APLIKACIJE: UPRAVLJANJE INTERNETOM (SNMP)

SNMP

MIB

Uvod

- Rukovanje Internetom obuhvata:
- (a) otkrivanje i otklanjanje problema (debug),
- (b) upravljanje usmeravanjem (routing) saobraćaja, i
- (c) pronalaženje računara koji narušavaju standarde protokola.

Nivo protokola upravljanja Internetom

- Originalno u WAN, protokol upravljanja je bio sastavni deo protokola nivoa 2 (*link level protocols*).
- U slučaju neodgovarajućeg ponašanja paketskog komutatora, rukovalac mrežom (*network manager*) je izdavao nalog njegovom susednom komutatoru da mu pošalje "upravljački paket" (*control packet*).
- Dalje je bilo moguće:
- (a) ispitati ili promeniti smer (route),
- (b) ispitati komunikacione priključke,
- (c) restartovati komutator, ili
- (d) nastaviti normalan rad.

Prednost pozicioniranja protokola upravljanja u drugi nivo

- U slučaju kad su sredstva upravljanja deo nivoa 2, rukovalac mrežom može upravljati komutatorom i u slučaju otkaza protokola višeg nivoa.

Pozicioniranje protokola upravljanja u TCP/IP Internetu

- Za razliku od homogenog WAN, TCP/IP Internet nema jedinstven L2 (nivo dva).
- Sasvim suprotno, Internet se sastoji od više različitih fizičkih mreža, koje su međusobno povezane.
- Elementi po kojima se razlikuje upravljanje Internetom su sledeći:
- (a) jedan rukovalac može upravljati raznorodnim konvertorima protokola,
- (b) entiteti koji su predmet upravljanja ne moraju imati isti L2, i
- (c) skup mašina kojima rukovalac upravlja mogu biti bilo gde u Internetu.

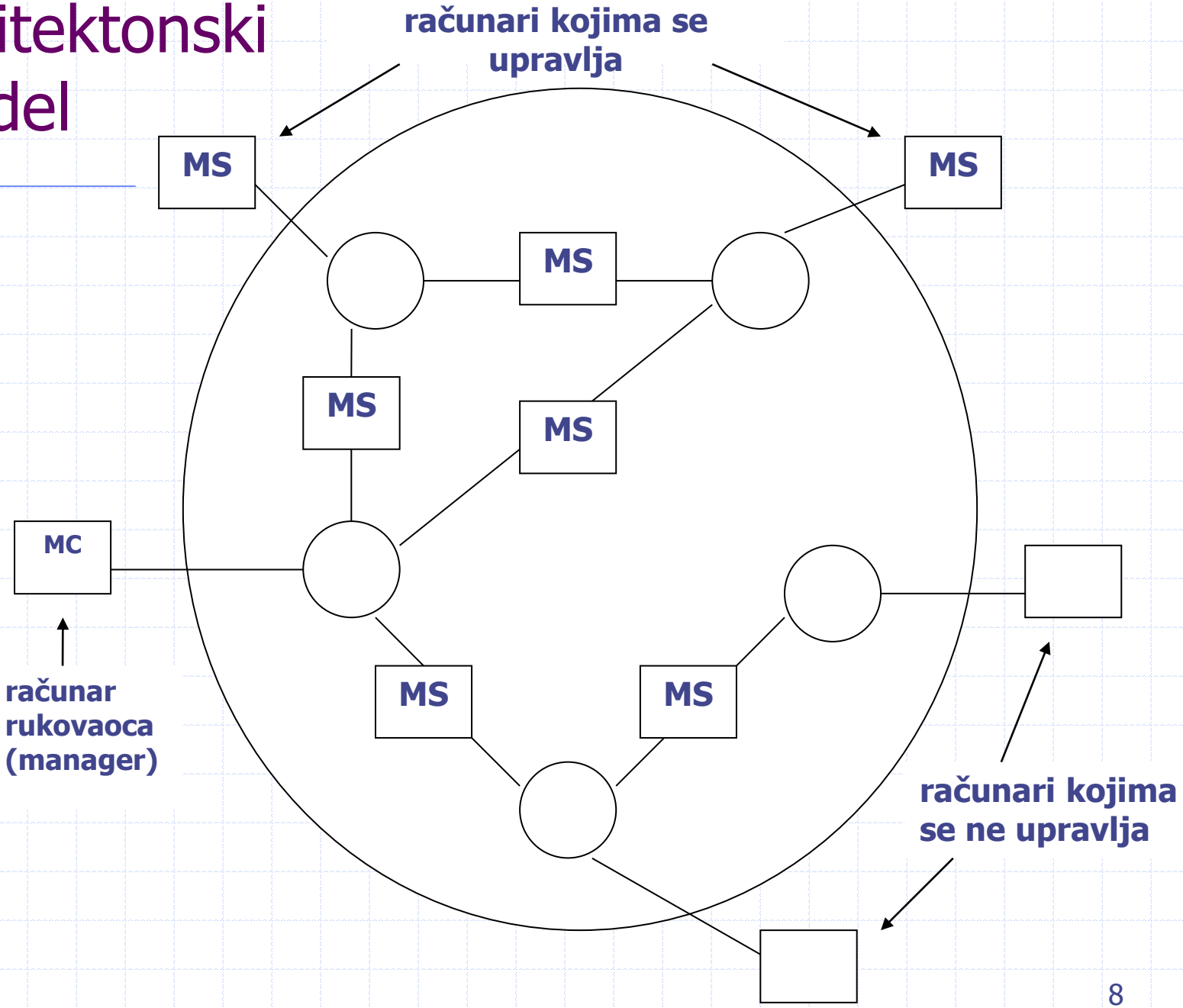
Pozicioniranje protokola upravljanja u aplikativni nivo u TCP/IP internetu

- Iz gornjig razloga, protokol upravljanja Internetom je smešten na aplikativnom nivou.
- Prednosti ovog pristupa su:
- (a) postoji jedan skup protokola za sve mreže, i
- (b) jedan skup protokola za sve uređaje kojima se upravlja,
- (c) jednoobraznost – svi konvertori protokola odgovaraju na identičan skup komandi, i
- (d) računar rukovaoca ne mora biti priključen na sve fizičke mreže Interneta.

Nedostaci smeštanja protokola upravljanja u aplikativni nivo

- Nedostaci ovog pristupa su što:
- (a) rukovalac ne može pristupiti konvertoru protokola ukoliko njegova programska podrška transportnog nivoa ne radi, ili
- (b) ukoliko je došlo do otkaza OS (operativnog sistema) na konvertoru protokola.

Arhitektonski model



Objašnjenje arhitektonskog modela

- Koristi se model klijent-server
- Program servera se zove *agent rukovaoca* (*management agent*).
- Rukovalac (operator) pokreće program klijenta radi slanja upita i komandi.
- U Internetu postoji veliki broj rukovalaca.
- Obavezna je njihova identifikacija i autentifikacija.
- Moguće je i više nivoa autorizacije, npr. više ovlašćenih da čita i jedan koji može da piše.

- Postoji pet tipova SNMP aplikacija. To su:
  - generatori komandi (command generators),
  - odgovarači na komande (command responders),
  - izvori objava (notification originators),
  - primaoci objava (notification receivers)
  - zastupnici (proxy forwarders).

- 1) Generator komandi. Šalje zahteve iz klase čitanja i/ili upisa i obrađuje odgovore na zahteve koje je poslao.
- 2) Odgovarač na komande. Prima zahteve iz klase čitanja i/ili upisa koji su namenjeni za lokalni system, izvršava traženu operaciju (u koordinaciji sa kontrolom pristupa) i generiše odgovore koji se šalju pošiljaoca zahteva.

- 3) Izvor objava. Nadzire system u potrazi za zadatim događajima i uslovima, i generiše poruke iz klase objava na osnovi tih događaja i uslova.
- 4) Primalac objava. Osluškuje poruke objava i generiše poruke odgovora kada je primljena poruka iz klase koja zahteva potvrdu (Confirmed Class).
- 5) Zastupnik. Prosleđuje SNMP poruke.

- SNMP sistem upravljanja obuhvata:
  - više čvorova, svaki sa SNMP entitetom koji sadrži aplikacije za odgovaranje na komande i izvore objava, i koji ima mogućnost upravljanja lokalnim uređajem (ovi entiteti se tradicionalno nazivaju agenti),
  - I bar jedan SNMP entitet koji sadrži aplikacije generator komandi i/ili primaoca objava (ovi entiteti se tradicionalno nazivaju upravljači ili menadžeri).

- SNMP poruke enkapsuliraju SNMP PDU. Ovaj PDU definiše operacije koje treba da realizuje SNMP modul primaoca. Svaka PDU pripada jednoj ili više od sledećij PDU klasa, po RFC 3416:
- 1) Klasa čitanja (Read Class): operacije protokola koje pribavljaju upravljačku informaciju. To su sledeće: GetRequest-PDU, GetNextRequest-PDU, i GetBulkRequest-PDU. GetNextRequest-PDU se koristi za preuzimanje tabelarnih podataka. GetBulkRequest se koristi za pribavljanje većih količina upravljačkih podataka u jednom zahtevu.

- 2) Klasa upisa (Write Class) obuhvata operacije protokola koje imaju za cilj izmenu upravljačke informacije. To je SetRequest-PDU.
- 3) Klasa odgovora (Response Class) obuhvata operacije koje predstavljaju odgovor na prethodno primljeni zahtev. To su: Response-PDU, Report-PDU.

- 4) Klasa objave (Notification Class) obuhvata operacije koje šalju objavu ka aplikaciji primaocu objava. To su: Trapv2-PDU, InformRequest-PDU.
- 5) Interna klasa (Internal Class) obuhvata operacije koje se razmenjuju interno između SNMP modula. To je Report-PDU.

- PDU još možemo podeliti na:
  - one koji se potvrđuju (Confirmed), što znači da SNMP modul primaoca mora da pošalje odgovor – to su GetRequest-PDU, GetNextRequest-PDU, GetBulkRequest-PDU, SetRequest-PDU, i InformRequest-PDU;
  - I one koji se ne potvrđuju (Unconfirmed): Unconfirmed Class: Report-PDU, Trapv2-PDU, i GetResponse-PDU.

Arhitektura protokola

- Standard upravljanja Internetom definiše:
- (1) Način komunikacije:
- (1a) oblik i značenje poruka
- (1b) oblik imena i adresa
- (2) Podaci koji su predmet upravljanja:
- (2a) koje podatke konvertor protokola mora održavati
- (2b) sintaksa imena pojedinih podataka
- Razdajanje standarda komunikacije od standarda podaka, omogućilo je postojanje više verzija obe vrste standarda.

Standardi komunikacije (Simple Network Management Protocol i njegove verzije)

- Standardi komunikacije su:
- (a) SNMP - jednostavni protokol za upravljanje Internetom sa vrlo slabom zaštitom.
- (b) SNMPv2 – uvodi GetBulkRequest koji se koristi za pribavljanje većih količina upravljačkih podataka u jednom zahtevu + pokušaj da se uvede jača zaštita.
- (c) SNMPv3 – uvođenje mehanizama zaštite u SNMP koji se oslanjaju na SSH i TLS i koje se odnose na: enkripciju poruka, zaštitu integriteta poruka (sprečavanje izmena poruka u prenosu) i autentikaciju strana u komunikaciji.

- SNMPv3 je objavljen u RFC 3411-3418 i ima nivo full Internet standard (najviši nivo) prema IETF
- Danas se SNMP uglavnom koristi za nadzor udaljenih objekata i upravljanje performansama njihovog rada

Standard za informaciju kojom se upravlja

- Sandard za podatke je MIB (Management Information Base), koji specificira obavezne podatke i operacije nad njima.
- Npr. MIB obavezuje IP da broji oktete primljene na svakom mrežnom priključku i omogućava NMS-u (network management software) da očitava te vrednosti.
- MIB standard razvrstava informaciju u 8 kategorija, u skladu sa narednom tabelom.
- Ako zahtevani element MIB-a ne postoji, vraća se poruka o grešci.

MIB kategorije informacije

MIB kategorija	Uključuje informaciju o:
system	OS računara ili konvertora protokola.
interfaces	Pojedinim mrežnim priključcima.
addr. trans.	Prevođenju adresa (npr. ARP preslikavanja).
ip	IP programska podrška.
icmp	ICMP programska podrška.
tcp	TCP programska podrška.
udp	UDP programska podrška.
egp	EGP programska podrška.

Nastavak objašnjenja MIB-a

- Pored MIB-II (MIB standard), mnogi drugi RFC dokumentuju MIB podatke za određene uređaje.
- MIB daje logičku definiciju podataka.
- Program agenta je dužan da obavi konverziju interne predstave podataka u njihovu logičku definiciju.
- Sledi primer MIB podataka.

Primer MIB podataka (1/2)

MIB podatak	Kategorija	Značenje
sysUpTime	system	Vreme od zadnjeg restarta.
ifNumber	interfaces	Broj mrežnih priključaka.
ifMtu	interfaces	MTU za određeni priključak.
ipDefaultTTL	ip	Vrednost koju IP koristi za TTL.
ipInReceives	ip	Broj primljenih datagrama.
ipForwDatagrams	ip	Broj usmerenih datagrama.
ipOutNoRoutes	ip	Broj grešaka usmeravanja.
ipReasmOKs	ip	Broj sastavljenih datagrama.

Primer MIB podataka (2/2)

MIB podatak	Kategorija	Značenje
ipFragOKs	ip	Broj rastavljenih datagrama.
ipRoutingTable	ip	IP tabela usmeravanja.
icmpInEchos	icmp	Broj primljenih ICMP zahteva za odjek.
tcpRtoMin	tcp	Najmanje vreme do ponovnog slanja.
tcpMaxConn	tcp	Maksimalan broj istovremenih TCP veza.
tcpInSegs	tcp	Broj primljenih segmenata.
udpInDatagrams	udp	Broj primljenih UDP datagrama.
egpInMsgs	egp	Broj primljenih EGP proruka.

Struktura informacije kojom se upravlja

- Standard SMI (*Structure of Management Information*) definiše skup pravila za definisanje i identifikaciju MIB podataka.
- SMI ograničava tipove podataka dozvoljene u MIB.
- SMI specificira:
- (a) pravila imenovanja podataka, i
- (b) pravila definisanja tipova.
- Npr. *IpAddress* je niz od 4 okteta, a *Counter* je ceo broj u opsegu 0-(exp(2,32)-1), itd.
- SMI pravila opisuju kako se referenciraju stavke tabele vrednosti (npr. tabele usmeravanja).

Formalna definicija korišćenjem ASN.1

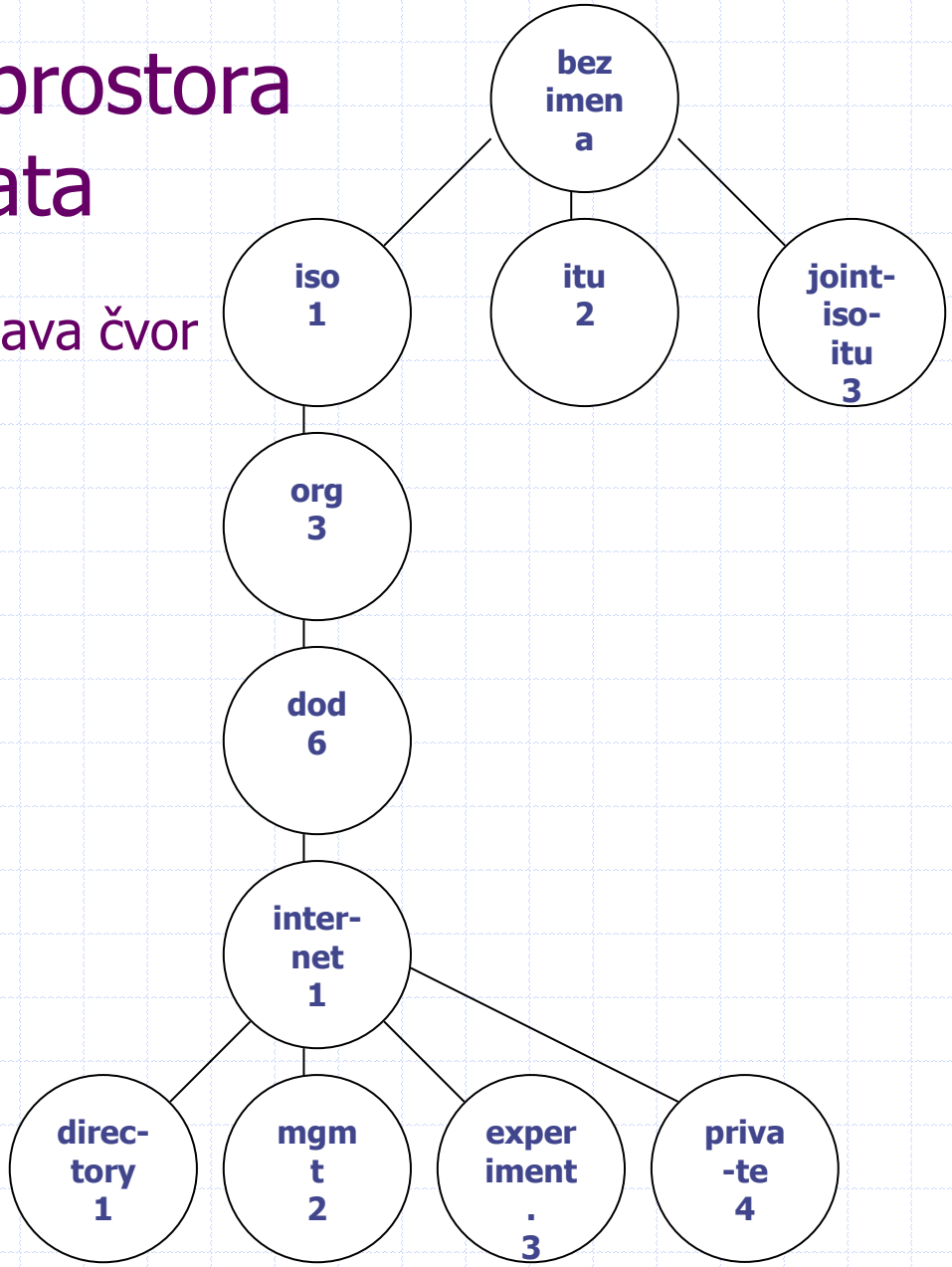
- Po SMI, MIB podaci se definišu i referenciraju u skladu sa ISO ASN.1 (*Abstract Syntax Notation No. 1*).
- ASN.1 je formalni jezik sa dve osobine:
- (a) to je notacija za dokumente, i
- (b) kompaktna kodovana predstava za komunikacione protokole.
- ASN.1 precizno definiše kodovanje imena i podataka u porukama.

Struktura i predstava imena MIB objekata

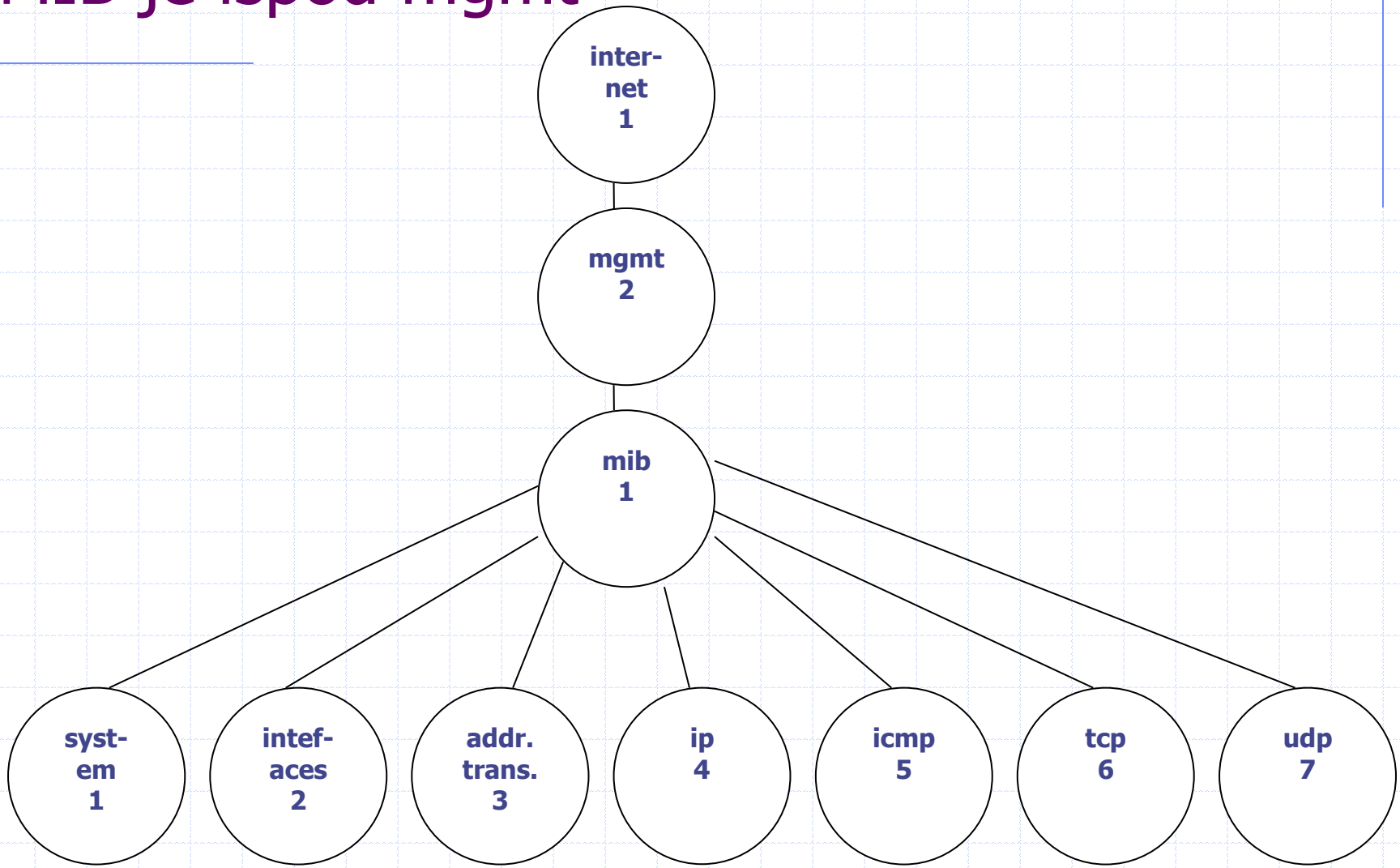
- Imena MIB podataka se daju iz prostora imena *identifikatora objekata*, koje administrira ISO i ITU.
- Ova imena su jedinstvena u svetu.
- Prostor imena je hijerarhijski uređen (slično kao DNS).
- Imenu se dodeljuje tekstualni niz znakova i ceo broj (koji koriste računari).
- Sledeća slika prikazuje hijerarhiju prostora imena ID objekata.
- Ime objekta u hijerarhiji se formira tako što se niz celih brojeva od korena do čvora objekta razdvoji sa ".".

Deo hijerarhije prostora imena ID objekata

(Npr. ime 1.3.6.1.1 označava čvor "directory")



MIB je ispod mgmt



Imena objekata u MIB (1/4)

- Objeku *ip* se dodeljuju imena:

iso.org.dod.internet.mgmt.mib.ip i

1.3.6.1.2.1.4

- MIB podatku *ipInReceives* odgovaraju:

iso.org.dod.internet.mgmt.mib.ip.ipInReceives i

1.3.6.1.2.1.4.3

- Protokoli dodaju imenima podataka sufikse.
- Sufiks 0 označava instancu podatka sa zadatim imenom, npr. za *ipInReceives* to je:

1.3.6.1.2.1.4.3.0

Imena objekata u MIB (2/4)

- Drugi, složeniji, primer je ipAddrTable, sa num. Ekvivalentom 1.3.6.1.2.1.4.20
- U programskom smislu to je jednodimenzionalan niz:
- ipAddrTable ::= SEQUENCE OF IpAddrEntry
- Sledi definicija stavke (entry) tabele.

Imena objekata u MIB (3/4): Definicija stavke IP tabele usmeravanja

Red definicije	Komentar
IpAddrEntry ::= SEQUENCE {	Stavka se definiše kao niz definisan između { i }.
ipAdEntAddr IpAddress,	IP adresa. Tip podatka je *IpAddress.*
ipAdEntIfIndex INTEGER,	Indeks priključka koji odgovara ovoj stavki. Tip podatka je *INTEGER.*
ipAdEntNetMask IpAddress,	IP maska podmreže. Tip podatka je *IpAddress.*
ipAdEntBcastAddr IpAddress	Adresa za slanje svima (*broadcast*). Tip podatka je *IpAddress.*
ipAdEntReasmMaxSize INTEGER(0..65535)	Maksimalna veličina datagrama koji se sklapa. Tip podatka je *INTEGER(0..65535).*
}	Kraj definicije.

Imena objekata u MIB (4/4)

- Daljim definicijama se dodeljuju vrednosti *ipAddrEntry* i svakoj stavki u *ipAddrEntry* sekvenci:

ipAddrEntry {ipAddrTable 1}

- što znači da spada pod *ipAddrTable* i da ima vred. 1, i

ipAdEntNetMask {ipAddrEntry 3}

- što znaći da spada pod ipAddrEntry i da ima vred. 3.
- ASN.1 ne koristi celobrojne indekse.
- S obzirom da nisu podržani indeksi postavlja se opravdano pitanje: Kako se pristupa elemetima tabele?

Referenciranje elemenata tabele u ASN.1

- Umesto da se koristi indeks, imenu MIB tabele se dodaje sufiks radi izbora određenog elementa tabele.
- Za primer tabele internet adresa, standard specificira da je sufiks za izbor stavke sama IP adresa.
- Tj. referenca se dobija tako što se IP adresa doda na kraj imena tabele, npr.:

iso.org...ipAddrTable.ipAddrEntry.ipAdEntMask.128.10.2.3

SNMP

- Specificira oblik i značenje poruka klijent-server.
- Obezbeđuje autentifikaciju rukovalaca.
- Ranije su protokoli upravljanja mrežom bili građeni oko komandi, kao što su:
  - REBOOT
  - ADD/DELETE ROUTE(S)
  - DISABLE/ENABLE NETWORK INTERFACE
  - REMOVE CACHED ADDRESS BINDINGS
- Osnovni nedostatak ovog prilaza je složenost.

Praksa prihvati-sačuvaj (FATCH-STORE Paradigm)

- SNMP koristi alternativan pristup: umesto velikog broja komandi, sve operacije se obavljaju po principu prihvati-sačuvaj.
- Ova praksa potiče iz protokola za upravljanje mrežom pod nazivom HEMS.
- Npr. komanda REBOOT se realizuje tako što se u promenljivu koja sadrži vreme do sledećeg REBOOT-a upiše 0.
- Osnovne prednosti ovog prilaza su: (a) stabilnost, (b) jednostavnost, i (c) prilagodljivost (fleksibilnost).

Pet osnovnih operacija u SNMP

(Operacije su atomske, tj neprekidive! TRAP je asinhroni događaj, npr. otkaz dela opreme i slično)

KOMANDA	ZNAČENJE
get-request	Prihvati vrednost zadate promenljive (podatka).
get-next-request	Prihvati vrednost bez poznavanja njenog tačnog imena.
get-response	Odgovor na operaciju prihvata vrednosti (fetch).
set-request	Sačuvaj vrednost zadatog podatka.
trap	Odgovor pobuđen događajem.

Pretraga tabele korišćenjem imena

- ASN.1 ne obezbeđuje mehanizam za klasično indeksiranje nizova.
- Elementu niza se pristupa dodavanjem sufiksa na kraj imena.
- Putem get-next-request operacije moguće je dobiti sledeći element niza:
  - Na početku se zada ime niza.
  - Kasnije se zadaje ime prethodnog elementa dobijenog u *get-response* (FULL OBJECT ID RETURNED BY SERVER).
- Npr. tako je moguće pročitati celu tabelu *ipAddrTable*.

Oblik SNMP poruka

- SNMP poruke nemaju fiksna polja.
- Poruke se kodiraju po ASN.1.

Postoji 8 tipova jedinica podataka:

```
SNMP_PDUs ::= CHOICE {
        get-request       GetRequest-PDU,
        get-next-request GetNextRequest-PDU,
        get-bulk-request GetBulkRequest-PDU,
        response          Response-PDU,
        set-request       SetRequest-PDU,
        inform-request    InformRequest-PDU,
        snmpV2-trap       SNMPv2-Trap-PDU,
        report            Report-PDU
}

GetRequest-PDU ::= [0] IMPLICIT PDU
-- …
```

Definicija PDU:

```
PDU ::= SEQUENCE {
        request-id INTEGER (-214783648..214783647),
        error-status                -- sometimes ignored
            INTEGER {
                noError(0),
                tooBig(1),
                noSuchName(2),      -- for proxy compatibility
    -- ...
                inconsistentName(18)
            },
        error-index                 -- sometimes ignored
            INTEGER (0..max-bindings),
        variable-bindings           -- values are sometimes ignored
            VarBindList
    }
```

Primer kodovanja SNMPv1 poruke

- Koriste se polja promenljive dužine.
- U opštem slučaju, polje počinje zaglavljem, koje specificira tip objekta, i njegovu dužinu u bajtima.
- Sledi primer niza kodovanih okteta u get-request poruci za podatak sysDescr (num. ekv. 1.3.6.1.2.1.1.1).

Format SNMPv1 poruke

```
Message ::=
        SEQUENCE {
         version        -- version-1 for this RFC
                INTEGER {
                        version-1(0)
                },

        community       -- community name
                OCTET STRING,

        data            -- e.g., PDUs
                ANY
        }
```

Primer iskodirane SNMPv1 poruke

(get-request SNMP poruka za podatak sysDescr - num. ekv. 1.3.6.1.2.1.1.1)

30	29	02	01	00	Okteti ulevo: 02,01,00 čine polje verzije protokola.		
SEQU-ENCE	dužina= 41	INTEG-ER	dužina= 1	verz.=0			
04	06	70	75	62	6c	69	63
string	dužina= 6	Gornji okteti: 70,75...63 sadrže tekst «public».					
A0	1C	02	04	05	AE	56	02
kod za get-req.	dužina= 28	INTEG-ER	dužina= 4	Gornji okteti: 05,AE,56,02 su identifikacija zahteva (request ID)			
02	01	00	02	01	00	Šest okteta ulevo sadrže kod stanja i indeks greške.	
INTEG-ER	dužina= 1	status	INTEG-ER	dužina= 1	indeks greške		
30	0E	30	0C	06	08		
SEQU-ENCE	dužina= 14	SEQU-ENCE	dužina= 12	identifi. objekta	dužina= 8		
2B	06	01	02	01	01	01	00
1.3	.6	.1	.2	.1	.1	.1	.0
05	00						
null	dužina= 0	Kraj poruke.					