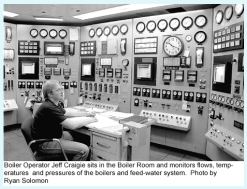
Komunikacijski protokoli in omrežna varnost

Nadzor in upravljanje z omrežji

Upravljanje z omrežjem

- Kaj je to upravljanje z omrežjem (network management)? Zakaj je potrebno?



Boiler Operator Jeff Craigie sits in the Boiler Room and monitors flows, temperatures and pressures of the boilers and feed-water system. Photo by Ryan Solomon

Mani Subramanian, *Network Management: An introduction to principles and practice*, Addison Wesley Longman, 2000

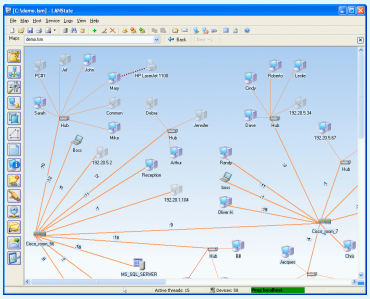
Upravljanje z omrežjem

- Z rastjo interneta in lokalnih omrežij so se majhna omrežja povezala v **VELIKO** infrastrukturo. Zato je s tem narasla tudi potreba po **SISTEMATIČNEM** upravljanju strojnih in programskih komponent tega sistema. Pogosta vprašanja:
  - Kateri viri so na razpolago v omrežju?
  - Koliko prometa gre skozi določeno omrežno opremo?
  - Kdo uporablja omrežne povezave, zaradi katerih direktor prepočasi dobiva elektronsko pošto?
  - Zakaj ne morem pošiljati podatkov določenemu računalniku?
- Definicija: Upravljanje z omrežjem vključuje **vpeljavo**, **integracijo** in **koordinacijo** s strojno opremo, programsko opremo in človeškimi viri z namenom **opazovanja**, **testiranja**, **konfiguriranja**, **analiziranja** in **nadzorovanja** omrežnih virov, pri katerih želimo zagotoviti **delovanje** v realnem času (ali delovanje z ustrezno kakovostjo - QoS) za sprejemljivo ceno.

Primeri aktivnosti upravljanja

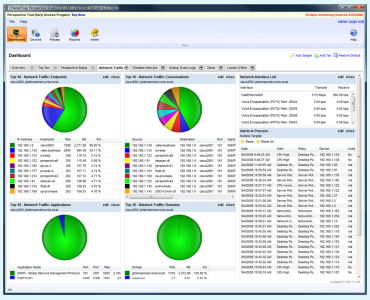
1. **zaznavanje napake na vmesniku računalnika ali usmerjevalnika**: programska oprema lahko sporoči administratorju, da je na vmesniku prišlo do težave (celo preden odpove!)
2. **nadzorovanje delovanja računalnikov in analiza omrežja**
3. **nadzorovanje omrežnega prometa**: administrator lahko opazuje pogoste smeri komunikacij in najde ozka grla,
4. **zaznavanje hitrih sprememb v usmerjevalnih tabelah**: ta pojav lahko opozarja na težave z usmerjanjem ali napako v usmerjevalniku,
5. **nadzorovanje nivoja zagotavljanja storitev**: ponudniki omrežnih storitev nam lahko jamčijo razpoložljivost, zanasnitev in določeno prepustnost storitev; administrator lahko meri in preverja,
6. **zaznavanje vdorov**: administrator je lahko obveščen, če določen promet prispe iz sumljivih virov; zaznava lahko tudi določen tip prometa (npr. množica SYN paketov, namenjena enem samem vmesniku)

Primeri aktivnosti



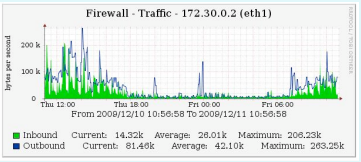
nadzorovanje delovanja računalnikov in analiza omrežja (odkrivanje topologije omrežja)

Primeri aktivnosti



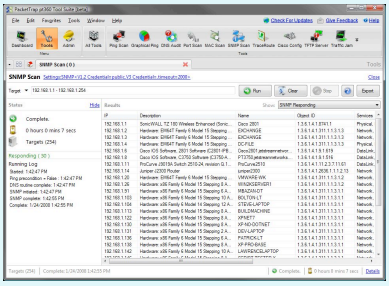
nadzorovanje omrežnega prometa (profiliranje)

Primeri aktivnosti



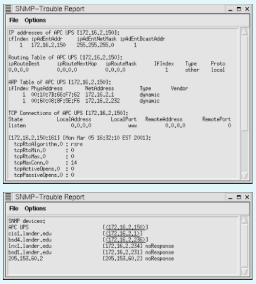
nadzorovanje nivoja zagotavljanja storitev (pretok podatkov)

Primeri aktivnosti



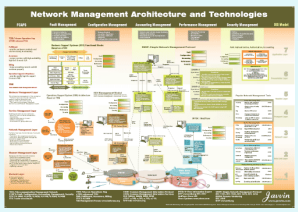
nadzorovanje delovanja računalnikov in analiza omrežja (popis IP naslovov)

Primeri aktivnosti



nadzorovanje delovanja računalnikov in analiza omrežja
(diagnostika in odkrivanje napak)

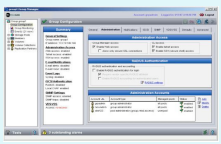
Področja upravljanja



Programska oprema za upravljanje

- CLI (*Command Line Interface*):
  - ✓ natančno upravljanje,
  - ✓ možnost rabe ukaznih datotek (*batch*),
  - – problem poznavanja sintakse, težavnost shranjevanja konfiguracije, manj splošno - specifično za posamezno omrežno opremo

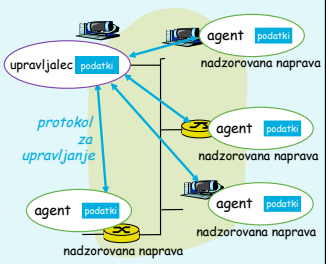
- GUI (*Graphical User Interface*) aplikacije:
  - ✓ vizuelno lepše, omogoča pregled delovanja cele naprave/omrežja, uporablja lahko svoj (zgoščen) protokol za komunikacijo z napravo - hitrost,
  - – izgubimo možnost shranjevanja berljive konfiguracije (binarni zapis), lahko maskira vse konfiguracijske možnosti



Infrastruktura za upravljanje

Komponente sistema za upravljanje:

- upravljalec = entiteta (aplikacija + človek), BOSS,
- nadzorovana naprava (vsebuje agenta NMA in nadzorovane OBJEKTE, ki vsebujejo nadzorovane PARAMETRE),
- protokol za upravljanje (npr. SNMP).



Zgodovina: protokoli za upravljanje

OSI CMIP

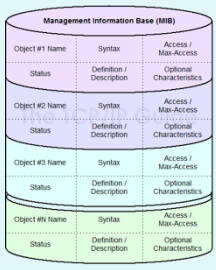
- *Common Management Information Protocol,*
- ITU-T X.700 standard
- nastal 1980: *prvi standard za upravljanje,*
- prepočasi standardiziran, ni zaživel v praksi.

SNMP

- *Simple Network Management Protocol,*
- IETF standard
- prva verzija zelo preprosta,
- hitra uvedba in razširitev v praksi,
- trenutno: SNMP V3 (dodana varnost!),
- *de facto* standard za upravljanje omrežij.

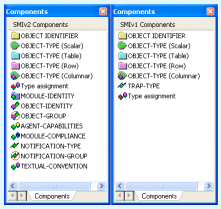
Podatki za upravljanje

- Za vsako vrsto nadzorovane naprave imamo svoj **MIB (Management Information Base),** kjer so podatki o upravljanih **OBJEKTIH** in njihovih **PARAMETRIH**.
- Upravljalec ima svoj **MDB (Management Database)**, kjer za vsako upravljano napravo hrani konkretne vrednosti za njihove MIB objekte/parametre.
- Potreben je jezik, ki definira zapis OBJEKTOV in PARAMETROV: **SMI (Structure of Management Information)**



SMI: jezik za definicijo objektov v MIB

- osnovni podatkovni tipi: INTEGER, Integer32,Unsigned32, OCTET STRING, OBJECT IDENTIFIED, IPaddress, Counter32, Counter64, Gauge32, Time Ticks, Opaque
- sestavljeni podatkovni tipi:
  - OBJECT-TYPE
  - MODULE-TYPE



SMI: definicija objekta

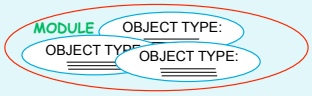
- definicija objekta: ima podatkovni tip, status, opis pomena

```
ipSystemStatsInDelivers 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}
```

SMI: združevanje objektov v module

- MODUL: vsebinsko povezana skupina objektov

```
ipMIB MODULE-IDENTITY
     LAST-UPDATED  "9411010002"
     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 "0193310002"
::= {mib-2 48}
```



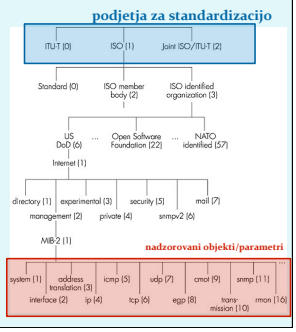
MIB moduli: standardizacija

- MODULI:
  - "standardizirani",
  - lastni proizvajalcem opreme (vendor-specific)
- IETF (Internet Engineering Task Force) zadolžena za standardizacijo MIB modulov za usmerjevalnike, vmesnike in drugo omrežno opremo
  - -> potrebno poimenovanje (označitev) standardnih komponent!
  - uporabi se poimenovanje ISO ASN.1 (Abstract Syntax Notation 1)

MIB moduli: standardizacija

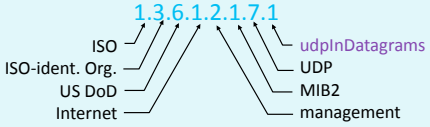
- hierarhična urejenost objektov z drevesom identifikatorjev
- vsak objekt ima ime, sestavljen iz zaporedja številčnih identifikatorjev od korena drevesa do lista
  - primer: 1.3.6.1.2.1.7 pomeni UDP protokol

➢ *izziv: kaj se nahaja na drugem in tretjem nivoju drevesa identifikatorjev?*



MIB: poimenovanje, primer

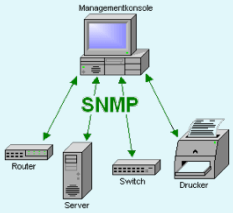
- Primer:
  - 1.3.6.1.2.1.7 določa protokol UDP
  - 1.3.6.1.2.1.7.* določa opazovane parametre UDP protokola



MIB: poimenovanje, primer

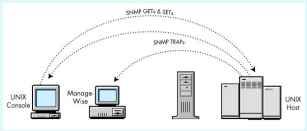
Object ID	Name	Type	Comments
1.3.6.1.2.1.7.1	UDPInDatagrams	Counter32	total # datagrams delivered at this node
1.3.6.1.2.1.7.2	UDPNoPorts	Counter32	# underliverable datagrams no app at portl
1.3.6.1.2.1.7.3	UDInErrors	Counter32	# undeliverable datagrams all other reasons
1.3.6.1.2.1.7.4	UDPOutDatagrams	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

Protokol SNMP



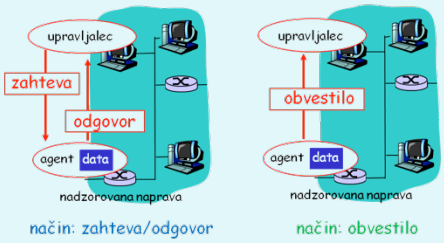
Protokol SNMP

- Simple Network Management Protokol
- protokol za izmenjavo nadzornih informacij med upravljalcem in nadzorovanimi objekti
- podatki o nadzorovanih objektih se prenašajo med nadzorovano opremo in upravljalcem skladno z definicijo MIB
- dva načina delovanja:
  - zahteva-odgovor (*request-response*): bere in nastavlja vrednosti,
  - obvestilo (*trap message*): naprava obvesti upravljalca o dogodku



Protokol SNMP

- dva načina delovanja



SNMP: tipi sporočil

Sporočilo	Smer	Pomen
GetRequest *GetNextRequest* *GetBulkRequest*	upravljalec -> agent	"daj mi podatke" (vrednost, naslednja v seznamu, blok podatkov-tabela)
InformRequest	upravljalec -> upravljalec	medsebojno posredovanje vrednosti iz MIB
SetRequest	upravljalec -> agent	nastavi vrednost v MIB
Response	agent -> upravljalec	"tukaj je vrednost", odgovor na Request
Trap	agent -> upravljalec	obvestilo upravljalcu o izrednem dogodku

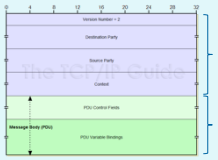
Protokol SNMP

- izziv: poiščite RFC dokumente o SNMP in ugotovite razlike med njimi

- SNMP uporablja transportni protokol UDP
  - vrata 161: "splošna" SNMP vrata, na katerih naprave poslušajo po SNMP zahtevah
  - vrata 162: vrata za *obvestila* (traps), na katerih običajno poslušajo sistemi za nadzorovanje in upravljanje z omrežjem

- implementacija SNMP mora reševati naslednje težave:
  - **velikost paketov**: SNMP paketi lahko vsebujejo obsežne informacije o objektih v MIB, UDP pa ima zgornjo mejo velikosti segmenta (TCP nima),
  - **ponovno pošiljanje**: ker se uporablja UDP, nimamo zagotovljene dostave in potrjevanja. Nadzor dostave je torej potrebno reševati na višjem OSI nivoju,
  - **problem z izgubljenimi obvestili**: če se obvestilo pri prenosu izgubi, pošiljatelj o tem nič ne ve; prejemnik pa ga tudi ne dobi
    - izziv: kako SNMPv3 rešuje navedene težave?

SNMP: oblika sporočila

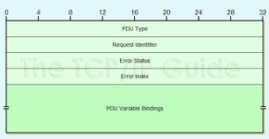


glava

podatkovna enota protokola
PDU (protocol data unit)

Verzija	Verzija SNMP protokola
Destination Party	Identifikator prejemnika
Source Party	Identifikator pošiljatelja
Context	Definira množico MIB objektov, ki je dosegljiva entiteti
PDU	Glavna vsebina sporočila, podatki iz MIB

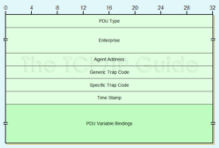
SNMP: sporočilo tipa *zahteva-odgovor*



PDU Type Value	PDU Type
0	GetRequest-PDU
1	GetNextRequest-PDU
2	Response-PDU
3	SetRequest-PDU
4	Obsolete, not used (this was the old Trap-PDU in SNMPv1)
5	GetBulkRequest-PDU (has its own format, see below)
6	InformRequest-PDU
7	Trap2-PDU
8	Report-PDU

Request ID	Integer	Številka, ki povezuje zahteve z odgovori. Naprava, ki odgovori, ko shrani v paket tipa *Response*. Uporablja se tudi za umetno kontrolo prejetih paketov (SNMP namreč uporablja UDP transportni protokol, ki tega ne zagotavlja!)
Error Status	Integer	Koda napake, ki ga agent posreduje v paketu tipa *Reponse*. Vrednost o pomeni, da do napake ni prišlo, ostale vrednosti definirajo točno napako. ➢ izziv: poglej različne [vse razvide]
Error Index	Integer	Če je prišlo do napake, je ta vrednost indeks objekta, ki je povzročil napako
Variable Bindings	Variable	Pari ime-vrednost (name-value), ki definirajo objekte in njihove vrednosti.

SNMP: sporočilo tipa *obvestilo*



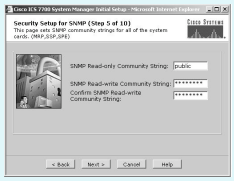
PDU Type	Integer	Vrednost, ki definira tip sporočila. Vrednost 4/7 pomeni obvestilo (trap message).
Enterprise	Sequence of Integer	Identifikator skupine.
Agent Address	Network Address	IP naslov agenta, ki je generiral obvestilo.
Generic Trap Code	Integer	Splošna koda napake - iz predefiniranega šifranta.
Specific Trap Code	Integer	Specifična koda napake (odvisna od proizvajalce opreme)
Time Stamp	TimeTicks	Čas, odkar se je naprava nazadnje inicializirala. Uporablja se za beleženje.
Variable Bindings	Variable	Pari ime-vrednost (name-value), ki definirajo objekte in njihove vrednosti.

Verzije SNMP

- **SNMPv1**
  - definiran konec 80-ih let
  - izkazal se je za prešibek za implementacijo vseh potrebnih zahtev (omejen pri sestavi PDU paketov)
- **SNMPv2**
  - izboljšan SNMPv1 na področjih hitrosti (dodan GetBulkRequest), varnosti (vendar prekompleksna implementacija), komunikacij med upravljalci ,
  - RFC 1901, RFC 2578
  - uporablja SMIv2 (izboljšan standard za strukturiranje informacij)
- **SNMPv3**
  - izboljšan SNMPv2 - ima dodane varnostne mehanizme,
  - omogoča kriptografijo, zagotavlja zaupnost, integriteto, avtentikacijo,
  - tudi uporablja SMIv2

Varnost

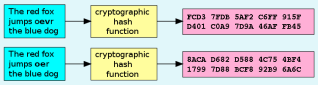
- Zakaj je pomembna?
  - SetRequest nastavlja nadzorovane naprave. Zahtevo lahko pošlje kdorkoli?
    - izziv: poišči še 3 primere drugih možnih zlorab protokola SNMP
- Varnostni elementi so vpeljani šele v SNMPv3, prejšnji dve različici jih nista imeli. SNMPv3 ima vgrajeno varnost na osnovi uporabniških imen
  - izziv: preberi RFC 3414 in poišči informacijo, proti kakšnim vdorom omogoča SNMPv3 zaščito? Kako je z napadi Denial of Service in prisluškovanjem prometa?



SNMP. Varnostni mehanizmi

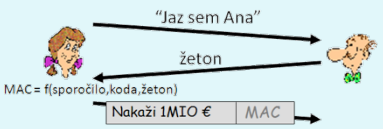
1. **kriptiranje vsebine paketov (PDU):** uporablja se DES (ključa je predhodno potrebno izmenjati)

2. **integriteta**: uporablja se zgoščanje sporočila s ključem, ki ga poznata pošiljatelj in prejemnik. S preverjanjem poslane zgoščene vrednosti imamo kontrolo pred aktivnim ponarejanjem sporočil



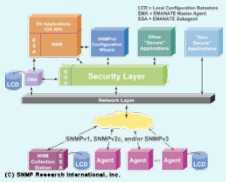
SNMP: Varnostni mehanizmi

3. **zaščita proti ponovitvi že opravljene komunikacije (replay attack):** uporaba enkratnih žetonov (angl. *nonce*): pošiljatelj, mora sporočilo kodirati glede na žeton, ki ga določa sprejemnik (to je običajno število vseh zagonov sistema pošiljatelja in čas, ki je minil od zadnjega zagona)



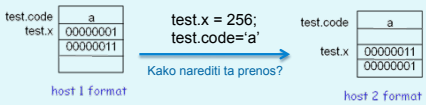
SNMP: Varnostni mehanizmi

4. **kontrola dostopa:** kontrola dostopa na osnovi uporabiških imen. Pravice določajo, kateri uporabniki lahko berejo/nastavljajo katere informacije. Podatki o uporabnikih se hranijo v bazi *Local Configuration DataStore*, ki ima ravno tako nadzorovane objekte s SNMP!
   - izziv: preuči RFC 3415. Kaj je to View-based Access Control Model Configuration MIB?



Kodiranje vsebine PDU

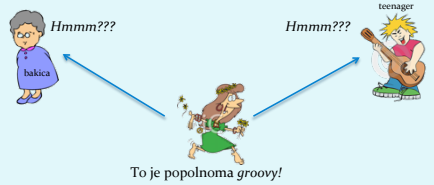
- Kako kodirati vsebino paketa, da bo razumljiva na vseh platformah (različni podatkovni tipi so različno dolgi, zapis debeli/tanki konec)?



- potrebujemo enotni način kodiranja ali nek **predstavitveni nivo teh podatkov**
  - ASN.1 standard poleg podatkovnih tipov definira tudi standarde kodiranja,
  - videli bomo, da se za predstavljanje teh operatorjev uporablja TLV notacija (Type, Length, Value - tip, dolžina, vrednost)

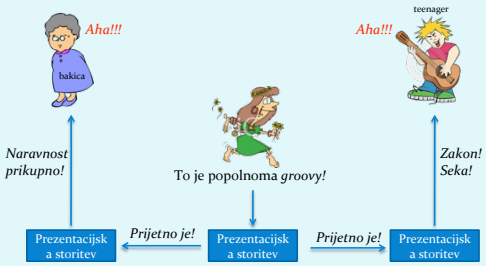
Kodiranje vsebine PDU

- Podoben problem:



Kodiranje vsebine PDU

- Podoben problem:



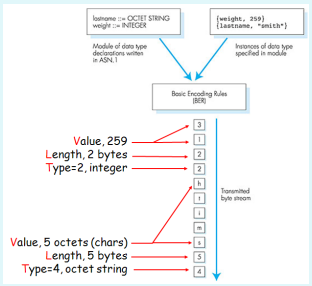
Prezentacijska storitev: možne rešitve

1. Pošiljatelj upošteva obliko podatkov, ki jo uporablja prejemnik: podatke pretvarja v njegovo obliko in nato šele pošlje.
2. Pošiljatelj pošlje podatke v svoji obliki, prejemnik pretvori v lastno obliko.
3. Pošiljatelj pretvori v neodvisno obliko in nato pošlje. Prejemnik neodvisno obliko pretvori v svojo lastno obliko.
   - izziv: kakšne so prednosti in slabosti gornjih treh pristopov?

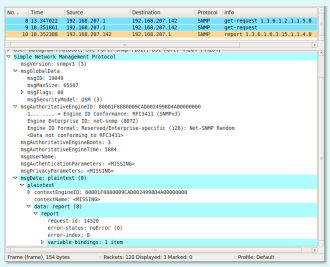
- ASN.1 uporablja 3. rešitev zgoraj (neodvisno obliko).
- Pri zapisovanju tipov se uporablja pravila BER (Binary Encoding Rules). Ta definirajo zapis podatkov po principu TLV (Type, Length, Value = tip, dolžina, vrednost).

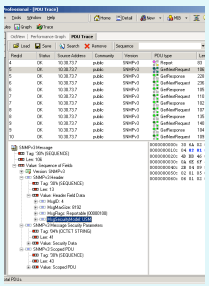
Primer BER kodiranja po principu TLV

Osnovni ASN.1 podatkovni tip	Št. tipa	Uporaba (angl.)
BOOLEAN	1	Model logical, two-state variable values
INTEGER	2	Model integer variable values
BIT STRING	3	Model binary data of arbitrary length
OCTET STRING	4	Model binary data whose length is a multiple of eight
NULL	5	Indicate effective absence of a sequence element
OBJECT IDENTIFIER	6	Name information objects
REAL	9	Model real variable values
ENUMERATED	10	Model values of variables with at least three states
CHARACTER STRING	*	Models values that are strings of characters from a specified character set

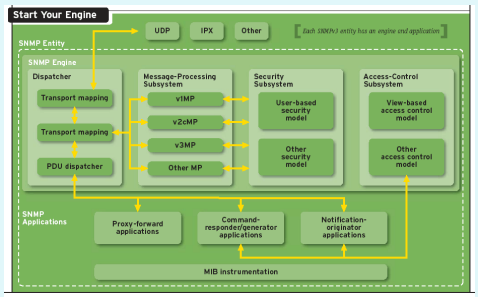


Zajem paketov SNMP

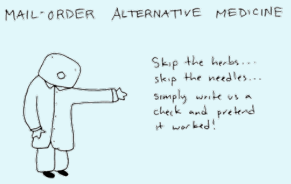




Struktura SNMP programja

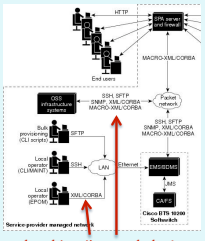


Drugi pristopi za nadzor



Alternativne butične rešitve

1. XML & SOAP (aplikacijski nivo): XML omogoča nazoren in hierarhičen način kodiranja podatkov, ki lahko predstavljajo elemente in vsebino nadzorovanih objektov v omrežju. SOAP je preprost protokol, ki omogoča izmenjavo XML dokumentov v omrežju.
   - ✓ enostavno branje in razumevanje vsebine na strani sprejemnika,
   - – velik overhead v primerjavi z binarnim kodiranjem podatkov
2. CORBA (Common Object Request Broker Architecture) (aplikacijski nivo): arhitektura, ki določa inter-uporabnost objektov različnih programskih jezikov in na različnih arhitekturah

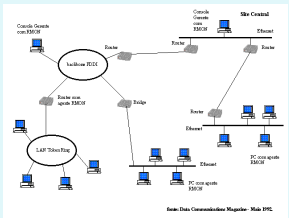


kombinacija protokolov!

Dogodkovno gnano opazovanje

RMON (Remote Monitoring) (dodatni mehanizem): Klasični SNMP lahko nadzoruje omrežje iz nadzorne postaje. RMON zbira in analizira meritve lokalno, rezultate pošlje oddaljeni nadzorni postaji. Ima svoj MIB z razširitvami za različne tipe medijev.

- ✓ vsak RMON agent je odgovoren za lokalni nadzor,
- ✓ pošiljanje že opravljenih analiz zmanjša SNMP promet med podomrežji
- ✓ ni nujno, da so agenti vedno vidni s strani centralnega nadzornega sistema
- – potreben daljši vzpostavitveni in namestitveni čas sistema



Domača naloga

Naloga za dodatne točke pri domačih nalogah:

Preberi RFC 789, ki opisuje znan izpad omrežja ARPAnet, ki se zgodilo v letu 1980.
Kako bi se izpadu omrežja lahko izognili ali pohitrili njegovo ponovno vzpostavitev, če bi administratorji omrežja imeli na razpolago današnja orodja za upravljanje in nadzorovanje omrežja?

Odgovor na nalogo lahko oddate preko učilnice preko povezave *"Dodatna domača naloga - izpad omrežja ARPAnet"*.

Naslednjič gremo naprej!

- promet za aplikacije v realnem času!