Verkonhalllinta

S-38.188 Tietoliikenneverkot
Markus Peuhkuri

Luennon aiheet

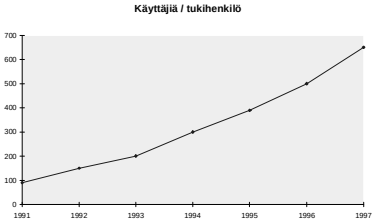
- Verkonvalvonta
- Verkonhallinta
- SNMP
- Hallintalaitteet
- Vianselvityslaitteet

Perinteinen verkonvalvonta

- Niin kauan kuin kaikki toimii ei tehdä mitään
- Kun vika tai häiriö tulee:
  - selvitettään häiriön laajuus
    - » “toimiiko sinulla”
    - » “toimiiko yhteys muualle”
  - mitataan/tutkitaan järjestelmää
  - korjataan epäilty vika
  - hommat seis kunnes korjattu, µ-tuki juoksee
- Ei tarjoa historiatietoa
- Ei tietoa liikenteestä

Tukihenkilöstö vs hallittavat laitteet

- 1 CPU / 200 käyttäjää => 300 CPU / 200 käyttäjää



Verkonhallinnan osa-alueet

- Vikojen, tapahtumien ja suorituskyvyn hallinta
- Käyttäjätuki “helpdesk”
- Hallinnan/resurssien laskutus
- Turvallisuuden hallinta
- Kuormituksen hallinta
- Asetusten hallinta
- Ohjelmiston hallinta
- Tallennuskapasiteetin hallinta
- Tukipalvelut
- = toimii myös suunnittelun tukena

Verkonhallinta (OSI)

- Kokoonpanon hallinta (*configuration* mgmt)
  - komponenttien nimeäminen, ominaisuudet, tilat => verkon ja laitteiden kuvaaminen
- Suorituskyvyn hallinta (*performance* mgmt)
  - hyödyntämisaste, suorituskyky
- Vikojen hallinta (*fault* mgmt)
  - tunnistaminen, eristäminen ja korjaaminen
- Turvallisuuden hallinta (*security* mgmt)
  - pääsyn ja sisällön suojaaminen
- Laskenta (*accounting*)
  - veloitusta varten

Verkonhallintaprotokollat

- Tarjoavat mahdollisuuden valvoa ja hallita verkkoa etäältä
- Hallittavien laitteiden tuettava käytettyä protokollaa
  - Simple Network Management Protocol (TCP/IP)
  - Common Management and Information Protocol (OSI)
    - » CMIP over TCP
    - » CMIP over LLC
  - IBM NetView (tuotteessa myös SNMP)
  - muita valmistajakohtaisia sovelluksia
    - » Decnet Maintanance Operation Protocol
- SNMP tietokoneverkoissa tärkein
  - CMIP:n ja SNMP yhteiskäyttö kehitteillä

SNMP - kehitys

- 1980-luvun puolivälissä Internet kasvoi voimakkasti
- Useita ehdokkaita
  - High-level Entity-Management System (<= HMP)
  - SNMP (<= Simple Gateway Management Protocol)
  - CMOT
- -88: SNMP välikaikaisratkaisu, CMOT tulevaisuudessa
- -89: de facto -standardi, -90 Internet-standardi
- Kehitystyö jatkuu

SNMP — kolmijako

- Verkonhallintaprotokolla
  - SNMP: RFC 1157, STD 15 [Std, Rec]
- Tiedon rakenne ja tunnistaminen
  - SMI: RFC 1155, STD 16 [Std, Rec]
- Hallittavat tiedot
  - MIB-I: RFC 1156 [Hist, NotRec]
  - MIB-II RFC 1213, STD 17 [Std, Rec]

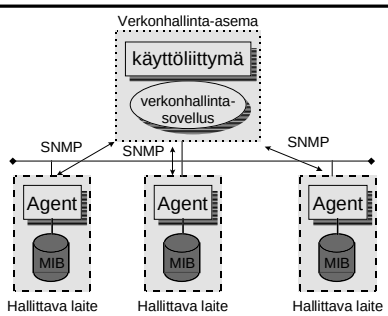
SNMP-protokolla

- Käyttää UDP-protokollaa
  - yhteydetön
- Viestit hallinta-asemalta agentille
  - GetRequest
  - GetNextRequest
  - SetRequest
- Viestit agentilta hallinta-asemalle
  - GetResponse
    - » vastaa hallinta-asemalle
  - Trap
    - » hallinta-asema ei kuittaa

CMIP <> SNMP operaatiot

CMIP	SNMP
get	get
	getnext
set	set
action	*set*
create	*set*
delete	*set*
event-report	trap

SNMP: toiminta



Structure of Management Information

- Määrittää kuinka MIB:t määritellään ja rakennetaan
  - mitkä tietotyypit ovat käytettävissä
    - » vain yksinkertaiset tietotyypit
  - miten resurssit esitetään
    - » syntaksi ja makrot
  - miten resurssi nimetään yksikäsitteisesti
    - » puumainen rakenne
    - » 1.3.6.1.2.1.4 määrittää MIB-II:n ip-ryhmän
    - » {iso org(2) dod(3) internet(1) mgmt(2) mib(1) ip(4)}
    - » {mib 4}

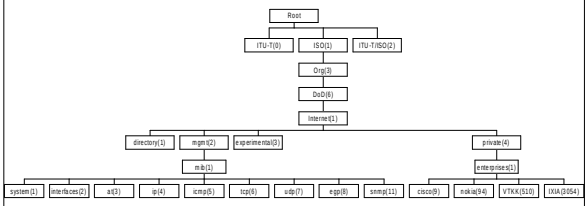
Sallitut tietotyypit *(v2 kursiivilla)*

Tietotyyppi	Kuvaus
INTEGER	Kokonaisluku -2^{31} — 2^{31}-1
OCTET STRING	Merkkijono tulostuvia tai mielivaltaisia merkkejä. Voidaan rajoittaa 255 merkkiin.
NULL	Tyhjä
OBJECT IDENTIFIER	Tieto-objektin tunnus. Maksimissaan 128 ei-negatiivisen kokonaisluvun sarja.
SEQUENCE	Sarja erilaisia tietotyyppejä
SEQUENCE OF	Sarja yhtä tietotyyppiä
BIT STRING	Nimettyjen bittien sarja.
UInterger32	Luonnollinen luku 0 — 2^{32}-1.
NetworkAddress	Verkko-osoite
IpAddress	32-bittinen internet-osoite
NsapAddress	OSI-osoite (0-20 oktettia)
Counter	Luonnollinen kasvava luku 0 — 2^{32}-1. Pyörähtää ympäri.
Counter64	Luonnollinen kasvava luku 0 — 2^64-1. Pyörähtää ympäri.
Gauge	Mittari, voi kasvaa ja pienentyä. 0 — 2^{32}-1
TimeTicks	Laskee aikaa sadasosasekunteina jostakin tapahtumasta kunten Counter.
Opaque	Mahdollistaa satunnaisen tiedon siirron.

Management Information Base

- Määrittää, mitkä hallintaoliot löytyvät msitäkin laitteesta
- Perusjoukko MIB-II
- Muita 75 määritelty (1996)
  - 60 standardiuralla
  - 1 standard, 8 draft standard, 42 proposed standard
  - 1 experimental, 4 historic
- Valmistajakohtaiset laajennukset
  - lämpötila, tulevan ja lähtevän ilman lämpötila, virtatilanne

MIB-rakenne



SNMP-PDU

Versio	yhteisö	SNMP PDU				
PDU-tyyppi	pyyntötunniste	error-index	error-status	muuttujalista		
nimi1	arvo1	nimi2	arvo2	ooo	nimiN	arvoN
PDU-tyyppi	järjestelmätunnus	agentin osoite	yleisvirhe	erikoisvirhe	aikaleima	muuttujalista

SNMP MIB-II-ryhmtät

- System (7)
- Interfaces (2/22)
- Address Translation (1+3, poistuva)
- IP (23/4+5+13)
- ICMP (26)
- TCP (15/5)
- UDP (5/2)
- EGP (6/15)
- Transmission
- SNMP (30)

Etäverkonhallinan tavotteet

- Off-line toiminta
  - yhteyden katkettua hallinta-asemaan, tilastotietoa kerätään silti
- Aktiivinen monitorointi
  - resurssi käytettävissä monitoriointiin
  - historiatieto ennen vikaantumista käytettävissä
- Ongelminen tunnistaminen ja raportointi
  - monitori voidaan konfiguroida tunnistamaan tilanteita
  - hallinta-asemalle voidaan ilmoittaa
- Tiedon lisäarvo
  - esim. eniten liikennöivien laitteiden tunnistus
- Useita hallinta-asemia
  - kyettävä toimimaan eri hallinta-asemien alaisuudessa

Rmon objektiryhmät

- Ethernet-tilastot (ethernet statistics)
- Historian hallinta (history control)
- Ethernet historia (ethernet history)
- Hälytykset (alarm)
- Asemat (host)
- Huippuasemat (hostTopN)
- Matriisi (matrix)
- Suodatin (filter)
- Pakettien kaappaus (packet capture)
- Tapahtumat (event)

Laitteistot

- RMON
  - verkkoliitännässä (reitittimet)
  - PC:n lisäkortti
  - PC ohjelmistolla
  - sulautettu järjestelmä
  - mahdollisesti varustettu modeemilla varayhteyksiä varten
- SNMP valtuusagentti
  - tarkoitettu muiden kuin SNMP-laitteiden hallintaan
  - toimii tulkkina
  - kaikkia laitteita ei ole tarkoituksenmukaista kuormittaa SNMP:n toiminnallisuudella

SNMPv1 puutteet

- Turvallisuus
- Heikko suorituskyky suurilla tietomäärillä
- Liikaa “kansanperinnettä“ ja “läksyjä“
- Tarve hallinnolliselle kehykselle
  - yhteydet, etäkonfigurointi, proxyjen suhteet
- Paljon toiveita

SNMPv2

- Useita keskinään epäyhteensopivia vaihtoehtoja
  - Party-based: proposed 1993
    - » ei *de facto*-standardiksi
  - SNMPv2u
  - SNMPv2*
  - SNMPv1.5

Party-based SNMP

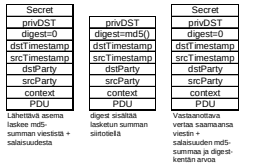
- Turvallisuus
- Hallinnollinen kehys
- SMI
  - uusia tietotyyppejä
  - taulukon rivien lisäys ja muokkaus helpompaa
- Yhteiskäytäntö
  - GetBulkRequest suurten tietomäärien siirtoon
  - InformRequest "trap" hallinta-asemalta toiselle

Party-based SNMP…

- Hallinta-aseminen välinen liikenne
- TCP/IP-riippuvuus poistettu
  - » OSI CLNS, AppleTalk DDP, Novell IPX
- MIB-määrittelyjen kieli parannettu

SNMPv2 (Pb)-turvamenetelmä

- Uudistettu viestin rakenne
- Autentikointi
  - MD5-tiiviste viestistä
  - yhteinen salaisuus
  - löysästi kytkettyjen kellojen aikaleimat
- Salaus DES-algoritmilla



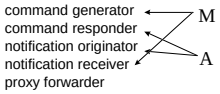
privDST	digest	dstTimestamp	srcTimestamp	dstParty	srcParty	context	PDU
	0-lenght OCTECT STRING						

Party-based SNMP, ongelmat

- Vaikea konfiguroida ja käyttää
- Vie liikaa agentin resursseja
- Ei valmistajien tukea
- Yksinkertaistusehdotukset aihetuttivat epävakautta
- ➔ 1995 julkistetaan selvät asiat
  - rfc1902-1908 SNMPv2 Draft Standard
- Viitekehys v1:teen perustuen
  - rfc1901: SNMPv2c, The Community Basend SNMPv2

SNMPv3

- SNMPv2* ja SNMPv2u yhdistettynä
- Työ alkanut keväällä 1997
- Paljon muutoksia; esimerkiksi
  - manager<=>agent muuttuu sovelluksiksi
  - eri osien standardointi erillisinä



Define an architecture that allows for longevity of the SNMP Frameworks that have been and will be defined.

Keep SNMP as simple as possible

Hallintajärjestelmät

- HP OpenView
- SunSoft Solstice
  - Solstice Domain Manager
  - Solstice Site Manager
- IBM Netview
- CA-Unicenter
  - TNG
- myös muita

Hallintajärjestelmien ominaisuuksia

- Hallinnointi
  - käyttäjien oikeuksien hallinta
- Varmuuskopiointi
  - hajautetussa järjestelmässä myös asiakkaiden varmuuskopiointi
  - levyjärjestelmien hallinta ja työkalut
- Kuorman hallinta
- Sovellusten hallinta
- Asiakkaiden hallinta
  - asiakkaisiin asenenttava komponentti
  - ohjelmistopäivitykset
- Järjestelmän “löytäminen”

Hallintajärjestelmien ominaisuuksia

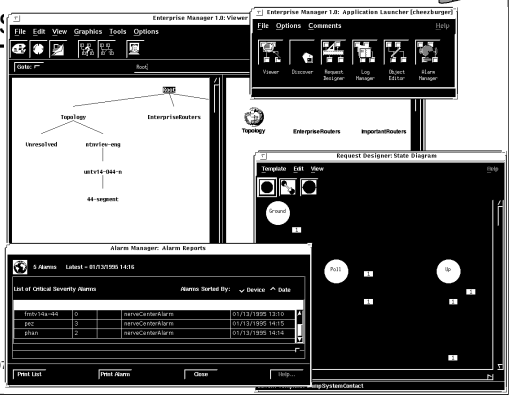
- Turvallisuuden hallinta
  - palomuurit, reitittimien konfigurointi, käyttäjien hallinta
- Käyttäjätuki
  - kysymysten ja vastausten tallennukset
- Hälytykset vikatilanteissa
- Räätälöidyt raportit
- Agentit
  - oltava pieni kuormitus
  - pullonkaulojen tunnistaminen

Käyttöliittymä

- Tekstipohjainen (sarja- / telnet-yhteys)
  - yksittäisille laitteille vakaassa ympäristössä
- Verkonhallinta-asema
  - verkon graafinen esitys
    - » Verkkotopologia, kartta, VR
  - suodatukset
    - » tietty protokolla, sovellus
    - » “toimintakokonaisuudet”
  - laajoissa verkoissa
- Web-pohjainen

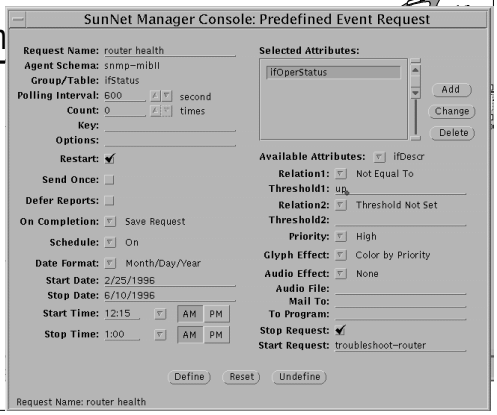
Sols

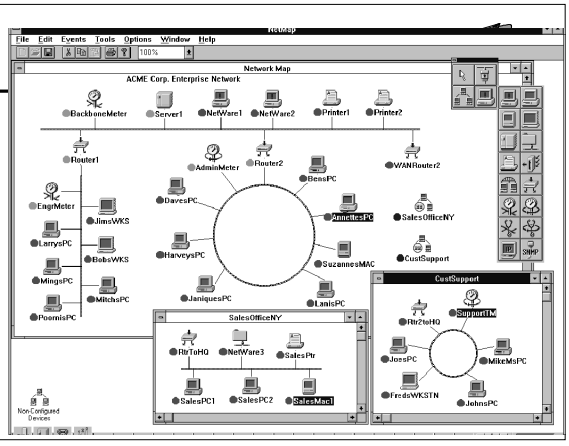
Solstice Domain Manager



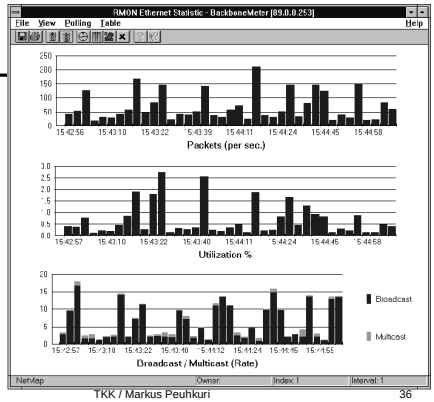
Toim

Toimintojen automatisointi

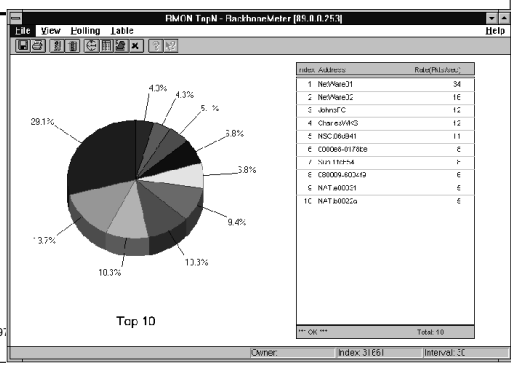




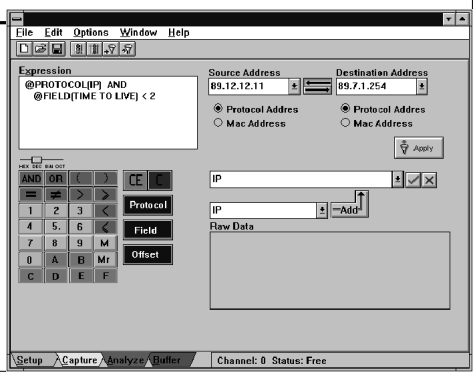
N.A.T



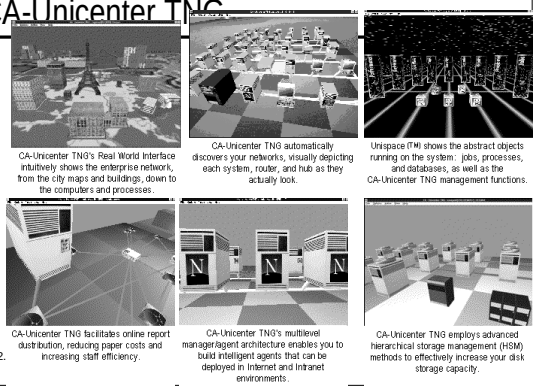
N.A.T



N.A.T



CA-Unicenter TNG



Web-pohjainen

- Täysin HTTP/HMMP-pohjainen
  - laitteessa HTTP-palvelin
  - ei yhtenäistä tietokantamuotoa tai APIa
- SNMP-pohjainen
  - laitteiden ohjaus + tiedonkeruu SNMP:llä
  - tietokantaan kerätään tietoa; jaellaan HTTP-palvelimella
  - WWW-selain + JAVA käyttöliittymänä
  - mahdollistaa hajautetun hallinnan ja tiedoituksen
    - » edullisempi kuin N kappaletta hallintaohjelmistoja
- vielä paljon kehittämistä

Vianetsintä verkosta

- Fyysiset viat
  - yleismittari
  - kaapelitutka
  - kaapelimittari
- Liikennöintivirhet
  - verkkomonitori
- Protokollavirheet
  - verkkoanalysaattori

Verkon fyysiset viat

- Oikosulku
- Katkos
- Impedanssimuutokset
- Parien kytkentävirhe
  - käänteinen kytkentä
  - parien ristiinkytkentä
  - parien “hajoaminen”
- Ylikuuluminen, häiriöt
- Vaimentuminen
- Liika pituus
- Maadotus

Liikennöinti- ja protokollavirheet

- Liian pitkät/lyhyet paketit
- Vialliset paketit
- Bittitahdistusvirheet
- Törmäykset
- Väärä paketointi
- Kuormitus
  - verkossa
  - verkkoelementeissä
- Levitysviestit
- Osoite- ja verkkotunnusvirheet

Mittauslaitteisto

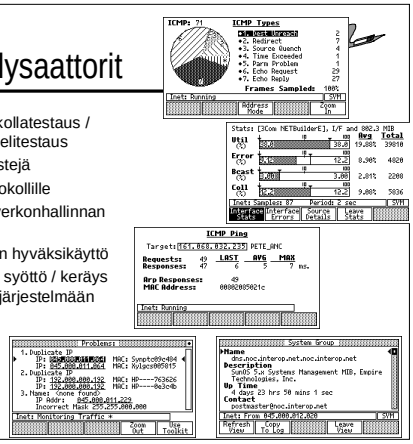
- Kaapelitesterit
  - nykyään useimmat kädessä pidettäviä
  - yksinkertaisista “katkos/pituus”-mittareista graafisella näytöllä varustettuihin kaapelitutkiin
- Verkkoanalysaattorit
  - erikoistuneet laitteistot
  - PC/Unix-ohjelmsitot
- Kehittyneimmät tarjoavat “nappia painamalla viat esiin”

Kaapelitesterit

- Asennuksen luokittelu
  - eri standardien mukaan, eri lähiverkkostandardeille
- Mittaukset
  - kaapelin pituus, impedanssi
  - vaimeneminen, ylikuuluminen
- Virhepaikkojen määritys
- Mittaukset kaapelin molemmista päistä
  - etäyksiköllä osa mittauksista

Verkkoanalysaattorit

- Vain protokollatestaus / myös kaapelitestaus
- Erilaisia testejä
  - eri protokollille
- Yhteistyö verkonhallinnan kanssa
  - SNMP:n hyväksikäyttö
  - tietojen syöttö / keräys hallintajärjestelmään



Yhteenveto

- Verkonhallinta ehkäisevää
- Hallintaprotokollan oltava laitteistoon skaalautuva
- Laitteissa yhä enemmän hallittavia komponentteja
  - virtuaaliverkot, kaistanleveys,…
- Tulevaisuus?
  - SNMPv3
  - CIM (DTMF)
  - JAVA
  - CORBA

In an ideal world, I’d use SNMP for data collection, browsers for display, Java for intelligence, and [a standard] schema for data protability.

- Jeffrey Case, an SNMP bigot