaan jokaisen verkossa olevan laitteen väliltä, kunnes se saavuttaa kohdelaitteen. Operaatio käyttää Traceroute-ominaisuutta havaitakseen verkonlaitteet matkalta. Alla olevassa kuvassa on esitetty, kun IP SLA -lähdelaite selvittää reitin kohdelaitteelle Traceroute-ominaisuutta käyttäen, jonka jälkeen vasteajat ovat määritetty verkon jokaisen laitteen väliltä käyttämällä pingiä. (IP SLAs Configuration Guide, 198)



Kuva 6. ICMP Path Echo -operaatio. (IP SLAs Configuration Guide, 198)

2.3.3 Muut mittausoperaatiot

HTTP-operaatio mittaa Ciscon laitteen ja HTTP-palvelimen välistä edestakaista viivettä internet-sivustoa ladattaessa. HTTP-palvelimen viiveaikojen mittaukset koostuvat kolmesta tyypistä:

- DNS-kysely, joka mittaa verkon hallinta-alueen kyselyyn kuluvan edestakaisen viiveen.
- TCP Connect, joka mittaa HTTP-palvelimeen otetun TCP-yhteyden edestakaisen viiveen.
- HTTP-tapahtuma-aika, joka mittaa HTTP-palvelimelle lähetetyn pyynnön ja saadun vastauksen edestakaisen viiveen (operaatio hakee vain HTML-etusivun). (IP SLAs Configuration Guide, 158)

Ensin tehdään DNS-operaatio, jonka jälkeen DNS:n edestakainen viive mitataan. Hallinta-alueen nimen löydyttyä sopivaan HTTP-palvelimeen tehdään TCP Connect -operaatio, jonka jälkeen edestakainen viive saadaan mitattua. Viimeinen operaatio on HTTP-pyyntö, jonka seurauksena mitataan HTML-sivun haun edestakainen viive. HTTP-operaation edestakainen kokonaisviive koostuu TCP Connect, DNS ja HTTP-operaatioiden edestakaisten viiveiden summasta. (IP SLAs Configuration Guide, 158)

GET-pyyntöjä varten IP SLA muotoilee pyynnön annetun verkko-osoitteen perusteella. RAW-pyyntöjä varten IP SLA vaatii koko HTTP-pyynnön sisällön. Kun RAW-pyyntö määritetään, komennot täsmennetään HTTP RAW -määrittelytilassa. RAW-pyyntö on joustava ja antaa mahdollisuuden hallita esimerkiksi autentikointia. HTTP-pyyntö voidaan tehdä välityspalvelimen läpi. (IP SLAs Configuration Guide, 158)

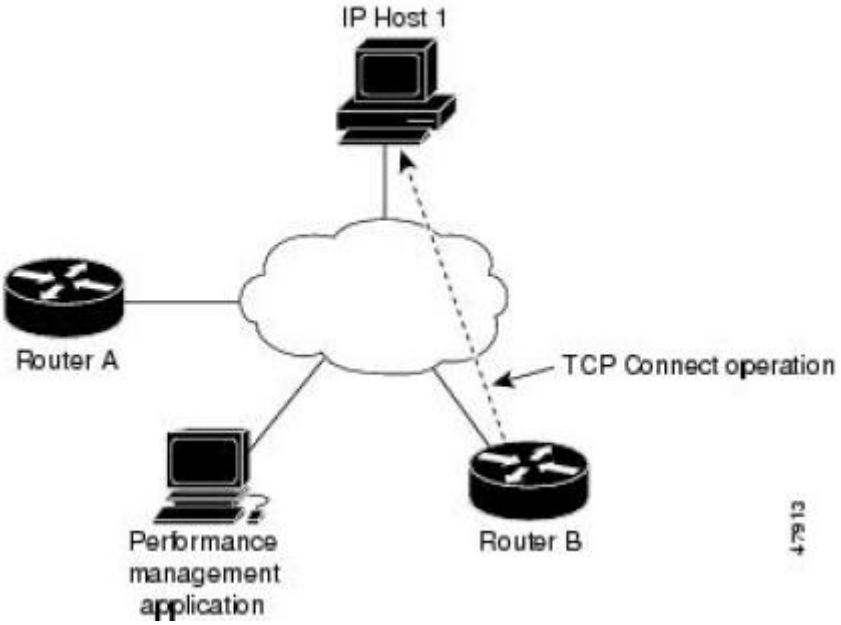
HTTP-operaation tulokset ovat hyödyllisiä internet-palvelimen suorituskyvyn monitoroinnissa mittaamalla edestakaista viivettä. (IP SLAs Configuration Guide, 158)

TCP Connect -operaatio mittaa Ciscon reitittimen ja IP-laitteiden välisen TCP Connect -operaation suorittamiseen kuluvan vasteajan. TCP on kuljetuskerroksen internet-protokolla, joka takaa luotettavan full-duplex -tiedonsiirron. Kohdelaitteena toimii

mikä tahansa laite joka käyttää IP-protokollaa tai IP SLA Responder -palvelua. (IP SLAs Configuration Guide, 171)

Alla olevassa kuvassa reititin B on määritetty IP SLA lähdelaitteeksi ja TCP Connect -operaatioon on määritetty kohdelaitteeksi IP-laite 1.

Figure 11: TCP Connect Operation



Kuva 7. TCP-operaation toimintamalli. (IP SLAs Configuration Guide, 172)

Yhteyden vasteaika lasketaan mittaamalla aika, joka kuluu reitittimeltä IP-laitteeseen lähetettyyn TCP-pyyntöön ja takaisin saatuun vastaukseen. (IP SLAs Configuration Guide, 172)

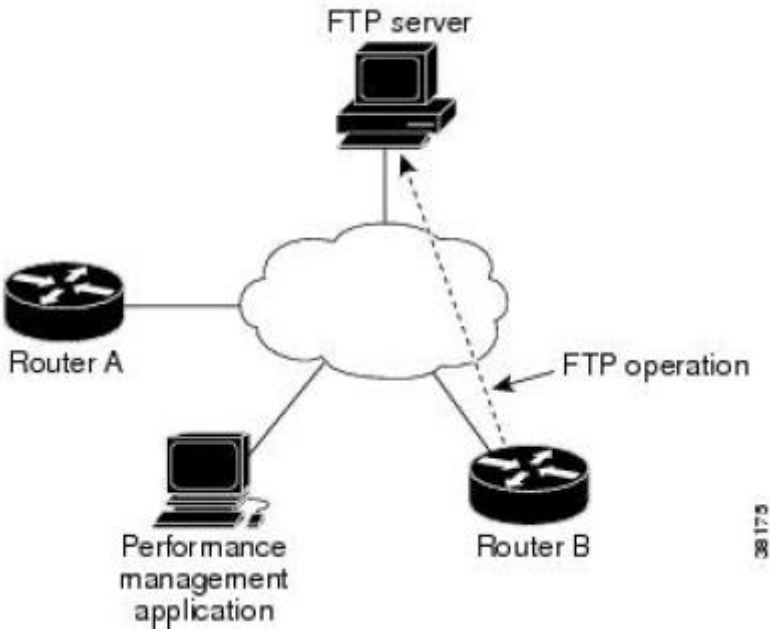
TCP Connectin tarkkuus parantuu, jos kohdelaitteessa on Responder-palvelu käytössä. Kohdelaitteen ollessa Ciscon reititin, IP SLA tekee TCP-yhteyden mihin tahansa määritettyyn porttiin. Jos kohde ei ole Ciscon IP-laite, niin kohdelaitteeseen on määritettävä jokin tunnettu kohdeportin numero, kuten 21 FTP:lle, 23 Telnetille tai 80 HTTP-palvelimelle. (IP SLAs Configuration Guide, 172)

TCP Connect -operaatiota käytetään virtuaalisten piirien tai sovellusten saatavuuden testaamiseen. (IP SLAs Configuration Guide, 172)

FTP-operaatio mittaa edestakaisen viiveen Ciscon laitteen ja FTP-palvelimen välillä, kun tiedosto ladataan. FTP on sovelluspohjainen protokolla, joka on kuljetuskerroksen osa. Sitä käytetään tiedostojen lataamiseen verkon solmukohtien välillä. (IP SLAs Configuration Guide, 222)

Alla olevassa kuvassa reititin B on määritetty IP SLA lähdelaitteeksi ja FTP-operaatioon kohdelaitteeksi on määritetty FTP-palvelin. (IP SLAs Configuration Guide, 222)

Figure 15: FTP Operation



Kuva 8. FTP-operaation toimintamalli. (IP SLAs Configuration Guide, 222)

Yhteyden vasteaika lasketaan mittaamalla aika, joka kuluu kun ladataan tiedosto reitittimelle FTP-palvelimelta käyttämällä FTP:tä TCP:n yli. Tämä operaatio ei käytä Responder-palvelua. (IP SLAs Configuration Guide, 222)

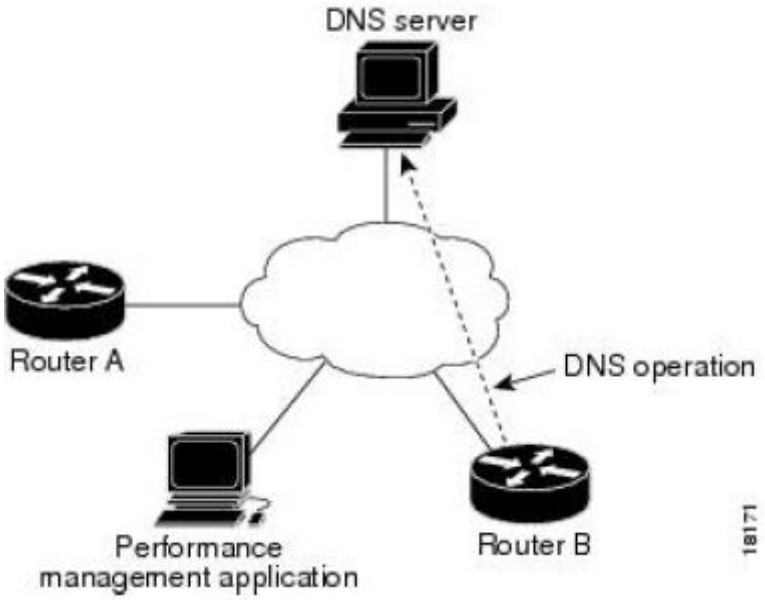
DHCP tarjoaa mekanismin jonka avulla IP-osoitteita voidaan jakaa eri laitteille dynaamisesti siten, että kun laite ei enää tarvitse osoitetta, niin se vapautetaan uudelleenkäytettäväksi. DHCP-operaatio mittaa edestakaista viivettä, joka kuluu siihen, että DHCP palvelin löytyy ja siltä saadaan IP-osoite. Kyseisiä edestakaisia viiveitä voidaan käyttää DHCP:n suorituskyvyn mittaamiseen. DHCP-operaatiolla on kaksi toimintatapaa. Oletuksena DHCP-operaatio lähettää DHCP-kyselyjä jokaiseen käytössä olevaan reitittimen porttiin. Jos reitittimeen on määritetty tietty DHCP-palvelin, kyse-

lyt lähetetään vain määritetylle DHCP-palvelimelle. (IP SLAs Configuration Guide, 243)

DNS-operaatiolla mitataan aikaeroa DNS-pyyntöjen ja saatujen vastauksien välillä. Internetissä DNS:ää käytetään IP-osoitteiden verkkonimiksi muuntamiseen ja päinvastoin. (IP SLAs Configuration Guide, 233)

Alla olevassa kuvassa reititin B on määritetty IP SLA lähdelaitteeksi ja DNS-operaatioon kohdelaitteeksi on määritetty DNS-palvelin.

Figure 16: DNS Operation



Kuva 9. DNS-operaation toimintamalli. (IP SLAs Configuration Guide, 234)

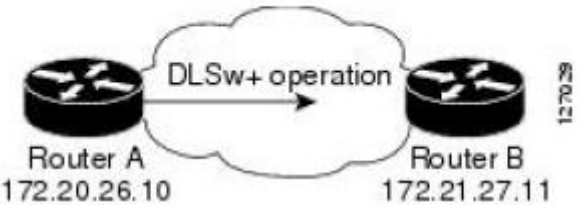
Yhteyden vasteaika lasketaan mittaamalla pyynnön lähettämiseen DNS-palvelimelle kuluvan ajan sekä saatuun vastaukseen kuluvan ajan ero. Tästä saadaan tuloksen DNS-hakuaika, joka auttaa analysoimaan DNS:n suorituskykyä. (IP SLAs Configuration Guide, 234)

DLSw+-operaatio mittaa DLSw+-protokollapinon sekä verkon vasteaikaa DLSw+-kohteiden välillä. DLSw+ on Ciscon paranneltu versio RCF 1795:stä. DLSw+ tunneloi reitittämätöntä siirtokerroksen liikennettä kuten SNA-liikennettä IP-runkoverkon yli TCP:n välityksellä. Verkkolaitteita, jotka tunneloivat reitittämätöntä liikennettä TCP/IP:lle kutsutaan DLSw+-vertaislaitteiksi. DLSw+-vertaislaitteet kommunikoivat

normaalisti TCP portin 2065 läpi. Kohdeverkkolaitteen ei tarvitse olla Ciscon reititin, jos se tukee RFC 1795:tä. (IP SLAs Configuration Guide, 254)

Alla olevassa kuvassa reititin A on määritetty IP SLA lähdelaitteeksi ja DLSw+-operaatioon DLSw+-etävertaislaitteeksi on määritetty reititin B. Reititin A ja B ovat määritetty yhdistetyiksi vertaislaitteiksi. Kohteena olevan vertaislaitteen ei tarvitse tukea IP SLA -toimintoa. (IP SLAs Configuration Guide, 254)

Figure 17: DLSw+ Operation



Kuva 10. DLSw+-operaation toimintamalli. (IP SLAs Configuration Guide, 254)

Verkon vasteaika lasketaan mittaamalla DLSw+-vertaislaitteeseen otetun TCP-etäyhteyden edestakainen viive. (IP SLAs Configuration Guide, 254)

2.4 Mittausoperaatioiden aikataulutus

Kun IP SLA -mittausoperaatio on määritetty, niin se pitää aikatauluttaa käynnistymään, jonka jälkeen tietojen kerääminen alkaa. Kun mittausoperaatio aikataulutetaan, se voidaan aloittaa heti tai haluttuna ajankohtana. Pending-tila mahdollistaa operaation aloittamisen myöhempänä ajankohtana. Pending-tilaa käytetään myös Threshold-operaatioihin, jotka odottavat käynnistymisen laukaisemista. Aikataulutuksen voi tehdä yhdelle mittausprosessille tai kokonaiselle mittausoperaatioryhmälle. (IP SLAs Configuration Guide, 6)

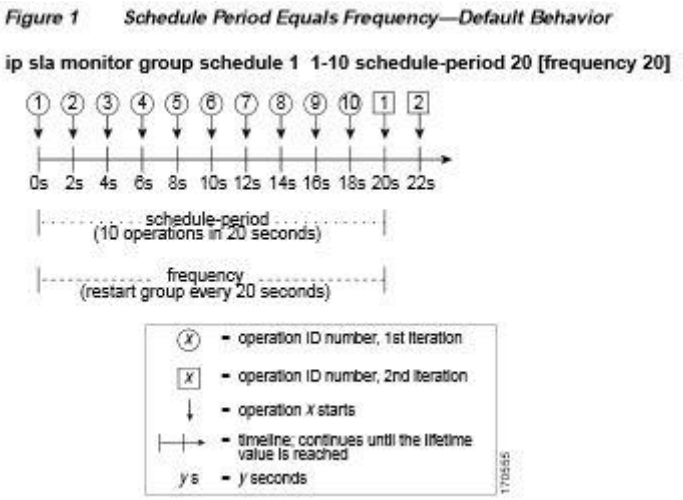
Mittausoperaation normaali aikataulutus-toiminto sallii käynnistää vain yhden operaation kerrallaan. Isommassa verkossa voi olla määritetty jopa tuhansia mittausoperaatioita, joiden aikatauluttaminen yksitellen olisi tehotonta ja aikaa vievää. (IP SLAs - Multiple Operation Scheduling, 2)

Useiden operaatioiden aikataulutus-toiminto mahdollistaa mittausoperaatioiden aikatauluttamisen ryhmänä. Ensin aikataulutus-toiminnolle annetaan ryhmänumero, jonka

jälkeen siihen määritetään mittausoperaatioiden prosessinumerot, jotka halutaan liittää kyseiseen ryhmään. Seuraavaksi määritetään ryhmälle aikajakso, johon mittausoperaatiot jaksotetaan (Schedule-Period) ja minkä aikavälein määritetyt mittausoperaatiot käynnistetään uudelleen (frequency). Lisäksi määritetään milloin operaatioryhmä aloittaa ja lopettaa mittaustietojen keräämisen. Mittausoperaatioiden frequency-arvon voi jättää määrittämättä, jos halutaan että jokainen mittausoperaatio aloittaa mittauksensa tasaisin väliajoin ryhmän aikataulun mukaisesti, koska arvoksi määräytyy oletusarvo, mikä on sama kuin ryhmälle asetettu aikajakso. (IP SLAs - Multiple Operation Scheduling, 3)

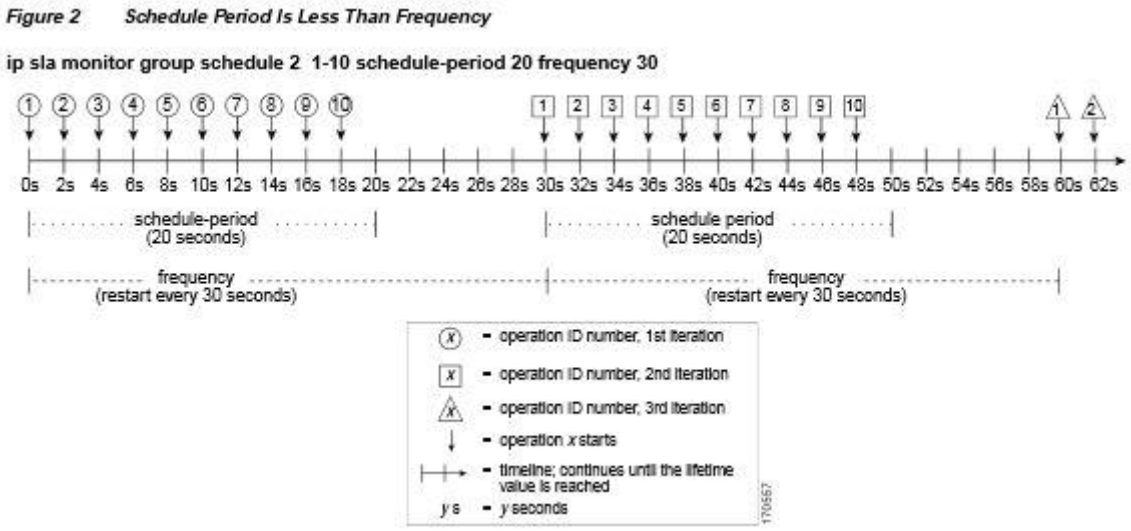
Useiden operaatioiden aikataulutus-toiminnolla saatava etu on se, että verkon kuorma vähenee, koska operaatiot hajautetaan tasaisin väliajoin ryhmän aikajaksolle. Tämän hajauttamisen ansiosta saadaan myös pidemmän aikavälin monitorointi aikaiseksi. Esimerkiksi määritetään 60 operaatiota aloittamaan mittauksensa samaan aikaan ja toistamaan mittauksensa 60 sekunnin välein. Jos verkossa tapahtuisi yhteyskatkos sen jälkeen, kun ensimmäiset mittaukset ovat suoritettu ja yhteyskatkoksesta palaudutaan ennen kuin seuraavat mittaukset alkavat, niin tässä tapauksessa ei tiedettäisi yhteyskatkosta edes tapahtuneen. Jos oltaisiin käytetty aikataulutus-toimintoa siten, että hajautetaan samat 60 mittausoperaatiota tasaisesti 60 sekunnin aikavälille, niin tämä yhteyskatkos oltaisiin huomattu. (IP SLAs - Multiple Operation Scheduling, 3)

Alla olevassa kuvassa on esitetty aikataulutus-toiminto, jolle on annettu ryhmänumero 1,johon on määritetty 10 mittausoperaatiota 20 sekunnin jaksoon, jolloin mittausoperaatiot aloittavat kahden sekunnin välein mittauksensa, koska jokaisen mittausoperaation aloitusaika jaksotetaan tasaisesti jakamalla aikajakso operaatioiden määrällä. Frequency-arvo on jätetty oletusarvoksi tai määritetty arvoon 20, jolloin mittausoperaatiot toistavat mittauksensa 20 sekunnin välein. (IP SLAs - Multiple Operation Scheduling, 4)



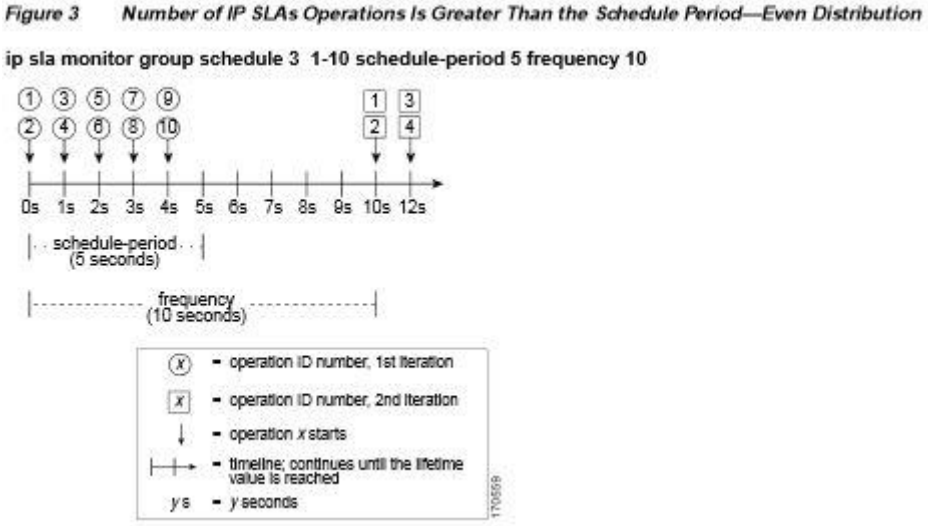
Kuva 11. Aikataulutus-toiminnon malli oletusarvoilla. (IP SLAs - Multiple Operation Scheduling, 4)

Alla olevassa kuvassa on esitetty toinen aikataulutus-toiminto, jolle on annettu ryhmänumero 2, johon on määritetty 10 mittausoperaatiota 20 sekunnin jaksoon, jolloin ne aloittavat kahden sekunnin välein mittauksensa ja jokainen mittausoperaatio toistaa mittauksensa 30 sekunnin välein. Kun Frequency-arvo on määritetty suuremmaksi kuin aikajakson arvo, niin aikajanalle jää hetkiä, jolloin mikään operaatio ei ole suorittamassa mittauksia. (IP SLAs - Multiple Operation Scheduling, 4)



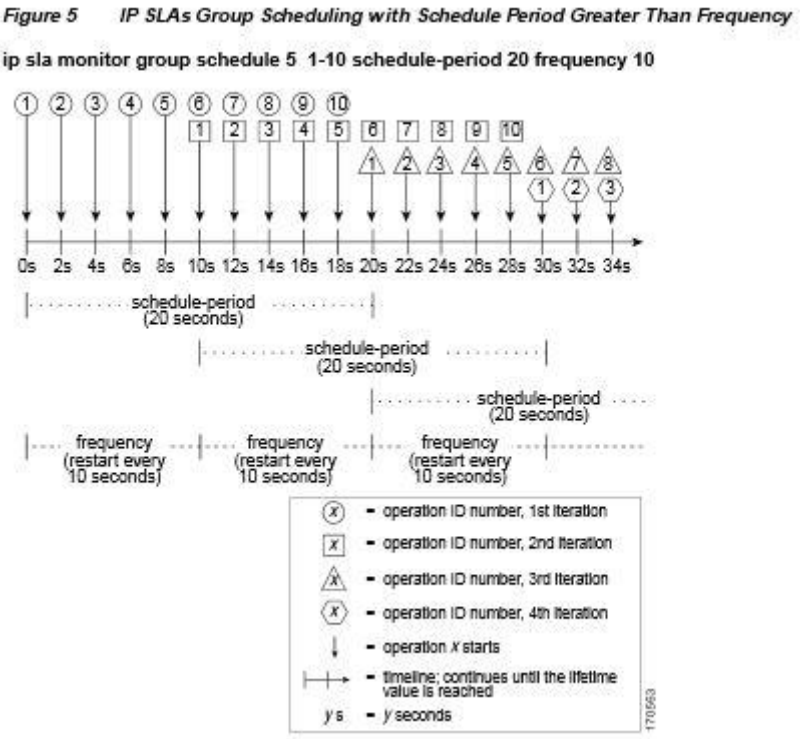
Kuva 12. Aikataulutus-toiminto, jossa aikajakso on pienempi kuin Frequency-arvo. (IP SLAs - Multiple Operation Scheduling, 5)

Alla olevassa kuvassa on esitetty kolmas aikataulutus-toiminto. Kyseiselle toiminnolle on annettu ryhmänumero 3, johon on määritetty 10 mittausoperaatiota 5 sekunnin jaksoon, jolloin ne aloittavat puolen sekunnin välein mittauksensa. Jokaisen mittausoperaation aloitusaika jaksotetaan tasaisesti jakamalla aikajakso operaatioiden määrällä, mutta mittausoperaatioiden lukumäärän ollessa suurempi kuin aikajakson arvo, tulokseksi saadaan vähemmän kuin 1 sekunti. Koska mittausoperaatioiden minimiaikaväli ryhmäoperaatiossa on 1 sekunti, niin aikataulutus-toiminto laskee kuinka monta mittausoperaatiota tulisi aloittaa jokaisen sekunnin aikavälein jakamalla operaatioiden määrä aikajaksolla. Tämän perusteella kyseisistä kymmenestä mittausoperaatioista kaksi uutta aloitetaan sekunnin välein. Jokainen mittausoperaatio toistaa mittauksensa 10 sekunnin välein, koska Frequency-arvoksi on määritetty 10 sekuntia. (IP SLAs - Multiple Operation Scheduling, 6)



Kuva 13. Aikataulutus-toiminto, jossa operaatioiden määrä on suurempi kuin aikajakso. (IP SLAs - Multiple Operation Scheduling, 6)

Alla olevassa kuvassa on esitetty neljäs aikataulutus-toiminto. Kyseiselle toiminnolle on annettu ryhmänumero 4, johon on määritetty 10 mittausoperaatiota 20 sekunnin jaksoon, jolloin ne aloittavat kahden sekunnin välein mittauksensa ja jokainen mittausoperaatio toistaa mittauksensa 10 sekunnin välein. Koska määritetty Frequency-arvo on pienempi kuin aikajakson arvo, niin ensimmäiset mittausoperaatiot aloittavat uudet mittauksensa, vaikka viimeiset mittausoperaatiot eivät ole ehtineet aloittaa mittauksiaan. Tästä syntyy päällekkäisyyksiä mittauksissa, kuten kuvasta nähdään. (IP SLAs - Multiple Operation Scheduling, 8)



Kuva 14. Aikataulutus-toiminto, jossa aikajakso on suurempi kuin Frequency-arvo. (IP SLAs - Multiple Operation Scheduling, 8)

2.5 IP SLA -operaatioiden raja-arvojen monitorointi

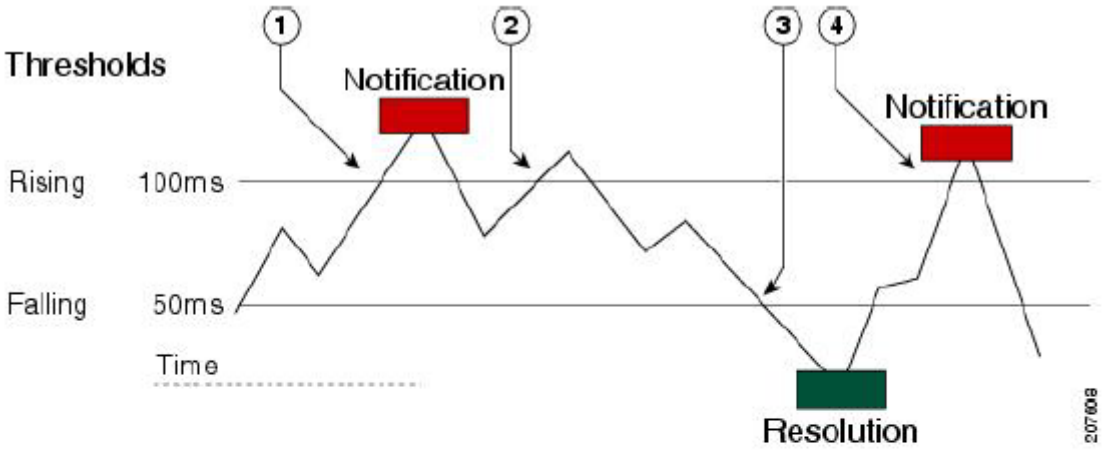
Threshold-toiminto on erittäin tärkeä, kun halutaan tukea palvelutasosopimuksen monitorointia tai mitata ennakoivasti verkon suorituskykyä. Johdonmukaiset ja luotettavat mittaustulokset auttavat tunnistamaan ongelmat heti, jonka johdosta vianhaku nopeutuu. Luotettavan palvelutasosopimuksen ylläpitämiseksi pitää olla mekanismeja, jotka ilmoittavat heti, kun mahdollisia ongelmia löytyy. IP SLA mahdollistaa SNMP-trap-viestien lähettämisen, jonka voi laukaista seuraavat seikat:

- Yhteyden katkeaminen
- Aikakatkaisu
- Edestakaisen viiveen raja-arvo
- Pakettien välisen viiveen keskiarvon raja-arvo
- Yksisuuntainen pakettihävikki

- Yksisuuntainen pakettien välinen viive
- Yksisuuntainen MOS
- Yksisuuntainen latenssi (IP SLAs Configuration Guide, 7)

Reaction-trigger komentoa käytetään laukaisemaan muita IP SLA-operaatioita raja-arvojen ylittyessä. Reaction-configuration komento käyttää perustason RMON-tyylistä raja-arvomenetelmää, joka käyttää ylä- sekä alarajoja. Jos mittaustulokset ylittävät asetetun ylärajan, jolloin trap-viesti voidaan lähettää. Uusi trap lähetetään vasta, kun mittaustulos ohittaa alarajan ja nousee uudelleen ylärajan ylitse. Näin saadaan vähennettyä lähetettyjen trap-viestien määrää. (Cisco IOS IP Service Level Agreements User Guide, 33)

Figure 23: IP SLAs Triggered Reaction Condition and Notifications for Threshold Exceeded



1	An event is sent and a threshold-exceeded notification is issued when the rising threshold is exceeded for the first time.
2	Consecutive over-rising threshold violations occur without issuing additional notifications.
3	The monitored value goes below the falling threshold.
4	Another threshold-exceeded notification is issued when the rising threshold is exceeded only after the monitored value first fell below the falling threshold.

Kuva 15. IP SLA raja-arvojen ylityksen ja reaktiotilailmoitusten toimintamalli. (Cisco IOS IP Service Level Agreements User Guide, 33)

3 SNMP-VERKONHALLINTA

SNMP:n ydin on yksinkertainen ryhmä operaatioita, jotka antavat järjestelmän ylläpitäjälle mahdollisuuden vaihtaa joidenkin SNMP-pohjaisten laitteiden tiloja. Esimerkiksi SNMP:n avulla voidaan määrittää pois käytöstä reitittimen portti tai tarkistaa sen toimintanopeus. SNMP pystyy myös monitoroimaan kytkimen lämpötilaa ja antaa siitä hälytyksen, mikäli se nousee liian korkeaksi. (Mauro & Schmidt 2005, 2)

SNMP:n käyttö yhdistetään useasti vain reitittimien hallintaan, mutta sitä voidaan käyttää myös moniin muihin laitetyyppeihin. Näihin laitetyyppeihin kuuluu Unix-järjestelmät, Windows-järjestelmät, tulostimet, modeemit, älykkäät virtalähteet sekä monet muut vastaavat järjestelmät ja laitteet. (Mauro & Schmidt 2005, 2)

3.1 Yleistä toimintaperiaatteesta

SNMP käyttää UDP-protokollaa siirtoprotokollana tiedon välittämisessä ja kuljettamisessa. Standardissa RFC 768 määritelty UDP valittiin siirtoprotokollaksi TCP:n sijaan. Valinta perustui siihen, että UDP ei vaadi yhteydeltä kohdelaitteen varmistusta, kun paketteja lähetetään. Tämä ominaisuus tuo myös mukanaan epäluotettavuuden, sillä protokollatasolla hävinneistä paketeista ei saada minkäänlaisia vastaus- tai varmistusviestejä. Tästä johtuen sovelluksen vastuulle jää päätellä mitkä paketit ovat hävinneet ja pitääkö ne mahdollisesti lähettää uudelleen. Yleensä kyseinen operaatio toteutetaan yksinkertaisen aikakatkaisujen monitoroinnin avulla. NMS-hallinta-asema lähettää UDP-kyselyn ja jää odottamaan vastausta. Jos tietyn ajan kuluessa sitä ei saada, niin tehdään aikakatkaisu. Tästä NMS-hallinta-asema päättelee paketin hävinneen ja lähettää uuden kyselyn. (Mauro & Schmidt 2005, 19)

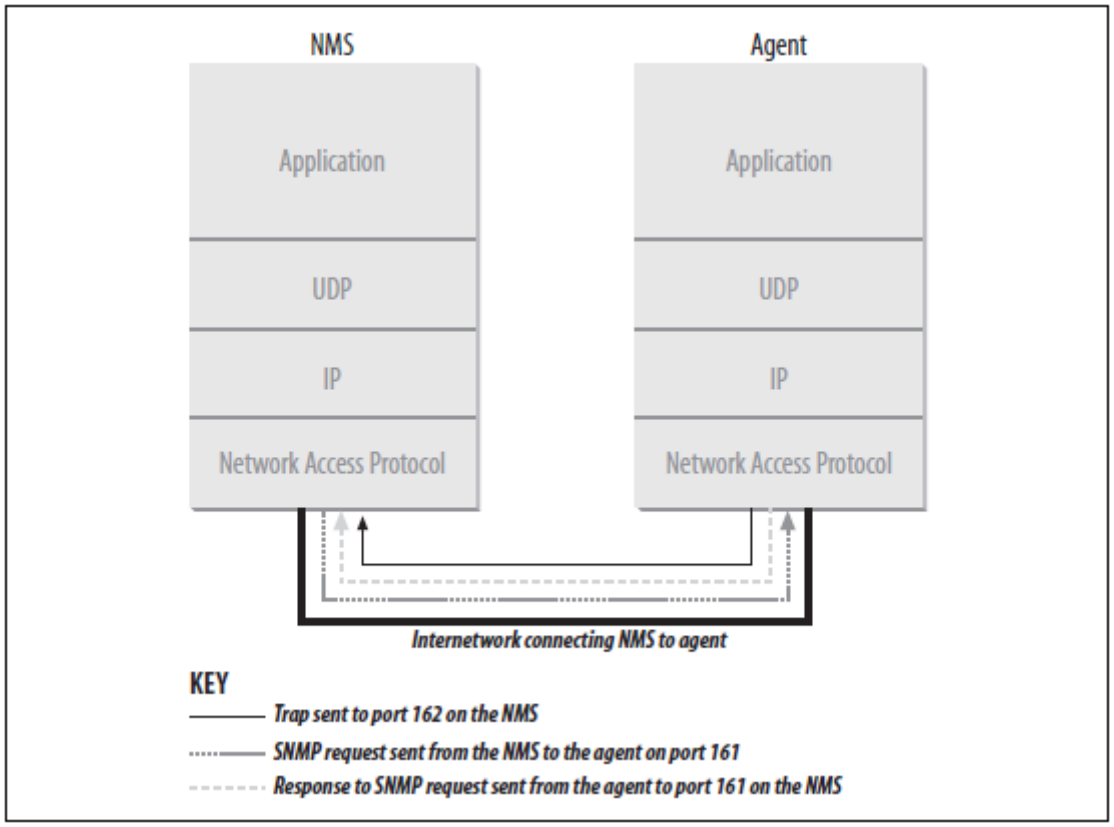
UDP:n epäluotettavuus ei ole kuitenkaan suuri ongelma yleisen tason verkonhallinnassa, sillä pahimmillaan NMS-hallinta-asema lähettää kyselyitä, joihin se ei saa koskaan vastausta. Trap-viestejä käytettäessä syntyy hieman suurempi ongelma, koska mikäli NMS-hallinta-asemalle lähetetty trap-viesti ei koskaan saavu perille, niin sillä ei ole mitään mahdollisuutta tietää, että paketti ylipäätään lähetettiin. Tämän vuoksi NMS-hallinta-asema ei lähetä takaisin mitään vastausta, jonka takia operaatio jää il-

man tuloksia. UDP:n epäluotettavuuden hyviin puoliin kuuluu se, että verkon kuormitus on pientä. (Mauro & Schmidt 2005, 19)

SNMP voidaan myös toteuttaa käyttämällä TCP-protokollaa, mutta näin tehdään vain erikoistapauksissa, kuten johonkin erityiseen laiteympäristöön. Ruuhkaisessa verkossa TCP:n avulla toteutettu SNMP on erittäin huono ratkaisu. Kun verkko on suurissa ongelmissa, on parempi käyttää protokollaa, joka luovuttaa jos paketit eivät saavuta kohdettaan sellaisen protokollan sijaan, joka ruuhkauttaa verkkoa entisestään lähettämällä jatkuvasti turhia uudelleenlähetyspaketteja. (Mauro & Schmidt 2005, 20)

SNMP käyttää kyselyiden lähettämiseen ja vastaanottamiseen UDP-porttia 161 ja muilta laitteilta tulevien trapsien vastaanottamiseen porttia 162. Jokaisen SNMP:tä käyttävän laitteen täytyy käyttää näitä portteja oletuksena. (Mauro & Schmidt 2005, 20)

Alla oleva kuva esittää NMS-hallinta-aseman ja hallittavan kohteen protokollapinot.



Kuva 16. SNMP-verkonhallinnan protokollapino. (Mauro & Schmidt 2005, 20)

3.2 Versiot

SNMPv1 on SNMP-protokollan ensimmäinen versio, joka on määritelty RFC 1157-standardissa. SNMPv1:n tietoturva perustuu yhteisöihin eli periaatteessa yksinkertaisiin salasanoihin, jotka sallivat hallintatietojen hakemisen minkä tahansa SNMP-pohjaisen sovelluksen toimesta, johon on määritetty kyseinen salasana. Yhteisöjen tyypit ovat yleensä vain luku, luku ja kirjoitus tai trap. Vaikka SNMPv1 on erittäin vanha, niin se on yhä laajasti käytössä ja yleisesti tuettuna. (Mauro & Schmidt 2005, 21-22)

SNMPv2:n tekninen kutsumanimi on SNMPv2c, johon kuitenkin yleensä viitataan vain v2:na. Se on määritelty standardeissa RFC 3416, RFC 3417 ja RFC 3418.

Viimeisin versio on SNMPv3, jonka suurin uudistus verkonhallinnan osalta on parannettu tietoturva. Siitä löytyy tuki erittäin vahvoille autentikaatiomenetelmille ja yksityiselle kommunikaatiolle hallittujen kohteiden välillä. SNMPv3 muutettiin vedoksesta täydeksi standardiksi vuonna 2002. Se määritellään seuraavissa standardeissa RFC 3410, RFC 3411, RFC 3412, RFC 3413, RFC 3414, RFC 3415, RFC 3416, RFC 3417, RFC 3418 ja RFC 2576. Vaikka kolmannessa versiossa on paljon tietoturvauudistuksia, niin se on yleistynyt hitaasti. (Mauro & Schmidt 2005, 2)

3.2.1 SNMP-versio 3

SNMPv3:n parannuksiin kuuluu kryptografinen tietoturva ja uudet tekstuaaliset konseptit sekä terminologiat. Ne määrittävät SNMP:n tarvittavat osat paljon tarkemmin. SNMPv3:n tärkein muutos on manageri-kohdelaite-suhteesta luopuminen. Sekä managerit että kohdelaitteet kulkevat nimellä SNMP entiteetti (entity). Jokainen entiteetti koostuu SNMP-moottorista sekä yhdestä tai useammasta SNMP-sovelluksesta. Nämä uudet konseptit ovat tärkeitä, koska ne määrittävät arkkitehtuurin pelkkien viestiryhmien sijaan. (Mauro & Schmidt 2005, 73)

SNMPv3-moottori koostuu neljästä osasta: lähettäjä (dispatcher), alijärjestelmä viestien prosessoinnille (message processing subsystem) ja alijärjestelmä tietoturvalle (security subsystem) sekä alijärjestelmä pääsynvalvonnalle (access control subsystem). (Mauro & Schmidt 2005, 74)

Lähettäjä hoitaa viestien lähetyksen ja vastaanoton. Se yrittää päätellä jokaisen vastaanotetun viestin version (v1, v2 tai v3) ja välittää viestin viestien prosessoinnista vastaavalle alijärjestelmälle, jos kyseinen versio on tuettu. Lähettäjä lähettää myös SNMP-viestejä muille entiteeteille. (Mauro & Schmidt 2005, 74)

Viestien prosessoinnin alijärjestelmä valmistelee lähetettävät viestit ja purkaa tiedot vastaanotetuista viesteistä. Viestien prosessoinnin alijärjestelmä voi sisältää useita viestinprosessointimoduuleita. Se voi esimerkiksi sisältää moduuleita eri SNMP:n versioiden kyselyjen prosessoinnille. Se voi myös sisältää moduuleita muille prosessointioperaatioille, joita ei ole vielä määritelty. (Mauro & Schmidt 2005, 74)

Tietoturvan alijärjestelmä tarjoaa yksityisille palveluille autentikaation. Se käyttää joko yhteisöjä (SNMPv1 ja SNMPv2) tai käyttäjäkohtaista autentikaatiota (SNMPv3). Käyttäjäkohtainen autentikointi käyttää MD5 tai SHA -algoritmeja autentikoidakseen käyttäjiä lähettämättä todennustietoa kuten salasanaa salaamattomana. Yksityisyyspalvelu käyttää DES-algoritmia SNMP-viestien salaamiseen ja purkamiseen. Tällä hetkellä DES on ainut käytössä oleva algoritmi, mutta tulevaisuudessa niitä voidaan lisätä. (Mauro & Schmidt 2005, 74-75)

Pääsynvalvonnan alijärjestelmä vastaa MIB-objektien pääsynvalvonnasta. Objektien ja operaatioiden käyttöä ja käyttöoikeuksia voidaan kontrolloida käyttäjäkohtaisesti. Esimerkiksi käyttäjän luku-kirjoitus-oikeus voidaan määrittää pätemään vain tiettyyn MIB-objektipuun osaan säilyttämällä kuitenkin lukuoikeus koko objektipuuhun. (Mauro & Schmidt 2005, 75)

SNMPv3 jakaa suuren osan SNMP:stä sovelluksiin:

- Command Generator. Luo get, getnext, getbulk ja set -pyyntöjä sekä prosessoi vastaukset. Tämä sovellus toimii NMS:ssä, jotta se voi lähettää kyselyitä sekä set-pyyntöjä entiteettjä vastaan esimerkiksi reitittimissä, kytkimissä sekä Unix-järjestelmissä.

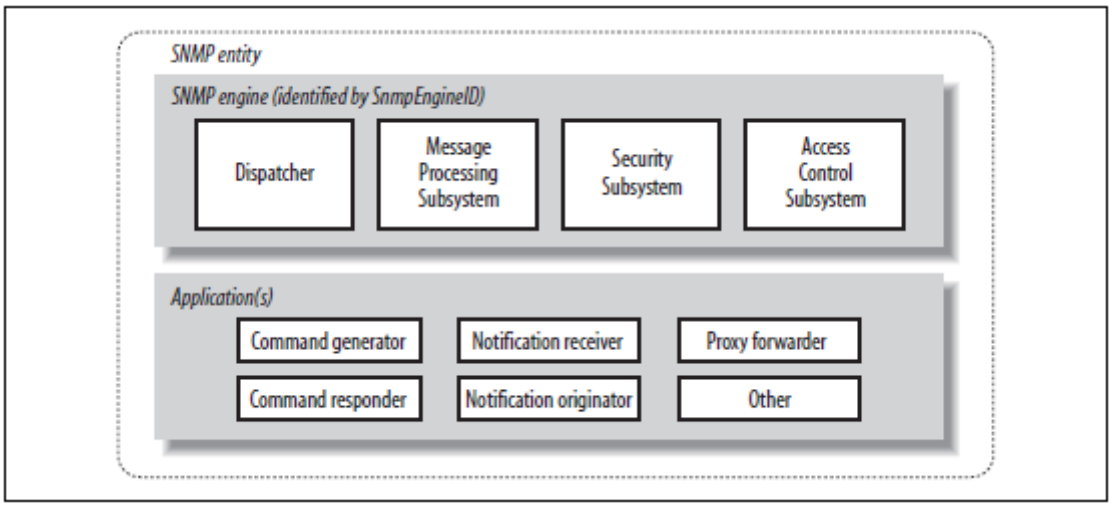
- Command Responder. Vastaa get, getnext, getbulk ja set -pyyntöihin. Command Responderia käytetään entiteetin toimesta Cisco reitittimessä tai Unix-järjestelmässä. SNMPv1:ssä ja SNMPv2:ssa sitä käyttää SNMP kohdelaite.

- Notification Originator. Luo SNMP trapseja sekä ilmoituksia. Sitä käyttää entiteetti reitittimessä tai Unix-järjestelmässä. SNMPv1:ssä ja SNMPv2:ssa Notification Originator on osa SNMP kohdelaitteen toimintaa. Trapsien luonttiin löytyy myös itsenäisiä työkaluja.

- Notification Receiver. Vastaanottaa trapseja sekä tiedotusviestejä. Tätä sovellusta käyttää NMS.

- Proxy Forwarder. Ohjaa ja välittää viestejä entiteettien välillä. (Mauro & Schmidt 2005, 75)

RFC 3411 -standardi sallii uusien sovellusten lisäämisen tarvittaessa. Tämä mahdollisuus SNMPv3:n rungon laajentamiseen on suuri etu vanhoihin versioihin verrattuna. Alla oleva RFC 3411 -standardin sisältämä kuva esittää miten entiteetin osat sopivat yhteen. (Mauro & Schmidt 2005, 75)

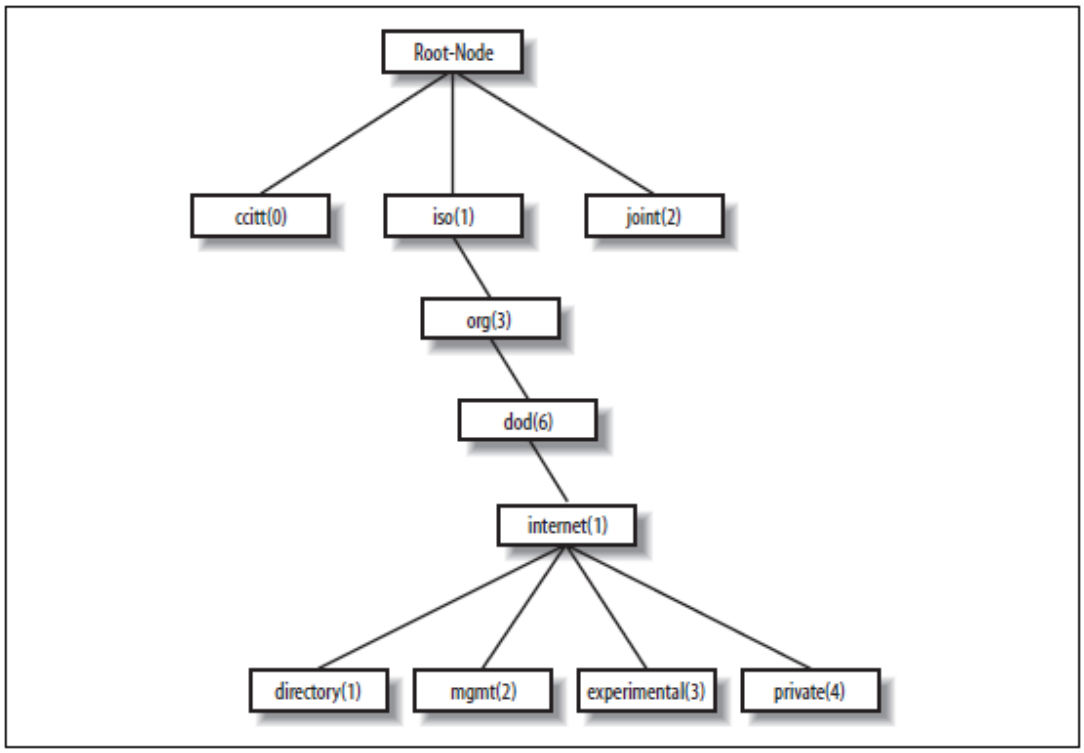


Kuva 17. SNMPv3:n entiteetti. (Mauro & Schmidt 2005, 75)

3.3 MIB-järjestelmä

MIB on taulukko, josta löytyy hallittavien objektien hierarkkinen rakenne sekä hallinnan rakenteen malli. MIB-objektit voivat olla yleisiä tai toimittajakohtaisia. Hallinta-objektilla tarkoitetaan todellisen verkon rakenteen loogista esitystä. Jokaisen objektin tehtäviin kuuluu kerätä ja ylläpitää kerättyä tietoa, kuten vastaanotettujen ja lähetettyjen pakettien määrää ja välittää ne verkon hallinta-asemalle. (Jaakohuhta 2005, 315)

Hallinnoidut objektit ovat organisoitu puumaiseen hierarkiaan. Tämä rakenne on SNMP:n nimeämismenetelmän perusta. ObjectID on numerosarja, joka muodostuu puun solmukohtien järjestysnumeroista pisteellä erotettuna. Numerosarjat voidaan esittää myös helpommin luettavassa muodossa, jossa numerot on korvattu nimillä, jotka vastaavat kyseistä solmukohtaa. Alla oleva kuva esittää rakennepuun alkukerrokset. Siinä puun alkupistettä kutsutaan juureksi (Root-Node). Sen alapuut ovat ccitt(0), iso(1) ja joint(2). Tässä kuvassa vain iso(1) sisältää alapuun ja kaksi muuta kohtaa ovat lehtiä (leaf node). (Mauro & Schmidt 2005, 24)



Kuva 18. Objektipuun ylimmät kerrokset. (Mauro & Schmidt 2005, 24)

Objektitunnukset voidaan merkitä numeroina 1.3.6.1 tai nimillä iso.org.dot.internet, kuten yllä olevasta kuvasta voi nähdä.

4 NAGIOS-OHJELMISTO

Nagios on avoimen lähdekoodin Linux/Unix -pohjalla toimiva järjestelmän- ja verkonvalvontaohjelmisto. Se voidaan määrittää tarkkailemaan isäntäkohteita sekä palveluita, joista on mahdollista saada myös sähköposti-ilmoituksia, jos asetetut hälytysparametrit ylittyvät. Joitain tärkeimpiä Nagioksen ominaisuuksia ovat:

- Verkkopalveluiden monitorointi (esimerkiksi SMTP, POP3, HTTP ja PING)
- Isäntäkohteen järjestelmäresurssien monitorointi (esimerkiksi prosessorikuormitus ja levytilan käyttö)
- Yksinkertainen ja joustava lisäosatuki, joka mahdollistaa omien palvelun tarkistukseen tehtyjen lisäosien käytön ja kehityksen
- Yhdensuuntaistetut palvelutarkastukset
- Ilmoitusviestien lähettäminen kohteiden tai palveluiden hälytysarvojen ylittymisestä käyttämällä sähköpostia, hakulaitetta tai muuta käyttäjän määrittämää yhteydenottotapaa
- Mahdollisuus asettaa tapahtumienkäsittelijöitä käynnistymään palveluiden ja kohteiden rinnalle ongelmien ennakoivan ratkaisun mahdollistamiseksi
- Automaattinen lokitiedostojen kierrättäminen
- Tuki reduntanttisen monitoroinnin määrittämiselle
- Vapaaehtoinen Web-käyttöliittymä, jolla voidaan tarkkailla esimerkiksi verkon tilaa, hälytysviesti- ja ongelmahistoriaa sekä lokitiedostoja (Nagios dokumentaatio, 4)

4.1 Lisäosat

Nagioksesta tekee tehokkaan se, että kohteiden ja palveluiden monitorointi voidaan suorittaa monilla eri tavoilla riippuen mitä lisäosaa käytetään. Jokainen näistä tavoista takaa luotettavan tiedon määritettyjen kohteiden tai palveluiden toimivuudesta. Nagioksen viralliset lisäosat sisältävät normaalitarpeisiin tarvittavat ominaisuudet ja toimintatavat. Näihin kuuluu esimerkiksi verkkopalveluiden tarkistus SNMP-protokollaa hyödyntäen. Jos tarvitaan joitakin erittäin edistyneitä tai harvinaisempia ominaisuuksia, niin lisäosia voi tehdä lisää tai ladata muiden käyttäjien tekemiä. (Kocjan, 2008, 87)

Nagios tekee tarkistuksia kohteisiin tai palveluihin suorittamalla lisäosien avulla ulkoisia komentoja, joista saadaan vastaukseksi palautuskoodi. Jokainen palautuskoodi sisältää oman ulostulonsa tietona, joka kertoo tarkistetun kohteen tai palvelun tilan. Komentojen velvollisuuksiin kuuluu varmistaa ja ilmoittaa onko kyseessä oleva kohde tai palvelu aktiivisena ja toimintakunnossa tarkistushetkellä. Nagios itse hoitaa kaikki sisäiset toiminnot ja komennot, kuten komentojen suorittamisen aikataulutuksen ja komentojen tuloksien varastoinnin. (Kocjan, 2008, 87)

Nagios vaatii, että kaikki lisäosat noudattavat tiettyä käyttäytymistä toimivuuden varmistamiseksi. Nämä käyttäytymissäännöt ovat yleisiä sekä kohde- että palvelutarkistuksille. Kaikille komennoille löytyy yhteiset pohjatason palautuskoodit. Nagios näyttää näiden koodien lisäksi myös kohteesta saatavat tulokset ja tiedot. (Kocjan, 2008, 87)

Exit code	Status	Description
0	OK	Working correctly
1	WARNING	Working, but needs attention (for example, low resources)
2	CRITICAL	Not working correctly or requires attention
3	UNKNOWN	Plugin was unable to determine the status for the host or service

Kuva 19. Komentojen yhteiset pohjatason palautuskoodit. (Kocjan, 2008, 87)

```
PING OK - Packet loss = 0%, RTA = 0.18 ms
DNS WARNING: 0.015 seconds response time
DISK CRITICAL - free space: /boot 18 MB (8% inode=99%)
```

Kuva 20. Esimerkki ulosannista, jossa näkyy palautuskoodin tila sekä tuloksien lisätiedot. (Kocjan, 2008, 87)

Nagioksen lisäosat käyttävät erityisiä parametreja, joilla voidaan tehdä määrityksiä toimintatapaan. Lisäosan tekijä määrittää mitä parametreja siinä voidaan käyttää. Kuitenkin useimmat komennot, jotka tulevat Nagioksen virallisten lisäosien mukana käyttävät standardeja määritysparametreja. Komennoilla, jotka varmistavat erilaisia taustaprosesseja käyttävät myös siihen tarkoitukseen määritettyjä standardeja parametreja. (Kocjan, 2008, 88)

Option	Description
-h, --help	Provide help
-V, --version	Print the exact version of the plugin
-v, --verbose	Make the plugin report more detailed information on what it is doing
-t, --timeout	Timeout (seconds); after this time plugin will report CRITICAL status
-w, --warning	Plugin-specific limits for the WARNING status
-c, --critical	Plugin-specific limits for the CRITICAL status
-H, --hostname	Host name, IP address or unix socket to communicate with
-4, --use-ipv4	Use IPv4 for network connectivity
-6, --use-ipv6	Use IPv6 for network connectivity

Kuva 21. Virallisten lisäosien standardit parametrit. (Kocjan, 2008, 88)

Option	Description
-p, --port	TCP or UDP port to connect to
-w, --warning	Response time that will issue a WARNING status (seconds)
-c, --critical	Response time that will issue a CRITICAL status (seconds)
-s, --send	String that will be sent to the server
-e, --expect	String that should be sent back from the server (option might be passed several times; see `--all` for details)
-q, --quit	String to send to the server to close the connection
-A, --all	In case multiple --expect parameters are passed, this option indicates that all responses need to be received; if this option is not present, at least one matching result indicates a success
-m, --maxbytes	The maximum number of bytes to read when expecting a string to be sent back from the server; after this number of bytes, a mismatch is assumed
-d, --delay	Delay in seconds between sending a string to server and expecting a response
-r, --refuse	Status that should be indicated in case the connection is refused (ok, warn, crit; defaults to crit)
-M	Status in case the expected answer is not returned by the server (ok, warn, crit; defaults to warn)
-j, --jail	Do not return output from the server in plugin output text
-D, --certificate	The number of days that the SSL certificate must still be valid; requires –ssl
-S, --ssl	Connect using SSL encryption
-E, --escape	Allows using \n, \r, \t or \\ in send or quit string; must be passed before --send or --quit option

Kuva 22. Standardit parametrit taustaprosessikomennoille. (Kocjan, 2008, 89)

4.2 Edistyneemmät toiminnot

Koska Nagios varastoi tarkistuksien tulostietoja, niin on järkevää käyttää niitä jollain tapaa hyödyksi. Yksi parhaimmista työkaluista tähän on graafisen kuvaajan käyttö. Yksi suosituimmista graafisista kuvaajista Nagiokselle on lisäosa nimeltä nagios-graph. Se prosessoi Nagioksen varastoiman tiedon palvelutarkistuksista ja sijoittaa ky-

seiset tiedot yhteen tai useampaan tietokantaansa. Kuvaajat voidaan määrittää näkymään suoraan Nagioksen Web-käyttöliittymässä. Kuvaajat näyttävät tiedot päivän, viikon sekä kuukauden aikajaksoilta. (nagiosgraph dokumentaatio)

Nagiosgraphin toiminta jakautuu kahteen osaan eli Nagioksen palvelutarkistusten tiedon keräämiseen sekä kuvaajien piirtämiseen niiden tietojen pohjalta. Kaikki kerätty tieto varastoidaan RRD-tiedostoihin. Map-tiedosto määrittää miten Nagiokselta saatu tieto nimetään ja mihin RRD-tiedostoihin se syötetään. Map-tiedosto myös prosessoi tiedon esimerkiksi vaihtamalla yksiköitä. Kyseinen map-tiedosto on perl-koodia, joka sisältää yleisen säännön lisäosien tuottaman tiedon keräämiseen ja hyödyntämiseen. (nagiosgraph dokumentaatio)

Kuvaajia varten nagiosgraph käyttää cgi-skriptejä. Pääskripti nimeltä show.cgi kerää tarvittavat tiedot yksittäiselle kohteelle tai palvelulle ja tuottaa oikeanlaiset kuvaajat. Muut skriptit näyttävät kaikki kohteet tietylle palvelulle, kaikki palvelut tietylle kohteelle tai vaihtoehtoiset erikseen määritetyt kohde- ja palveluryhmät. Nämä skriptit ajetaan oletuksen minimimäärityksillä, mutta ne voidaan myös muokata käyttämällä määritystiedostoa. (nagiosgraph dokumentaatio)

Hyödyllisiin edistyneisiin toimintoihin kuuluu myös hälytysviestien automaattinen lähetys. Nagios voidaan määrittää lähettämään automaattisesti hälytysviestejä, kun havaitaan ongelmia tai kun niistä palaudutaan. Hälytysviestit lähetetään oletuksena sähköpostilla, joka on ainut Nagiokseen valmiiksi sisältyvä metodi. Erilaisilla lisäosilla ja ohjelmallisilla tukirakenteilla voidaan saada määritettyä hälytysviestien lähetys esimerkiksi tekstiviestillä tai hakulaiteilmoituksena. (Kocjan, 2008, 137)

Value	Description
PROBLEM	A service or host has just entered (or is still in) a problem state. If this is a service notification, it means the service is either in a WARNING, UNKNOWN or CRITICAL state. If this is a host notification, it means the host is in a DOWN or UNREACHABLE state.
RECOVERY	A service or host recovery has occurred. If this is a service notification, it means the service has just returned to an OK state. If it is a host notification, it means the host has just returned to an UP state.
ACKNOWLEDGEMENT	This notification is an acknowledgement notification for a host or service problem. Acknowledgement notifications are initiated via the web interface by contacts for the particular host or service.
FLAPPINGSTART	The host or service has just started flapping.
FLAPPINGSTOP	The host or service has just stopped flapping.
FLAPPINGDISABLED	The host or service has just stopped flapping because flap detection was disabled..
DOWNTIMESTART	The host or service has just entered a period of scheduled downtime. Future notifications will be supressed.
DOWNTIMESTOP	The host or service has just exited from a period of scheduled downtime. Notifications about problems can now resume.
DOWNTIMECANCELLED	The period of scheduled downtime for the host or service was just cancelled. Notifications about problems can now resume.

Kuva 23. Taulukko, joka kuvaa eri hälytysviestitapahtumia. (Kocjan, 2008, 138)

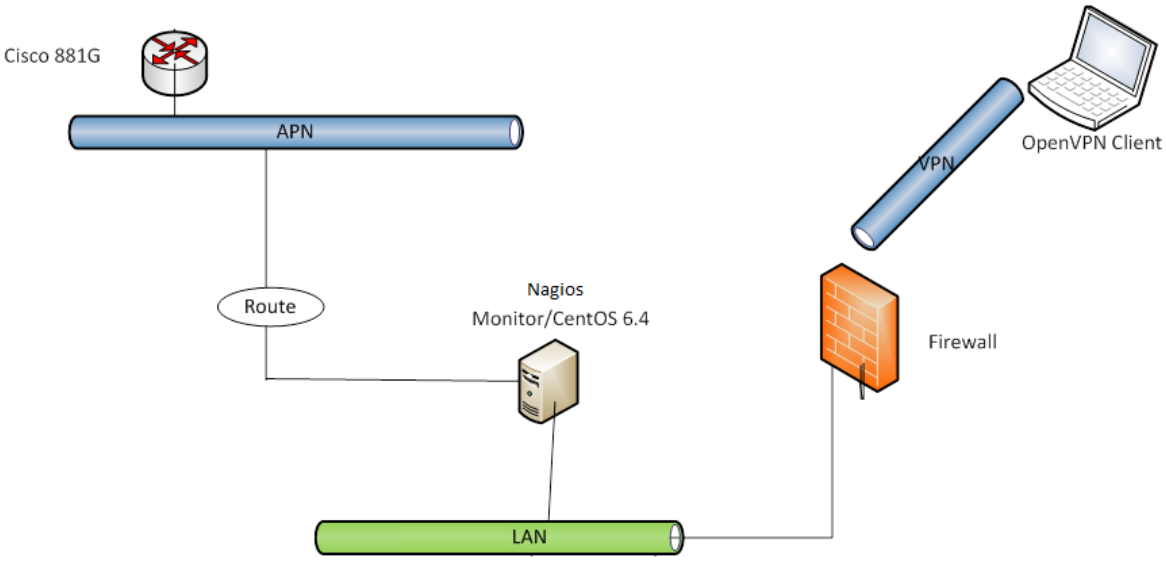
Yllä olevassa kuvassa näkyy tapahtumatilat, jotka voivat aiheuttaa hälytys- tai ilmoitusviestin. Nämä tilat ovat ongelma, palautuminen, kuittaus, tilojen vaihtelut ja häiriöaika. Esimerkiksi, jos palvelu joutuu kriittiseen tai muuhun ongelmatilaan tai mikäli ongelmasta palautuminen, kuittaus, häiriöaika tai palvelutilojen jatkuva muutos ilmaantuu, niin hälytysviestin lähettäminen laukaistaan. (Kocjan, 2008, 138)

5 KÄYTÄNNÖN TOTEUTUS

Alkutilanteessa kohdeverkkoon oli asennettu valmiiksi Linux-koneen pohja, jota oli tarkoitus rakentaa eteenpäin tarpeiden mukaan siihen pisteeseen asti, että saatiin Nagios asennettua toimintakuntoon.

Tehtävänä oli ensin saada VPN-yhteys kohdeverkkoon auki, jonka jälkeen SSH-yhteyden avulla täytyi saada Linux-koneen komentorivi esiin. Tarkoituksena oli komentorivin kautta saada graafinen käyttöliittymä ja VNC-palvelin asennettua etäyhteyden mahdollistamiseksi.

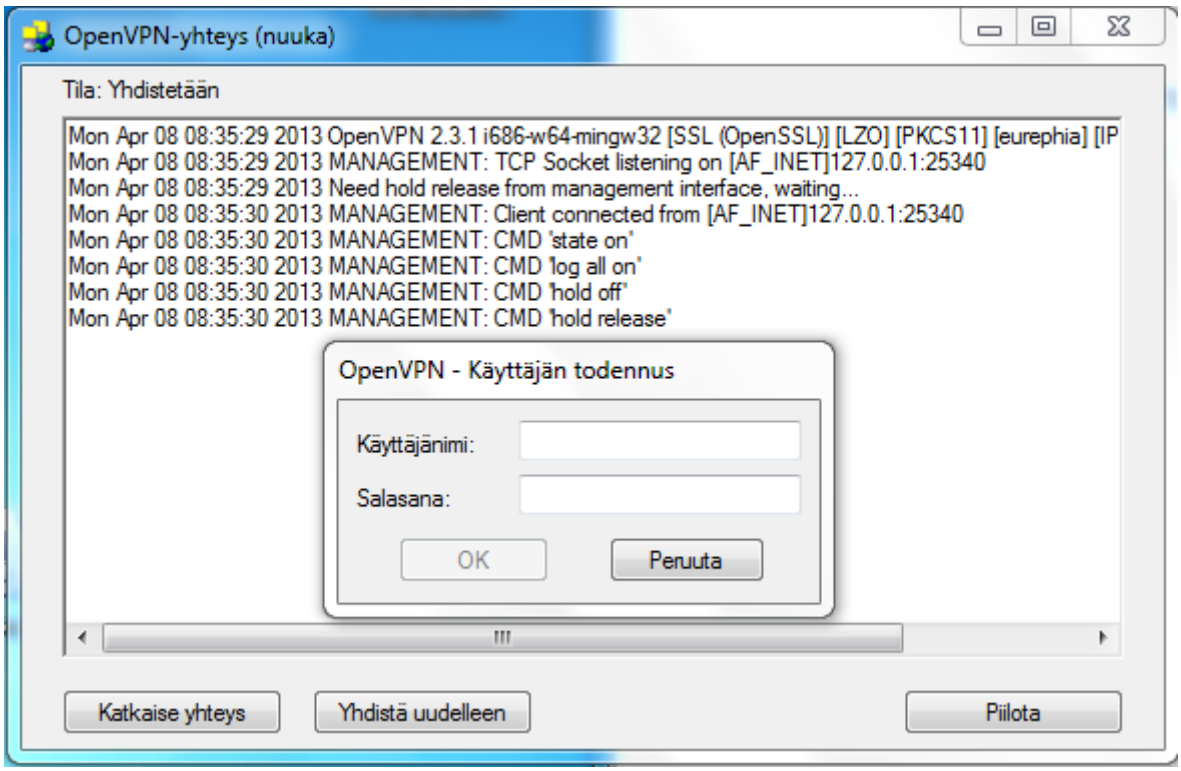
Nagios sekä tarvittavat lisäosat täytyi saada asennettua ja määriteltyä siten, että vaaditut toiminnot ja valvonnan vaatimat tarkistukset saatiin haluttuun toimintakuntoon. Web-käyttöliittymä oli myös määrä saada näkymään suoraan verkkoselaimen kautta, jonka vuoksi Linux-koneen palomuurisääntöjä täytyi muokata.



Kuva 24. Kytkentäkaavio.

5.1 Valmistelu

Aluksi tarkoitus oli ottaa VPN-yhteys Nuukan verkkoon, jossa tarvittu Linux-kone sijaitsi. Käyttöön saatiin tarvittavat yhteysmääritystiedostot, joiden avulla oli tarkoitus saada VPN-yhteys auki käyttäen OpenVPN Desktop Clienttiä. Huomattiin, että yhteyttä ei saatu muodostettua kokonaan. Yhteys aukesi osaksi, mutta pysähtyi Obtaining Configuration -tilaan. Lokitiedostoja tarkastelemalla havaittiin, että ohjelma ei osannut käyttää hyväksi asetusmääritystiedostoja. Asennus aloitettiin alusta asentamalla OpenVPN Desktop Clientin community-versio ja sijoittamalla tarvittavat yhteysmääritystiedostot config-alakansioon. Tämän jälkeen käynnistettiin ohjelma, joka avasi tunnuksia vastaan yhteyden kohdeverkkoon. VPN-yhteyden auettua otettiin SSH-yhteys tarvittuun Linux-koneeseen, johon Nagios oli tarkoitus asentaa.



Kuva 25. OpenVPN Community Desktop Client.

Linux-koneessa oli aluksi minimaalinen asennus, joten siihen asennettiin graafinen käyttöliittymä (Gnome GUI) komennolla **yum groupinstall basic-desktop desktop-platform x11 fonts**. Myös VNC päätettiin asentaa, jotta olisi mahdollista ottaa etäyhteydellä työpöytänäkymä Windows-koneelle. VNC:n asennuksessa käytettiin komentoja **sudo yum install tigervnc-server** ja **sudo yum install vnc**. Seuraavaksi asetettiin VNC-palvelin käynnistymään käynnistyksen yhteydessä komennolla **sudo chkconfig vncserver on** ja VNC-salasana asetettiin komennolla **vncpasswd**. Tämän jälkeen lisättiin vncservers-määritystiedostoon seuraavat rivit:

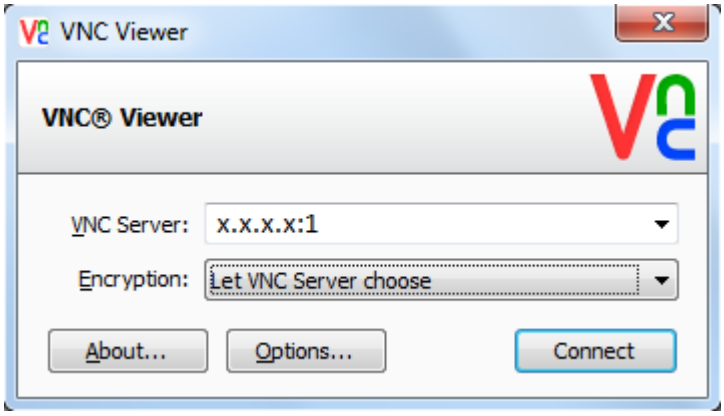
- VNCSERVERS=”1:root”
- VNCSERVERARGS[1]=-geometry 1024x600

VNC vaati toimiakseen myös IP-taulujen muokkausta, joka tapahtui komennoilla:

- sudo iptables -I INPUT 5 -m state --state NEW -m tcp -p tcp -m multiport --dports 5901:5903,6001:6003 -j ACCEPT
- sudo service iptables save

- sudo service iptables restart

Edellä olevien määritysten jälkeen VNC-palvelin piti käynnistää uudelleen käskyllä **sudo service vncserver restart** ja tappaa palvelinprosessi käskyllä **vncserver -kill :1**. Lopuksi VNC:n xstartup-määritystiedostoon lisättiin rivi **exec gnome-session &** sekä käytöstä poistettiin rivi **twm &**. Tämän päätteeksi VNC-palvelin käynnistettiin uudelleen. Käyttämällä VNC Viewer -ohjelmaa ja yhdistämällä oikeaan osoitteeseen oikealla käyttäjällä (IP-osoite:1) saatiin Linux-koneen työpöydän näkymään etänä Windows-koneella.



Kuva 26. VNC Viewer -etähallintaohjelma.

Mikäli halutaan useamman käyttäjän samanaikainen VNC-yhteys, niin pitää lisätä uusi käyttäjä komennolla **sudo adduser käyttäjänimi** sekä määrittää lisätylle käyttäjälle salasana komennolla **sudo passwd käyttäjänimi**. Uuden käyttäjän kanssa pitää ottaa superuser-oikeudet komennolla **su käyttäjänimi** sekä määrittää VNC-salasana komennolla **vncpasswd**. Lisäksi vncservers-määritystiedostoon täytyy lisätä uusi käyttäjä ensimmäisen käyttäjän rinnalle ja määrittää lisätylle käyttäjälle resoluutio. Lopuksi VNC-palvelin pitää käynnistää uudelleen, tappaa prosessi ja käynnistää vielä uudelleen. Tämän jälkeen yhteyden saa auki VNC Viewer -ohjelmaa käyttämällä lisätyn käyttäjän käyttäjänumeroa (IP-osoite:2).

5.2 Nagioksen asennus

Aluksi jouduttiin asentamaan Apache, PHP, GlibC, MySQL sekä GD -paketit, joita Nagios vaatii toimiakseen. Pakettien asentaminen tapahtui komennoilla:

- yum install httpd php
- yum install gcc glibc glibc-common
- yum install gd gd-devel
- yum install mysql mysql-devel

Pakettien asentamisen jälkeen luotiin Nagiosta varten uusi käyttäjä nimeltä nagios ja määritettiin lisätylle käyttäjälle salasana. Web-käyttöliittymän kautta tehtävien ulkoisten komentojen sallimiseksi piti myös määrittää käyttäjäryhmä, johon lisättiin käyttäjät nagios ja apache.

```
/usr/sbin/groupadd nagcmd
/usr/sbin/usermod -a -G nagcmd nagios
/usr/sbin/usermod -a -G nagcmd apache
```

Kuva 27. Komentoryhmän luominen.

Juureen tehtiin downloads-kansio, johon ladattiin Nagioksen sekä lisäosien asennuspaketit.

```
wget http://prdownloads.sourceforge.net/sourceforge/nagios/nagios-3.2.3.tar.gz
wget http://prdownloads.sourceforge.net/sourceforge/nagiosplug/nagios-plugins-1.4.11.tar.gz
```

Kuva 28. Pakettien latauskomennot.

Nagios-paketti purettiin komennolla **tar xzf nagios-3.2.3.tar.gz** ja siirryttiin purettuun kansioon, jossa ajettiin määritysskripta komennolla **./configure --with-command-group=nagcmd**. Lopuksi lähdekoodi käännettiin komennolla **make all**. Kääntämisen jälkeen asennettiin tiedostot, skriptat ja esimerkkimääritystiedostot sekä asetettiin oikeudet ulkoisten komentojen hakemistoon.

```
make install

make install-init

make install-config

make install-commandmode
```

Kuva 29. Asennuskomennot.

Nagioksen Web-käyttöliittymän määritystiedostot asennettiin komennolla **make install -webconf**. Web-käyttöliittymää varten luotiin tunnus nimeltä nagiosadmin. Apache käynnistettiin uudelleen komennolla **service httpd restart**. Lopuksi purettiin, käännettiin ja asennettiin nagioksen lisäosat.

```
cd ~/downloads

tar xzf nagios-plugins-1.4.11.tar.gz

cd nagios-plugins-1.4.11
```

Kuva 30. Purku- ja kääntämiskomennot.

```
./configure --with-nagios-user=nagios --with-nagios-group=nagios

make

make install
```

Kuva 31. Määritys- ja asennuskomennot.

Nagios lisättiin järjestelmäpalveluiden listalle, jotta se käynnistyy Linux-koneen käynnistyksen yhteydessä. Tämä tapahtui komennoilla **chkconfig --add nagios** ja **chkconfig nagios on**. Lopuksi Nagioksen määritystiedostot verifioitiin ja Nagios käynnistettiin komennoilla **/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg** ja **service nagios start**.

Huomattiin, että Nagioksesta löytyi vielä uudempi versio (3.5.0), joten se päivitettiin ajantasalle.

5.3 Nagioksen määrittely

Linux-koneen toisen verkkokortin osoitte määritettiin oikeaksi siten, että saatiin yhteys valvottavaksi tarkoitettujen laitteiden suuntaan. Tämän lisäksi määritettiin myös staattinen reitti valvottavien laitteiden verkkoa kohti. Palomuurin määritystyökalu asennettiin komennolla **yum install system-config-firewall**. Tämän jälkeen tehtiin kyseisen työkalun kautta sääntö palomuuriin, joka sallii sisään tulevan HTTP-yhteyden. Tämä mahdollisti sen, että VPN-yhteyden ollessa auki Nagioksen Web-käyttöliittymän sai auki suoraan menemällä selaimella osoitteeseen http://x.x.x.x/nagios.

5.3.1 Valvottavat kohteet

Määrittelyt aloitettiin lisäämällä yksi valvottava kohde ja sille joitain valvottavia palveluita, kuten ping ja porttilinkkien tila. Valvottavat kohteet, palvelut ja kohderyhmät lisättiin alla olevien kuvien mukaisesti tekemällä määritykset switch.cfg -tiedostoon.

```
define host{
        use             generic-switch
        host_name       Cisco-881g
        alias           Cisco 881g 3G Router
        address         x.x.x.x
        hostgroups      switches
        }
```

Kuva 32. Valvottavan kohteen lisääminen, tässä tapauksessa Cisco 881g 3G reititin.

```
define hostgroup{
        hostgroup_name  switches
        alias           Network Switches
        }
```

Kuva 33. Kohderyhmä, johon kaikki haluttavat kohteet liitetään.

```
define service{
        use                     generic-service
        host_name               Cisco-881g
        service_description     PING
        check_command           check_ping!200.0,20%!600.0,60%
        normal_check_interval   1

        retry_check_interval    1
        }
```

Kuva 34. Ping-palvelun lisääminen 3G-reitittimen valvottavien palveluiden listalle.

Yllä lisätty ping-mittauspalvelu kuuluu vakiomittauksiin, johon riittää integroitu check_ping -lisäosa. Mikäli halutaan tehdä IP SLA-mittauksia yhteyksien suorituskyvyistä, niin tarvitsemme check_snmp-lisäosaa. Tämän lisäosan avulla voidaan hakea laitteeseen määritettyjen erinäisten operaatioiden mittaamia tuloksia MIB-tietokannoista OID:n avulla. Käytimme pääsääntoisesti hyväksi Ciscon SNMP Object Navigator -työkalua, jolla pystyi selaamaan ja etsimään halutut objektitunnukset. Näillä objektitunnuksilla oli mahdollista saada halutut palvelut määritetyksi Nagioksen valvottavaksi. Objektitunnuksen viimeinen numero määräytyy valvottavaan kohteeseen määritetyn operaation prosessinumeron tai mahdollisen portin perusteella. Kaikki IP SLA -objektitunnukset löytyvät CISCO-RTTMON-MIB -taulukosta eli polusta enterprises.9.9.42. Alla oleva kuva on esimerkki kyseisestä palvelusta.

```
define service{
        use                     generic-service,graphed-service
        host_name               Cisco-881g
        service_description     ICMP Echo RTT
        check_command           check_snmp!-C public -o enterprises.9.9.42.1.2.10.1.1.5.3 -r 1 -m RFC1213-MIB
        normal_check_interval   1
        }
```

Kuva 35. IP SLA-mittausoperaatio, joka on määritetty käyttämällä objektitunnusta.

5.3.2 Graafiset kuvaajat

Kohteiden ja palveluiden lisäämisen jälkeen asennettiin nagiosgraph-lisäosa, jolla on mahdollista saada palveluista graafiset kuvaajat näkyviin. Kuvaajat näyttävät päivän, viikon ja kuukauden aikajaksojen mittaustulokset. Ensin asennettiin perl-rrdtool ja perl-GD -paketit. Tämän jälkeen ladattiin nagiosgraph sekä purettiin ja asennettiin se Nagioksen hakemistoon. Asennuksen jälkeen tehtiin tarvittavat määritykset, joista tärkeimpiä olivat nagiosgraphin päämääritystiedostoon muokatut tiedosto- ja hakemisto-

polut lokitiedostoille, ohjaustiedostolle sekä muille tarvittaville tiedostoille. Myös käyttöoikeudet määritettiin nagiosgraphin tiedostoille ja hakemistoille siten, että lukeminen ja kirjoittaminen olivat mahdollista. Lopuksi lisättiin Nagioksen commands.cfg sekä templates.cfg -tiedostoihin määritykset, jotka mahdollistivat nagiosgraphin toiminnan ja käyttöönoton alla olevan kuvan mukaisesti. Graafiset kuvaajat saatiin käyttöön lisäämällä graphed-service -komento halutuiden palveluiden määrityksiin.

```
define command {
  command_name  process-service-perfdata
  command_line  /usr/local/nagios/libexec/insert.pl
}
```

Kuva 36. Määritys, joka sallii datan keräämisen nagiosgraphin kuvaajia varten.

```
define service {
      name graphed-service
      action_url /nagiosgraph/cgi-bin/show.cgi?host=$HOSTNAME$&service=$SERVICEDESC$'
                 onMouseOver='showGraphPopup(this)' onMouseOut='hideGraphPopup()'
                 rel='/nagiosgraph/cgi-bin/showgraph.cgi?
                 host=$HOSTNAME$&service=$SERVICEDESC$&period=week&rrdopts=-w+450+-j
      register 0
      }
```

Kuva 37. Määritys, jolla saadaan graphed-service niminen palvelupohja käyttöön.

```
define service{
        use                     generic-service,graphed-service
        host_name               Cisco-881g
        service_description     Total Processes
        check_command           check_snmp!-C public -o hrSystemProcesses.0
        normal_check_interval   1
        }
```

Kuva 38. Palvelu, johon on määritetty graafisen kuvaajan käyttö graphed-service komennon avulla.

Alla olevassa kuvassa on esimerkkinä Nagios-palvelimen prosessimäärää esittävä graafinen kuvaaja. Siinä näkyy päivä-, viikko- ja kuukausikohtaiset kuvaajat. Kuvissa näkyvät mittaamattomat hetket johtuvat siitä, että Nagios oli pysäytettynä kyseisinä ajankohtina.

Kuva 39. Nagiosgraphin tuottamia graafisia kuvaajia.

5.3.3 Automaattiset sähköposti-ilmoitukset

Koska verkonvalvoja ei voi tarkkailla verkon tilaa jatkuvasti, oleellinen toiminto on automaattiset varoitus- ja hälytysviestit. Tästä johtuen määritettiin sähköposti-ilmoitukset käyttöön, kun verkossa havaitaan ongelmia. Varoituksille ja kriittisille tilanteille voidaan määrittää ilmoitusherkkyydet halutuiksi. Tätä varten täytyi luoda Nagioksen templates.cfg sekä contacts.cfg -tiedostoihin alla olevien kuvien mukaiset kontaktimääritykset.

```
define contact{
        contact_name                    nagiosadmin
        use                             generic-contact
        alias                           Nagios Admin

        email                           esimerkki@osoite.fi
        }
```

Kuva 40. Kontaktimääritys, joka kertoo minne ilmoitukset lähetetään.

```
define contact{
        name                            generic-contact
        service_notification_period     24x7
        host_notification_period        24x7
        service_notification_options    w,u,c,r,f,s
        host_notification_options       d,u,r,f,s
        service_notification_commands   notify-service-by-email
        host_notification_commands      notify-host-by-email
        register                        0
        }
```

Kuva 41. Yhteinen pohja ilmoitusviesteille.

Kontaktipohjalla voidaan määrittää oletukset ilmoitusherkkyyksille seuraavien parametrien avulla:

- w = ilmoitus asetetun varoitusarvon ylittämisestä
- c = ilmoitus kriittisistä tiloista
- r = ilmoitus ongelmista palautumisesta
- f = ilmoitus tilojen nopeiden vaihteluiden alkamisesta tai loppumisesta
- d = ilmoitus, mikäli palvelut tai portit menevät alas (down states)
- u = ilmoitus palveluiden tai kohteiden saavuttamattomuudesta
- s = ilmoitus pysähtyneistä palveluista

Lopuksi määritettiin kontaktiryhmä sisältämään aikaisemmin luodun kontaktin. Kontaktiryhmä täytyi lisätä jokaiseen palveluun tai kohteeseen, johon ilmoitukset haluttiin ottaa käyttöön.

```
define contactgroup{
        contactgroup_name       admins
        alias                   Nagios Administrators
        members                 nagiosadmin
        }
```

Kuva 42. Kontaktiryhmän määritys contacts.cfg -tiedostossa.

```
define host{
        use             generic-switch
        host_name       Cisco-881g
        alias           Cisco 881g 3G Router
        address         x.x.x.x
        hostgroups      switches
        }
```

Kuva 43. Määritys, jossa ilmoitukset on otettu käyttöön kaikille kyseisen kohteen palveluille.

Sähköposti-ilmoitusten määritykset asetettiin valmiiksi siten, että ylläpitäjän sähköpostiosoite täytyy vain vaihtaa oikeaksi contacts.cfg tiedostoon ja käynnistää Nagios uudelleen. Tämän seurauksena ongelmista lähetetään automaattisesti ilmoitus- tai hälytysviesti. Asetetut raja-arvot switch.cfg tiedostossa on muokattavissa mieleisiksi.

Koska Nagios maskeeraa sähköpostiviestit, niin sähköpostiosoitteessa näkyvä verkkoaluetunnus ei ole aito. Tämän takia viestit voivat helposti ohjautua roskapostikansioon tai joutua kokonaan estetyksi sähköpostipalvelimen toimesta, joten roskapostisuodattimia voi ehkä joutua muokkaamaan, jotta viestit pääsevät läpi.

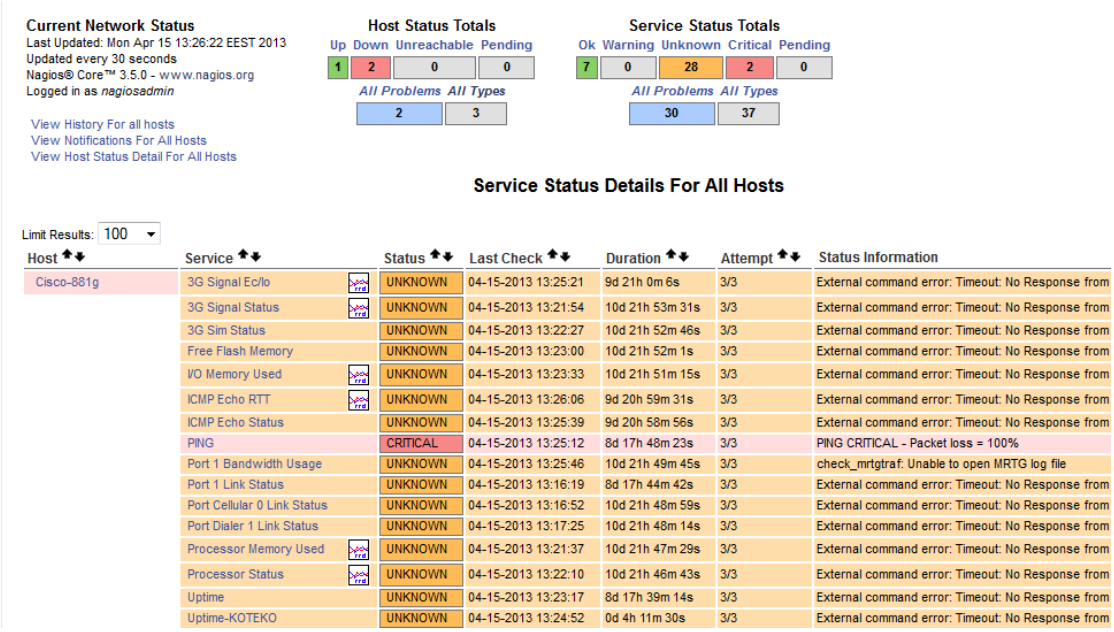
6 YHTEENVETO

Opinnäytetyön tavoitteeksi saatiin asentaa Linux-pohjalla toimiva Nagios-verkonvalvontaohjelmisto, jossa oli tarkoitus hyödyntää IP SLA -mittauksia ja monitoroida Nagioksen avulla kohdeverkossa olevia 3G-reitittimiä. Tärkeää oli myös määrittää Nagios lähettämään automaattisesti ilmoitus- ja hälytysviestejä ongelmatilanteissa.

Työ aloitettiin päivittämällä ja asentamalla tarvittavat paketit ja ohjelmistot Linux-koneeseen, jonka jälkeen sen ohelle asennettiin Nagios-verkonvalvontaohjelmisto. Nagiokseen tehtiin tarvittavat määritykset, joihin sisältyi valvottavien kohteiden ja palveluiden lisääminen, graafiset kuvaajat, sähköposti-ilmoitukset sekä muita pieniä operaatioita, joilla saatiin hiottua Nagiosta hieman paremmaksi.

Työosuuden loppuvaiheessa Nagios oli määritetty niin valmiiksi kuin mahdollista, mutta aikataulun kireyden ja ulkoisten syiden takia yhteyttä valvottaviin laitteisiin ei ehditty saada. Tämän takia palvelut ja kohteet lisättiin valmiiksi siten, että kun laitteet

tulevaisuudessa saadaan yhdistettyä, niin monitorointi pitäisi kuitenkin toimia suoraan. Tästä johtuen alla olevassa kuvassa ei saada mittaustuloksia kohteilta tai palveluilta.



Current Network Status
Last Updated: Mon Apr 15 13:26:22 EEST 2013
Updated every 30 seconds
Nagios® Core™ 3.5.0 - www.nagios.org
Logged in as *nagiosadmin*

View History For all hosts
View Notifications For All Hosts
View Host Status Detail For All Hosts

Host Status Totals

Up	Down	Unreachable	Pending
1	2	0	0

All Problems	All Types
2	3

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
7	0	28	2	0

All Problems	All Types
30	37

Service Status Details For All Hosts

Limit Results: 100

Host	Service	Status	Last Check	Duration	Attempt	Status Information
Cisco-881g	3G Signal Ec/Io	UNKNOWN	04-15-2013 13:25:21	9d 21h 0m 6s	3/3	External command error: Timeout: No Response from
	3G Signal Status	UNKNOWN	04-15-2013 13:21:54	10d 21h 53m 31s	3/3	External command error: Timeout: No Response from
	3G Sim Status	UNKNOWN	04-15-2013 13:22:27	10d 21h 52m 46s	3/3	External command error: Timeout: No Response from
	Free Flash Memory	UNKNOWN	04-15-2013 13:23:00	10d 21h 52m 1s	3/3	External command error: Timeout: No Response from
	I/O Memory Used	UNKNOWN	04-15-2013 13:23:33	10d 21h 51m 15s	3/3	External command error: Timeout: No Response from
	ICMP Echo RTT	UNKNOWN	04-15-2013 13:26:06	9d 20h 59m 31s	3/3	External command error: Timeout: No Response from
	ICMP Echo Status	UNKNOWN	04-15-2013 13:25:39	9d 20h 58m 56s	3/3	External command error: Timeout: No Response from
	PING	CRITICAL	04-15-2013 13:25:12	8d 17h 48m 23s	3/3	PING CRITICAL - Packet loss = 100%
	Port 1 Bandwidth Usage	UNKNOWN	04-15-2013 13:25:46	10d 21h 49m 45s	3/3	check_mrtgtraf: Unable to open MRTG log file
	Port 1 Link Status	UNKNOWN	04-15-2013 13:16:19	8d 17h 44m 42s	3/3	External command error: Timeout: No Response from
	Port Cellular 0 Link Status	UNKNOWN	04-15-2013 13:16:52	10d 21h 48m 59s	3/3	External command error: Timeout: No Response from
	Port Dialer 1 Link Status	UNKNOWN	04-15-2013 13:17:25	10d 21h 48m 14s	3/3	External command error: Timeout: No Response from
	Processor Memory Used	UNKNOWN	04-15-2013 13:21:37	10d 21h 47m 29s	3/3	External command error: Timeout: No Response from
	Processor Status	UNKNOWN	04-15-2013 13:22:10	10d 21h 46m 43s	3/3	External command error: Timeout: No Response from
	Uptime	UNKNOWN	04-15-2013 13:23:17	8d 17h 39m 14s	3/3	External command error: Timeout: No Response from
	Uptime-KOTEKO	UNKNOWN	04-15-2013 13:24:52	0d 4h 11m 30s	3/3	External command error: Timeout: No Response from

Kuva 44. Yleinen näkymä Cisco reitittimen palveluiden tilasta.

6.1 Jatkokehitysmahdollisuudet

Tarkempien IP SLA -mittauksien kannalta kohdelaitteeseen pitäisi saada käynnistettyä IP SLA Responder-palvelu. Kyseinen palvelu mahdollistaa tarkemmat mittaustulokset ja yhteyden suorituskyvyn mittaamisen molempiin suuntiin. Monet mittausoperaatiot vaativat Responder-palvelun toimiakseen. Sitä hyödyntäen pystyisi käyttämään useita UDP-protokollaa käyttäviä mittausoperaatiota ICMP:n sijaan. UDP Jitter -operaation hyötyihin kuuluu erilaiset pakettitason mittaukset, kuten pakettihävikki, pakettien väliset viiveet ja latenssit sekä monia muita mittauksia. Jitter-operaation mittaustuloksien objektitunnuksia löytyy polusta enterprises.9.9.42.1.3.5. ICMP Jitter -operaatioiden mittaustuloksien objektitunnuksien taulukko löytyy polusta enterprises.9.9.42.1.3.8.

6.1.1 IP SLA -mittausoperaatioiden luominen SNMP:llä

Myös snmpset-komentoa päätettiin tutkia kevyesti. Sillä on mahdollisuus luoda IP SLA -mittausoperaatioita syöttämällä parametritiedot suoraan MIB-tietokantoihin objektitunnuksien avulla. Tämä on erittäin mielenkiintoinen ja kätevä ratkaisu komento-

jen ja määritysten tekeminen etänä, joten sen tarjoamia mahdollisuuksia kannattaisi tutkia tarkemmin.

Kokeilu aloitettiin määrittämällä ICMP Echo -mittausoperaatio syöttämällä snmpset-aloituskomento, jonka jälkeen rivi kerrallaan määritettiin halutut parametrit käyttämällä niitä vastaavia objektitunnuksia. Ensin ei saatu suoritettua lisäyskomentoa loppuun asti, koska vastaan tuli **Error in packet. Reason: noAccess** -virhesanoma. Tästä pääteltiin, että ei ollut tarvittavia oikeuksia tietojen kirjoittamiseen kyseisiin MIB-tietokantoihin. Asiaa hieman pintaa syvemmältä tutkittua opittiin, että ensin täytyi lisätä kirjoitusoikeudet kyseessä olevan laitteen snmp-määrityksiin. Kun määrityksiin lisättiin kirjoitusoikeudet private-käyttäjälle, niin saatiin suoritettua lisäyskomento onnistuneesti loppuun, jonka tuloksena laitteeseen käynnistyi kyseinen haluttu IP SLA mittausoperaatio.

Parametrit, jotka testin vuoksi määritettiin, ovat:

- rttMonCtrlAdminStatus, joka määrittää kyseisen operaation luonnin ja mahdollisen käynnistyksen riippuen syötetystä integer-arvosta

- rttMonCtrlAdminRttType, jolla määritetään mittausoperaation tyyppi integer-arvona

- rttMonEchoAdminProtocol, jonka avulla määritetään protokolla integer-arvona, jota halutaan käyttää

- rttMonEchoAdminTargetAddress, eli kohdeosoite jonka syötimme hexa-arvoina (172.16.120.30 = AC 10 78 1E)

Alla olevat kuvat selventävät tilanteita.

```
snmp-server community public RO
snmp-server community private RW
snmp-server host 172.16.120.10 version 2c private
snmp-server host 172.16.120.10 version 2c public
```

Kuva 45. Eri "käyttäjien" oikeuksien määritys. RO = vain luku, RW = luku ja kirjoitus.

```
[root@Nagios /]# snmpset -v2c -c private 172.16.120.20 enterprises.9.9.42.1.2.1.1.9.5 i 4
enterprises.9.9.42.1.2.1.1.4.5 i 1 enterprises.9.9.42.1.2.2.1.1.5 i 2 enterprises.9.9.42.1
.2.2.1.2.5 x 'AC 10 78 1E'
SNMPv2-SMI::enterprises.9.9.42.1.2.1.1.9.5 = INTEGER: 4
SNMPv2-SMI::enterprises.9.9.42.1.2.1.1.4.5 = INTEGER: 1
SNMPv2-SMI::enterprises.9.9.42.1.2.2.1.1.5 = INTEGER: 2
SNMPv2-SMI::enterprises.9.9.42.1.2.2.1.2.5 = Hex-STRING: AC 10 78 1E
[root@Nagios /]#
```

Kuva 46. Snmpset-komento sekä haluttujen parametrien määritykset.

```
IP SLAs Infrastructure Engine-III
Entry number: 5
Owner:
Tag:
Operation timeout (milliseconds): 5000
Type of operation to perform: icmp-echo
Target address/Source address: 172.16.120.30/0.0.0.0
Type Of Service parameter: 0x0
Request size (ARR data portion): 28
Verify data: No
Vrf Name:
Schedule:
   Operation frequency (seconds): 60  (not considered if randomly scheduled)
   Next Scheduled Start Time: Pending trigger
   Group Scheduled : FALSE
   Randomly Scheduled : FALSE
   Life (seconds): 3600
   Entry Ageout (seconds): never
   Recurring (Starting Everyday): FALSE
   Status of entry (SNMP RowStatus): Active
Threshold (milliseconds): 5000
Distribution Statistics:
   Number of statistic hours kept: 2
   Number of statistic distribution buckets kept: 1
   Statistic distribution interval (milliseconds): 20
Enhanced History:
History Statistics:
   Number of history Lives kept: 0
   Number of history Buckets kept: 15
   History Filter Type: None
```

Kuva 47. Show ip sla configuration 5 -komennon näyttämät tiedot lisätystä operaatiosta.

6.1.2 Syslogien hakeminen SNMP:llä

IP SLA voi luoda järjestelmälokiviestejä (syslog), kun reaktiotila ilmaantuu. Järjestelmälokiviestejä voidaan lähettää SNMP-trapseina käyttämällä CISCO-RTTMON-MIB:iä. IP SLA:n SNMP-trapsit ovat tuettuja sekä CISCO-RTTMON-MIB:ssä että CISCO-SYSLOG-MIB:ssä.

Syslogin toimintojen käyttöönottamiseksi tarvitaan ainakin komennot ip sla reaction-configuration, jolla saadaan operaation pohja tehtyä sekä komento ip sla logging traps, joka määrittää syslog-viestit aktiiviseksi. Edellä mainittujen lisäksi tarvitaan vielä ainakin snmp-server enable traps syslog -komento, jolla saadaan järjestelmä luomaan CISCO-SYSLOG-MIB trapseja.

Koska aika loppui kesken, niin ei ehditty tutkia syslog-viestejä tarkemmin, joten se päätettiin jättää seuraaville tekijöille. Ehdittiin kuitenkin raapaista pintaa sen verran, että syslogien avulla pitäisi saada generoitua ja lähetettyä melko kattavia häiriöilmoituksia vikatilanteiden sattuessa. Syslogien MIB-tietokannat löytyvät polusta enterprises.9.9.41.

LÄHTEET

Cisco IOS IP Service Level Agreements User Guide. Dokumentti. Saatavissa: http://www.cisco.com/en/US/technologies/tk648/tk362/tk920/technologies_white_paper09186a00802d5efe.html [viitattu 23.4.2013]

Hakala M. & Vainio M. 2005. Tietoverkon rakentaminen. Docendo Finland Oy, Jyväskylä.

IP SLAs Configuration Guide, Cisco IOS Release 12.4T. Verkkojulkaisu. Saatavissa: http://www.cisco.com/en/US/docs/ios-xml/ios/ipsla/configuration/12-4t/sla-12-4t-book.pdf [viitattu 17.4.2013]

IP SLAs - Multiple Operation Scheduling. Dokumentti. Saatavissa: http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/hsla_c/hsmulti.pdf [viitattu 18.4.2013]

ITU-T:n X.700 -standardi. Verkkojulkaisu. Saatavissa: http://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.700-199209-I!!PDF-E&type=items [viitattu 15.4.2013]

Jaakohuhta H. 2005. Lähiverkot - Ethernet, Ethernet-tekniikan soveltaminen käytännössä. Edita Prima Oy, Helsinki.

Kocjan W. 2008. Learning Nagios 3.0. Packt Publishing Ltd.

Mauro D. & Schmidt K. 2005. Essential SNMP, 2nd Edition. O'Reilly Media. Saatavissa: http://it-ebooks.info/book/367

Musardo M. 2010. Working with cisco IP SLA: Measuring IP SLA in enterprise networks

Nagiosgraph. Dokumentti. Saatavissa: http://nagiosgraph.svn.sourceforge.net/viewvc/nagiosgraph/trunk/nagiosgraph/README.html [viitattu 12.4.2013]

Puska, M. 1999. Lähiverkkojen tekniikka - Pro Training. Gummerus Kirjapaino Oy, Jyväskylä.

KYMENLAAKSON AMMATTIKORKEAKOULU

Tietoverkkotekniikka

NAGIOS MANUAALI

Kevyt käyttöohje

Tekijät: Ville Leppänen
Tomi Tähti

Päiväys: 10.4.2013

TÄRKEIMMÄT HAKEMISTOT JA KOMENNOT

Nagioksen asennuskansio: /usr/local/nagios/

Nagiosgraphin asennuskansio: /usr/local/nagios/nagiosgraph/

Määritystiedosto kohteille ja palveluille: /usr/local/nagios/etc/objects/switch.cfg

Määritystiedosto komentojen määrityspohjille (templates):
/usr/local/nagios/etc/objects/templates.cfg

Määritystiedosto kontakteille: /usr/local/nagios/etc/objects/contacts.cfg

Pluginien ja skriptien hakemisto: /usr/local/nagios/libexec/

Nagioksen uudelleenkäynnistyskomento: service nagios restart

WEB-KÄYTTÖLIITTYMÄ

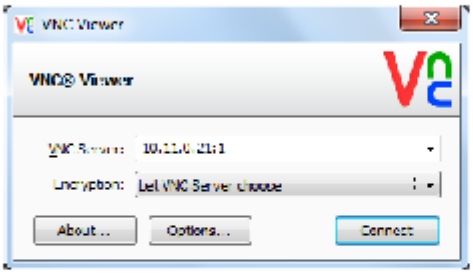
VPN-yhteyden ollessa auki, mene selaimella osoitteeseen http://10.11.0.21/nagios ja syötä yllä löytyvät tunnukset saadaksesi web-käyttöliittymän näkyviin.

VNC- SEKÄ SSH-YHTEYDET

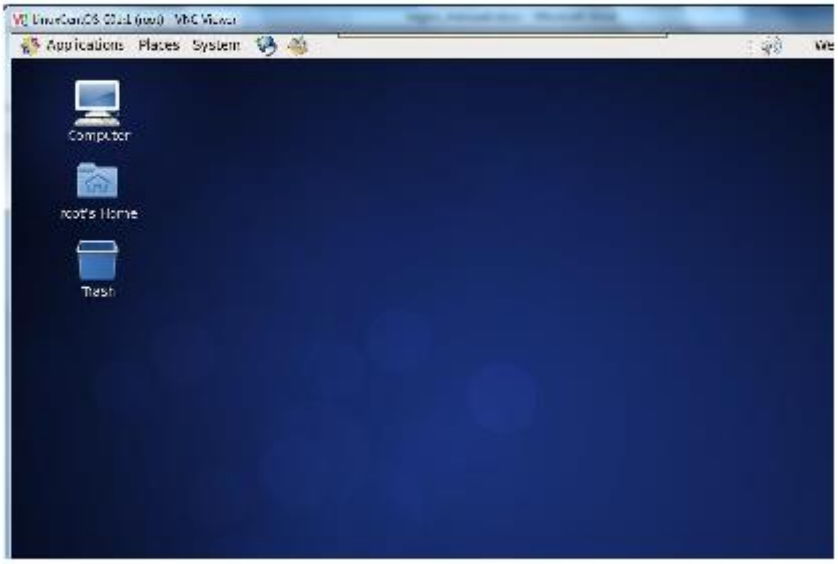
Ennen SSH- tai VNC-yhteyttä tarvitaan VPN-yhteyden avaaminen.

Jos halutaan esiin vain komentorivi, järkevin tapa on avata esimerkiksi puttyn kautta SSH-yhteys osoitteeseen 10.11.0.21, jolloin komentoriville pääsee kirjautumaan käyttämällä root-tunnuksia.

Jos halutaan linuxin työpöytänäkymä etänä, pitää avata VNC Viewer –ohjelmalla etäyhteys linux-koneeseen, jolloin saadaan työpöytänäkymä esiin.



Kuva 1. VNC Viewer -ohjelma, jolla saadaan linux-koneen työpöytä etänä näkyviin.



Kuva 1. Nagioksen työpöytänäkymä VNC Viewerin kautta.

SÄHKÖPOSTI-ILMOITUKSET

Ilmoitus-/hälytysviestien päälle kytkemiseksi pitää määrittää contacts.cfg –tiedostoon toimiva sähköpostiosoite, johon ilmoitukset lähetetään.

Jos nagios lähettää viestejä ja niitä ei näy sähköpostin saapuneissa, tarkista roskapostikansio!

Jotkin sähköpostipalvelimen estävät nagioksen ilmoitusviestit jo oletuksena palvelimen ulkoreunalla.

KOHTEIDEN JA PALVELUIDE N LISÄÄMINEN

Jos Nagioksen monitoroinnin piiriin halutaan lisätä uusia laitteita tai palveluita, niin alla olevien kuvien mukaisilla komennoilla saa perustason määritykset tehtyä.

```
detine host{
        use             generic-switch
        host_name       Cisco 881g
        alias           Cisco 881g 3G Router
        address         10.10.0.75
        hostgroups      switches
        }
```

Kuva 2. Laitteen lisääminen.

Laitteen lisäämisessä use-komennolla määritetään template (määrityspohja), jota laite noudattaa. Generic-switch –template on täysin sopiva yleisille laitteille mikäli erikoisia määrityksiä ei haluta eli sitä voi käyttää oikeastaan jokaisessa laitteessa.

Host_name –komennolla määritetään laitteelle nimi, jota käytetään palveluissa viittaamaan oikeaan laitteeseen.

Alias –komennolla määritetään laitteelle ns. kuvaus/nimi joka antaa paremman ymmärryksen siitä mikä laite on kyseessä.

Address –komennolla määritetään laitteen ip-osoite.

Hostgroups –komennolla määritetään laiteryhmä, johon lisätty laite halutaan sisällyttää. Olemme itse käyttäneet samaa ”switches” ryhmää jokaiselle laitteelle. Ryhmiä voi myös luoda lisää, mikäli laitteita halutaan erotella erinimisiin laiteryhmiin.

```
define hostgroup{
        hostgroup_name  switches
        alias           Network Switches
        }
```

Kuva 1. Kyseisellä tavalla voi luoda uuden ryhmän.

```
define service{
        use                     generic-service
        host_name               Cisco-88lg
        service_description     ICMP Echo Status
        check_command           check_snmp!-C public -o enterprises.9.9.42.1.2.10.1.2.3 -r 1 RFC1213-MIB
        normal_check_interval   1
        }

define service{
        use                     generic-service,graphed-service
        host_name               Cisco 88lg
        service_description     Tasliprosessit
        check_command           check_snmp!-C public -o hrSystemProcesses.0
        normal_check_interval   1
        }
```

Kuva 2. Palveluiden lisääminen.

Use-komennolla määritetään käytettävät määrityspohjat, tässä tapauksessa generic-service sekä graafisille kuvaajalle graphed-service.

Host_name –komennolla määritetään laite, jonka palvelu on kyseessä. HUOM! TÄYTYY OLLA SAMA KUIN LAITTEELLE DEFINE HOST –KOHDASSA MÄÄRITETTY HOST_NAME!

Service_description –komennolla määritetään palvelulle kuvaus.

Check_command –komennolla määritetään, että mitä lisäosaa/komentoa palvelun tarkistuksessa käytetään sekä kyseisen komennon parametrit. Yllä olevissa kuvissa parametreiksi on määritetty object-id jota tarvitaan tunnistamaan, että mitä palvelun tietoa ollaan hakemassa.

Normal_check_interval –komennolla määritetään palveluiden tarkistuksen aikaväli minuutteina.