SNMP

Effektiviserad drift av datorsystem 1DV427

Innehåll

- Introduktion till SNMP
- Versioner (SNMP version 1, 2 och 3)
- Konfiguration
  - Communities
  - SMI, MIBs, OIDs
  - Polling
  - Traps
- SNMP-agenter
  - Nätverksenheter
  - Servrar

Introduktion till SNMP

- En samling enkla operationer för att kommunicera med SNMP-enheter
- Stänga av interface på router
- Kontrollera hastighet på interface
- Kontrollera temperatur
- Ge dig varning om temperaturen blir för hög

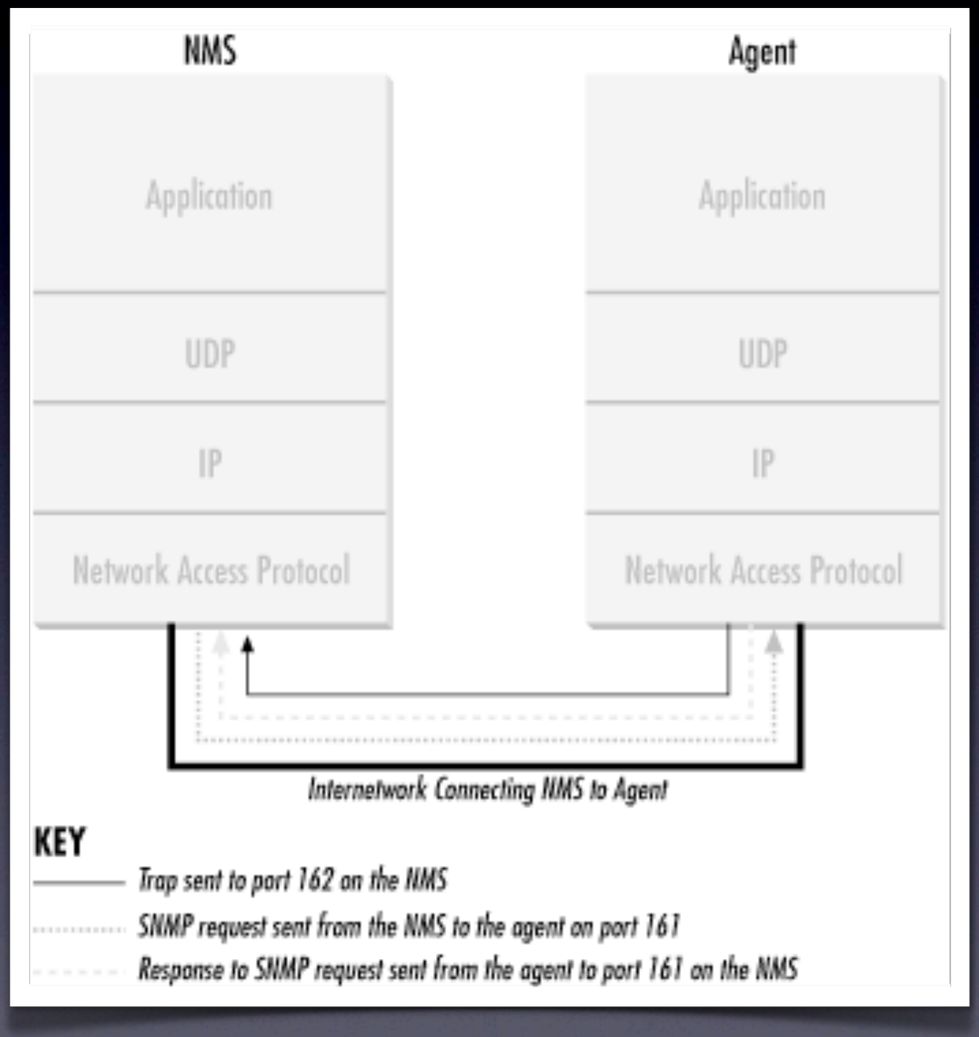
- Associeras oftast med nätverksenheter såsom routrar och switchar men fungerar för nästan all nätverksansluten utrustning

Kommunikation

- Kommunikation via UDP
- Fungerar bra för hämtande av information
- Värre för traps som bara skickas en gång

- Fördelar med UDP är låg overhead
- TCP över ett överbelastat nätverk är en dålig idé

- Använder UDP-port 161 för vanlig information och port 162 för traps



SNMPv1

- Första versionen, definierad genom RFC1157 och en hisktorisk IETF-standard
- Säkerheten är communitybaserad
- Finns tre communitys: read-only, read-write och trap
- SNMPv1 är historisk, dvs. den används normal sett inte längre
- Tyvärr fortfarande vanlig, speciellt på gamla enheter
- Kan köra över andra protokoll förutom UDP såsom CLNS, DDP och IPX

SNMPv2

- Är mycket lik SNMPv1, men har en del förbättringar
- Om en förfrågan skickas men förfrågan innehåller fel så behandlas detta korrekt
- Förbättrad säkerhet
- Allt utom destinationen i paketet är krypterat

SNMPv3

- Framför allt bättre säkerhet
- Meddelandeintegritet
- Autentisiering
- Kryptering
- Större möjligheter att använda SNMPv3 för fjärrkonfigurering av enheter

SNMP-communities

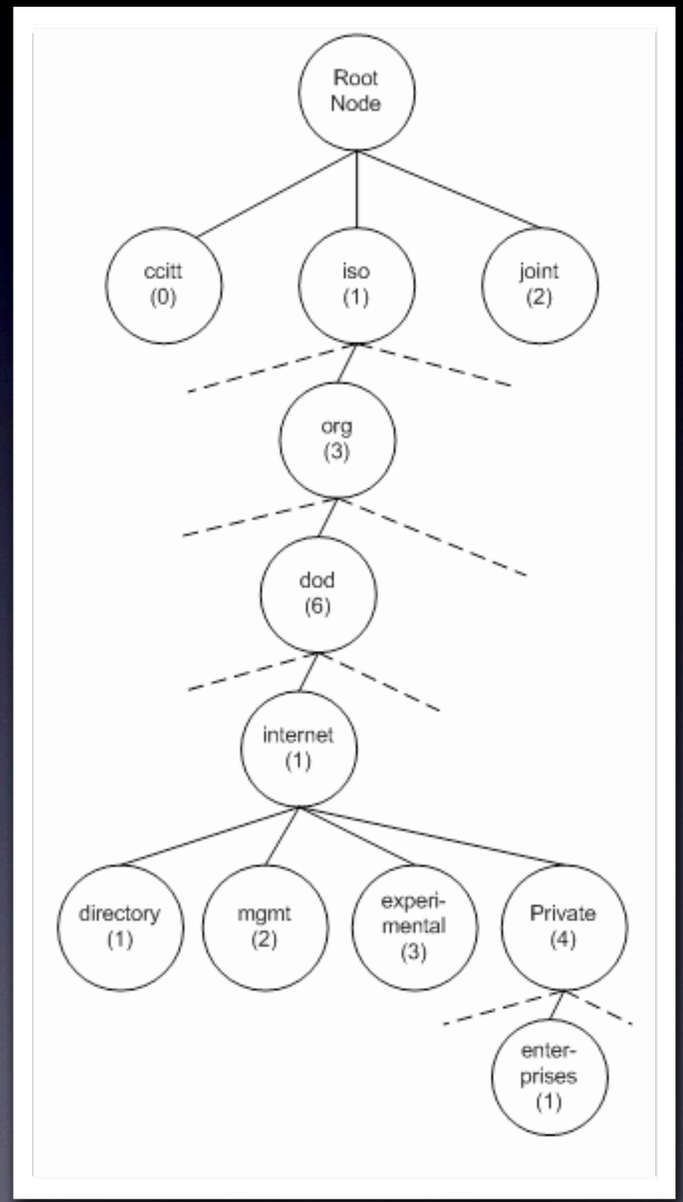
- Sätter upp relationer mellan managers och agenter
- Tre communities som tar hand om olika aktiviteter
  - Read-only – Bara för att läsa ut värden
  - Read-write – Läsa och modifera värden
  - Trap – Ta emot traps från agenter
- Glöm inte att ändra standardnamnen
- Skickas i klarttext i SNMPv1
- Finns möjlighet för säker autentisiering och överföring i SNMPv3
- Ska behandlas som lösenord

SMI – Struktur på managementinformation

- Namn
  - Kallas OID (Object IDentifier)
  - Numeriskt och läsbart
- Typ och attribut
  - Datatypen hos ett objekt sätt som ett subvärde till ASN.1 (Abstract Syntax Notation One)
  - Detta är totalt maskin/OS-oberoende
- Kodning
  - Bestämmer hur data kodas för att skickas över t.ex. Ethernet

OID

- Objekt som kan anropas via SNMP organiseras i träd
  - I detta fallet 1.3.6.1.4.1 om man följer trädet
- Alla kan registrera egna enterprise-nummer för sina specifika enheter
- Cisco har t.ex. 1.3.6.1.4.1.9 eller iso.org.did.internet.private.enterprises.cisco
- Detta utökar möjligheterna för företag och tillverkare



MIB-2

- MIB-2 innehåller objekt som alla SNMP-enheter har stöd för
- Innehåll (du kan läsa full beskrivning i RFC 1213)
  - system (1.3.6.1.2.1.1)
  - interfaces (1.3.6.1.2.1.2)
  - at (1.3.6.1.2.1.3)
  - ip (1.3.6.1.2.1.4)
  - icmp (1.3.6.1.2.1.5)
  - tcp (1.3.6.1.2.1.6)
  - udp (1.3.6.1.2.1.7)
  - egp (1.3.6.1.2.1.8)
  - transmission (1.3.6.1.2.1.10)
  - snmp (1.3.6.1.2.1.11)

SNMP-kommandon

- PDU (Protocol Data Unit)
  - get
  - getnext
  - getbulk
  - set
  - getresponse
  - trap
  - notification
  - inform
  - report

get

- Initieras av NMS
- Agenten svarar med get response
- Som exempel kan den efterfråga OIDt 1.3.6.1.2.1.1.6.0
- Svar: system.sysLocation.0 = “Building 18, cabinet 2”

getnext

- Hämtar hem information från en grupp av värden i en MIB
- get och getresponse genereras till varje enskild variabel i gruppen
- Detta kan ses som en slags sökning i en MIB
- Du kan t.ex. skicka med “system” till detta kommandot så kommer du att få ut alla variabler i gruppen “system”
- Exempel:
  - system.sysDescr.0 = “Cisco IOS Software...”
  - system.sysObjectID.0 = OID: enterprises.9.1.19
  - system.sysUpTime.0 = TimeTicks: (27210723) 3 days, 3:35:07.23
  - system.sysContact.0 = “”
  - system.sysName.0 = “cisco.hik.se”
  - system.sysLocation.0 = “Building 18, cabinet 2”
  - system.sysServices.0 = 6

getbulk

- get kan försöka hämta flera MIB-objekt på en gång, men svarets storlek är begränsad
- getbulk gör samma sak, men tillåter svar som inte är fullständiga

set

- NMSen skickar set och försöker ändra sysLocation till “Kalmar”
- Agenten tar emot set-kommandot och undersöker om NMSen har rätt att ändra sysLocation
- När alla checks har gåtts genom skickar den get response med error-kod om något gick fel, om allt gick som det ska sätter den sysLocation och svarar med noError.

SNMP-traps

- Skickas från agent till NMS
- Skickas när något händer efter vissa regler
- Ingen bekräftelse på att det kommer fram
- Vad en trap betyder bestäms med ett visst nummer
- Följande nummer finns
  - coldStart(0) – Agenten har startats om, alla variabler nollställda
  - warmStart(1) – Ominitiering av agent, variabler finns kvar
  - linkDown(2) – Ett interface på enheten har gått ner
  - linkUp(3) – Ett interface på enheten har kommit upp
  - authenticationFailure(4) – Någon har försökt ansluta och skicka ett kommando till enheten med en felaktig communitysträng
  - egpNeighborLoss(5) – En EGP-granne har gått ner
  - enterpriseSpecific(6) – Indikerar att trapen är enterprisespecifik, dvs. egendefinierade traps som ligger under private-enterprise under SMI-objektträdet

Egendefinierade traps

- Exempel på en egendefinierad trap i MIBen RDBMS

```
rbmsOutOfSpace TRAP-TYPE
        ENTERPRISE    rdbmsTraps
        VARIABLES     {rdbmsSrvInfoDiskOutOfSpaces }
        DESCRIPTION
            "An rdbmsOutOfSpace trap signifies that one of the database
            servers managed by this agent has been unable to allocate
            space for one of the databases managed by this agent. Care
            should be taken to avoid flooding the network with these traps."
    ::=2
```

- Exempelvis Oracle skickar med egna SNMP-agenter till sina databaser

SNMP-agenter

- Måste finnas på alla enheter som ska SNMP-övervakas
- Består av mjukvara som finns på enheten du ska övervaka
- Specialskriven på t.ex. nätverksenheter
- Specialskriven eller generell på servrar och datorer

SNMP-agenter

- Gemensamma parametrar
- sysLocation – Var enheten finns
- sysContact – Administratörens mail eller annan kontaktinfo
- sysName – Enhetens namn (FQDN)
- Communitysträngar för read-write, read-only och (oftast) trap
  - Som standard satta till private, public och trap
- Trapdestination – NMS som traps ska skickas till

Net-SNMP

- Programvarusvit för SNMP på datorer
- Mer innehållsrik än t.ex. Windows inbyggda SNMP-stöd
- Stöd för Windows, Linux, Solaris, Mac OS X, etc
- Open Source under BSD-licens

MIBs

- Bytesphere
- http://www.oidview.com/mibs/detail.html

- MIB Search
- http://www.mibsearch.com/

- Finns även ofta på tillverkarens hemsida

Demo