

SNMP

Lennart Franked

email:lennart.franked@miun.se

Avdelningen för informationssystem och -teknologi (IST)
Mittuniversitetet

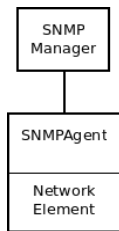
25 november 2019

Inför *föreläsning fem* bör ni ha läst [5, kap 4, 5, 6 samt 9.1] alternativt [2, kap 2].

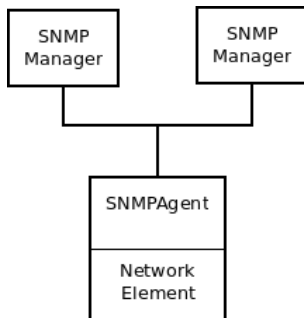
- Började som en industristandard.
- Första RFCerna för SNMP kom 1988 [4], [3] samt [1].
- Ursprungligen framtaget för att övervaka Internetkomponenter.
- Används numera till att övervaka allt från backbone-routrar till skrivare.

SNMPv1

Tvålayersmodellen

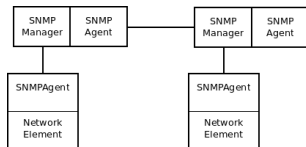


Figur: En manager, en agent [5]



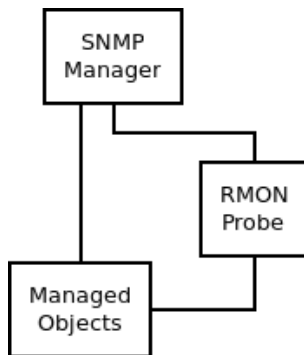
Figur: Flera managers, en agent [5]

Två stycken Managers kommunicerar sinsemellan.



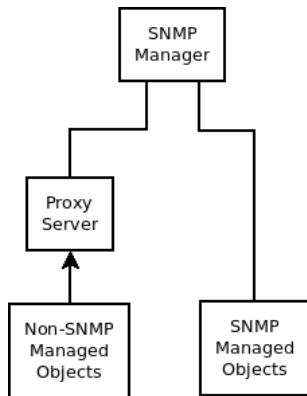
Figur: Flera managers, flera agenter [5]

Trelagersmodellen med RMON



Figur: RMON [5]

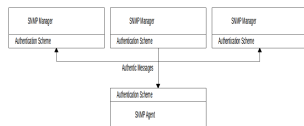
Trelagersmodellen med RMON, övervaka icke SNMP-kompatibla enheter.



Figur: RMON [5]

SNMP Community.

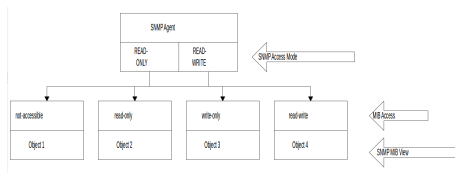
- Kopplingen Manager och Agent kallas en Community.
- Säkerheten i SNMPv1 är baserad på en community profil.
- Authentisering finns i agent och manager.
- Community-namnet anges som en textsträng.
- Agent och Manager måste tillhöra samma community för att kommunicera.
- Agent och manager kan tillhöra flera communities.



Figur: SNMP Community överblick [5]

SNMP Community Profil.

- Agenten har enbart tillgång till en delmängd av MIB-trädet.
 - ▶ Community MIB View
- Varje Community har en åtkomstmetod: Läs-Skriv.
- Community profilen: Community MIB View + åtkomstmetod.

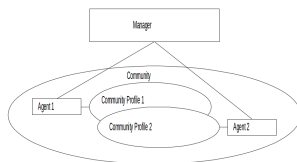


Figur: SNMP Community Profile [5]

- Administrativa modellen är SNMPs access policy
- Access policyn är baserad på Community och Community Profilen.

SNMP Access Policy.

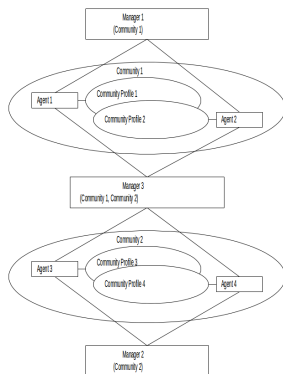
- Manager tillhör Community 1 samt 2.
- Agent 1 har enbart tillgång till Community 1
- Agent 2 har enbart tillgång till Community 2



Figur: SNMP Access Policy [5]

Överblick Administrativa modellen.

- Manager 1 administrerar community 1.
- Manager 2 administrerar community 2.
- Manager 3 administrerar community 1,2.



Figur: SNMP Administrativa modellen[5]

SNMP har utvecklats och kommit i nya versioner sedan den första RFCen publicerades.

- SNMPv1 - Utvecklades som en kortsiktig lösning.
- SNMPv2 - Bryta sig loss från OSI-standarden
- SNMPv2c - Community-baserad säkerhet, defacto för v2.
- SNMPv3 - Säkerhet lades till.

Fem SNMP PDU-typer måste vara implementerade i samtliga SNMP versioner.

- GetRequest
- GetNextRequest
- GetResponse
- SetRequest
- Trap
 - ▶ Generic
 - ▶ Specific/Enterprise
 - ▶ Time-stamp

SNMP TRAP

- Enterprise – System-Id av enheten.
- Agent Address – agentens adress
- Generic Trap Type – typ av trap
- Specific Trap Type – specifik trap
- Time-Stamp – Tidsstämpel sedan agenten startades
- VarBind Name/Value – Objektskalären



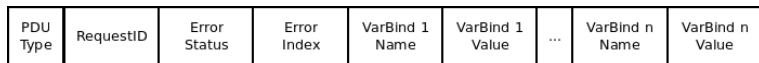
Figur: SNMPv1 Trap PDU [5]

Tabell: Generella traps

Generic-Trap Type	Description
coldStart(0)	SNMP-agenten startar, information kan vara ändrad
warmStart(1)	SNMP-agenten startar, information oförändrad
linkDown(2)	En länk har gått ner
linkUp (2)	En länk har gått upp
authenticationFailure(4)	Ej godkänd autentisering
egpNeighborLoss	Koppling mot en EGP-enhet har tappats
enterprise	Enterprise specifikt trapmedelande.

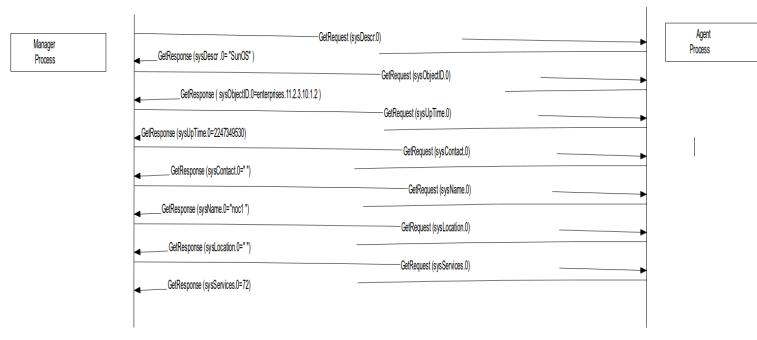
SNMP GET/Request PDU

- RequestID – Spåra meddelande.
- Error Status – Felmeddelande.
- Error Index – Ytterligare information.
- VarBind Name – Objektamn.
- VarBind Value – Objektets värde.



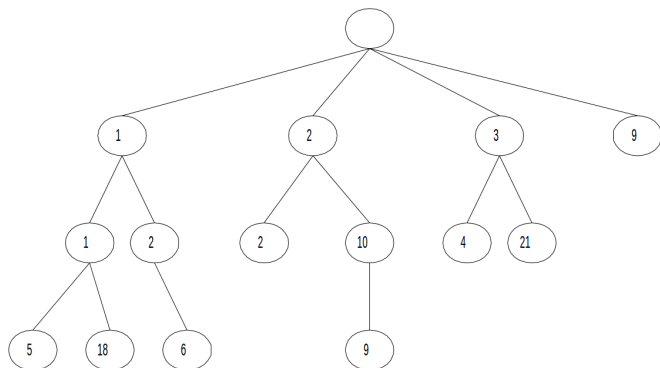
Figur: SNMP Get och SET PDU [5]

SNMP GetRequest.



Figur: Get-Request [5]

SNMP GetNextRequest.



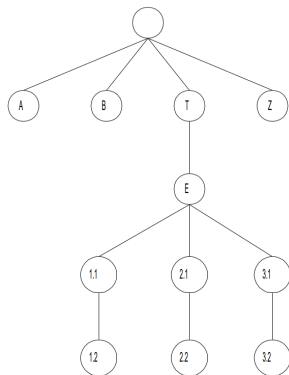
Figur: MIB-träd - GetNext [5]

MIB GetNextRequest hämtar objekt utifrån en lexikografisk ordning.

Numerisk ordning	Lexikografisk ordning
1	1
2	1118
3	115
9	126
15	15
22	2
34	22
115	250
126	2509
250	3
321	321
1118	34
2509	9

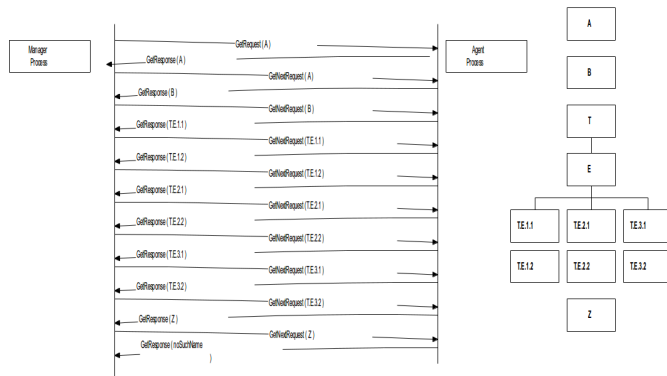
Tabell: Exempel, Numerisk mot Lexikografisk ordning [5]

MIB GetNext



Figur: GetNextRequest [5]

MIB GetNextRequest meddelanden.



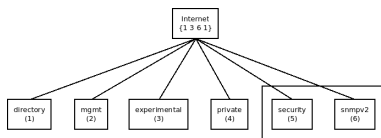
Figur: GetNextRequest [5]

SNMPv2

Uppdateringar SNMPv2 mot SNMPv1

- Skicka data i bulk.
- Kommunikation direkt mellan två managers.
- Uppdaterad SMI, SMIv2.
- Underlätta skapandet av nya datatyper.
- Standardisera kompatibiliteten, krav på funktionalitet.
- Underlätta användningen utav tabeller för datapresentation.
- Utökat MIB med två grupper, security och snmpv2.
- Möjliggör användandet av andra transportprotokoll än UDP.
- Säkerhetsfunktioner implementerades ej, bordlades till v3.

SNMPv2 internet MIB.

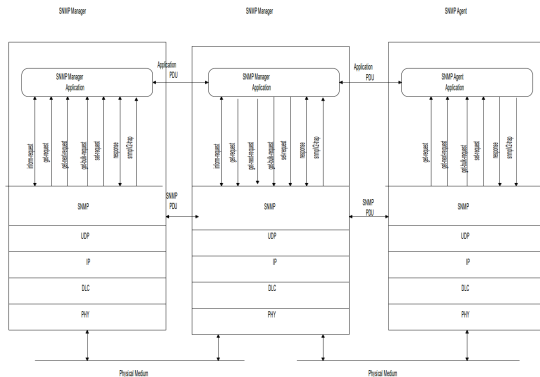


Figur: förändringar under internet-gruppen [5]

- Utökad antal objekt under System.
- Sett över SNMP-gruppen.
- SNMPv2 tillagt.
- Security lades till (ej använd).

SNMPv2 Systemarkitekturen.

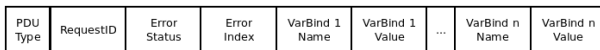
- 7 typer av meddelanden.
- Två managers kan kommunicera direkt med varandra.
- Report - meddelande, används ej.



Figur: SNMPv2 arkitekturen [5]

SNMPv2 PDU struktur

- Samma PDU för samtliga meddelandetyper bortsett från bulk.
- Error-status satt till 0 eller ignoreras vid get, req, set.
- Error används vid svarspaketen.



Figur: SNMPv2 PDU [5]

SNMPv2 Felhantering.

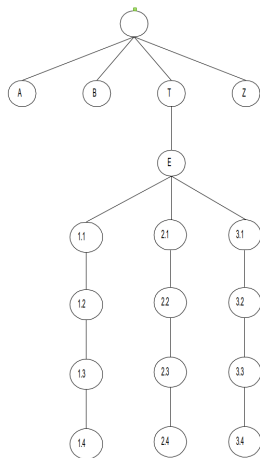
- I SNMPv1 returneras enbart variabler om error-status är satt till 0.
- I SNMPv2 ignoreras variabelfältet(n) om error-status är $0 <$.
- Om error-status och error-index är $0 <$ ignoreras enbart berört värde och övriga variabler läses in.

SNMP getBulk PDU strukturen.

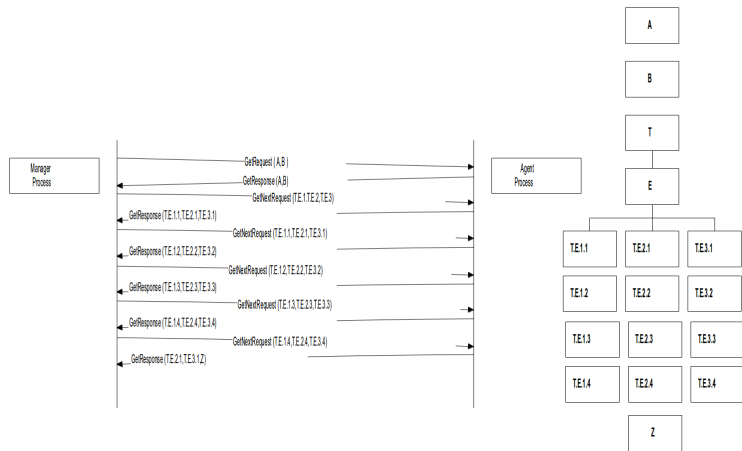
- Error status utbytt mot Non-repeaters.
- Error index utbytt mot Max repetitions.
- Non-repeaters – anger hur många objekt som skall hämtas enbart en gång (för skalärer).
- Max repetitions – anger hur många fält i en tabell som skall hämtas.

PDU Type	RequestID	Non-Repeater	Max Repetitions	VarBind 1 Name	VarBind 1 Value	...	VarBind n Name	VarBind n Value
----------	-----------	--------------	-----------------	----------------	-----------------	-----	----------------	-----------------

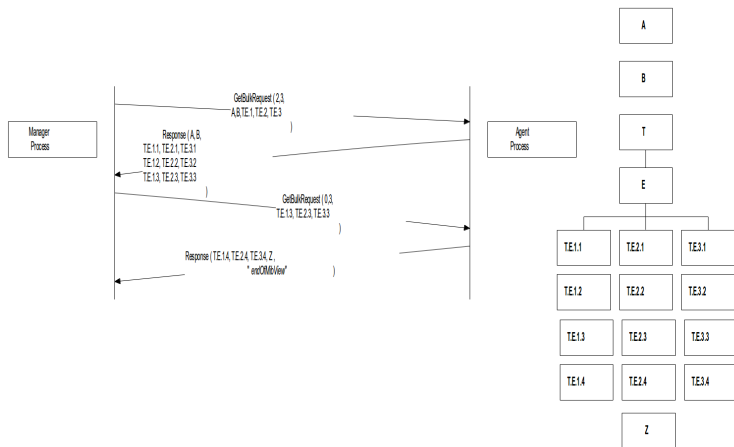
Figur: SNMPv2 getBulk PDU [5]



Figur: MIB Träd [5]



Figur: Hämta data med GetNext [5]



Figur: Hämta data med getBulk [5]

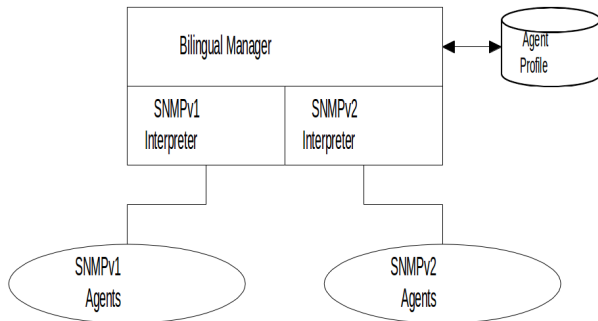
Inform-Request

- Skickas oombedd.
- Svar skickas med ett SNMP Response.

PDU Type	RequestId	Error Status	Error Index	VarBind1 SysUpTime	VarBind 1 Value	VarBind 2 snmpTrapOID	...	VarBind n Name	VarBind n Value
----------	-----------	--------------	-------------	--------------------	-----------------	-----------------------	-----	----------------	-----------------

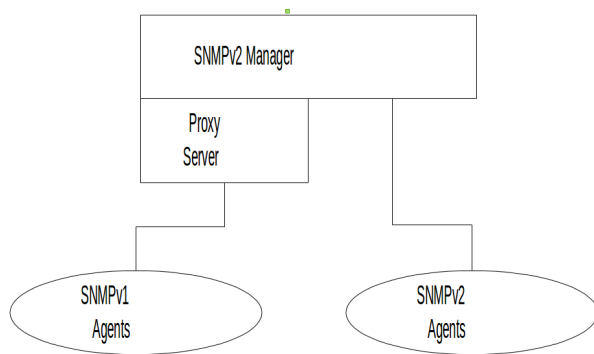
Figur: Inform-Request PDU [5]

SNMPv1 kompatibilitet - Tvåspråkig manager.







Figur: Tvåspråkig Manager [5]

SNMPv1 kompatibilitet - Proxy.



Figur: SNMPv1 Proxy [5]

-  J.D. Case m. fl. *Simple Network Management Protocol*. RFC 1067. Obsoleted by RFC 1098. Internet Engineering Task Force, aug. 1988. URL: <http://www.ietf.org/rfc/rfc1067.txt>.
-  Douglas R. Mauro och Kevin J. Schmidt. *Essential SNMP [help for system and network administrators]*. 2. ed.. Farnham: O'Reilly, 2005. ISBN: 0-596-00840-6.
-  K. McCloghrie och M.T. Rose. *Management Information Base for network management of TCP/IP-based internets*. RFC 1066. Obsoleted by RFC 1156. Internet Engineering Task Force, aug. 1988. URL: <http://www.ietf.org/rfc/rfc1066.txt>.
-  K. McCloghrie och M.T. Rose. *Structure and identification of management information for TCP/IP-based internets*. RFC 1065 (INTERNET STANDARD). Obsoleted by RFC 1155. Internet Engineering Task Force, aug. 1988. URL: <http://www.ietf.org/rfc/rfc1065.txt>.



Mani. Subramanian, Timothy A. Gonsalves och N. Usha Rani.
Network management : principles and practice. 2. utg. Noida, India:
Dorling Kindersley, 2011. ISBN: 978-81-317-3404-9.