SNMPv3 – Nätverksövervakning

Lennart Franked
email:lennart.franked@miun.se

Informations och Kommunikationssystem (IKS)
Mittuniversitetet

21 september 2015

Läsanvisningar

Inför *föreläsning sex* bör ni ha läst [2, kap 7-8].

1. SNMPv3
   - Översikt
   - SNMP Motor
   - Identifiering
   - SNMPv3 Application
   - Säkerhet

2. RMON
   - Remote Monitoring
   - RMON1 – MIB grupper
   - RMON2 – MIB grupper

- Modulariserat SNMP arkitekturen och dokumentationen.
- Integrerade SNMPv1 och SNMPv2, tillåter bakåtkompatibilitet.
- SNMP-engine
- Säkerhet.

- SNMP entitet är en nod med SNMP funktionalitet.
- Antingen Agent eller Manager.
- En entitet associeras med tre namn.
  - Entitetsnamnet.
  - Identitetsnamnet.
  - Management Information

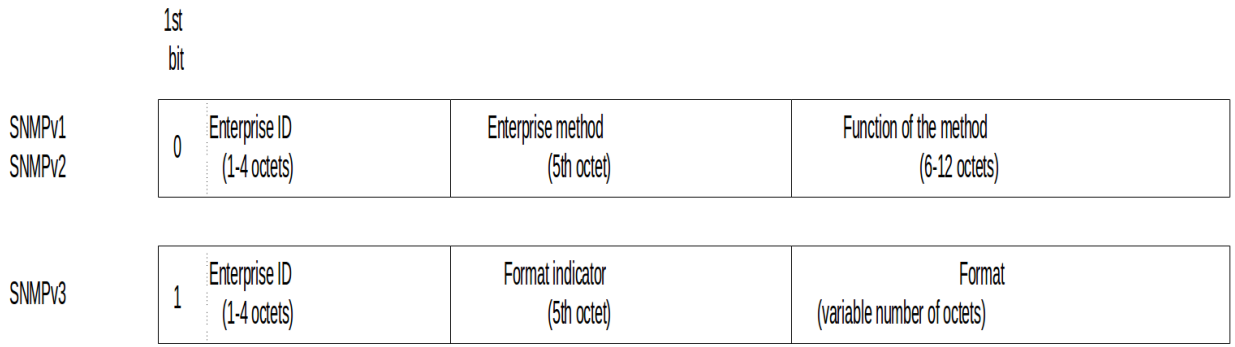
SNMPv3 Arkitekturen.

Figur: SNMPv2 arkitektur överblick [2]

SNMP motorn (SNMP Engine).

- Varje entitet har en motor.
- Består utav:
  - En sändare (dispatcher).
  - Meddelandebearbetningsubsystem (Message Processing Subsystem).
  - Säkerhetssubsystem.
  - Accesskontrolssubsystem (Access Control Subsystem).

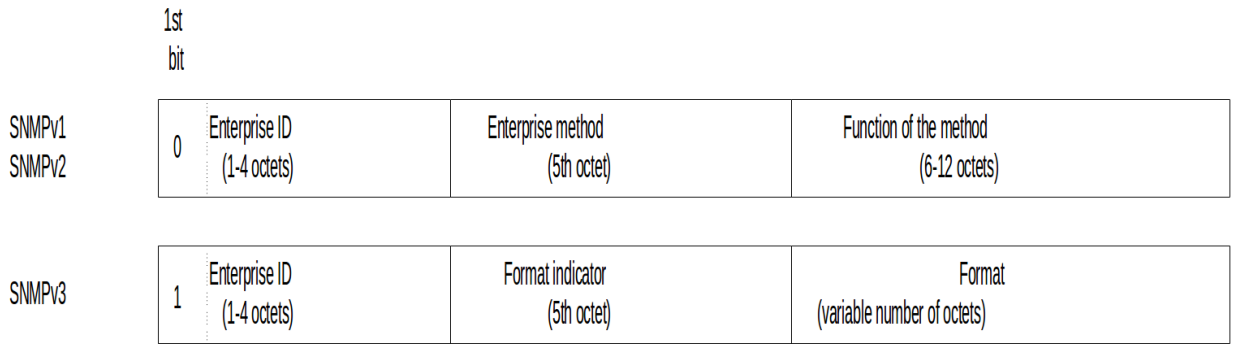
- Identifieras med hjälp av motorId (engine ID).
- 12 oktetter för SNMPv1 och SNMPv2.
- variabel längd för SNMPv3.



Figur: Engine ID [2]

EngineID för SNMPv1 och SNMPv2.

- Första fyra oktetterna agentens företagsnummer (Enterprise number).
- Femte oktetten för SNMPv1 och v2 anger hur Id:t togs fram. (IP).
- Oktett 6 - 12 - Värdet av funktionen.



Figur: Engine ID [2]

EngineID för SNMPv3.

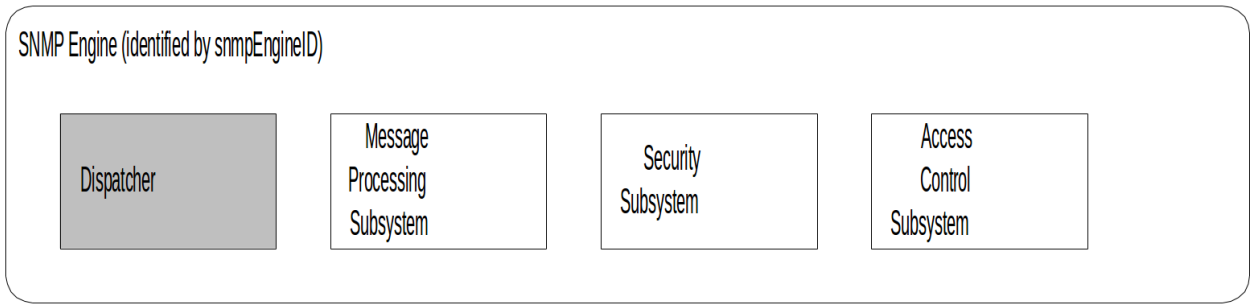
- Första fyra oktetterna agentens företagsnummer (Enterprise number).
- Femte oktetten anger formatet.
- Oktett 6 - 12 - Värdet av funktionen.

0	Reserverad, oanvänd
1	IPv4 adress (4 oktetter)
2	IPv6 adress (16 oktetter)
3	MAC adressen (6 oktetter)
4	Text, administrativt satt
5	Oktetter, administrativt satt
6-127	Reserverad, oanvänd
128-255	Företagsdefinierat

Tabell: SNMPv3 Engine ID, femte oktetten[2]

SNMPv3 Sändare (dispatcher)

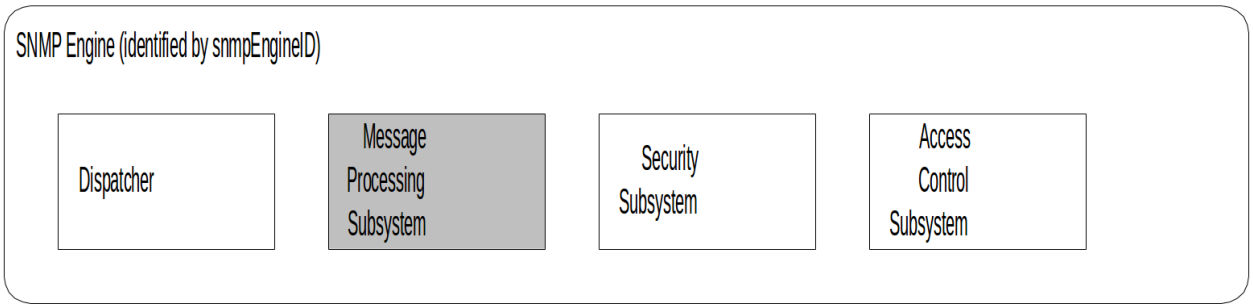
- En sändare i motorn, hanterar både SNMPv1,2 och 3.
- Funktion:
  - Skickar och tar emot meddelanden på nätverket.
    - ★ Transport mapper
  - Identifierar vilken version an SNMP som används.
    - ★ Message dispatcher – Koppling nätverk - MPS.
  - Tillhandahåller ett interface för SNMP-applikationen.
    - ★ PDU dispatcher – Koppling applikation och MPS.



Figur: SNMP sändare [2]

SNMPv3 meddelandebearbetningssubsystem (Message Processing Subsystem)

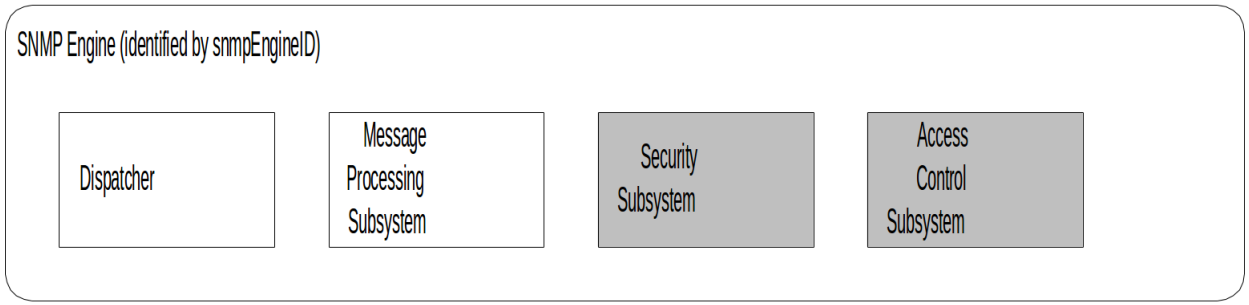
- Består utav en eller flera meddelandebearbetningsmoduler
- En modul för varje SNMP version.
- Identifieras av dispatcher via PDU header.



Figur: SNMP MPS [2]

SNMPv3 Säkerhet och Access subsystem (Security och Access Subsystem)

- Förser protokollet med konfidentialitet, Integritet och Authentisering.
- Möjliggör att man kan styra vem som har åtkomst och vad de har tillgång till.



Figur: SNMP SM [2]

Två namngivelser används för att identifiera en enhet.

- Huvudsakligt namn (principal name)
  - Vem skickar begäran.
  - En person eller applikation.
- Säkerhetsnamn (securityName)
  - Mänskligt läsbar textsträng.
  - Representerar en person.

Principal vs. SecurityName

Principal (huvudsakligt namn); dolt, baserat på säkerhetsmodellen.
SecurityName, läsbart och tillgängligt för alla.

SNMP Context

An SNMP context, or just "context" for short, is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context. An SNMP entity potentially has access to many contexts. [1]

- Kontext definieras som en samling av information tillgänglig för en specik entitet.
- Kontext ges ett unikt kontextID samt kontextNamn.
- Möjliggör att unikt kunna identifiera en kontext om en agent hanterar flera instanser av ett objekt.

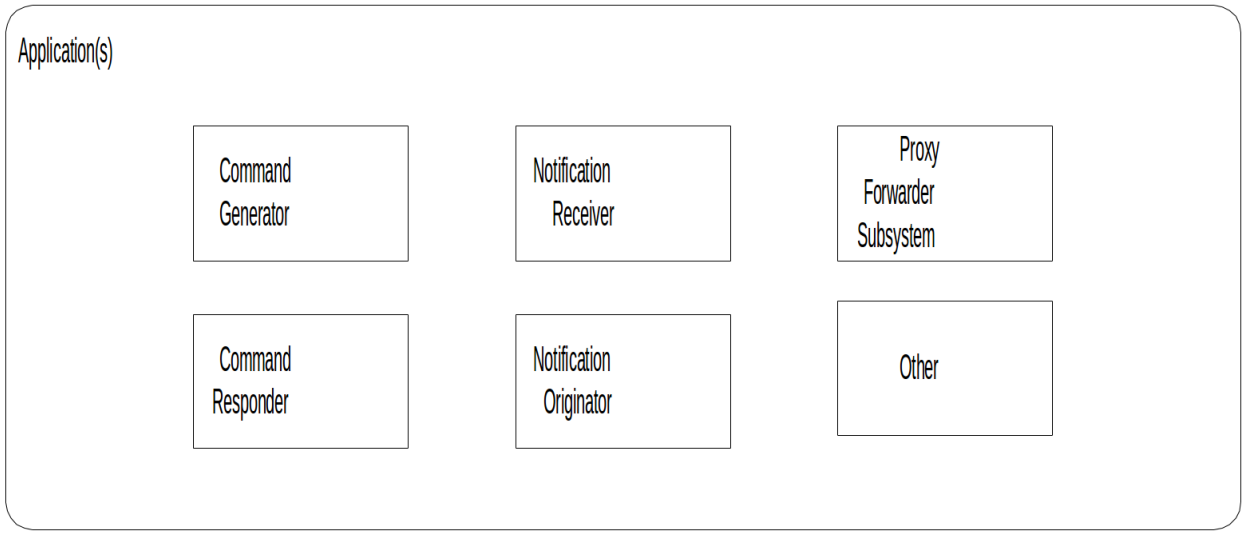
Exempel

En router med ett flertal interfacemoduler där varje modul har en egen kontext. Varje modul har exempelvis ett objekt för IP, MAC osv.

SNMPv3 har definierat 5st typer av applikationer som skall finnas i en SNMPv3 implementering.

- Command generator
- Command responder
- Notification originator
- Notifiation receiver
- Proxy Forwarder
- Other

SNMPv3 Applikation II



Figur: SNMPv3 applikationer[2]

Command generator

Används för att generera *get-request*, *get-next-request*, *get-bulk* och *set-request*.

- Genererar meddelanden att skicka.
- Hanterar svarsmeddelanden.

Command responder

Hanterar inkommande förfrågningar från legitima källor. Utför förfrågad funktion därefter skapar ett svarspaket.

Notification originator

Genererar trap/notification/inform meddelanden. Samma funktion som *Command Responder*, med undantag för att den även måste ta reda på destination, SNMP-version samt säkerhetsparametrar.

Notification Receiver

Som *Command Responder* fast tar emot SNMP trap/notifikation/inform meddelanden.

Proxy Forwarder

Skickar vidare SNMP meddelanden oavsett innehåll. Hanterar enbart SNMP-PDUer.

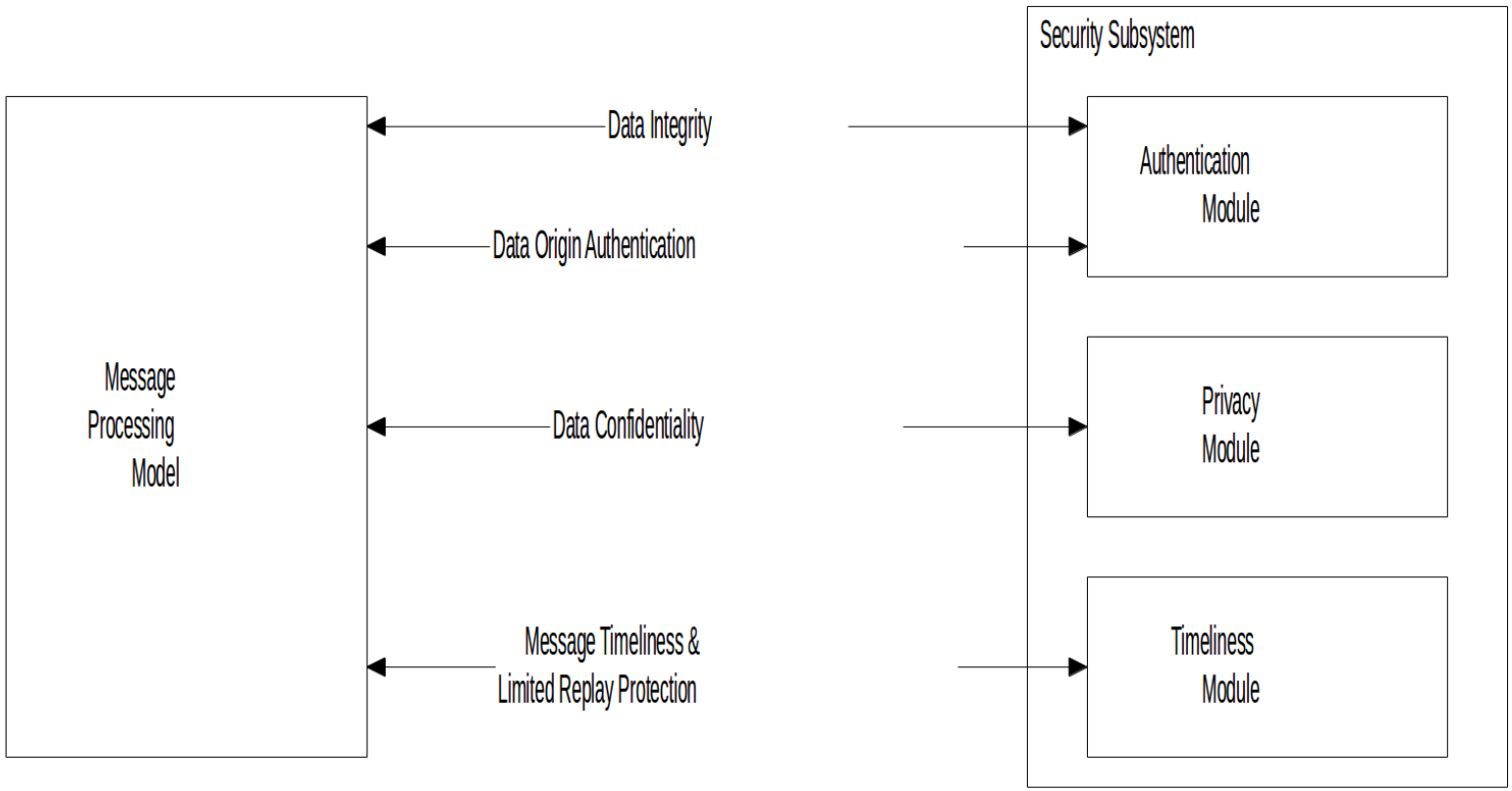
- Skickar SNMP-data vidare till en annan manager.
- Vidarebefordrar traps/notifiering/inform meddelanden beroende på källa.
- Om vidarebefordring av meddelande skedde, skickas även svarsmeddelanden tillbaka via proxy-applikationen.

- Brist på säkerhet i tidigare versioner.
- Authentisering, privacy, konfidentialitet samt integritetskontroll.
- Tillåter användandet av frivilligt protokoll för authentisering och konfidentialitet.
- IETF har specificerat HMAC-MD5-96 samt HMAC-SHA-96 för authentisering och
- CBC-DES för konfidentialitet.

Hot mot SNMP.

- Modifiering och förvanskning utav data.
- Spoofing – Utge sig för att vara en authentiserad användare.
- Avlyssning.

SNMPv3 Säkerhet III



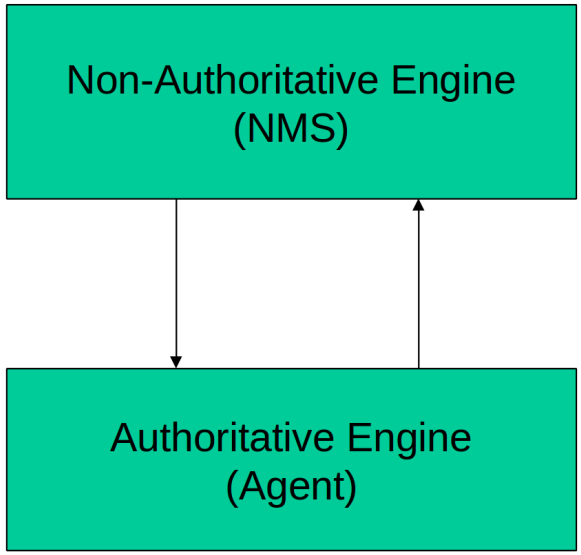
Figur: Säkerhetstjänster [2]

Auktoritativ

Mottagare av get, get-next, set, inform eller sändare av response och trap är den auktoritativa motorn. Ansvarig för att tillhandahålla en korrekt tidsstämpel och ett unikt ID.

Ej-Auktoritativ

Skapar en tabell med tid och ID för varje SNMP motor som den kommunicerar med.



Figur: Auktoritativa och icke-auktoritativa SNMP engines. [2]

SNMPv3 Authentiseringsmodul.

Authentiseringsmodul

Förser SNMPv3 med två tjänster *integritet* och *avsändar authentisering*.

Authentiseringsmekanism

Authentiseringsmodulen förser varje meddelande med ett unikt ID som är kopplat till den auktoritativa SNMP motorn. Försäkrar att avsändaren och mottagaren är behörig och den som den utger sig för att vara.

SNMPv3 Privacy.

Privacy

Förser SNMPv3 med *data konfidentialitet*.

Authentiseringsmekanism

Privacymodulen krypterar varje meddelande och på så vis försäkrar att ingen obehörig får tillgång till innehållet.

SNMPv3 Timeliness.

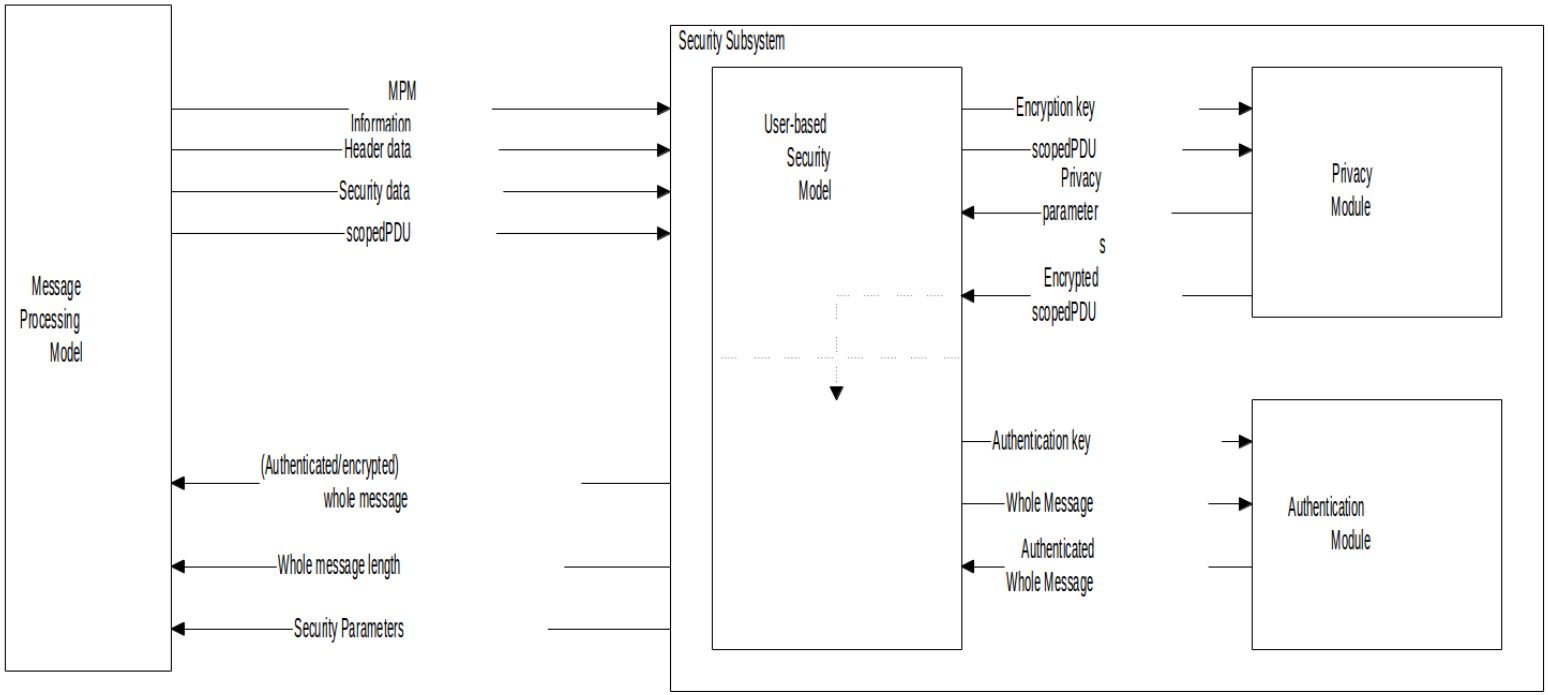
Timeliness

Förser SNMPv3 med *korrekt tidsdata*.

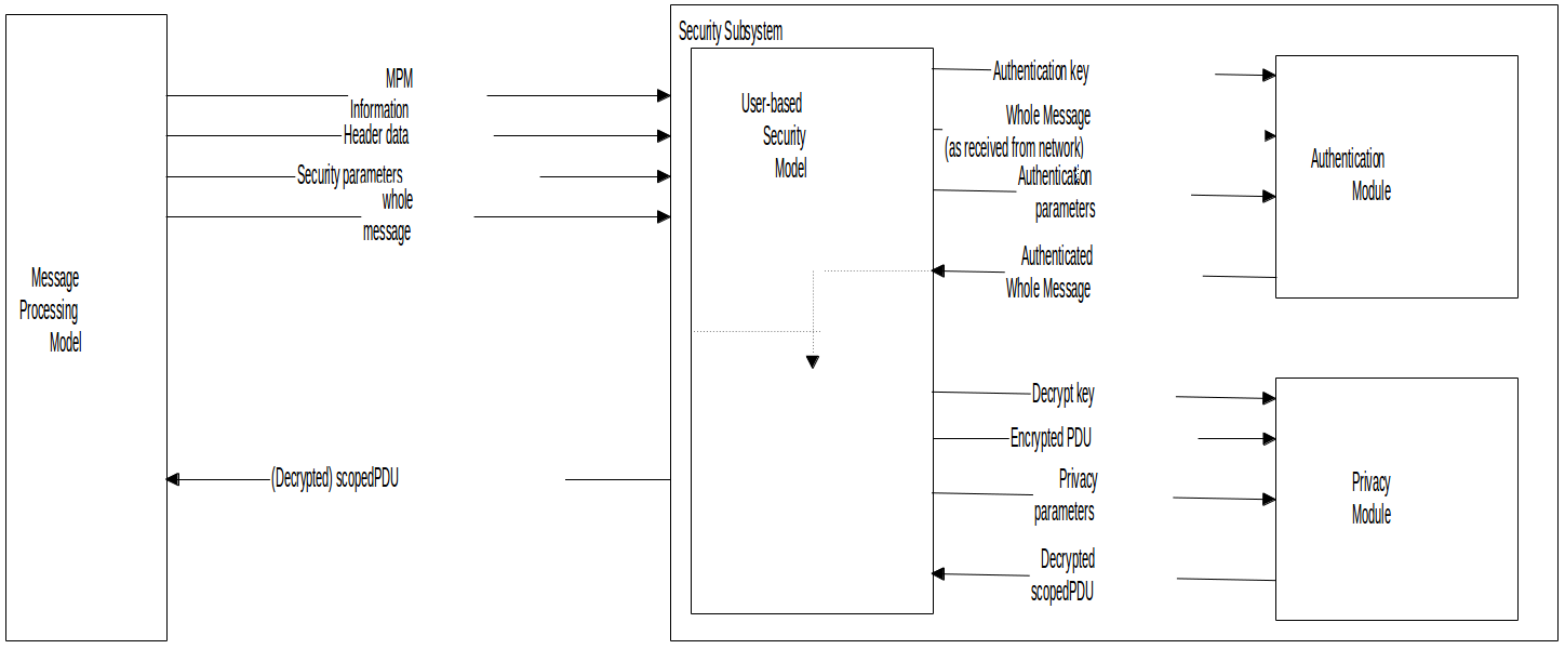
Mekanism

Sätter en tidsram för en mottagare att motta paketet. Försvårar replay, man-in-the-middle.

Användarbaserad Säkerhetsmodell (User-based Security Model)



Figur: Utgående meddelanden [2]



Figur: Inkommande meddelanden [2]

Säkerhetsnivåer

- Auth
- Priv
- AuthPriv

- Vem är du?
- Vart vill du?
- Hur är du säkrad?
- Syfte för åtkomst?
- Vilket objekt vill du ha tillgång till?
- Vilken instans av objektet vill du ha tillgång till?

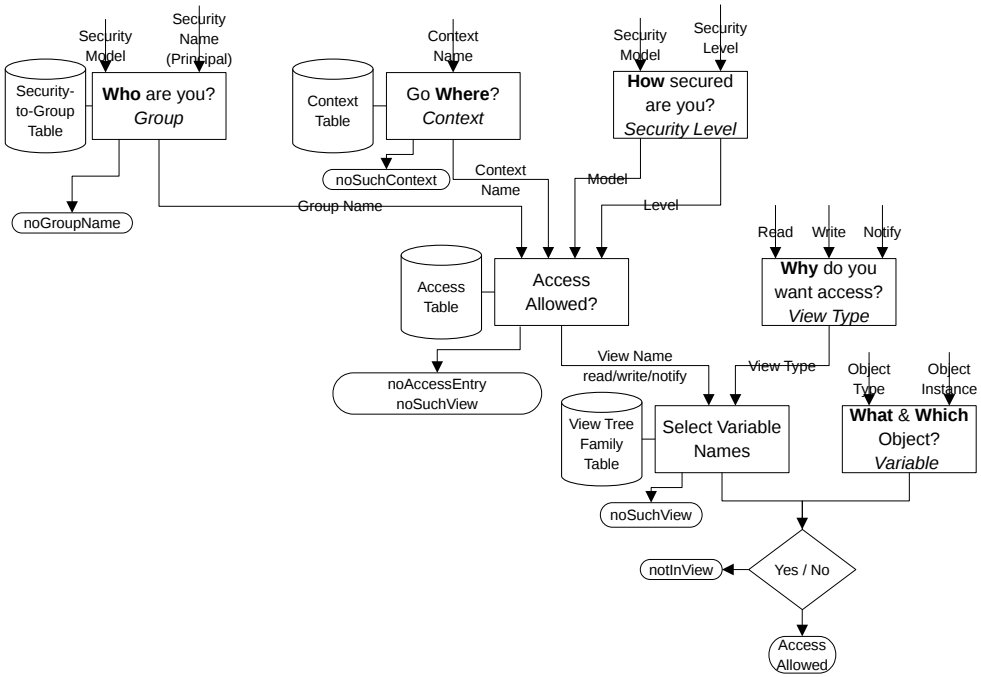


Figure 7.16 VACM Process

Figur: VACM[2, Fig 7.16]

- Distribuerar ut insamling och analys av data.
- Skickar enbart vidare sammanställd information (statistik) samt
- ifall ett alarm (trap/notifikation) triggas.

- Placera övervakning och insamling närmare källan
- Minska SNMP-trafiken, trafik skickas enbart vid behov.
- Enklare att segmentera uppnätverket.
- Lämpad för att analysera flöden, inte specifika enheter.

RMON1

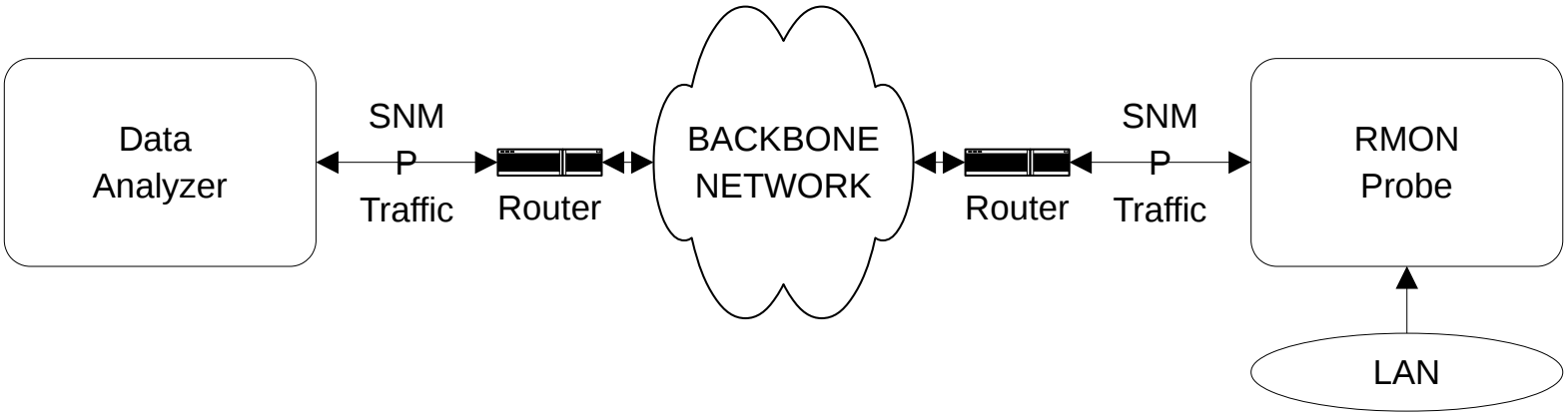
- Togs fram för att övervaka Ethernet och Token Ring.
- Enbart lager 2.

RMON2

- Jobbar upp mot applikationslagret.
- Genererar statistik och skickar till en central NMS

- Sond (probe)
- Data analysator

RMON komponenter



Figur: RMON Komponenter[2]

RMON forts.

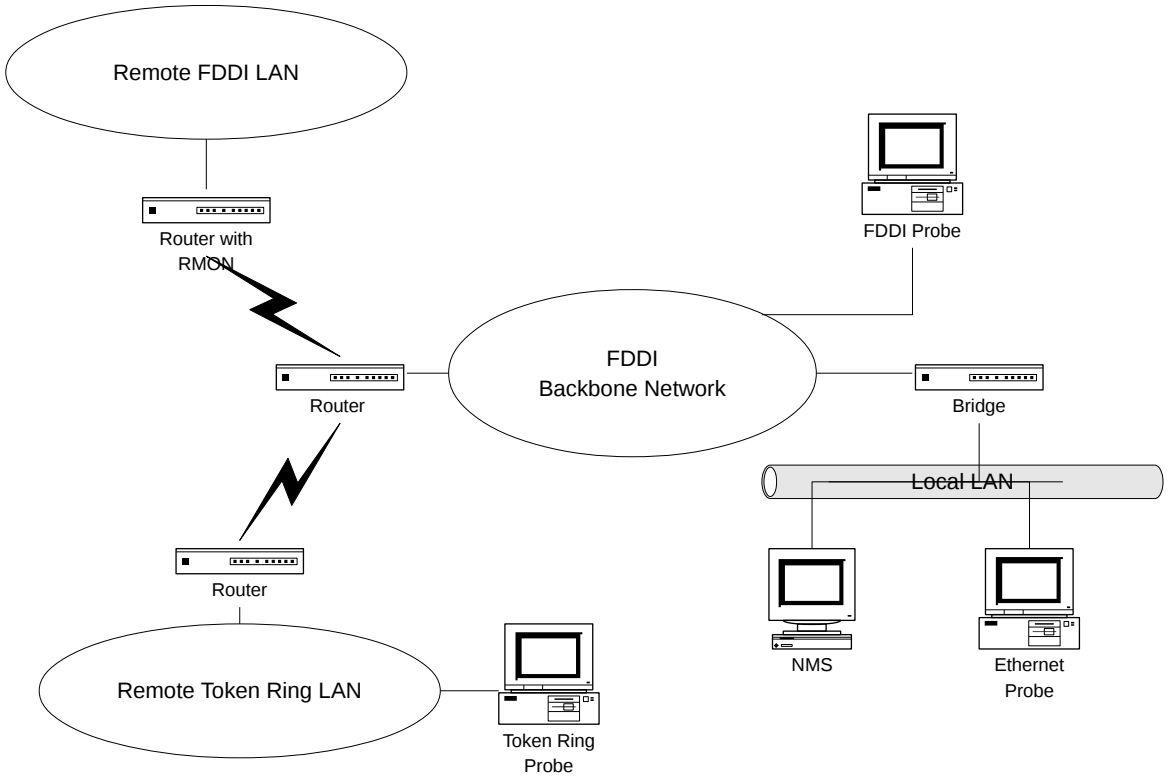


Figure 8.1 Network Configuration with RMONs

Figur: RMON Komponenter[2, Fig 8.1]

RMON MIB-grupper

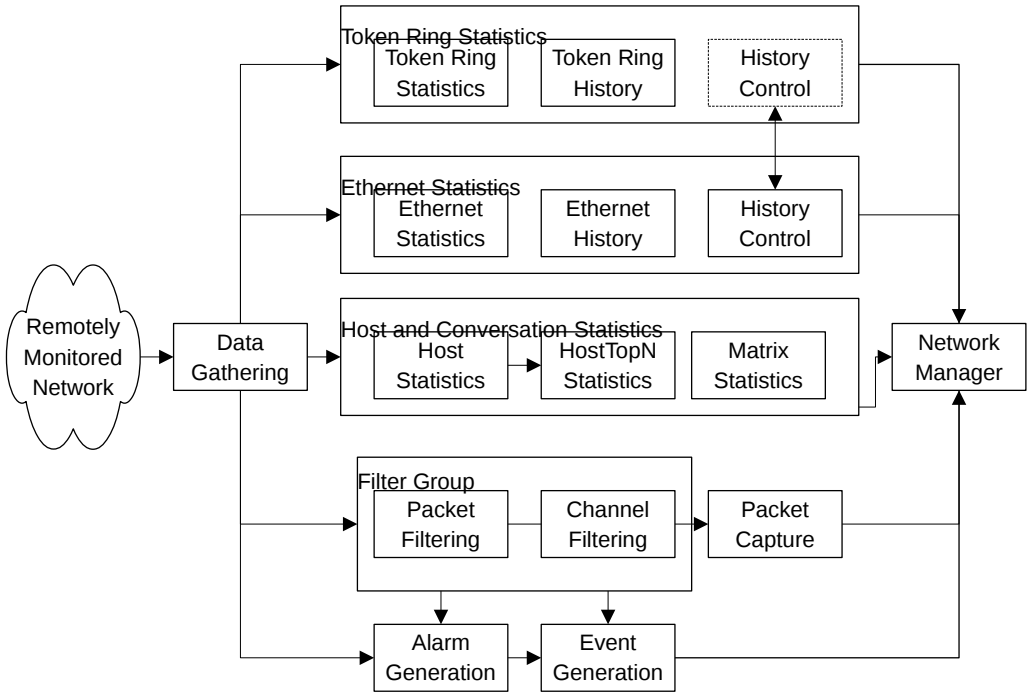


Figure 8.3 RMON1 Groups and Functions

Figur: RMON Komponenter[2, Fig 8.3]

- Statistics
  - Samlar in statistik (användning, kollisioner, fel)
- History
  - Lagrar historiska data
- Alarm
  - Periodiskt plockar in data och jämnför mot fördefinierade gränsvärden. Genererar ett alarm vid överskridit värde
- Host
  - Information kring de noder som finns på nätverket.

- Host top N
  - En top Nlista över noder och dess nätverksanvändning.
- Matrix
  - Lagrar statistik över konversationer.
- Filter
  - Möjliggör skapandet av filter vid insamling av data.
- Packet Capture
  - Möjliggör insamling av paket med hjälp av fördefinierade filter.

- Events
  - Skapar event och notifikationer.
- Token Ring
  - Funktioner kopplade mot Token Ring.

- Protocol Directory
  - Lista över protokoll som går att övervaka.
- Protocol Distribution
  - Statistik för respektive protokoll.
- Address Map
  - Tabell över IP – MAC.
- Network-Layer Host
  - Lager-3 statistik för varje host på nätverket.
- Network-Layer Matrix
  - Lager-3 statistik för kommunikationen mellan hosts.

- Application-Layer Host
  - Statistik applikationslagersprotokoll per host.
- Application-Layer Matrix
  - Statistik applikationslagerprotokoll för kommunikation mellan hosts.
- User History
  - Alarm och history från RMON1.
- Probe Configuration
  - Möjlighet att konfigurera RMON sonden.
- RMON Conformance
  - Anger vilka grupper som måste implementeras.

Referenser I

[1] D. Harrington, R. Presuhn, and B. Wijnen. An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks. RFC 3411 (INTERNET STANDARD), December 2002. URL `http://www.ietf.org/rfc/rfc3411.txt`. Updated by RFCs 5343, 5590.

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