SNMP

Simple Network Management Protocol

Henrik Thomsen/EUC MIDT

2007

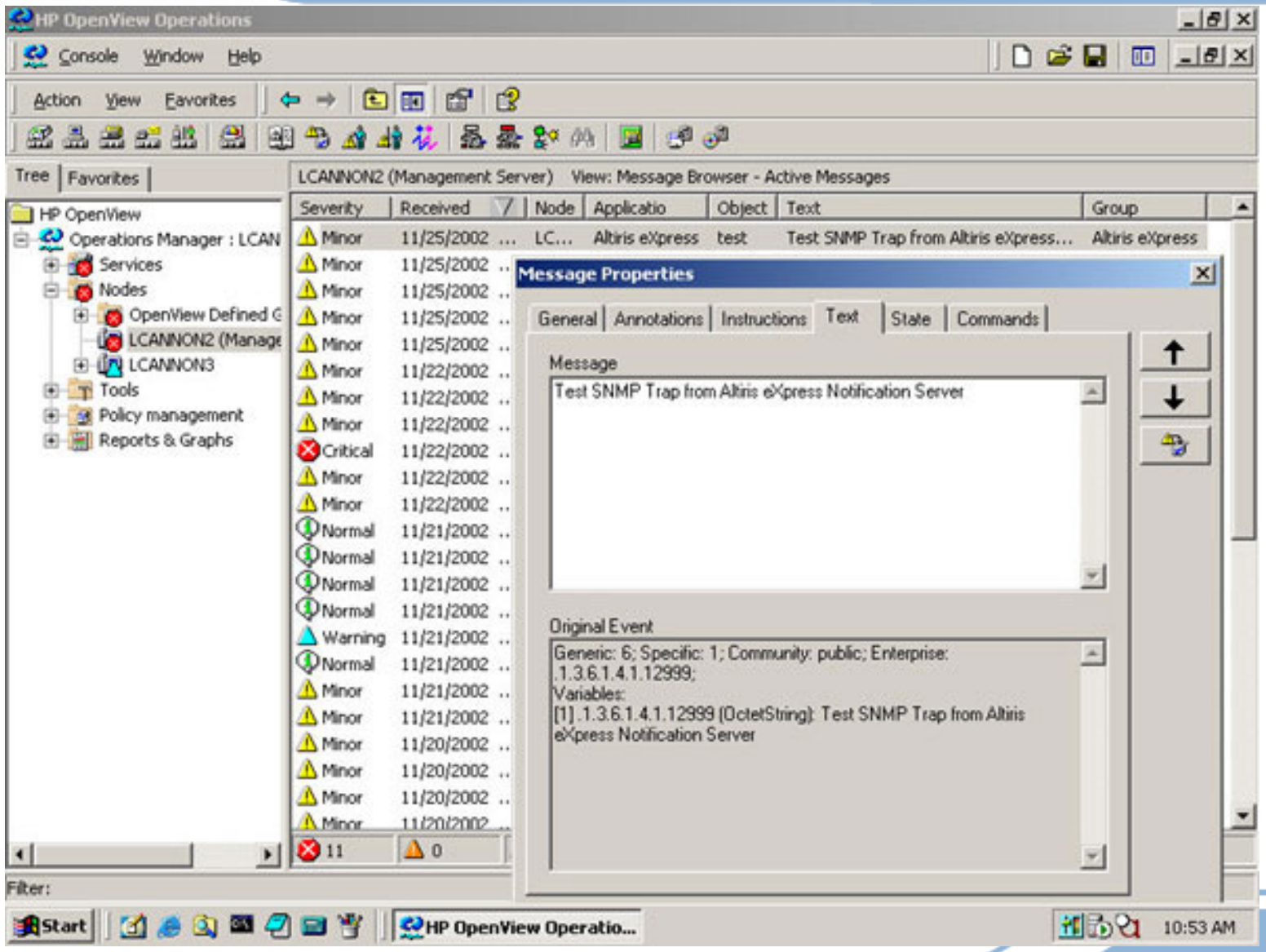
Overvågning

- Network Management
  - At overvåge kritiske netværksenheder
- System Management
  - At overvåge kritiske servere
- Application Management
  - At overvåge kritiske programmer på servere
- Enterprise Management
  - At overvåge alle kritiske enheder i et firma
  - Inkluderer Network, System og Application

Network Management

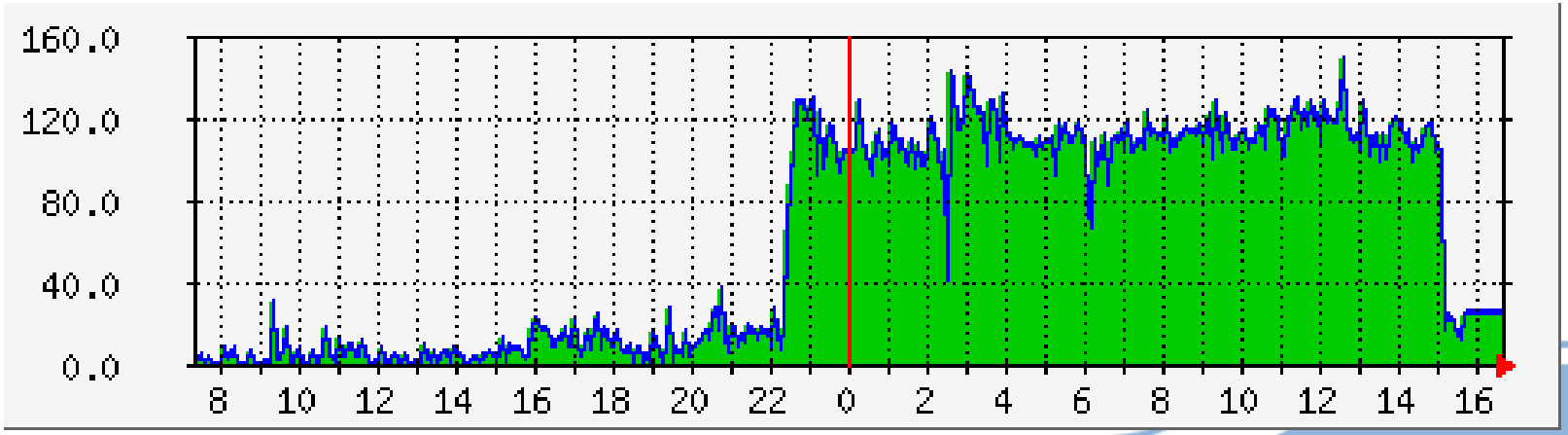
- Der anvendes oftest et NMS
  - Network Management System
- HP OpenView
  - Vel det mest udbredte NMS
- IBM Tivoli NetView
- CastleRock SNMPc
- Og mange andre

HP OpenView Screen shot



Hvad er SNMP

- SNMP
  - Simpel Network Management Protocol
- Kan hente informationer fra netværksenheder
  - For eksempel antal bytes sendt fra serial0/0
  - Hent antal bytes sendt hvert femte minut.
    - Der kan laves en tidsgraf over trafikken.

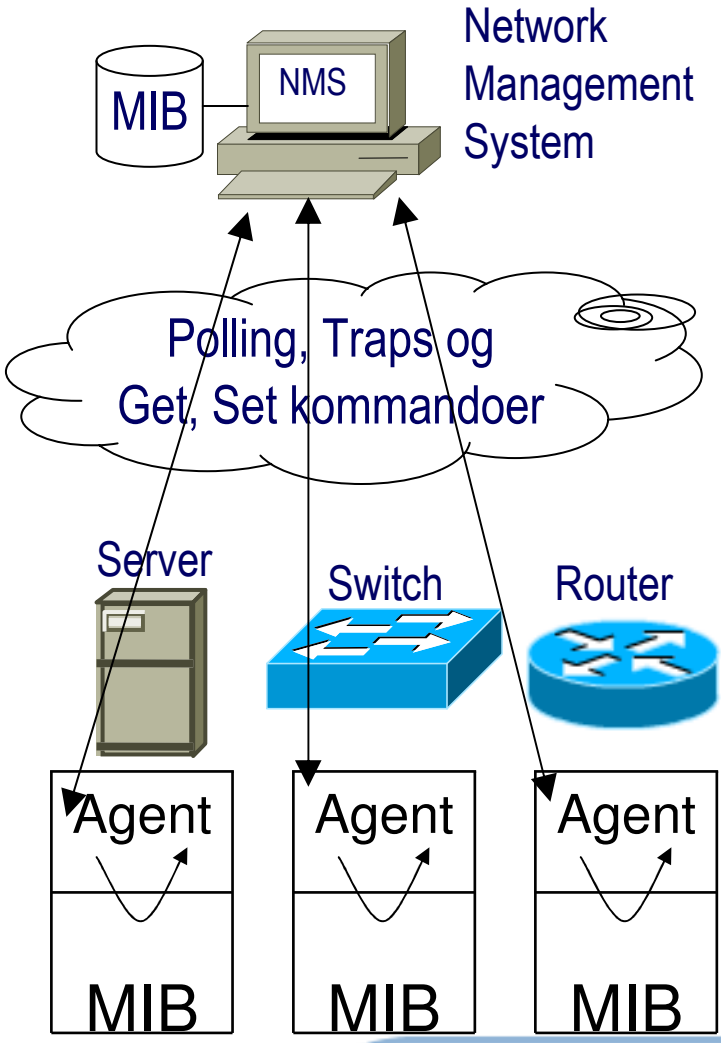


Hvad er SNMP

- Overvågede enheder skal havs SNMP agent
  - Software der forstår SNMP protokollen
- Overvågede enheder kan sender trap til NMS
  - Hvis et netværk for eksempel går ned

SNMP enheder

- 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.



Network Management Software

- 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)
  - CastleRock SNMPc

SNMP kommandoer

- 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.

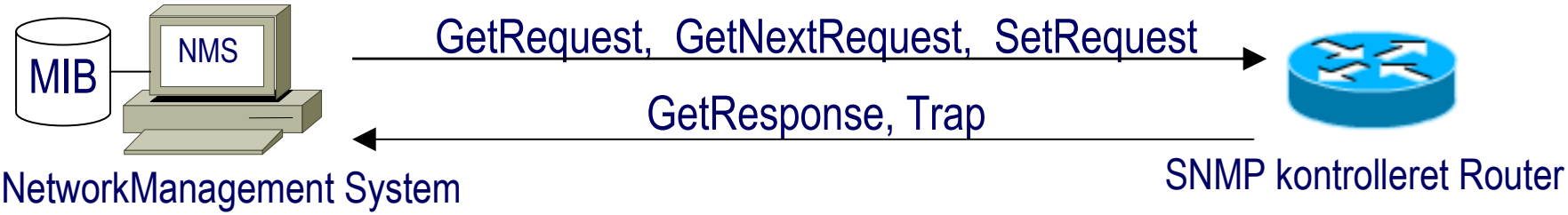
- Det er også muligt at sætte en tærskelværdi (threshold) ind en variabel fx til alarmering hvis trafikken på nettet overstiger 90% af max. kapasitet. Det betyder at enheden sender en Trap meddelelse til management konsollen hvis værdien overskrides.

SNMP kommandoer

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

SNMP kommandoer (fortsat)

- 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.



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

SNMP versioner

- 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).

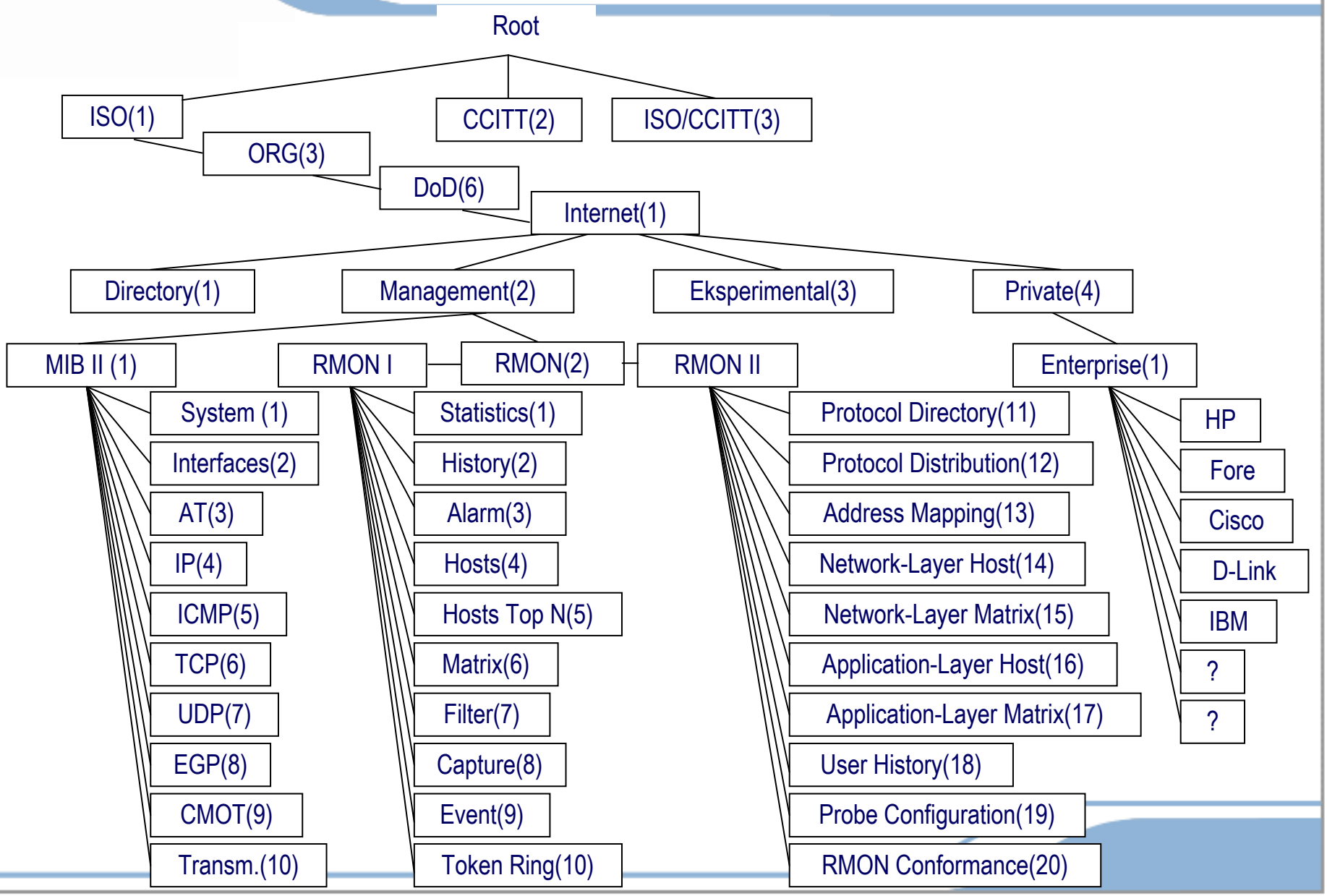
MIB (Management Information Base)

- I netværks enhederne er der placeret en database som indeholder informationer om enheden.
  - Ligger i en database kaldes MIB'en (Management Information Base)
  - 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.

MIB (Management Information Base)

- 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.

MIB træ


Root
ISO(1)
CCITT(2)
ISO/CCITT(3)
ORG(3)
DoD(6)
Internet(1)
Directory(1)
Management(2)
Eksperimental(3)
Private(4)
MIB II (1)
RMON I
RMON(2)
RMON II
Enterprise(1)
System (1)
Interfaces(2)
AT(3)
IP(4)
ICMP(5)
TCP(6)
UDP(7)
EGP(8)
CMOT(9)
Transm.(10)
Statistics(1)
History(2)
Alarm(3)
Hosts(4)
Hosts Top N(5)
Matrix(6)
Filter(7)
Capture(8)
Event(9)
Token Ring(10)
Protocol Directory(11)
Protocol Distribution(12)
Address Mapping(13)
Network-Layer Host(14)
Network-Layer Matrix(15)
Application-Layer Host(16)
Application-Layer Matrix(17)
User History(18)
Probe Configuration(19)
RMON Conformance(20)
HP
Fore
Cisco
D-Link
IBM
?
?

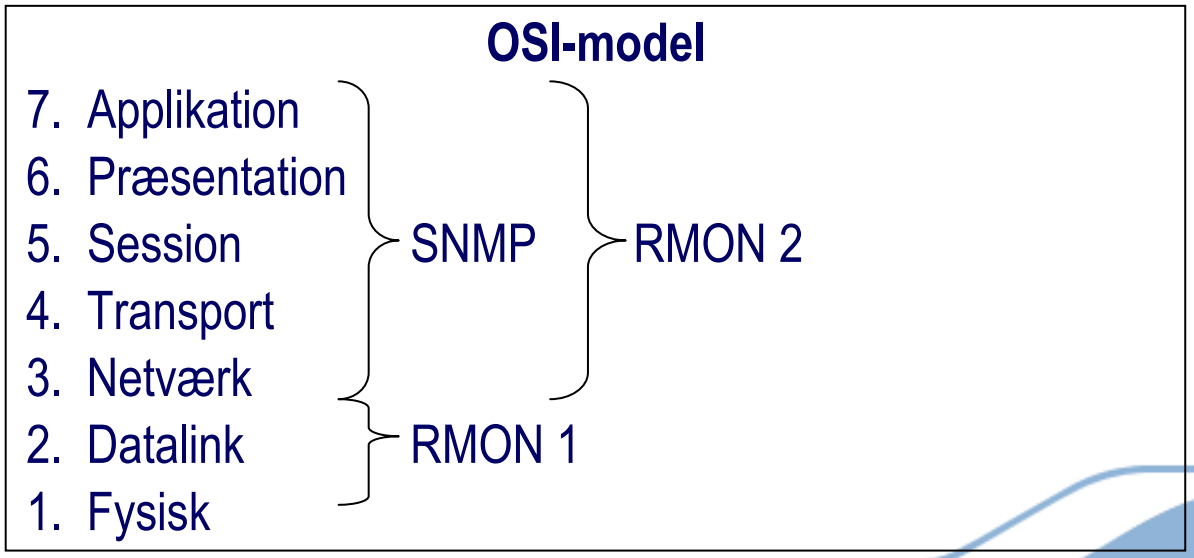
MIB varianter

- MIB I er opdelt i 8 gruppe 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 Monitorering.
- Udover disse MIB's findes der mange producent MIB's

MIB II kategorier		Beskrivelse
1	System	System beskrivelse, uptime, name, location,
2	Interfaces	Forbindelser
3	Addr.	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
10	Transmission	Support for fx Token Ring, Ethernet højhastighed,
11	SNMP	SNMP oplysninger

RMON (Remote Monitoring)

- Remote network MONitoring (RMON) er en videreudvikling af SNMP. RMON definere 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.



RMON I kategorier

Kategorier		Beskrivelse
1	Statistics	Opsamling af trafik fx broadcast, unicast, fejl, pakkestørelse
2	History sets	Historiske 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	Nye enheder på nettet identificeres hvis nye MAC adr. viser sig
5	Host top N	Sortere host informationen ud fra bestemte statistiske data
6	Traffic matrix	Sporer data trafik mellem 2 systemer
7	Filter	Kan filtrere datapakker. Kun bestemte data fra pakkerne ses
8	Packet capt.	Kan opsamle og gemme udvalgte datapakker
9	Events	Styre afsendelse af SNMP Trap's til remote clienter
10	Token Ring	Opsamling af data fra Token Ring baserede netværk

RMON II kategorier

RMON 2 kategorier		Beskrivelse
11	Protocol Directory	Viser hvilke protokoller en probe kan monitere. 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 konfigurering af probe parametre fx Trap destination
20	RMON Conformance	

Konfiguration af cisco

```
snmp-server community public RO
snmp-server community private RW
snmp-server location EUC MIDT lokale A22
snmp-server contact Henrik Thomsen - Phone: 89281000
snmp-server chassis-id Cisco 1721
snmp server ifindex persist
```

Perl og SNMP

- Der findes mange SNMP moduler
- Vi bruger blandt andet Net::SNMP

Anvendelse af Net::SNMP modulet

```
!#/usr/bin/perl -w
use strict;
use Net::SNMP;  #Brug Net::SNMP modulet

my $sysUpTime = '1.3.6.1.2.1.1.3.0';  # OID der skal hentes

my ($session, $error) = Net::SNMP->session(
                        -hostname      => '192.168.22.50',
                        -community     => 'public');

my $result = $session->get_request(  -varbindlist => [$sysUpTime] );

printf("sysUpTime for host '%s' is %s\n",
   $session->hostname, $result->{$sysUpTime} );

$session->close;

exit 0;
```

Resultat når programmet køres