

KRESTEN JACOBSEN

NETWORK MANAGEMENT

Hvad: Simple Network Management Protocol (oprindeligt design fra '80'erne.)

Hvorfor:SNMP: Kortlægning, overvågning og håndtering af netværks enheder.

Ikke kun enheder, som arbejder MED netværk, men alle typer enheder, som kobles PÅ netværk.

Eks.: industrielt udstyr; komplekse motorer; men også mere traditionelle it-enheder.

OVERBLIK: SNMP

- ▶ SMI: Defines rules for (MIB) objects og modules
- ▶ MIB: Management Information Base
- ▶ OID: Object Identifier
- ▶ SNMP: Simple Network Management Protocol
- ▶ Security and Administration (nyt i version 3)

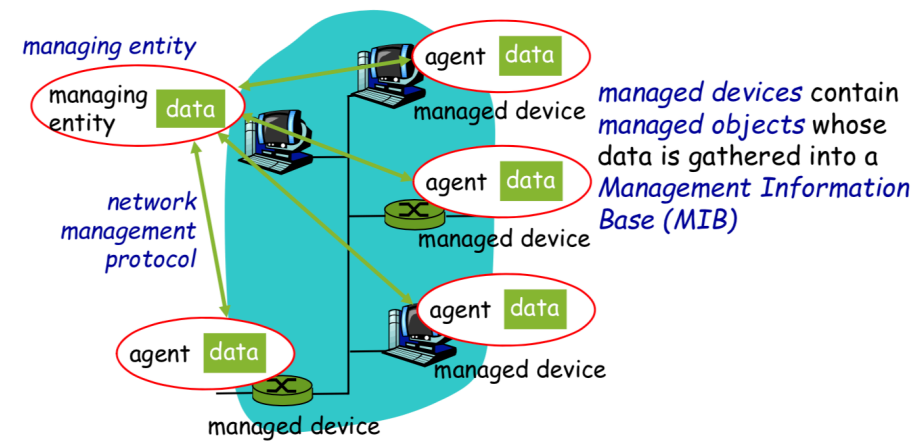
SMI: *Structure of Management Information:*
sprog-definition for MIB objekter.

MIB: *Management information base:*
distribueret informations datalager om 'network management' data.
(hvad kan vi interagere med og hvordan gør vi det)

OID: *Object Identifier:*
Måden hvorpå vi identificerer et givent objekt.
Navnet på objektet.

SNMP: *Simple Network Management Protocol:*
Protokollen vi kommunikerer over.

OVERBLIK: SNMP



1.3.6.1.4.1.9.XXX - Cisco's proprietære gren af OID-træet.

TEORI: SNMP BESKEDER OG VERSIONER

▸ Besked Typer

- GetRequest
- SetRequest
- Response
- Trap (og inform)

▸ Versioner

- V1 - Initiel version; begrænset funktionalitet, performance og sikkerhed
- V2 - Primært forbedring performance.
- V3 - Forbedret sikkerhed (kryptering)

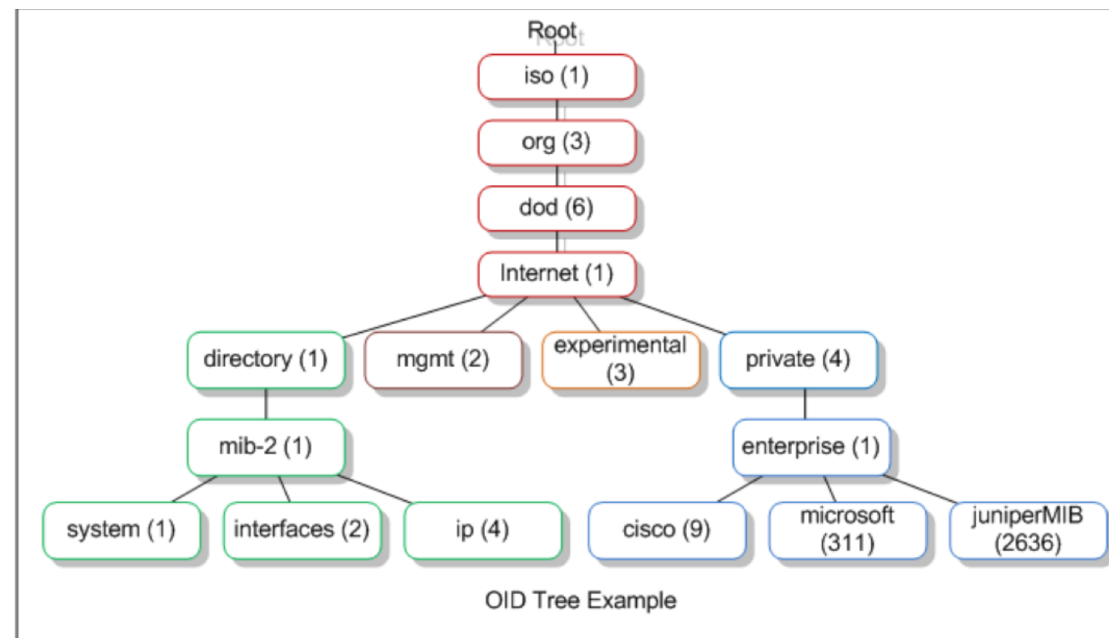
GetRequest - Forespørgsel mod udstyr

SetRequest - Ordre til udstyr

Response - Svar fra udstyr

Trap (og Inform) - Alarm fra udstyr (inform kræver besked tilbage om at alarmen er modtaget)

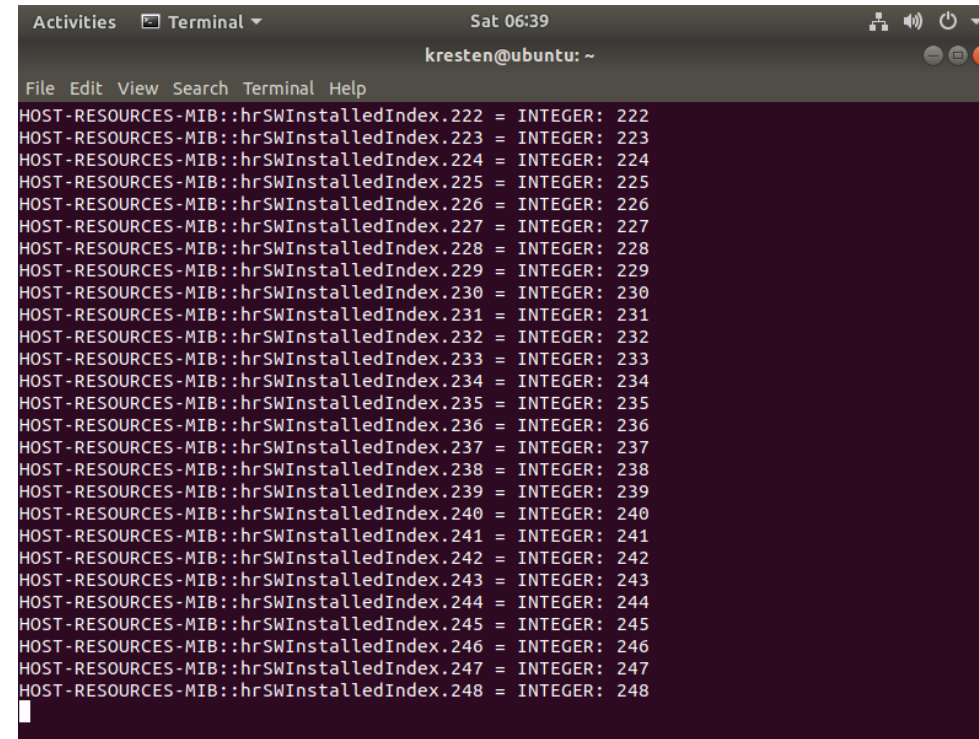
INDBLIK: SNMP



1.3.6.1.4.1.9.XXX - Cisco's proprietære gren af OID-træet.

EKSEMPEL: SNMPWALK

`snmpwalk -v3 -l authPriv -u user3 -a MD5 -A "user3password" -x DES -X "user3encryption" localhost`



```
Activities Terminal Sat 06:39
kresten@ubuntu: ~
File Edit View Search Terminal Help
HOST-RESOURCES-MIB::hrSWInstalledIndex.222 = INTEGER: 222
HOST-RESOURCES-MIB::hrSWInstalledIndex.223 = INTEGER: 223
HOST-RESOURCES-MIB::hrSWInstalledIndex.224 = INTEGER: 224
HOST-RESOURCES-MIB::hrSWInstalledIndex.225 = INTEGER: 225
HOST-RESOURCES-MIB::hrSWInstalledIndex.226 = INTEGER: 226
HOST-RESOURCES-MIB::hrSWInstalledIndex.227 = INTEGER: 227
HOST-RESOURCES-MIB::hrSWInstalledIndex.228 = INTEGER: 228
HOST-RESOURCES-MIB::hrSWInstalledIndex.229 = INTEGER: 229
HOST-RESOURCES-MIB::hrSWInstalledIndex.230 = INTEGER: 230
HOST-RESOURCES-MIB::hrSWInstalledIndex.231 = INTEGER: 231
HOST-RESOURCES-MIB::hrSWInstalledIndex.232 = INTEGER: 232
HOST-RESOURCES-MIB::hrSWInstalledIndex.233 = INTEGER: 233
HOST-RESOURCES-MIB::hrSWInstalledIndex.234 = INTEGER: 234
HOST-RESOURCES-MIB::hrSWInstalledIndex.235 = INTEGER: 235
HOST-RESOURCES-MIB::hrSWInstalledIndex.236 = INTEGER: 236
HOST-RESOURCES-MIB::hrSWInstalledIndex.237 = INTEGER: 237
HOST-RESOURCES-MIB::hrSWInstalledIndex.238 = INTEGER: 238
HOST-RESOURCES-MIB::hrSWInstalledIndex.239 = INTEGER: 239
HOST-RESOURCES-MIB::hrSWInstalledIndex.240 = INTEGER: 240
HOST-RESOURCES-MIB::hrSWInstalledIndex.241 = INTEGER: 241
HOST-RESOURCES-MIB::hrSWInstalledIndex.242 = INTEGER: 242
HOST-RESOURCES-MIB::hrSWInstalledIndex.243 = INTEGER: 243
HOST-RESOURCES-MIB::hrSWInstalledIndex.244 = INTEGER: 244
HOST-RESOURCES-MIB::hrSWInstalledIndex.245 = INTEGER: 245
HOST-RESOURCES-MIB::hrSWInstalledIndex.246 = INTEGER: 246
HOST-RESOURCES-MIB::hrSWInstalledIndex.247 = INTEGER: 247
HOST-RESOURCES-MIB::hrSWInstalledIndex.248 = INTEGER: 248
```

List alle resultater fra et OID-subtree

Løber alle 'management values' igennem med masser af SNMP GetNext-kommandoer

Se den installerede MIB struktur: `snmptranslate -Tp`

EKSEMPEL: NAGIOS

Service	Status	Last Check	Duration	Attempt	Status Information
Current Load	OK	2017-12-16 06:53:46	11d 21h 17m 4s	1/4	OK - load average: 1.41, 1.08, 0.57
Current Users	OK	2017-12-16 06:49:24	11d 21h 16m 14s	1/4	USERS OK - 1 users currently logged in
Disk Space	CRITICAL	2017-12-16 06:50:01	11d 21h 15m 24s	4/4	DISK CRITICAL - /run/user/1000/gvfs is not accessible: Permission denied
FTP	OK	2017-12-16 06:50:39	11d 21h 4m 28s	1/4	FTP OK - 0.052 second response time on 127.0.0.1 port 21 [220 (vsFTPd 3.0.3)]
HTTP	OK	2017-12-16 06:51:16	11d 21h 14m 34s	1/4	HTTP OK: HTTP/1.1 200 OK - 11192 bytes in 0.128 second response time
SSH	OK	2017-12-16 06:51:54	11d 21h 13m 44s	1/4	SSH OK - OpenSSH_7.5p1 Ubuntu-10

Hvad er Nagios?
Overvågningssystem baseret på SNMP.

- 1) Definér custom snmp-kald
- 2) Opsæt regl
- 3) Load Nagios