Upravljanje IP omrežij z uporabo SNMP

doc. dr. Iztok HUMAR
prof.dr. Janez BEŠTER

Upravljanje omrežij

- Upravljanje omrežij pomeni
  - razvijanje
  - integracijo
  - koordiniranje

  strojne in programske opreme ter človeških virov s cilji
  - nadzorovanja
  - testiranja
  - konfiguriranja
  - analiziranja
  - vrednotenja
  - krmiljenja

  omrežja in njegovih elementov, da z zmogljivostmi zagotavljajo delovanje v realnem času in v skladu z zahtevami QoS.

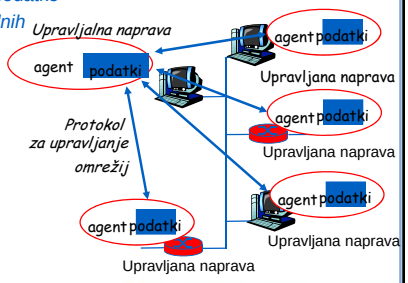
Agenda

- Upravljanje omrežij
  - namen
  - glavne komponente
- SNMP
  - MIB: management information base
  - SMI: data definition language
  - SNMP in komunikacija preko sporočil
  - varnost

Infrastruktura za upravljanje omrežij

- Definicije pojmov:

Upravljana naprava vsebuje *upravljane objekte* ki podatke zbirajo v *bazi upravljalnih podatkov (MIB)*



Upravljanje omrežij

- Omrežja in podobne avtonomne sisteme sestavlja več sto oziroma več tisoč med seboj sodelujočih enot, ki vsebujejo različno strojno in programsko opremo.
- Večina ostalih sistemov je večina krmiljena iz centralnega nadzornega in upravljalskega sistema. Primer:
  - jedrska elektrarna
  - letalo

Organizacije za standardizacijo

- IETF: Internet Engineering Task Force
  - Operation and Management Area:
    - Simple network Management protocol
- ISO: International Standardization Organization
  - ISO-IEC / JCT 1 / WG4:
    - Common Management Information Protocol
    - Common Management Information Service

Standardi za upravljanje omrežij

OSI CMIP
- Common Management Information Protocol
- Izdelan v osemdesetih – zamišljen kot poenoten standard za upravljanje omrežij
- Predolg proces pisanja standardov
- Zelo kompleksen
- Redka uporaba

IETF SNMP
- Simple Network Management Protocol
- Nastal zaradi Internet
- Prvotna standardizacija zelo enostavna
- Razvit in sprejet izjemno hitro
- Rast: velikosti in kompleksnosti protokola,
- Trenutno: SNMP v3
- *de facto* stanard za uporavljanje omrežij

Pregled SNMP: 4 ključni elementi

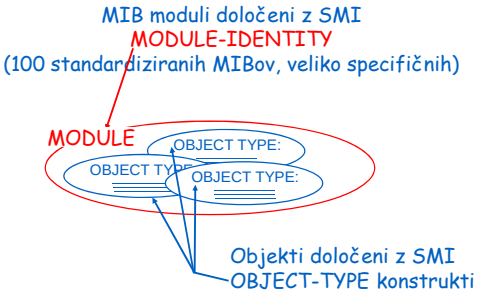
- **Management information base (MIB):**
  - porazdeljeno skladišče za informacije za upravljanje omrežja
- **Structure of Management Information (SMI):**
  - jezik za definicijo podatkov za MIB objekte
- **SNMP protokol**
  - prenos informacij in instrukcij med upravljalcem in upravljanimi objekti
- **Varnost, zmožnost administracije**
  - nove zmožnosti v SNMPv3

SNMP (RFC 1157) in njegova arhitektura

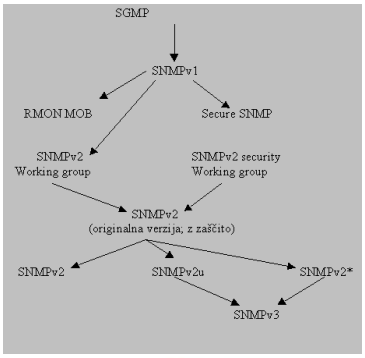
- SNMP = Simple Network Management Protocol
- Protokol za upravljanje TCP/IP in drugih omrežij
- Prednik: SGMP = Simple Gateway Monitoring Protocol (RFC 1028, 1987)
- Razvil IETF – Internet Engineering Task force, RFC 1157
- Razširil leta 1993

- Arhitektura odjemalec/strežnik (C/S)
- Odjemalec = Upravljalec
  - navadno aplikacija na osebnem računalniku
  - lahko implementiran na komunikacijsko napravo (sodeluje z drugimi)
- Strežnik (SNMP agent) = Upravljan
  - komunikacijska naprava (Router, Switch)
  - lahko tudi spletni strežnik, osebni računalnik

MIB



Razvoj protokola



SMI: Jezik za definicijo podatkov

- Namen: Nedvoumna in dobro definirana sintaksa in semantika za tvorjenje upravljalskih podatkov
- Osnovni podatkovni tipi:
  - Text, Integer, OCTET STRING, Opaque
  - Counter, Integer32, OBJECT IDENTIFIED,
  - Time Ticks Unsigned32, IPaddress,
- OBJECT-TYPE
  - vsebujejo statistične upravljalske podatke
  - podatkovni tip, status, semantika upravljanega objekta
  - diskretni, tabelirani
  - ASN.1 Notacija (Abstract Syntacx Notation)
- MODULE-IDENTITY
  - standardni nizi, definirani v RFC 1213
  - skupina logično povezanih objektov je združena v MIB modul
  - za posamezne naprave definirane vnaprej, lahko pa jih dodajamo sami

SMI primer: definicija objekta, modula

OBJECT-TYPE: ipInDelivers

```
ipInDelivers OBJECT TYPE
  SYNTAX       Counter32
  MAX-ACCESS   read-only
  STATUS   current
  DESCRIPTION
    "The total number of input
     datagrams successfully
     delivered to IP user-
     protocols (including ICMP)"
::= { ip   9}
```

MODULE-IDENTITY: ipMIB

```
ipMIB MODULE-IDENTITY
  LAST-UPDATED "941101000Z"
  ORGANZATION "IETF SNPv2
               Working Group"
  CONTACT-INFO
    " Keith McCloghrie
    ....."
  DESCRIPTION
    "The MIB module for managing IP
     and ICMP implementations, but
     excluding their management of
     IP routes."
  REVISION "019331000Z"
  .........
::= {mib-2 48}
```


MIB primer: UDP modul

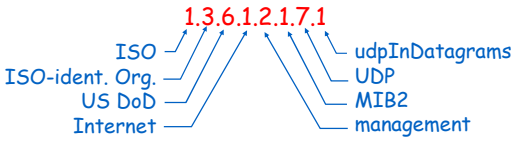
Object ID	Name	Type	Comments
1.3.6.1.2.1.7.1	UDPInDatagrams	Counter32	total # datagrams delivered at this node
1.3.6.1.2.1.7.2	UDPNoPorts	Counter32	# underliverable datagrams no app at portl
1.3.6.1.2.1.7.3	UDInErrors	Counter32	# undeliverable datagrams all other reasons
1.3.6.1.2.1.7.4	UDPOutDatagrams	Counter32	# datagrams sent
1.3.6.1.2.1.7.5	udpTable	SEQUENCE	one entry for each port in use by app, gives port # and IP address

Poimenovanja v SNMP

vprašanje: **kako poimenovati vsak možen standardni objekt (protokol, podatek, ...) v vsakem izmed razvitih omrežnih standardov?**

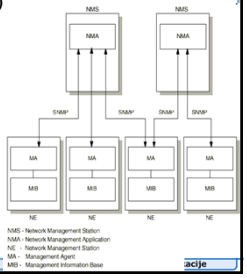
odgovor: ***ISO Object Identifier tree:***

- **hierarhično poimenovanje vseh objektov**
- **vsaka veja ima svoje ime, številko**



Delovanje SNMP

- **Strežnik ima podatkovno bazo MIB (Managment Information Base)**
- **Upravljalec pošilja ukaze, ki vsebujejo**
  - **MIB identifikator (ime MIB spremenljivke)**
  - **navodilo, kaj storiti s spremenljivko**
  - **dostop s Comunity Name, določi admin**



Poimenovanja v SNMP

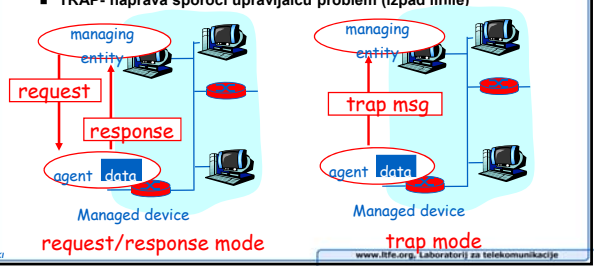
- **Več na: http://www.alvestrand.no/harald/objectid/top.html**

Dostop do MIB

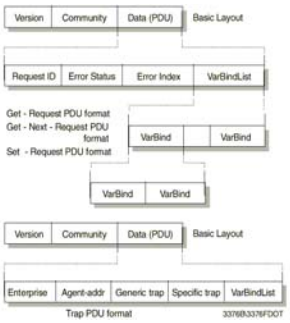
- **Dostop do MIB objektov:**
  - **RO**
  - **RW**
  - **WO**
- **Struktura (standard):**
  - **mgmt**
  - **private**
  - **experimental & directory**

Formati sporočila

- Sporočila kodirana v PDU (protocol data unit)
- Standardni formati sporočila SNMP
  - GET – prebere vrednost niza; ugotovi stanje naprave
  - GET NEXT – preleti vse vrednosti objektov (ugotovi imena)
  - SET – izvajamo aktivnosti (onemogočimo vmesnike), konfiguracija
  - TRAP- naprava sporoči upravljalcu problem (izpad linije)



SNMP sporočilo (II):



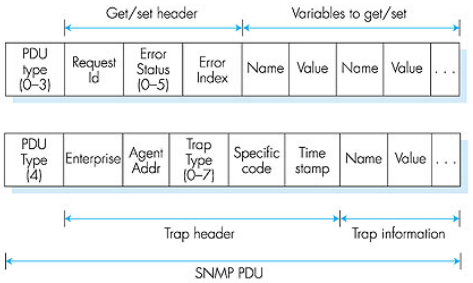
SNMP protocol: message types

Tip sporočila	Namen
GetRequest GetNextRequest GetBulkRequest	Mgr-to-agent: "želim podatke" (instance, next in list, block)
InformRequest	Mgr-to-Mgr: pošiljajo vrednosti MIB
SetRequest	Mgr-to-agent: nastavi vrednost MIB
Response	Agent-to-mgr: vrednost, odziv na zahtevo.
Trap	Agent-to-mgr: obvesti mngr o problematičnem dogodku

Prednosti / slabosti

- Prednosti:
  - velika popularnost
  - fleksibilnst in razširljivost
- Slabosti
  - kljub "Simple" je relativno kompliciran (SNMP–v2)
  - ni učinkovit (velika količina redundančnih informacij)

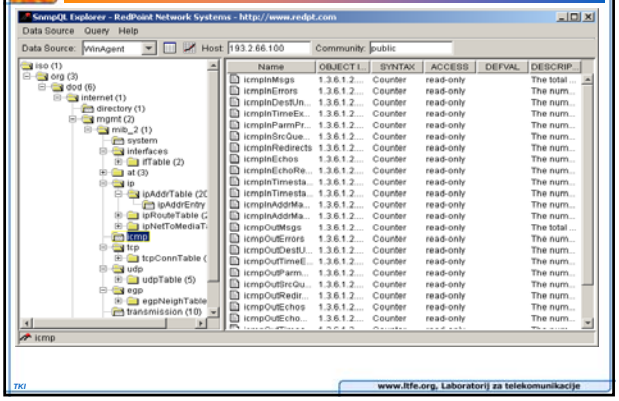
SNMP sporočilo (I):



SNMP v3: varnost in administracija

- Šifriranje: DES-šifriranje SNMP sporočilo
- Avtentikacija:
  - izračunamo in pošljemo MIC(m,k):
  - izračunamo hash funkcijo (MIC) over message (m),
  - skriti ključ (k), ki ga poznata obe strani
- Zaščita proti ponovni uporabi ključev
- Kontrola dostopa do objektov:
  - SNMP entiteta vzdržuje podatkovno bazo o pravicah za dostop do objektov, (različne pravice za različne uporabnike)
  - podatkovna baza se uporablja kot ostali objekti

Primer uporabe



HVALA ZA POZORNOST,
VPRAŠANJA !?

Primer uporabe: mrtg

- Aplikacija za zbiranje statističnih podatkov
- Podatke zajema preko SNMP protokola
- Podatke zajemamo v zaporednih časovnih intervalih
- Zajemamo podatke
  - o prometu
  - o času delovanja naprave
- Statistično obdelani, prikazani s pomočjo grafov
- Opazujemo lahko:
  - promet v omrežju
  - izpade naprav
- Možnost prirejanja različnim aplikacijam (customization)