


Netværksovervågning og -administration

HOUSE OF TECHNOLOGY
mercantec

- Network management (eng. ord for netværksovervågning og administration) er den brede betegnelse for styring og overvågning af alle netværksenheder og brugere. Enhederne kan fx være: routere, hubs, switches, servere, workstations osv., altså alle nettets enheder.
- Med styring og overvågning af enhederne menes:
 - Fjernstyring (fx konfiguration af routere eller servere).
 - Automatisk installation og afinstallation af software.
 - Hardware og software inventarlistar og forespørgsler på disse.
 - Fejlmeldinger fra enheder.

© Mercantec 2013




Netværksovervågning og -administration


HOUSE OF TECHNOLOGY
mercantec

- Årsagen til at interessen for network management er så stor er at:
 - Mange netværk er i dag så komplekse at der skal overvågning til for at sikre fejlfindingsmulighed og der med en stabil drift.
 - Muligheden for at outsource driften af et komplet netværk.
 - Der er penge at spare med et velfungerende network management.
 - http://en.wikipedia.org/wiki/Network_management
 - <http://www.slac.stanford.edu/xorg/nmtf/nmtf-tools.html#nmp>

© Mercantec 2013




HOUSE OF TECHNOLOGY




...mercantec*

SNMP og CMIP

- For at et Network management system kan arbejde sammen med enheder fra forskellige producenter, er det vigtigt at have nogle management standarder, som producenterne kan implementere i deres produkter.
- De to vigtigste standarder er:
 - SNMP (Simple Network Management Protocol)
En IETF (Internet Engineering Task Force) protokol. IETF standardisere protokoller til Internettet. SNMP er den mest brugte Network management protokol og her på kurset skal vi kun arbejde med SNMP.
 - CMIP (Common Management Information Protocol)
En OSI Network management protokol som er konstrueret til at monitere og kontrollere netværk.




International Organization for Standardization




I E T F

© Mercantec 2013



HOUSE OF TECHNOLOGY



...mercantec*


SNMP oversigt - historie

- SNMP er designet så netværksenheder kan udveksle management informationer.
- SNMP (Simple Network Management Protocol) er en applikationslags protokol, men er i princippet placeret fra netværkslaget og opefter.
- SNMP blev udviklet i 1988 for at lette arbejdet med styring og overvågning af routere på Internettet. Årsagen til at man skulle udvikle en ny protokol, var at den data bærende protokol på Internettet, TCP/IP suiten ikke indeholder styrings værktøjer til routere. Producenterne af netværksenheder fik derefter hurtigt implementeret SNMP i mange af deres netværks produkter, og i dag kan næsten alle netværksenheder fås med SNMP.
- SNMP blev i 1989 adopteret som standard i TCP/IP.


OSI-model

7. Applikation	}	SNMP
6. Præsentation		
5. Session		
4. Transport		
3. Netværk		
2. Datalink		
1. Fysisk		

© Mercantec 2013

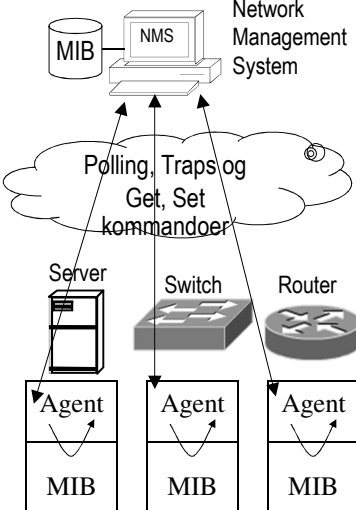


SNMP enheder




mercantec


- Et SNMP administreret system består af 2 typer enheder: Kontrollerede enheder m. SNMP agenter og Network Management Station (NMS).
 - NMS (Network Management Station) er normalt en PC med management software installeret. Fra NMS kan man styre og overvåge de enkelte netværksenheder. NMS kan sende kommandoer og modtage svar og traps (alarmer) fra SNMP agenter.
 - En SNMP Agent er et stykke Network Management software som er installeret på en kontrolleret enhed fx switch, router eller server. Agenter svare på forespørgsler fra NMS, dvs. agenten henter management informationer fra enhedens MIB og oversætter den til SNMP format. Agenter kan også modtage kommandoer fra NMS om ændringer der skal foretages i MIB'en.



© Mercantec 2013




Network Management Software



mercantec


- Network management software er programmer som kan styre og overvåge netværks enheder. Programmerne kan være proprietære dvs. at de kun virker sammen med producentens enheder eller de kan være generelle og virke sammen med alle type af produkter.
- Efter udviklingen af protokollerne SNMP og RMON er det blevet muligt at lave generelle programmer som kan styre og overvåge alle produkter, når blot de anvender SNMP / RMON.
- Network Management Stationen er normalt en pc som anvender Linux, Unix eller Windows 2000.
- De mest udbredte Network management programmer er:
 - HP Open View (Hewlett Packard)
 - Tivoli (IBM)
 - Unicenter TNG (Computer Associates)
 - Ciscoworks2000 (Cisco)
 - SunNET Mgr (SUN)

© Mercantec 2013



SNMP kommandoer

HOUSE OF TECHNOLOGY




mercantec

- Management konsollen og netværks enheden kommunikere vha. SNMP kommando sættet. Filosofien er at der skal være få og meget simple kommandoer, som skemaet herunder også viser.
- Så hvis man skal have en variabel fra en enheden fx oppe tid sender man "Get request variabel" kommandoen. Enheden sender derefter "Get response variabelværdi".
- Anderledes er det hvis man skal have en variabel værdi hvor man ikke kender variabel navnet. Her kan det være nødvendigt at anvende en "Get request" kommando og derefter et antal "Get next request" kommandoer indtil man finder værdien. Det er derfor SNMP kan give meget trafik på nettet.
- Det er også muligt at sætte en tærskelværdi (threshold) ind en variabel fx til alarmering hvis trafikken på nettet overstiger 90% af max. kapacitet. Det betyder at enheden sender en Trap meddelelse til management konsollen hvis værdien overskrides.


SNMP kommando	Funktion
Get – request	Hent værdien fra den angivne variabel
Get – next request	Hent værdien fra den næste variabel – efter Get request
Get – response	Svar på en "Get req." eller "Get next req." kommando
Set – request	Gem en værdi i den angivne variabel
Trap	Send en alarm hvis en angivet hændelse (event) opstår

© Mercantec 2013



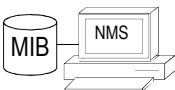
SNMP kommandoer (fortsat)

HOUSE OF TECHNOLOGY



mercantec

- Kommunikationen mellem Network Manager Stationen og SNMP agenten foregår med applikationslags protokollen SNMP (Simple Network Management Protocol).
- SNMP bruger transport protokollen UDP og anvender portene 161-162 til udveksling af meddelelser.




NetworkManagement System

GetRequest, GetNextRequest, SetRequest

←


GetResponse, Trap



SNMP kontrolleret Router


SNMP kommando	Funktion
Get – request	Hent værdien fra den angivne variabel
Get – next request	Hent værdien fra den næste variabel – efter Get request
Get – response	Svar på en "Get req." eller "Get next req." kommando
Set – request	Gem en værdi i den angivne variabel
Trap	Send en alarm hvis en angivet hændelse (event) opstår

© Mercantec 2013



SNMP versioner


HOUSE OF
TECHNOLOGY



mercantec


- Udviklingen fra SNMP v1 til v2 indeholder tre store ændringer:
 - GetBulkRequest kommandoen som kan hente mange data fra MIB'en på en gang, i stedet for at anvende de ineffektive "GetRequest" kommando og derefter et antal "GetNextRequest" kommandoer indtil man finder værdien.
 - 64 bit tællere i MIB'en i stedet for 32 bit tællere.
 - Trap kommandoen (Send en alarm hvis en angivet hændelse opstår).
- Udviklingen fra SNMP v1-2 til v3 er mest på sikkerheds området:
 - SNMP v1 og v2 kun anvender Community strings (SNMP gruppe navn) i klartekst som authentication (adgangsgivende). Husk desuden at ændre de default community strings som SNMP agenter og NMS opsat med.
 - Read-only agent adgang: public
 - Read-write agent adgang: private
 - SNMP v3 giver mulighed for at sikre kommunikationen mellem NMS og agentens MIB ved adgangskontrol og kryptering. Følgende er muligt med SNMP v3:
 - Brugernavn som adgangskontrol.
 - Adgangskontrol baseret på MD5 (Message Digest algorithm 5).
 - Adgangskontrol baseret på MD5 og kryptering med DES (Data Encryption Standard).

© Mercantec 2013



MIB - Management Information Base

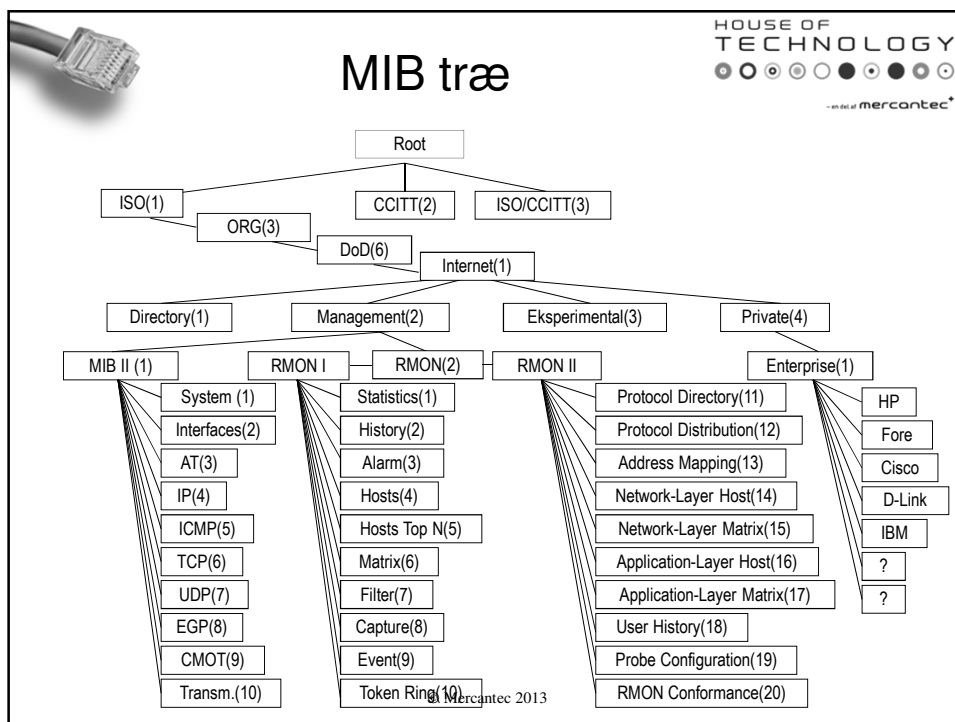
HOUSE OF
TECHNOLOGY



mercantec

- I netværks enhederne er der placeret en database som indeholder informationer om enheden. Database kaldes MIB'en (Management Information Base) og er opbygget som en træstruktur som er beskrevet i SMI (Structure of Management Information).
- Under Root i træet findes 3 grene som administreres af henholdsvis ISO, CCITT og et som administreres af begge organisationer.
- Grenen som har vores interesse administreres af ISO. Under denne er ORG (organisationer), hvor vi finder DOD (Department of Defence) det Amerikanske forsvarsministerium, som har udviklet store dele af Internettet.
- Under DOD finder vi Internet og det er her SNMP er placeret. Adressen for Internet er (1.3.6.1). Under Internet er der placeret 2 grene som er interessante i management øjemed nemlig Management og Private. Hvor Private indeholder leverandør specifikke MIB's og Management indeholder MIB I – II og RMON MIB.

© Mercantec 2013




MIB varianter



- MIB I er opdelt i 8 grupper med i alt 114 standard objekter.
- MIB II udvider MIB I til 185 objekter fordelt på 11 grupper.
- RMON I og II er standard MIB's til Remote Monitoring.
- Udover disse MIB's findes der mange producent MIB's

MIB II kategorier	Beskrivelse
1 System	System beskrivelse, uptime, name, location, services, object ID
2 Interfaces	Forbindelser
3 Addr. Translation	Adresse oversættelse fx ARP
4 IP	Internet Protocol software
5 ICMP	Internet Control Message Protocol software
6 TCP	Transmission Control Protocol software
7 UDP	User Datagram Protocol software
8 EGP	Exterior Gateway Protocol software
9 CMOT	Common Management information protocol Over Tcp/ip
10 Transmission	Support for fx Token Ring, Ethernet højhastighed, FDDI osv.
11 SNMP	SNMP oplysninger

© Mercantec 2013



RMON (Remote Monitoring)


HOUSE OF TECHNOLOGY



- Remote network MONitoring (RMON) er en videreudvikling af SNMP. RMON definerer nogle intelligente agenter / prober som kan fortælle når der sker noget management konsollen skal vide.
- RMON er en MIB som opsamler netværks statistik ved at analyserer alle pakker på nettet.
- RMON 1 er beskrevet i RFC 1757 -1513 (Ethernet/Token ring).
- RMON 2 er beskrevet i RFC 2021 og 2074.
- RMON 1 er placeret i IOS-OSI modellens 1-2 nederste lag og RMON 2 i lagene 3-7.



OSI-model

7. Applikation	}	SNMP	}	RMON 2
6. Præsentation				
5. Session				
4. Transport				
3. Netværk	}			
2. Datalink				
1. Fysisk				

© Mercantec 2013




RMON I kategorier


HOUSE OF TECHNOLOGY



RMON 1 kategorier	Beskrivelse
1 Statistics	Opsamling af netværkstrafik fx broadcast, unicast, fejl, pakkestørelse
2 History sets	Historiske sæt af Statistics(1) til sammenligning og trend analyse
3 Alarm thresholds	Bruges til alarmering hvis en af de 2 tærskel værdier (op/ned) er nået
4 Hosts	Proben kan finde nye enheder på nettet hvis en ny MAC adr. viser sig
5 Host top N	Proben kan sortere host informationen ud fra bestemte statistiske data
6 Traffic matrix	Sporer data trafik mellem 2 systemer
7 Filter	Kan filtrere datapakker så man kun ser bestemte data fra pakkerne
8 Packet capture	Kan opsamle og gemme udvalgte datapakker
9 Events	Styre afsendelse af SNMP Trap's til remote clienter (manage consol)
10 Token Ring	Opsamling af data fra Token Ring baserede netværk

© Mercantec 2013



HOUSE OF
TECHNOLOGY



www.mercantec*

RMON II kategorier

RMON 2 kategorier		Beskrivelse
11	Protocol Directory	Viser hvilke protokoller en probe kan monitorere. Bruges af Network Management Station
12	Protocol Distribution	Trafik statistik for hver protokol fx IPX, IP, AppleTalk
13	Address Mapping	Kortlægger Netværks-lag adr. til MAC-lag adr. Letter analyse af data
14	Network-Layer Host	Trafik statistik til og fra hver host
15	Network-Layer Matrix	Trafik statistik mellem host par
16	Network-Layer Host	Trafik statistik til og fra hver host vha. protokoller op til applikations protokol
17	Application-Layer Matrix	Trafik statistik mellem host par vha. protokoller op til applikations protokol
18	User History	Periodiske målinger på bruger specificere variable
19	Probe Configuration	Standard til fjern konfiguration af probe parametre fx Trap destination
20	RMON Conformance	

© Mercantec 2013