Tietoliikenneverkon valvonta eräässä yrityksessä

Diplomityöseminaari 14.3.2006

Outokumpu Stainless

Tunnistetiedot

- Otsikko: Tietoliikenneverkon valvonta eräässä yrityksessä
- Tekijä: Antti Palokangas
- Valvoja: Professori Raimo Kantola
- Ohjaaja: FL Raimo Pelkonen
- Suorituspaikka: Outokumpu Stainless Oyj, Tornio Works

Sisällysluettelo

- Työn taustaa
- Verkonvalvontajärjestelmän toteutus
- Liikenteen analysointi
- Lopputulokset

OUTOKUMPU

Taustaa

- Työntekijät ja tuotanto tarvitsevat toimivia yhteyksiä
  -> käyttökatkokset aiheuttavat töiden seisomista
  -> yritykselle kuluja
- Tavoitteena on rakentaa järjestelmä, joka valvoo verkkolaitteiden tilaa, jotta viat havaittaisiin nopeammin ja vikoja voitaisiin jopa ennaltaehkäistä
  -> lyhyemmät käyttökatkokset
  -> vähemmän kuluja

OUTOKUMPU

Taustaa

- Yrityksen lähiverkosta puuttui järjestelmä, josta voitiin valvoa koko lähiverkon tilaa keskitetysti
- Lähiverkko on laaja, noin 270 reititintä/kytkintä/WLAN-tukiasemaa hallittavana
- Järjestelmä oli rakennettava HP OpenView Network Node Manager (NNM) ja CiscoWorks LAN Management Solution –ohjelmistoja käyttäen
- Lisäksi analysoitiin yrityksen verkossa kulkevaa liikennettä

OUTOKUMPU

Metodiikka

- Lähtökohdat olivat selvät, ohjelmistot oli jo hankittu yritykseen ja valittu käytettäväksi
- Näillä työkaluilla oli rakennettava järjestelmä, joka täytti asetetut vaatimukset ja tarkasteltava lisämahdollisuuksia hyödyntämiseen
- Ensiksi oli asennettava ohjelmat ja konfiguroitava ne kuntoon
- Myös valvottavat laitteet oli konfiguroitava oikein
- Lopuksi testattiin ja vertailtiin ohjelmistoja ja rakennettiin toimiva järjestelmä

FCAPS

- Verkonhallinta jaoteltiin FCAPS-mallin mukaisesti eri osa-alueisiin:
  Vianhallinta (Fault Management)
  Kokoonpanon hallinta (Configuration Management)
  Laskutuksen hallinta (Accounting Management)
  Suorituskyvyn hallinta (Performance Management)
  Turvallisuudenhallinta (Security Management)
- Verkonhallintaa parannettu tässä työssä useilla FCAPS:n osa-alueilla. Vianhallinta oli tärkein yksittäinen osa-alue, jonka parantamisesta lähdettiin liikkeelle

Verkonvalvonnan vaihtoehdot

- Valinta oli tehtävä HP OpenView Network Node Managerin (NNM) ja CiscoWorksin Device Fault Managerin (DFM) välillä, jotka molemmat hoitavat FCAPS:n vianhallinnan osa-aluetta
- Molemmat listaavat hälytykset reaaliaikaisesti ruutuun, josta verkon operaattori voi tarkkailla häiriöitä. Molemmat pollaavat laitteita ja ottavat vastaan trap-ilmoituksia. Ne voivat myös hälyttää ylläpitäjän hälytysten tullessa.
- Molemmat siis tarkkailevat vikoja ja häiriöitä ja ilmoittavat niistä

Vertailun tulokset

- Vertailun jälkeen valittiin verkonvalvontaan käytettäväksi ohjelmaksi HP OpenView Network Node Manager (NNM)
- NNM esittää väreillä havainnollistavan karttakuvan verkosta ja sen tilasta
- Kaikki hälytykset kirjataan Alarm Browseriin, josta ylläpitäjät tarkkailevat hälytyksiä

Vertailun tulokset

- NNM soveltuu verkonvalvontaan paremmin selkeytensä ja paremman käytettävyytensä ansiosta
- Testausvaiheessa NNM:n hälytyksiä pidettiin selkeämpinä
- Loppukäyttäjät pitivät NNM:a sopivampana
- Lisäksi CiscoWorks hallitsee vain Ciscon laitteita
- Vaikka NNM valittiin verkonvalvonnan käyttöliittymäksi, ei CiscoWorks jäänyt turhaksi
- CiscoWorks ja NNM täydentävät toisiaan verkonhallinnassa tarjoten yhdessä vahvan verkonhallintaratkaisun

OUTOKUMPU

Saavutettavuuden tarkkailu

- NNM:n verkonvalvonta perustuu pitkälti SNMP- ja ICMP-protokolliin
- NNM määritetty pingaamaan verkkolaitteita 30 sekunnin välein
- Jos laite ei vastaa pingiin -> Node Down -> Merkintä Alarm Browseriin ja hälytyssähköposti ja –tekstiviesti kyseisen laitteen ylläpitäjälle

OUTOKUMPU

Trap-ilmoitukset

- Laitteet voivat lähettää myös itse ilmoituksia ongelmistaan
- Trap-ilmoitukset lähtevät verkonhallinta-asemalle, kun esim. työryhmäkytkimien ympäristömuuttujien (lämpötila, prosessorin kuormitus, jännite) raja-arvot ylittyvät
- Muita trap-ilmoituksia:
  snmp = warmStart, coldStart, linkUp, linkDown, authentication
  syslog (kriittisen tason virheistä)
  config (kun tehdään konfiguraatiomuutoksia laitteelle)
  rogue-ap (WLAN-tukiasemilta, kun havaitaan vieras tukiasema)
- Trap-ilmoitukset riippuvat laitteen mallista, jokainen malli piti katsoa erikseen
- SNMPv2c –version inform-ilmoitukset käytössä (niillä laitteilla, jotka tukevat tätä). Parannuksena trap-ilmoituksiin se, että kuittauksilla varmistetaan ilmoituksen perillemeno

SNMP-asetukset

- Asetukset oli käytävä läpi kaikilta verkkolaitteilta
- Yhteinen linja, että kaikilla on samanlaiset SNMP-asetukset ja laitteet lähettävät trap-ilmoitukset samoista asioista

OUTOKUMPU

Syslog

- Syslogin kriittisistä tilanteista tulee jo hälytykset NNM:lle trap-ilmoituksina
- Matalamman tason ongelmatilanteista määriteltiin lähtemään CiscoWorksiin ilmoitukset, esim. huonosti toimivat tai väärin konfiguroidut portit lähettävät ilmoitukset virhetilanteista
- Näin vähemmän vakavat viestit eivät häiritse vakavien hälytysten tarkkailua, mutta eivät jää huomiotta

Proaktiivisuus

- Proaktiivisuutta eli vikojen ennaltaehkäisyä on mm. se, että tarkkaillaan laitteiden ympäristömuuttujia ja niiden joutuessa kriittisille rajoille voidaan puuttua ongelmaan jo ennen vikaantumista
- Myös linkkien virhetasoja ja porttien käyttöasteita tarkkaillaan ja näiden rajojen ylittyessä hälytys tulee Alarm Browseriin. Nämä tilanteet voivat ennakoida ongelmia

Vianhallinnan tulokset

- Vianhallintaan saatiin rakennettua toimiva järjestelmä, joka tarkkailee verkon vikoja aktiivisesti
- Työn vaatimukset saatiin näiltä osin täytettyä ja parannettua huomattavasti aikaisempaa tilannetta
- Myös muita kuin kriittisiä häiriöitä alettiin seuraamaan keskitetysti

Kokoonpanon hallinta

- Kuten mainittiin jo aikaisemmin, CiscoWorks hoitaa verkonhallinnan muita osa-alueita
- Esimerkiksi Ciscon laitteiden kokoonpanon hallinta onnistuu nyt CiscoWorksin avulla. Tämä pitää sisällään mm. konfiguraatiotiedostojen helpotettua editoimista, varmuuskopiointia ja laitteiden hallinnointia graafisen käyttöliittymän avulla

Suorituskyvyn hallinta

- CiscoWorksin Internet Performance Monitor (IPM) tarkkailee latenssiaikoja runkoreitittimien välillä
- Myös tärkeimpien palvelimien saavutettavuusaikoja tarkkaillaan

Liikenteen analysointi

Taustaa

- Haluttiin tarkastella linkkien käyttöasteita, verkon kuormitusta ja millaista liikennettä verkossa liikkuu
- Jatkotoimenpiteet havaintojen mukaan

OUTO KUMPU

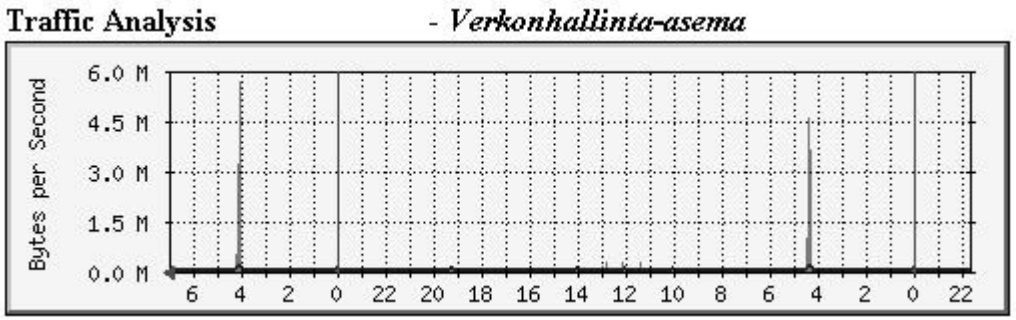
Liikennemäärien tarkkailu

- MRTG asennettiin palvelimelle ja asetettiin tarkkailemaan kahta runkoreititintä ja kaikkia sen portteja
- Näin saatiin yleinen kuva linkkien käyttöasteista ja liikennemalleista
- Pitkäaikaisella seurannalla voidaan seurata kuinka liikennemäärät kehittyvät esim. vuodessa
- Mahdollistaa reagoimisen ennalta, jos havaitaan että liikennemäärät kasvavat ja lähestyvät maksimikapasiteettia

OUTOKUMPU

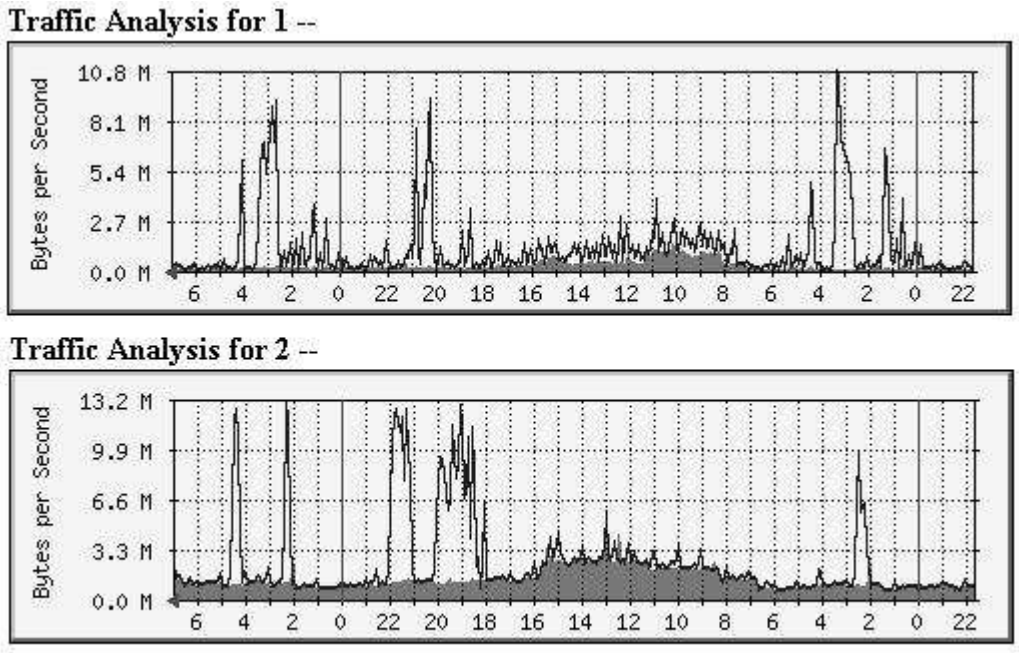
Havaintoja

- Huippuliikenneajat ovat öisin. Palvelimien varmuuskopiointi aiheuttaa selvästi eniten liikennettä verkkoon
- Tyypillinen profiili palvelimen päivittäisestä liikenteestä:



Havaintoja

- Verkossa riittää kapasiteettia hyvin
- Vilkkaimmat linkit toimialueen kahden sisäisen runkoreitittimien välillä. Huippuajat muodostuvat palvelimien varmuuskopioinnista



OUTO KUMPU

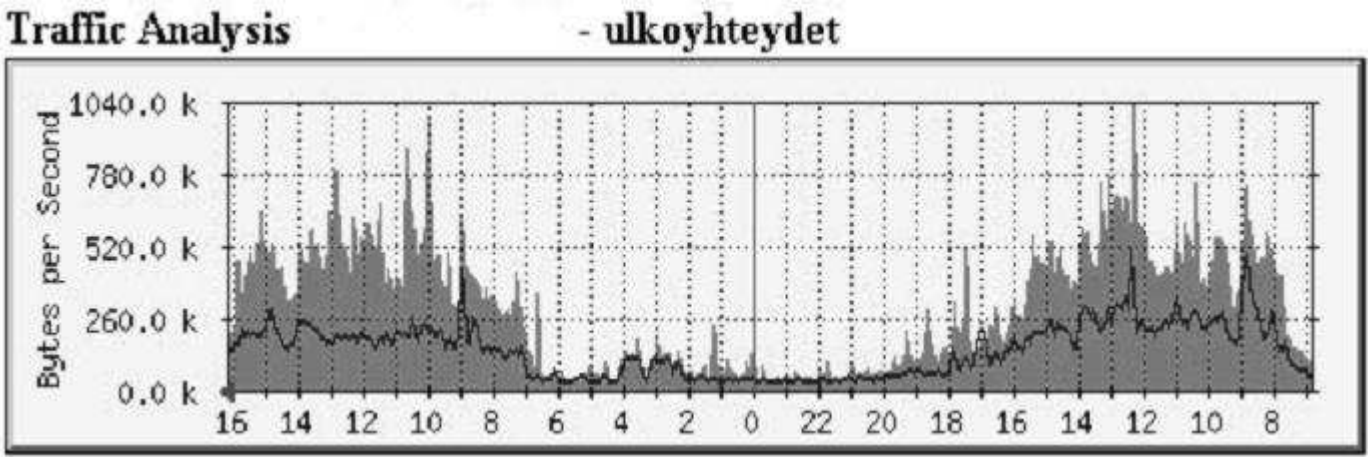
Runkoverkon linkit

- Runkoverkossa toimialueiden välillä riittää myös kapasiteettia erittäin hyvin
- Korkeimmat liikennehuiput 2-3 % maksimikapasiteetista
- Ei tarvetta liikenteen uudelleenjärjestelyille, koska kasvun varaa on huimasti

OUTO KUMPU

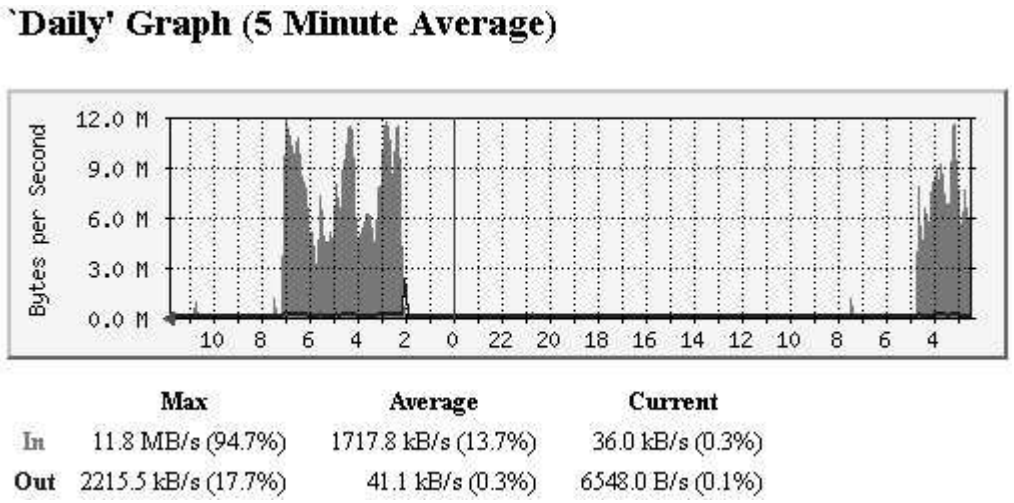
Ulkoyhteydet

- Hyvin odotettavissa olevan mukainen profiili, liikenne vilkkainta päivällä, kun on eniten työntekijöitä paikalla ja ulospäin menevän liikenteen osuus on suurempi kuin tulevan



Eräs palvelin

- Varmuuskopiointi kesti viitisen tuntia yössä ja linkin kapasiteetti (100 Mbit/s) oli maksimikäytössä
- Varmuuskopioitavan datan määrää tarkasteltiin uudestaan ja vähennettiin -> ongelma korjaantui



Resurssien suurkäyttäjien etsintä

- MRTG:n ja Etherealin avulla voitiin selvittää resurssien suurkäyttäjiä. MRTG:lla huomattiin, että eräältä kytkimeltä alkoi tulemaan yllättävän paljon liikennettä. Kun kytkimeltä tulevaa liikennettä kaapattiin ja tutkittiin Etherealilla, huomattiin helposti että verkkoon liitetty web-kamera oli ylivoimaisesti suurin liikenteen lähde

Liikenteen kaappaus - ToDo

- Etherealilla kaapataan liikennettä reitittimiltä ja analysoidaan
- Selvitellään millaista liikennettä verkossa kulkee ja analysoidaan eri järjestelmien verkkoresurssien käyttöä
- Ulkoyhteyksien kapasiteetti rajallinen ja maksetaan kaistan mukaan. Tutkitaan millaisesta liikenteestä huippuaikojen liikenne koostuu ja onko järkeviä keinoja vähentää liikennettä.

Lopputulokset

OUTOKUMPU

Lopputulokset

- Vianhallinnan vikojen havainnointi oli tämän työn tärkein kohta ja sitä on parannettu huomattavasti
- Kokoonpanon hallinta on hyvällä mallilla CiscoWorksin käyttöönoton myötä
- Laskutuksen hallintaan ei ollut kiinnostusta yrityksessä
- Suorituskyvyn hallintaa parannettu MRTG:n avulla. Seurataan käyttöasteita ja liikennemäärien muuttumista, myös pitkällä aikavälillä. Myös NNM tutkii linkkien käyttöasteita. CiscoWorksin IPM mittaa latenssiaikoja.
- Turvallisuuden hallintaan oli jo valmiina useita ratkaisuja, tässä työssä hiukan paranneltu niiltä osin kuin mahdollista

Jatkokehittelyä

- Vielä mietinnässä…

OUTOKUMPU