Översikt – Nätverksövervakning

Lennart Franked
email:lennart.franked@miun.se

Informations och Kommunikationssystem (IKS)
Mittuniversitetet

2014-04-03

Introduktion

Ett nätverk består utav:

- Noder (klienter, servrar, skrivare, routrar...),
- länkar,
- passiva (hub, repeater) och aktiva (router, switch) enheter,
- data.

Övervaka ett nätverk

Nätverksprotokoll för övervakning

För att övervaka dessa komponenter behövs ett speciellt protokoll som kan kommunicera med alla komponenter, samla in data och presentera detta i ett överskådligt format

Många tillverkare utvecklade egna system för just detta ändamål.

Heterogent nätverk

Nätverk idag är heterogena.

- Det finns ett otaligt antal tillverkare av nätverksenheter,
- flertal olika länktyper,
- olika protokoll och standarder,
- olika operativsystem,
- mm.

Standardisera övervakning

Vi behöver ett sätt att standardisera övervakningsmöjligheterna i ett nätverk.

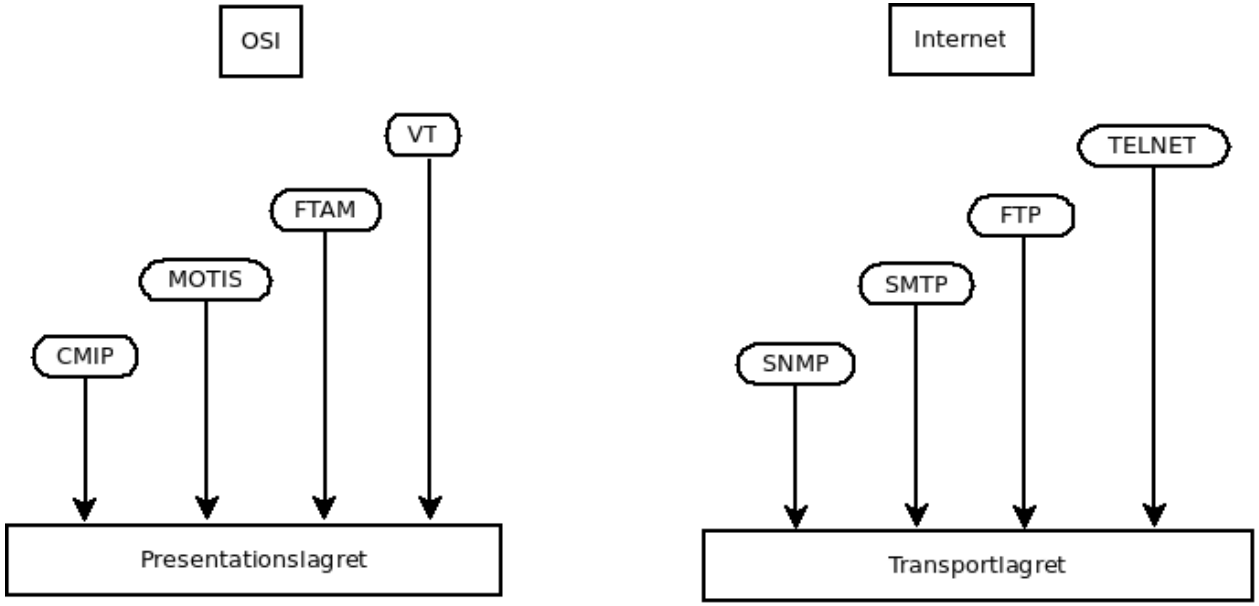
Standardisera nätverksövervakning

- Standardiserad protokollstack,
- Kompatibelt med de mest använda protokollen.
- Enkelt för tillverkare att kunna göra sina enheter kompatibla med protokollet.

Diverse standarder

- OSI/CMIP
- Internet/SNMP
- TMN
- IEEE
- nya specialiserade standarder
  - Web-Based Enterprise Management(WBEM)
  - Java Management Extension
  - XML-Based Network Management
  - CORBA-based Network Management

OSI/CMIP vs. Internet/SNMP)



Figur 1 : OSI jämnfört med Internet-modellens protokoll[8]

Internet/SNMP

Vi kommer primärt kolla på Internetmodellens SNMP-protokoll.

- Började som en industristandard.
- Första RFCerna för SNMP kom 1988 [4], [5] samt [2].
- Ursprungligen framtaget för att övervaka Internetkomponenter.
- Används numera till att övervaka allt från backbone-routrar till skrivare.

Begrepp

- Manager:
  - Efterfrågar data från en agent.
  - Övervakar Alarm.
  - Förser användaren med ett gränssnitt.
- Agent:
  - Hämtar data från objekt vid begäran.
  - Konfigurerar objekt.
  - Skapar alarm och skickar till en manager.
- Objekt:
  - Element i nätverket som hanteras
  - Alla objekt är inte hanterbara.
- NMS – Network Management System.
  - Sammanställer data.

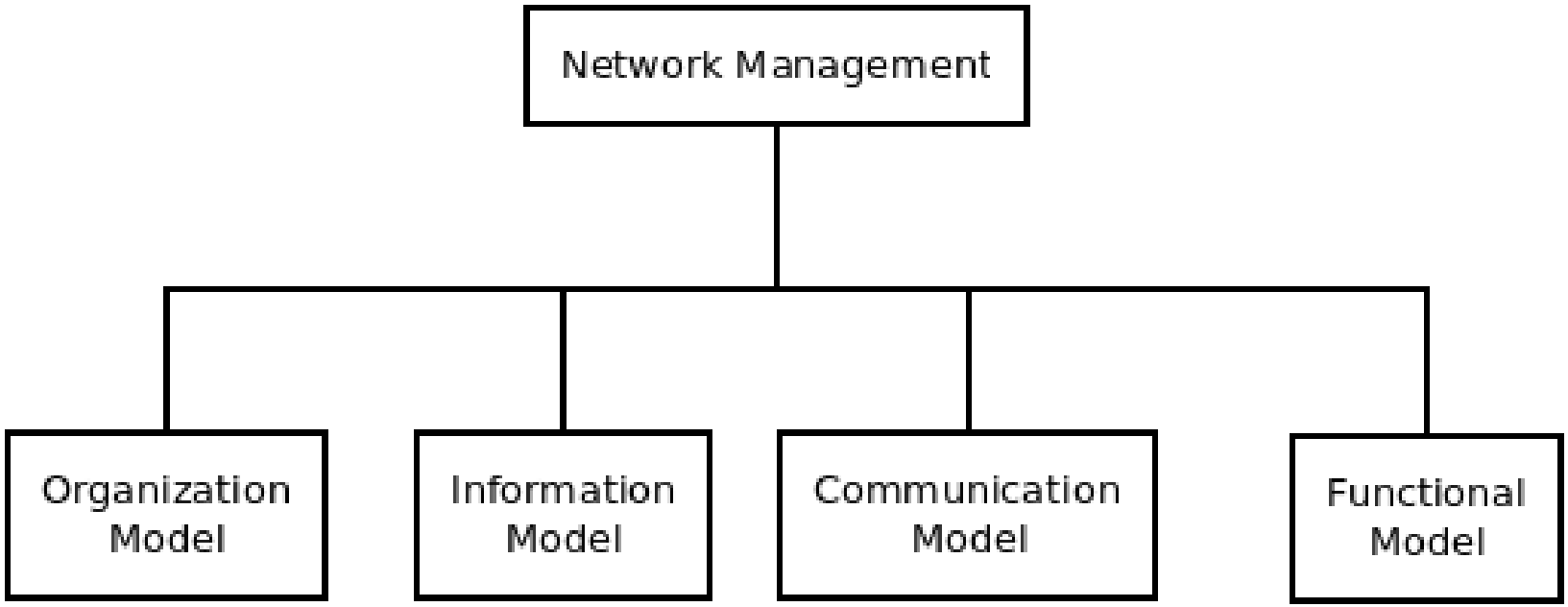
Definition av data och information

Data och Information

"Data – Physical phenomena chosen by convention to represent certain aspects of our conceptual and real world. The meanings we assign to data are called information. Data is used to transmit and store information and to derive new information by manipulating the data according to formal rules."Hansen [3]

Förvaltningsmodeller

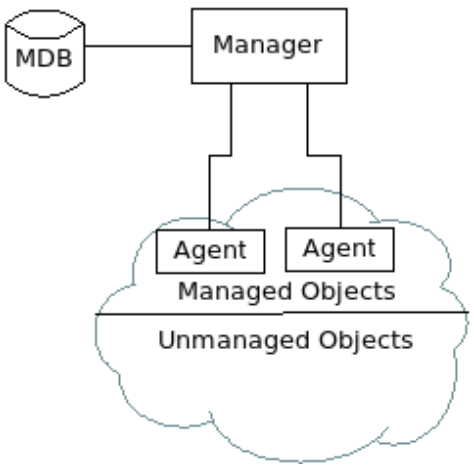
- SNMP har ingen egen förvaltningsmodell specifierad.
- Använder i stort samma modell som OSI (Figur 2).



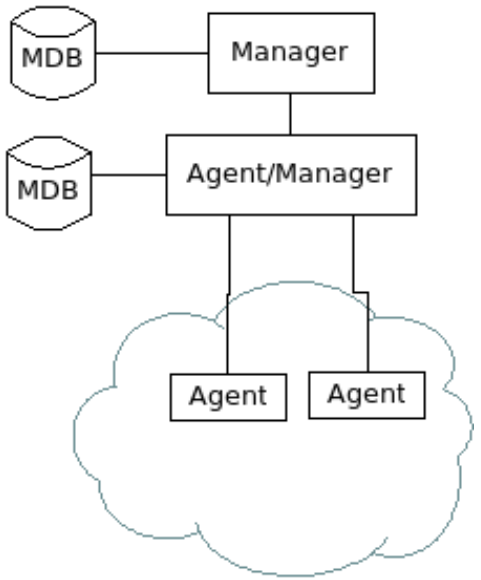
Figur 2 : OSI Förvaltningsmodel [8]

Organisationsmodellen

- Behandlar de komponenter som förvaltningsmodellen ska innehålla.
- Två (figur 3) eller tre nivåer (figur 4).



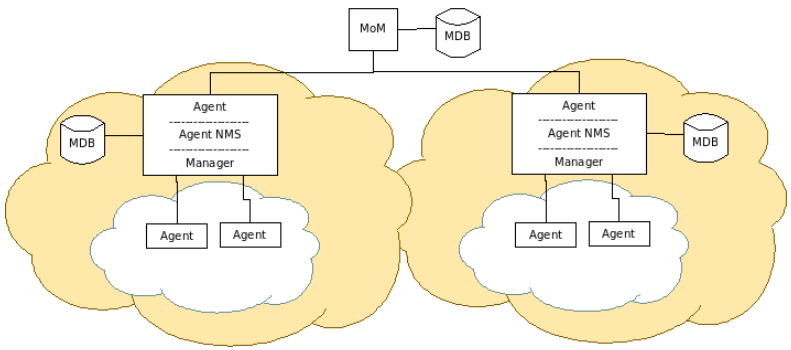
Figur 3 : Tvånivås organisationsmodellen[8]



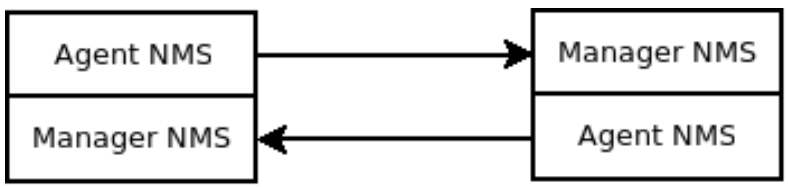
Figur 4 : Trenivås organisationsmodellen[8]

Organisationsmodellen forts.

- Variationer av två eller trenivås modellen.
- Vid ett större nätverk (figur 5).
- Mellan två enheter (figur 6).



Figur 5 : Företagsnätverk - Manager of Manager[8]



Figur 6 : Peer-to-Peer[8]

Informationsmodellen

Informationsmodellen

Behandlar strukturen av data och hur det ska lagras.

Analogi från boken

- För att hitta en specifik figur i en bok används följande
  - Figurnummer: 6
  - Kapitelnummer: 3
  - ISBN: 978-81-317-3404-9
  - Ex. ISBN:978-81-317-3404-9 kap 3 figur 3.6

Informationsmodellen forts.

Structure of Management Information

- Liknande struktur definieras i Informationsmodellen.
- Benämns som Structure of Management Information (SMI).
- Anger strukturen på ett övervakningsbart objekt.
- Beskriver detta med hjälp utav ASN.1.
- Ett objekt kan innehålla i princip vilken typ av data som helst.

Abstract Syntax Notation One

- En formell notation utvecklat utav ITU-T och OSI gemensamt.
- Kommunikation mellan applikationer på applikationslagret.
- Anger bland annat hur data skall, kodas, representeras, sändas, avkodas.
- Syntax och Semantik.
- Några fördefinierade datatyper (Integer, boolean, char string...)
- Går att skapa egna datatyper.

Informationsmodellen forts.

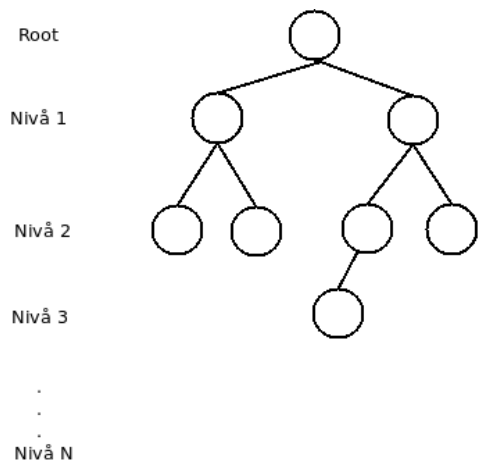
Management Information Base (MIB)

- Vilket data som finns att hämta anges som objekt i MIB (Management Information Base).
- Anges enligt SMIv2 strukturen.
- Skapar ett hierarkiskt träd över övervakningsbara objekt i ett nätverk, så kallat MIB-träd.
- Virtuel databas över övervakningsbara objekt.
- Data som hämtats från ett objekt i MIB lagras i Management Database (MDB).

Informationsmodellen forts.

Management Information Tree

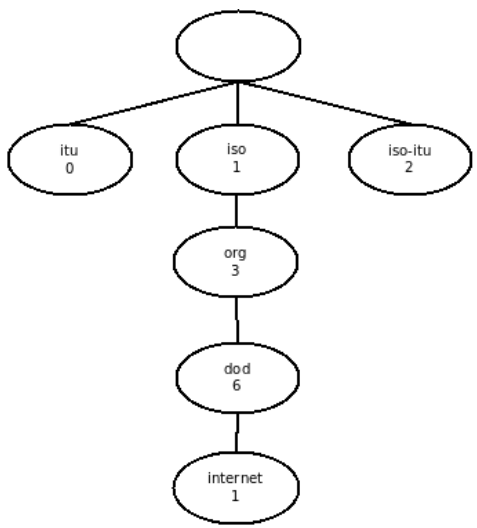
- Del av Management Information Base.
- Även kallat MIB-träd.
- Hierarkiskt träd över övervakningsbara objekt, figur 7.



Figur 7 : Enkel representation utav Management Information Tree[8]

Informationsmodellen forts.

- Varje objekt (undantag för root) ges ett unikt objekt-id (OID) och ett beskrivande namn, figur 8
- Exempelvis objektet 1.3.6.1.2.1.4.1 indikerar om IP Forwarding är aktiverat.
- iso.org.dod.internet.mgmt.mib-2.ip.ipForwarding



Figur 8 : Representation utav Management Information Tree. [8]

Informationsmodellen forts.

Agent och Manager har varsitt MIB-träd

- Agent MIB innehåller enbart information om de moduler som finns att hämta på den enhet som agenten administrerar.
- Management MIB innehåller samtliga MIB-moduler som finns tillgängliga i det nät som den hanterar.
- Liknelse, Nationalbibliotek bevara i princip allt tryckt material från sverige sedan 1661[1].
- Stadsbibliotek, har enbart en delmängd av ovan material.

MIB moduler

En MIB modul är en samling av relaterade övervakningsbara objekt.

Konsekvent definition utav MIB

Standardisera formatet

1990 släpptes RFC1155 [6] som standardiserade hur objekt under Internet-noden skall definieras.

Följande fem parametrar måste finnas med:

- Objekt identifierare – Unikt ID.
- Syntax – Vilka regler objekttypen måste följa.
- Definition – En textbeskrivning utav objektets semantik.
- Access – Läs och eller skrivrättigheter, ej access.
- Status – Måste objektet vara implementerat i MIB-modulen.

Tillägg till detta finns att läsa i RFC1212[7]

Exempel Objekt: 1.3.6.1.2.1.4.1 - ipForwarding

```
ipForwarding OBJECT-TYPE
  SYNTAX  INTEGER {
    forwarding(1),
    not-forwarding(2)
  }
  ACCESS  read-write
  STATUS  mandatory
  DESCRIPTION
    "The indication of whether this entity is acting
    as an IP gateway in respect to the forwarding of
    datagrams received by, but not addressed to, this
    entity.  IP gateways forward datagrams.  IP hosts
    do not (except those source-routed via the host).

    Note that for some managed nodes, this object may
    take on only a subset of the values possible.
    Accordingly, it is appropriate for an agent to
    return a 'badValue' response if a management
    station attempts to change this object to an
    inappropriate value."
  ::= { ip 1 }
```

Kommunikationsmodellen

Informationsutbyte

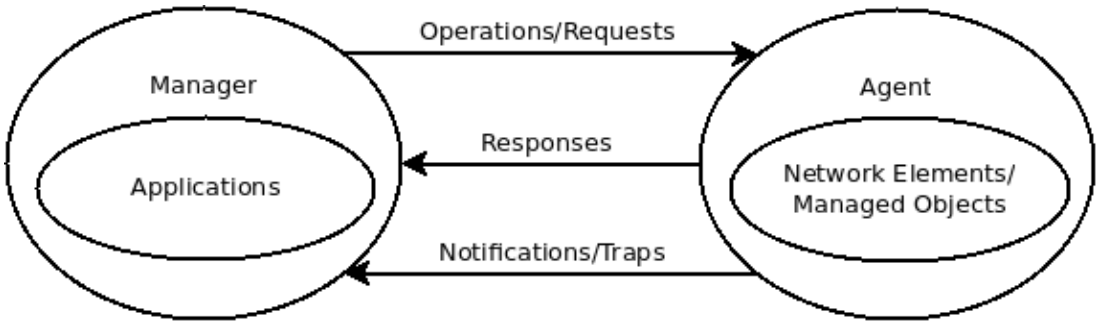
Kommunikationsmodellen behandlar hur informationen utbyts mellan systemen.

Kommunikationsmodellen måste hantera tre delar i kommunikationen.

- Meddelandeutbyte (Transportlagret)
- Meddelandeformatet. (Applikationslagret)
- Nyttodatat. (förfrågan och begäran)

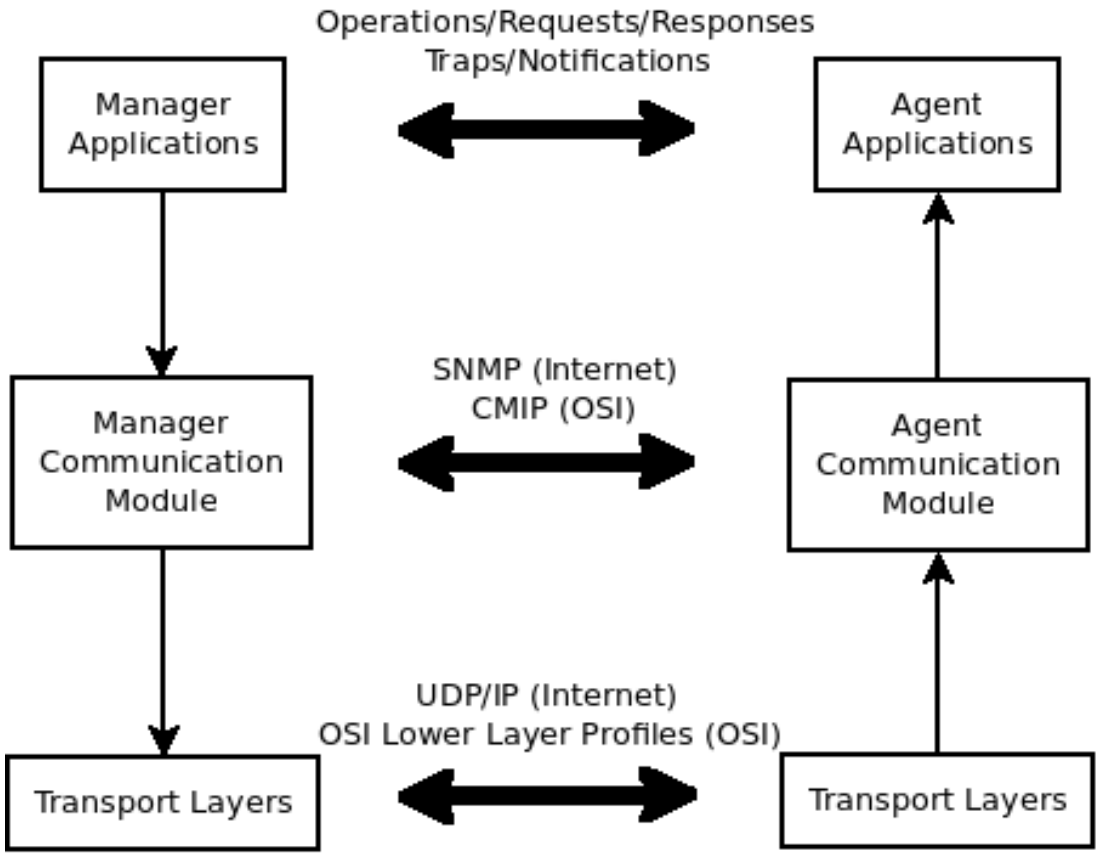
Kommunikationsmodellen forts.

Management Communication Model



Figur 9 : Kommunikationsmodellen Manager / Agent [8]

Kommunikationsmodellen forts.

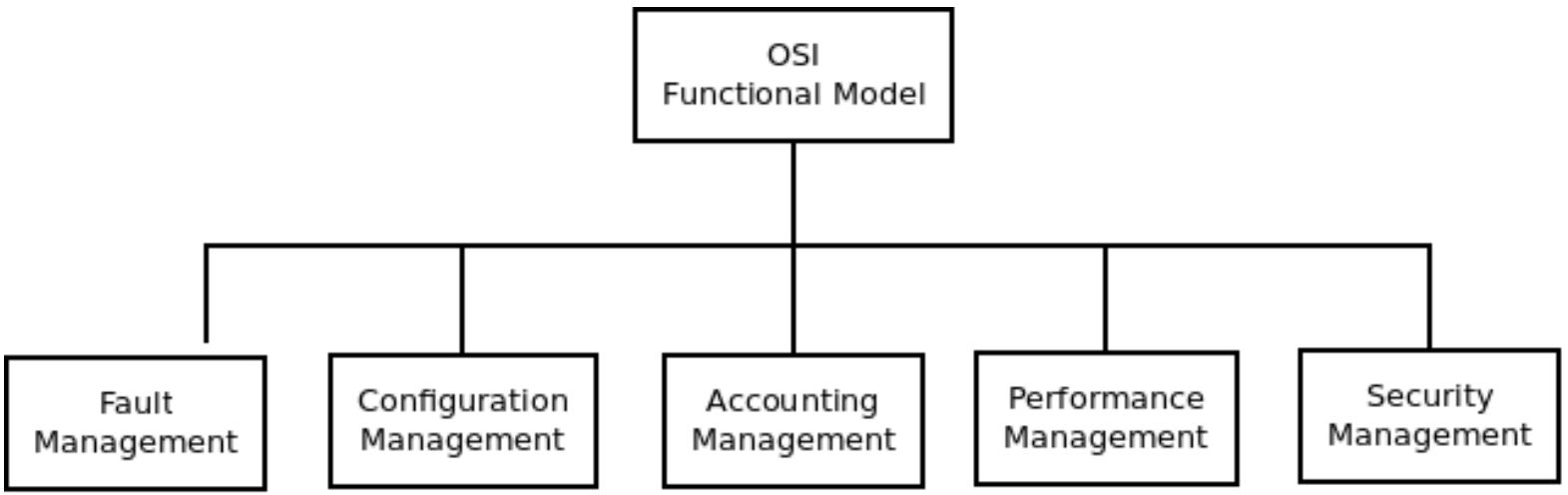


Figur 10 : Kommunikationsmodellen överföringsprotokoll [8]

Funktionsmodellen

Applikationsfunktionalitet

Funktionsmodellen specificerar vilka funktioner applikationerna bör ha, indelad i fem stycken grupper, figur 11



Figur 11 : OSI Funktionsmodell [8]

FCAPS:

- Felhantering – Upptäcka och isolera problem i nätverket.
- Konfigurationshantering – Möjlighet att sätta eller ändra konfigurationer på enheter.
- Kontering – Styra nätverk och objektets resursanvändning.
- Prestanda – Övervakar nätverket och objektets resursanvändning och prestanda.
- Säkerhet – Behandlar allt rörande säkerhet.

Network Management System

Ett bra NMS ska klara av att hantera samtliga fem punkter.

Referenser I

[1] Kungliga Biblioteket. KB - nationens minne. 2013. URL `http://www.kb.se/om`.

[2] J.D. Case, M. Fedor, M.L. Schoffstall, and J. Davin. Simple Network Management Protocol. RFC 1067, August 1988. URL `http://www.ietf.org/rfc/rfc1067.txt`. Obsoleted by RFC 1098.

[3] P. Brinch Hansen. *Operating Systems Principles*. Prentice Hall, 1973.

[4] K. McCloghrie and M.T. Rose. Structure and identification of management information for TCP/IP-based internets. RFC 1065 (INTERNET STANDARD), August 1988. URL `http://www.ietf.org/rfc/rfc1065.txt`. Obsoleted by RFC 1155.

Referenser II

[5] K. McCloghrie and M.T. Rose. Management Information Base for network management of TCP/IP-based internets. RFC 1066, August 1988. URL `http://www.ietf.org/rfc/rfc1066.txt`. Obsoleted by RFC 1156.

[6] M.T. Rose and K. McCloghrie. Structure and identification of management information for TCP/IP-based internets. RFC 1155 (INTERNET STANDARD), May 1990. URL `http://www.ietf.org/rfc/rfc1155.txt`.

[7] M.T. Rose and K. McCloghrie. Concise MIB definitions. RFC 1212 (INTERNET STANDARD), March 1991. URL `http://www.ietf.org/rfc/rfc1212.txt`.

[8] 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.