Communication protocols and network safety

Network control and management

Network management

- What is network management??
  Why is it needed?

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

Network management

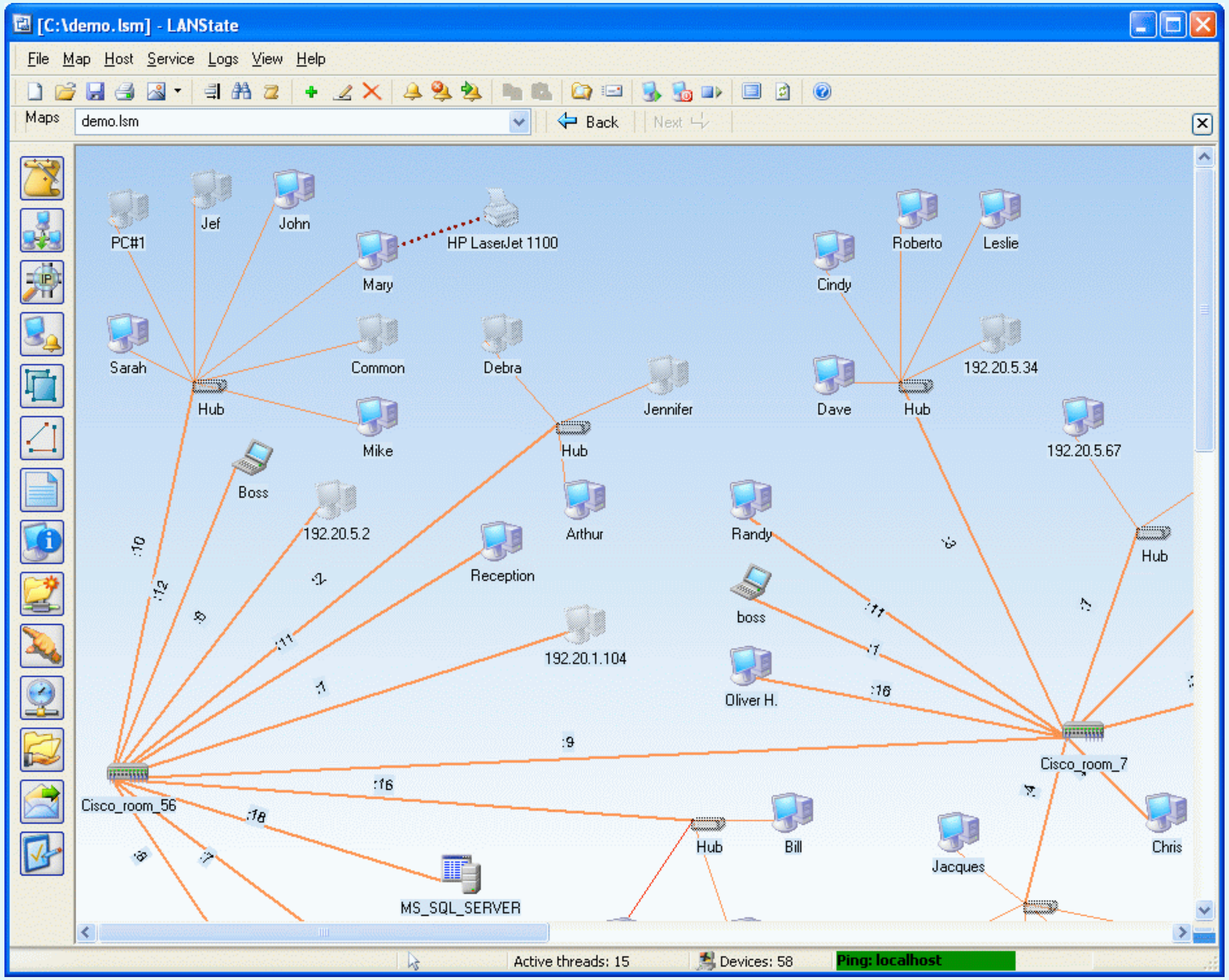
- Growth of internet and local networks caused small networks to connect into one **LARGE** infrastructure. With it increased the need for **SISTEMATIC** management of hardware and software components of this system. Frequent questions:
- Which resources are available in the network?
- How much traffic is traveling through a certain network equipment?
- Who uses network connections that cause their director to receive his email too slowly?
- Why cant I send data to a certain computer?

- Definition: Managing a network involves **deployment**, **integration** and **coordination** of hardware, software and human resources for the purpose of **observation**, **testing**, **configuration**, **analysis** and **control** of network resources, for which we want to provide **operation** in real-time (or operation with appropriate quality - QoS) at an affordable price.

Examples of management activities

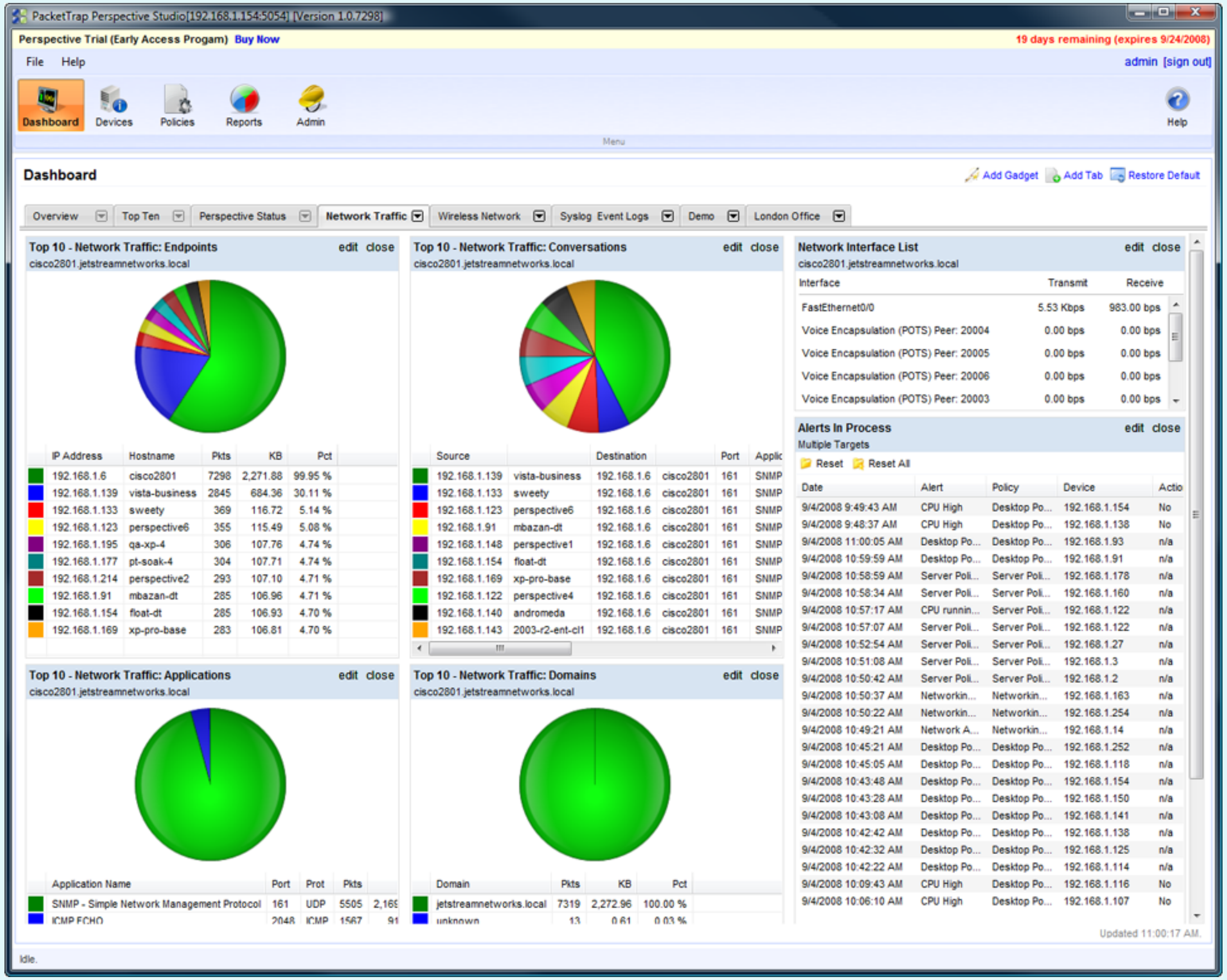
1. **detection of errors on the computer or router interface**: administrator can be notified by the software that the interface has a problem (even before it fails!)
2. **controlling computer operation and network analysis**
3. **controlling network traffic**: administrator can observe frequent communications and direction finding bottlenecks,
4. **detection of rapid changes in routing tables**: this phenomenon may indicate problems with routing or error in the router,
5. **controlling levels of service provision**: network service providers are able to guarantee availability, latency and certain service throughput; administrator can measure and verify,
6. **intrusion detection**: administrator can be notified if certain traffic arrives from suspicious sources; he can also detect a particular type of traffic (eg, a set of SYN packets intended for one single interface)

Examples of activities



controlling computer operation and network analysis (detection of network topology)

Examples of activities



Dashboard

Top 10 - Network Traffic: Endpoints
cisco2801.jetstreamnetworks.local

	IP Address	Hostname	Pkts	KB	Pct
🟩	192.168.1.6	cisco2801	7298	2,271.88	99.95 %
🟦	192.168.1.139	vista-business	2845	684.36	30.11 %
🟥	192.168.1.133	sweety	369	116.72	5.14 %
🟨	192.168.1.123	perspective6	355	115.49	5.08 %
🟪	192.168.1.195	qa-xp-4	306	107.76	4.74 %
🟦	192.168.1.177	pt-soak-4	304	107.71	4.74 %
🟫	192.168.1.214	perspective2	293	107.10	4.71 %
🟩	192.168.1.91	mbazan-dt	285	106.96	4.71 %
⬛	192.168.1.154	float-dt	285	106.93	4.70 %
🟧	192.168.1.169	xp-pro-base	283	106.81	4.70 %

Top 10 - Network Traffic: Conversations
cisco2801.jetstreamnetworks.local

	Source		Destination		Port	Applic
🟩	192.168.1.139	vista-business	192.168.1.6	cisco2801	161	SNMP
🟦	192.168.1.133	sweety	192.168.1.6	cisco2801	161	SNMP
🟥	192.168.1.123	perspective6	192.168.1.6	cisco2801	161	SNMP
🟨	192.168.1.91	mbazan-dt	192.168.1.6	cisco2801	161	SNMP
🟪	192.168.1.148	perspective1	192.168.1.6	cisco2801	161	SNMP
🟦	192.168.1.154	float-dt	192.168.1.6	cisco2801	161	SNMP
🟫	192.168.1.169	xp-pro-base	192.168.1.6	cisco2801	161	SNMP
🟩	192.168.1.122	perspective4	192.168.1.6	cisco2801	161	SNMP
⬛	192.168.1.140	andromeda	192.168.1.6	cisco2801	161	SNMP
🟧	192.168.1.143	2003-r2-ent-cl1	192.168.1.6	cisco2801	161	SNMP

Network Interface List
cisco2801.jetstreamnetworks.local

Interface	Transmit	Receive
FastEthernet0/0	5.53 Kbps	983.00 bps
Voice Encapsulation (POTS) Peer: 20004	0.00 bps	0.00 bps
Voice Encapsulation (POTS) Peer: 20005	0.00 bps	0.00 bps
Voice Encapsulation (POTS) Peer: 20006	0.00 bps	0.00 bps
Voice Encapsulation (POTS) Peer: 20003	0.00 bps	0.00 bps

Alerts In Process
Multiple Targets

Date	Alert	Policy	Device	Actio
9/4/2008 9:49:43 AM	CPU High	Desktop Po...	192.168.1.154	No
9/4/2008 9:48:37 AM	CPU High	Desktop Po...	192.168.1.138	No
9/4/2008 11:00:05 AM	Desktop Po...	Desktop Po...	192.168.1.93	n/a
9/4/2008 10:59:59 AM	Desktop Po...	Desktop Po...	192.168.1.91	n/a
9/4/2008 10:58:59 AM	Server Poli...	Server Poli...	192.168.1.178	n/a
9/4/2008 10:58:34 AM	Server Poli...	Server Poli...	192.168.1.160	n/a
9/4/2008 10:57:17 AM	CPU runnin...	Server Poli...	192.168.1.122	n/a
9/4/2008 10:57:07 AM	Server Poli...	Server Poli...	192.168.1.122	n/a
9/4/2008 10:52:54 AM	Server Poli...	Server Poli...	192.168.1.27	n/a
9/4/2008 10:51:08 AM	Server Poli...	Server Poli...	192.168.1.3	n/a
9/4/2008 10:50:42 AM	Server Poli...	Server Poli...	192.168.1.2	n/a
9/4/2008 10:50:37 AM	Networkin...	Networkin...	192.168.1.163	n/a
9/4/2008 10:50:22 AM	Networkin...	Networkin...	192.168.1.254	n/a
9/4/2008 10:49:21 AM	Network A...	Networkin...	192.168.1.14	n/a
9/4/2008 10:45:21 AM	Desktop Po...	Desktop Po...	192.168.1.252	n/a
9/4/2008 10:45:05 AM	Desktop Po...	Desktop Po...	192.168.1.118	n/a
9/4/2008 10:43:48 AM	Desktop Po...	Desktop Po...	192.168.1.154	n/a
9/4/2008 10:43:28 AM	Desktop Po...	Desktop Po...	192.168.1.150	n/a
9/4/2008 10:43:08 AM	Desktop Po...	Desktop Po...	192.168.1.141	n/a
9/4/2008 10:42:42 AM	Desktop Po...	Desktop Po...	192.168.1.138	n/a
9/4/2008 10:42:32 AM	Desktop Po...	Desktop Po...	192.168.1.125	n/a
9/4/2008 10:42:22 AM	Desktop Po...	Desktop Po...	192.168.1.114	n/a
9/4/2008 10:09:43 AM	CPU High	Desktop Po...	192.168.1.116	No
9/4/2008 10:06:10 AM	CPU High	Desktop Po...	192.168.1.107	No

Updated 11:00:17 AM.

Top 10 - Network Traffic: Applications
cisco2801.jetstreamnetworks.local

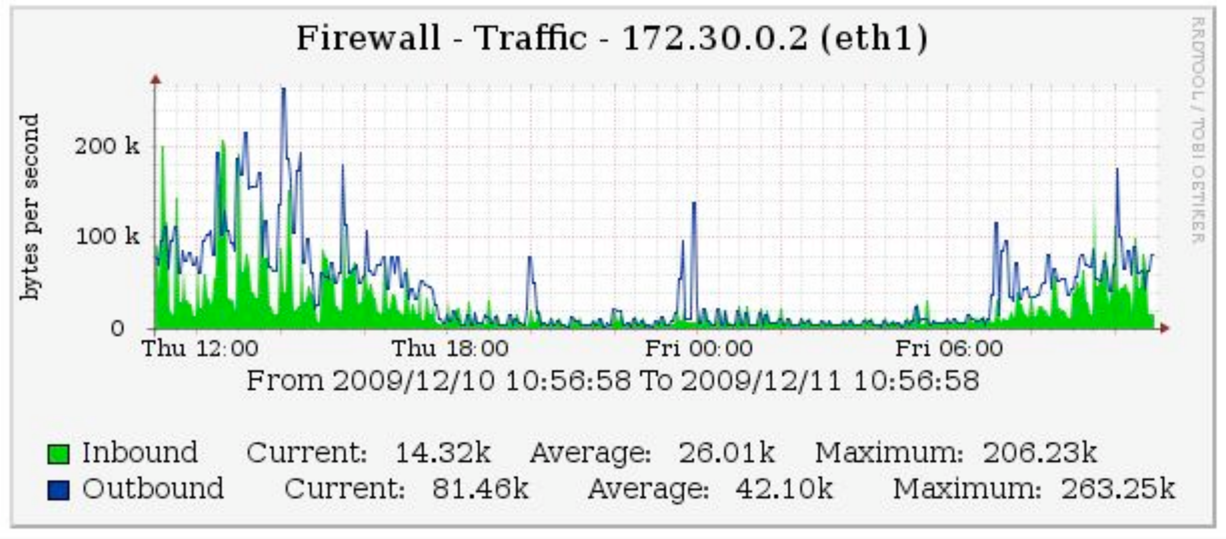
	Application Name	Port	Prot	Pkts	
🟩	SNMP - Simple Network Management Protocol	161	UDP	5505	2,169
🟦	ICMP ECHO	2048	ICMP	1567	91

Top 10 - Network Traffic: Domains
cisco2801.jetstreamnetworks.local

	Domain	Pkts	KB	Pct
🟩	jetstreamnetworks.local	7319	2,272.96	100.00 %
🟦	unknown	13	0.61	0.03 %

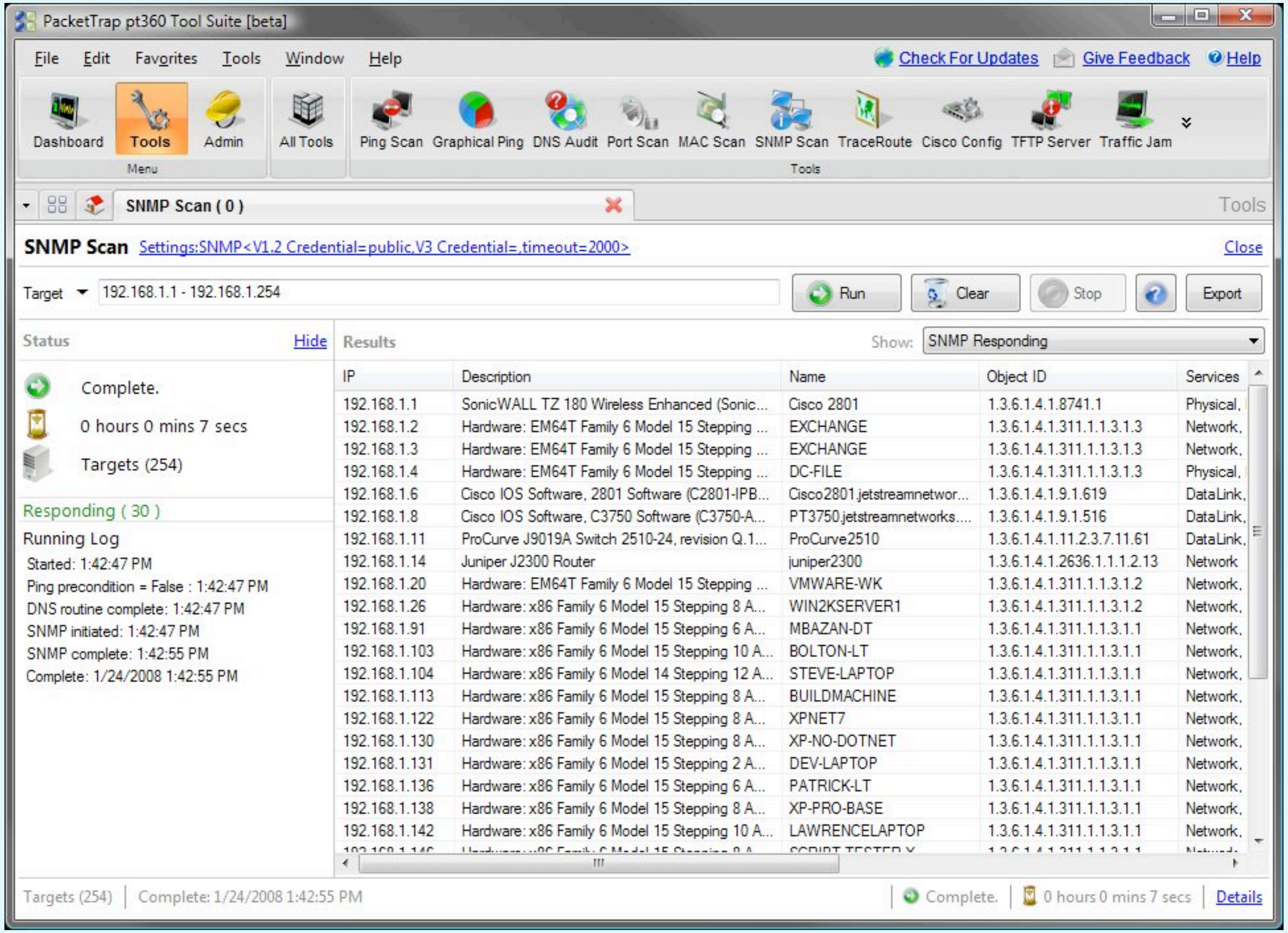
controlling network traffic (profiling)

Examples of activities



controlling the level of service provision (data flow)

Examples of activities



SNMP Scan Settings:SNMP<V1.2 Credential=public,V3 Credential=,timeout=2000>

Target: 192.168.1.1 - 192.168.1.254

Status

Complete.

0 hours 0 mins 7 secs

Targets (254)

Responding (30)

Running Log

```
Started: 1:42:47 PM
Ping precondition = False : 1:42:47 PM
DNS routine complete: 1:42:47 PM
SNMP initiated: 1:42:47 PM
SNMP complete: 1:42:55 PM
Complete: 1/24/2008 1:42:55 PM
```

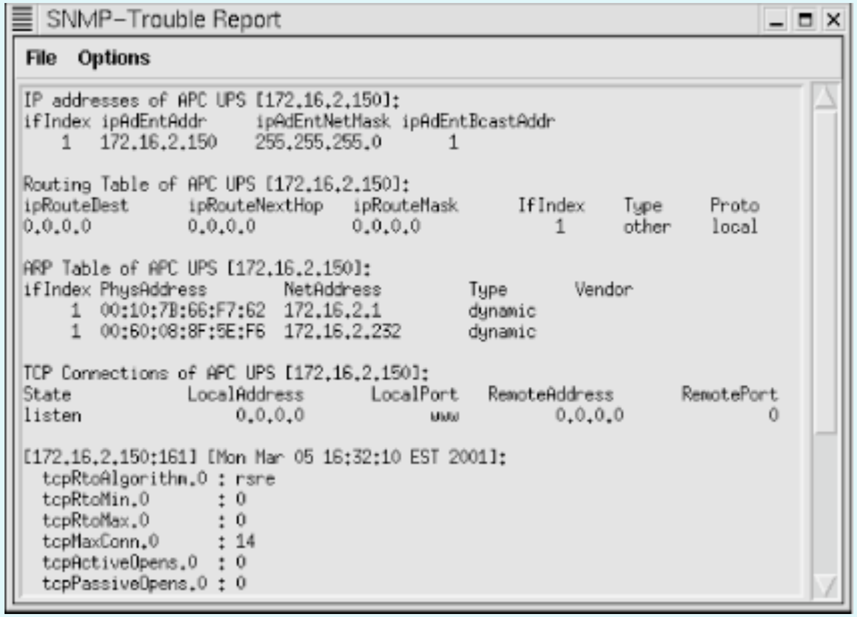
Results — Show: SNMP Responding

IP	Description	Name	Object ID	Services
192.168.1.1	SonicWALL TZ 180 Wireless Enhanced (Sonic...	Cisco 2801	1.3.6.1.4.1.8741.1	Physical,
192.168.1.2	Hardware: EM64T Family 6 Model 15 Stepping ...	EXCHANGE	1.3.6.1.4.1.311.1.1.3.1.3	Network,
192.168.1.3	Hardware: EM64T Family 6 Model 15 Stepping ...	EXCHANGE	1.3.6.1.4.1.311.1.1.3.1.3	Network,
192.168.1.4	Hardware: EM64T Family 6 Model 15 Stepping ...	DC-FILE	1.3.6.1.4.1.311.1.1.3.1.3	Physical,
192.168.1.6	Cisco IOS Software, 2801 Software (C2801-IPB...	Cisco2801.jetstreamnetwor...	1.3.6.1.4.1.9.1.619	DataLink,
192.168.1.8	Cisco IOS Software, C3750 Software (C3750-A...	PT3750.jetstreamnetworks....	1.3.6.1.4.1.9.1.516	DataLink,
192.168.1.11	ProCurve J9019A Switch 2510-24, revision Q.1...	ProCurve2510	1.3.6.1.4.1.11.2.3.7.11.61	DataLink,
192.168.1.14	Juniper J2300 Router	juniper2300	1.3.6.1.4.1.2636.1.1.1.2.13	Network
192.168.1.20	Hardware: EM64T Family 6 Model 15 Stepping ...	VMWARE-WK	1.3.6.1.4.1.311.1.1.3.1.2	Network,
192.168.1.26	Hardware: x86 Family 6 Model 15 Stepping 8 A...	WIN2KSERVER1	1.3.6.1.4.1.311.1.1.3.1.2	Network,
192.168.1.91	Hardware: x86 Family 6 Model 15 Stepping 6 A...	MBAZAN-DT	1.3.6.1.4.1.311.1.1.3.1.1	Network,
192.168.1.103	Hardware: x86 Family 6 Model 15 Stepping 10 A...	BOLTON-LT	1.3.6.1.4.1.311.1.1.3.1.1	Network,
192.168.1.104	Hardware: x86 Family 6 Model 14 Stepping 12 A...	STEVE-LAPTOP	1.3.6.1.4.1.311.1.1.3.1.1	Network,
192.168.1.113	Hardware: x86 Family 6 Model 15 Stepping 8 A...	BUILDMACHINE	1.3.6.1.4.1.311.1.1.3.1.1	Network,
192.168.1.122	Hardware: x86 Family 6 Model 15 Stepping 8 A...	XPNET7	1.3.6.1.4.1.311.1.1.3.1.1	Network,
192.168.1.130	Hardware: x86 Family 6 Model 15 Stepping 8 A...	XP-NO-DOTNET	1.3.6.1.4.1.311.1.1.3.1.1	Network,
192.168.1.131	Hardware: x86 Family 6 Model 15 Stepping 2 A...	DEV-LAPTOP	1.3.6.1.4.1.311.1.1.3.1.1	Network,
192.168.1.136	Hardware: x86 Family 6 Model 15 Stepping 6 A...	PATRICK-LT	1.3.6.1.4.1.311.1.1.3.1.1	Network,
192.168.1.138	Hardware: x86 Family 6 Model 15 Stepping 8 A...	XP-PRO-BASE	1.3.6.1.4.1.311.1.1.3.1.1	Network,
192.168.1.142	Hardware: x86 Family 6 Model 15 Stepping 10 A...	LAWRENCELAPTOP	1.3.6.1.4.1.311.1.1.3.1.1	Network,

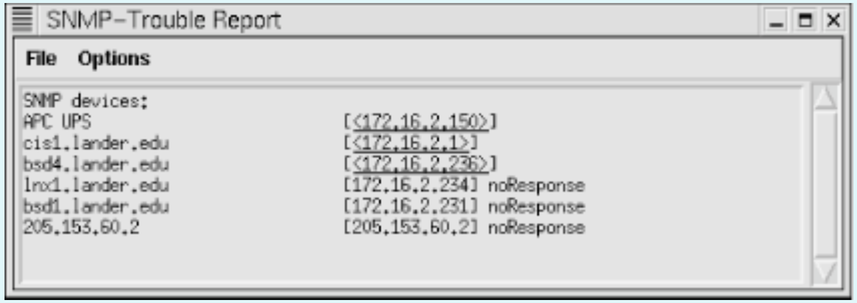
Targets (254) | Complete: 1/24/2008 1:42:55 PM | Complete. | 0 hours 0 mins 7 secs

controlling computer operation and network analysis (list of IP addresses)

Examples of activities



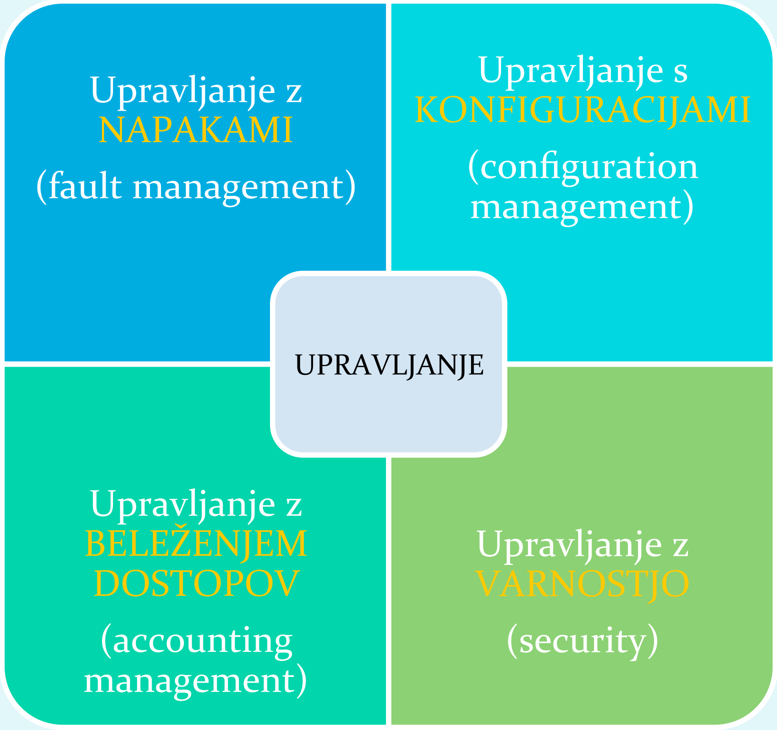
```
IP addresses of APC UPS [172.16.2.150]:
ifIndex ipAdEntAddr     ipAdEntNetMask ipAdEntBcastAddr
    1   172.16.2.150    255.255.255.0        1

Routing Table of APC UPS [172.16.2.150]:
ipRouteDest        ipRouteNextHop   ipRouteMask        IfIndex   Type     Proto
0.0.0.0            0.0.0.0          0.0.0.0                1     other    local

ARP Table of APC UPS [172.16.2.150]:
ifIndex PhysAddress        NetAddress          Type        Vendor
     1  00:10:7B:66:F7:62  172.16.2.1          dynamic
     1  00:60:08:8F:5E:F6  172.16.2.232        dynamic

TCP Connections of APC UPS [172.16.2.150]:
State                LocalAddress        LocalPort    RemoteAddress        RemotePort
listen                    0.0.0.0              www          0.0.0.0                 0

[172.16.2.150:161] [Mon Mar 05 16:32:10 EST 2001]:
  tcpRtoAlgorithm.0 : rsre
  tcpRtoMin.0       : 0
  tcpRtoMax.0       : 0
  tcpMaxConn.0      : 14
  tcpActiveOpens.0  : 0
  tcpPassiveOpens.0 : 0
```



```
SNMP devices:
APC UPS                                [<172.16.2.150>]
cis1.lander.edu                        [<172.16.2.1>]
bsd4.lander.edu                        [<172.16.2.236>]
lnx1.lander.edu                        [172.16.2.234] noResponse
bsd1.lander.edu                        [172.16.2.231] noResponse
205.153.60.2                           [205.153.60.2] noResponse
```

controlling computer operation and network analysis (diagnostics and fault detection)

Areas of management



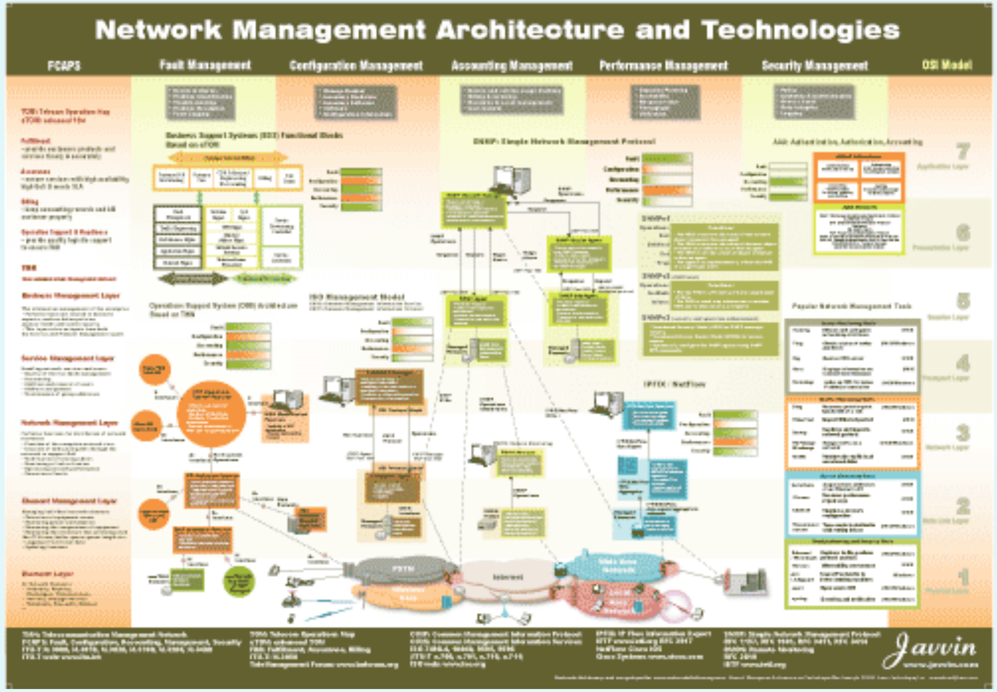
Upravljanje z NAPAKAMI (fault management)

Upravljanje s KONFIGURACIJAMI (configuration management)

UPRAVLJANJE

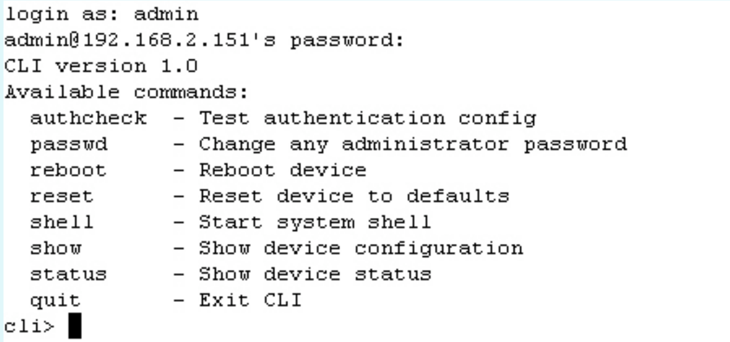
Upravljanje z BELEŽENJEM DOSTOPOV (accounting management)

Upravljanje z VARNOSTJO (security)



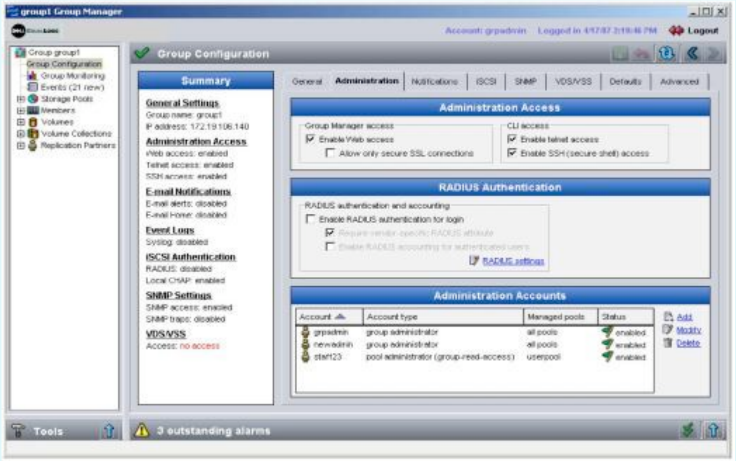
Management software

- CLI (*Command Line Interface*):
  - ✓ precise control,
  - ✓ possibility of using command lines (*batch*),
  - – problem of syntax knowledge, storage configurations difficulty, less general – specific to a particular network equipment



```
login as: admin
admin@192.168.2.151's password:
CLI version 1.0
Available commands:
  authcheck   - Test authentication config
  passwd      - Change any administrator password
  reboot      - Reboot device
  reset       - Reset device to defaults
  shell       - Start system shell
  show        - Show device configuration
  status      - Show device status
  quit        - Exit CLI
cli> █
```

- GUI (*Graphical User Interface*) applications:
  - ✓ visually beautiful, provides an overview of the whole system/network, uses its own (concise) protocol to communicate with a device – speed,
  - – we loose the ability of readable configuration storage (binary), it can mask all configuration options



Summary

General Settings
Group name: group1
IP address: 172.19.106.140

Administration Access
Web access: enabled
Telnet access: enabled
SSH access: enabled

E-mail Notifications
E-mail alerts: disabled
E-mail Home: disabled

Event Logs
Syslog: disabled

iSCSI Authentication
RADIUS: disabled
Local CHAP: enabled

SNMP Settings
SNMP access: enabled
SNMP traps: disabled

VDS/VSS
Access: no access

Administration Access

Group Manager access
☑ Enable Web access
□ Allow only secure SSL connections

CLI access
☑ Enable telnet access
☑ Enable SSH (secure shell) access

RADIUS Authentication

RADIUS authentication and accounting
□ Enable RADIUS authentication for login
☑ [illegible]
□ [illegible]
RADIUS settings

Administration Accounts

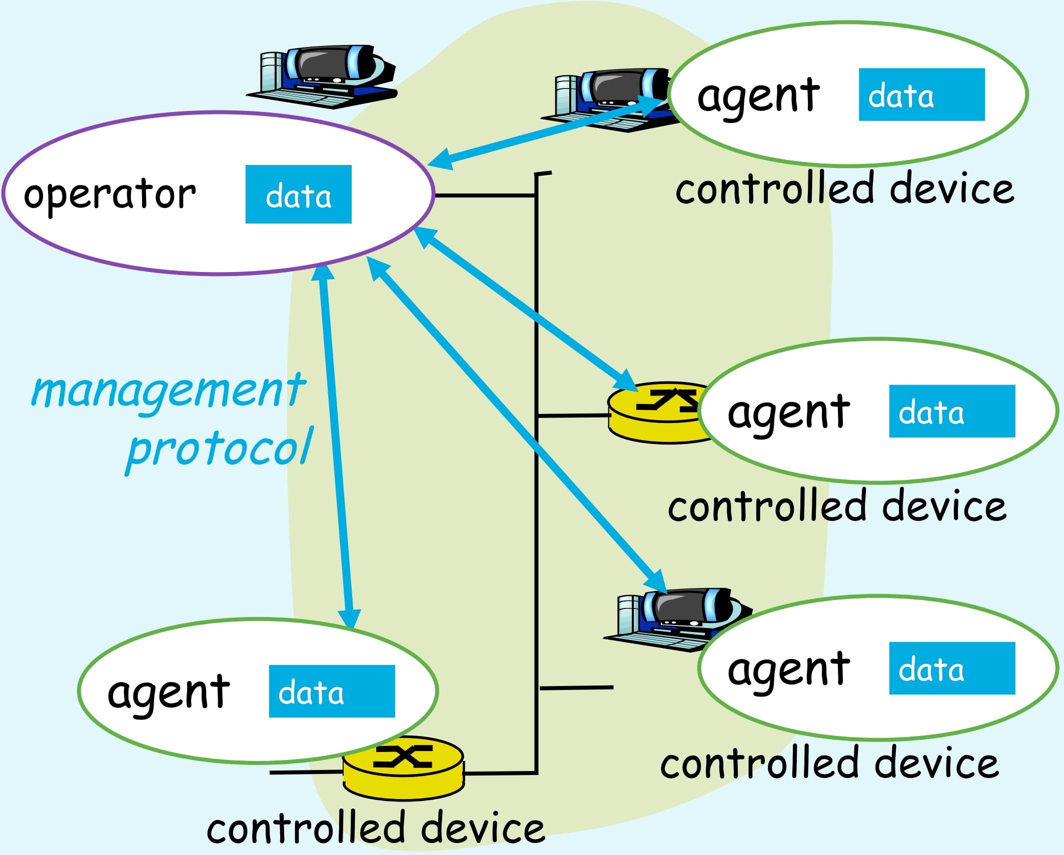
Account	Account type	Managed pools	Status
grpadmin	group administrator	all pools	enabled
newadmin	group administrator	all pools	enabled
staff123	pool administrator (group-read-access)	userpool	enabled

Add
Modify
Delete

Management infrastructure

Management system components:

- operator = entity (application + human), BOSS,
- controlled device (contains NMA agent and controlled OBJECTS containing controlled PARAMETERS),
- management protocol (eg, SNMP).



History: management protocols

OSI CMIP

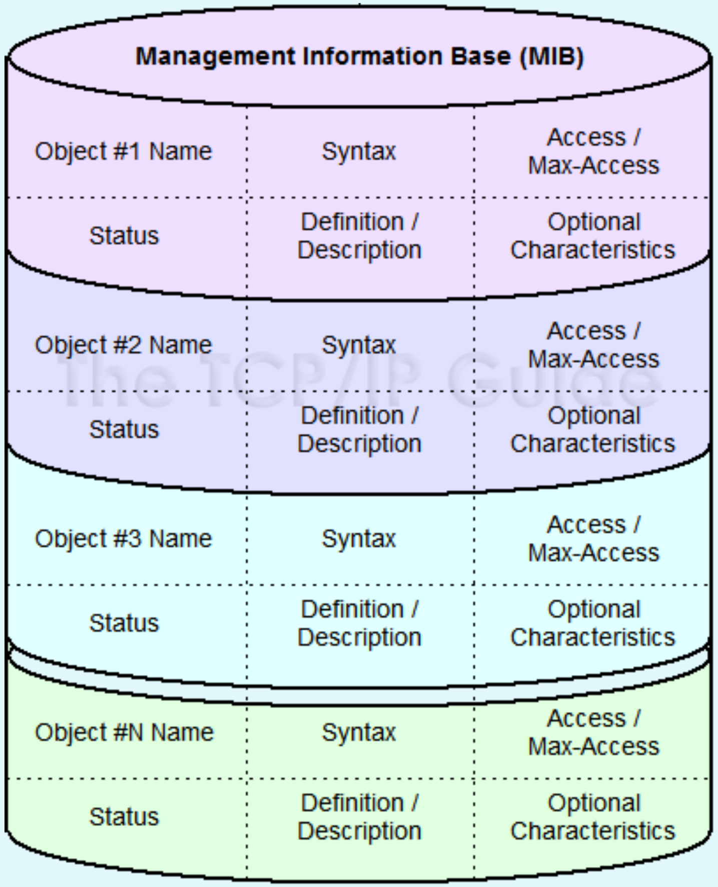
- *Common Management Information Protocol,*
- ITU-T X.700 standard created in 1980: first management standard,
- standardized too slow, never implemented in practice

SNMP

- *Simple Network Management Protocol,*
- IETF standard
- very simple first version,
- rapid deployment and expansion in practice
- currently: SNMP V3 (added safety!),
- *de facto* standard for network management.

Management data

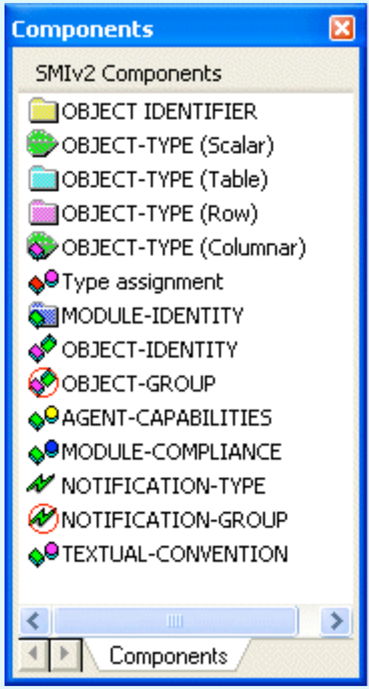
- For each type of controlled device we have our own **MIB (Management Information Base)** where information regarding managed **OBJECTS** and their **PARAMETERS** is stored.
- The operator has his own **MDB** (**Management Database**), where he stores concrete values for MIB objects/ parameters for each managed device.
- A language that defines how OBJECTS and PARAMETERS are written is needed: **SMI (Structure of Management Information**)



SMI: language for defining objects in MIB

- basic data types: INTEGER, Integer32,Unsigned32, OCTET STRING, OBJECT IDENTIFIED, IPaddress, Counter32, Counter64, Gauge32, Time Ticks, Opaque

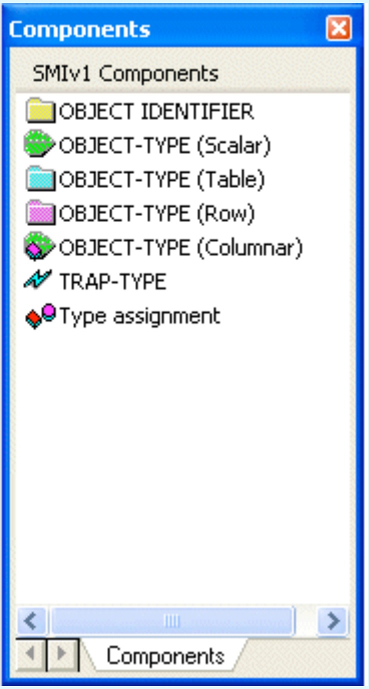
- structured data types:
  - OBJECT-TYPE
  - MODULE-TYPE



Components

SMIv2 Components

- OBJECT IDENTIFIER
- OBJECT-TYPE (Scalar)
- OBJECT-TYPE (Table)
- OBJECT-TYPE (Row)
- OBJECT-TYPE (Columnar)
- Type assignment
- MODULE-IDENTITY
- OBJECT-IDENTITY
- OBJECT-GROUP
- AGENT-CAPABILITIES
- MODULE-COMPLIANCE
- NOTIFICATION-TYPE
- NOTIFICATION-GROUP
- TEXTUAL-CONVENTION



Components

SMIv1 Components

- OBJECT IDENTIFIER
- OBJECT-TYPE (Scalar)
- OBJECT-TYPE (Table)
- OBJECT-TYPE (Row)
- OBJECT-TYPE (Columnar)
- TRAP-TYPE
- Type assignment

SMI: object definition

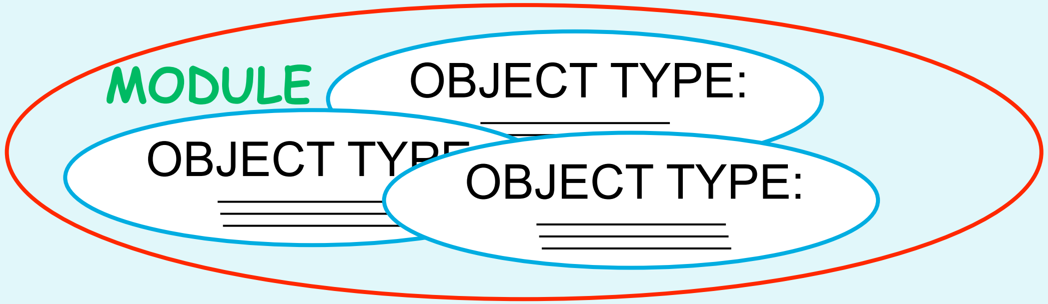
- object definition: it contains data type, status, and meaning description

```
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: grouping objects into modules

- MODULE: content-related group of objects

```
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 modules: standardization

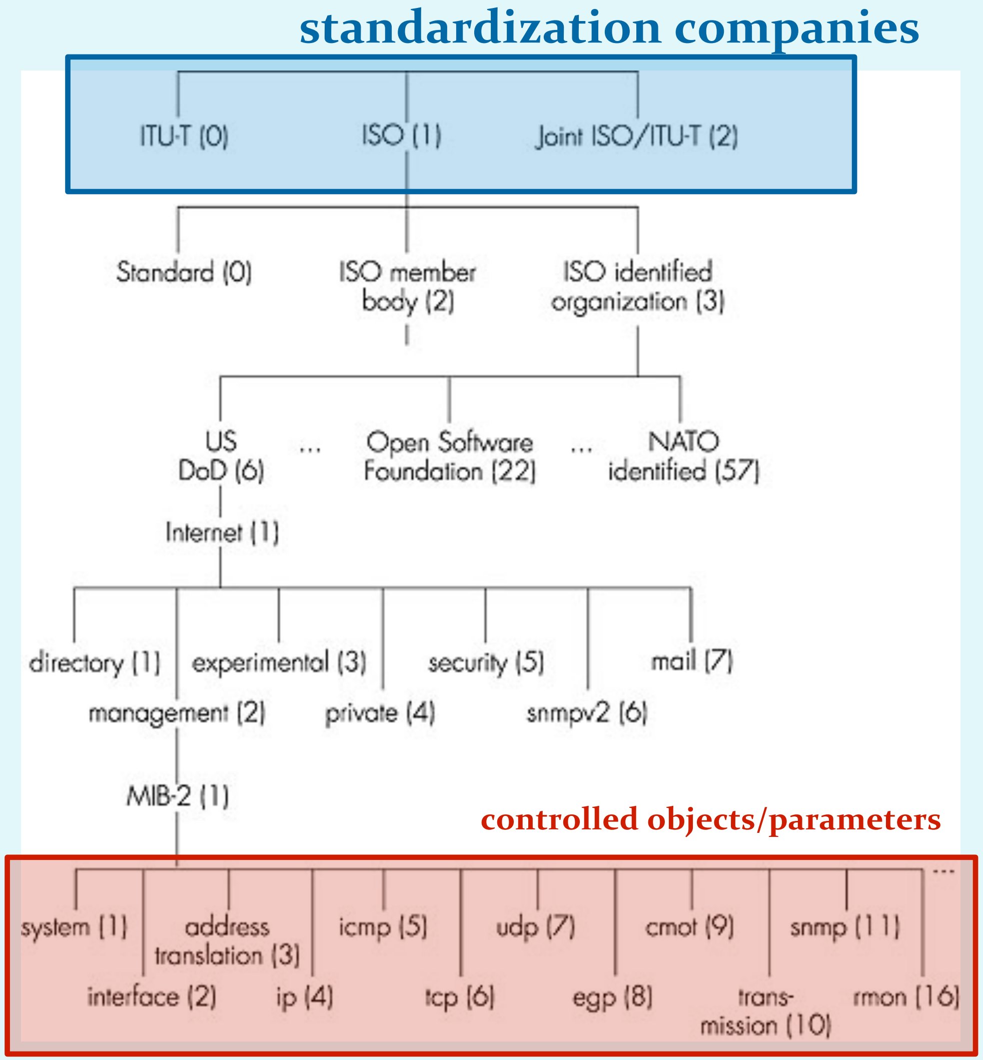
- MODULES:
  - “standardized”,
  - vendor-specific

- IETF (Internet Engineering Task Force) responsible for standardization of MIB modules for routers, interfaces and other network equipment
  - -> naming (labeling) of standard components is required!
  - ISO ASN.1 (Abstract Syntax Notation 1) designation is used

MIB modules: standardization

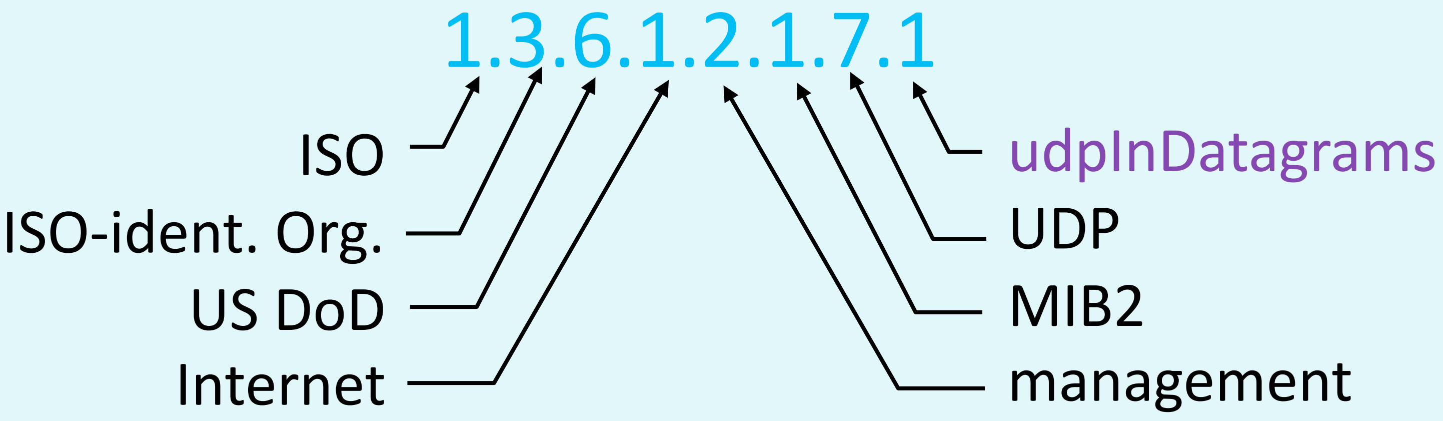
- hierarchical arrangement of objects with tree identifiers
- each object has a name consisting of a sequence of number identifiers from the tree root to a leaf
  - example: 1.3.6.1.2.1.7 means UDP protocol

➢ *challenge: what is on the second and third level of the tree identifiers?*



MIB: naming, example

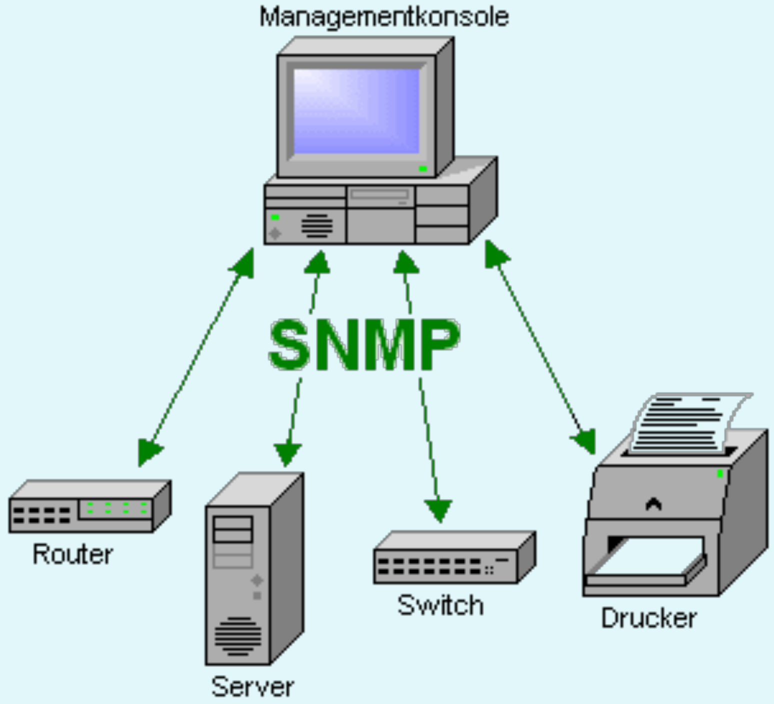
- Example:
  - 1.3.6.1.2.1.7 provides protocol UDP
  - 1.3.6.1.2.1.7.* provides the observed parameters of the UDP protocol



MIB: naming, example

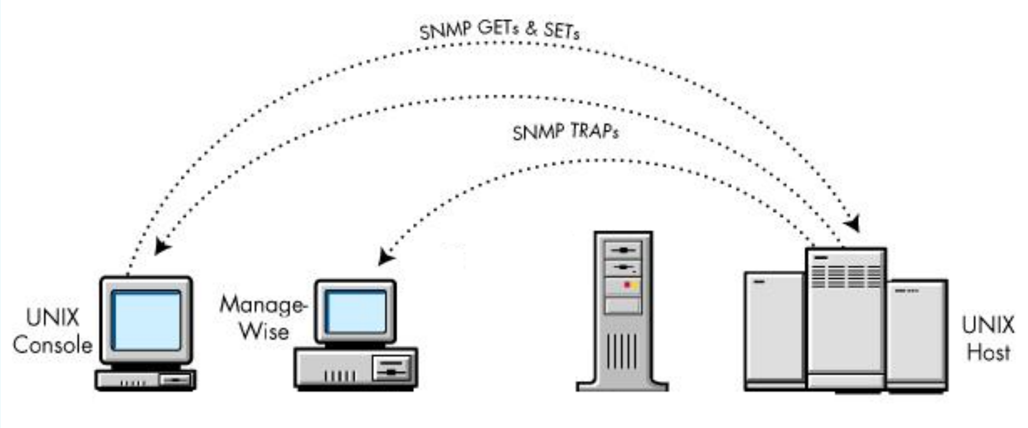
Object ID	**Name**	**Type**	**Comments**
1.3.6.1.2.1.7.1	UDPInDatagrams	Counter32	total # datagrams delivered at this node
1.3.6.1.2.1.7.2	UDPNoPorts	Counter32	# underliverable datagrams no app at portl
1.3.6.1.2.1.7.3	UDInErrors	Counter32	# undeliverable datagrams all other reasons
1.3.6.1.2.1.7.4	UDPOutDatagrams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

SNMP protocol



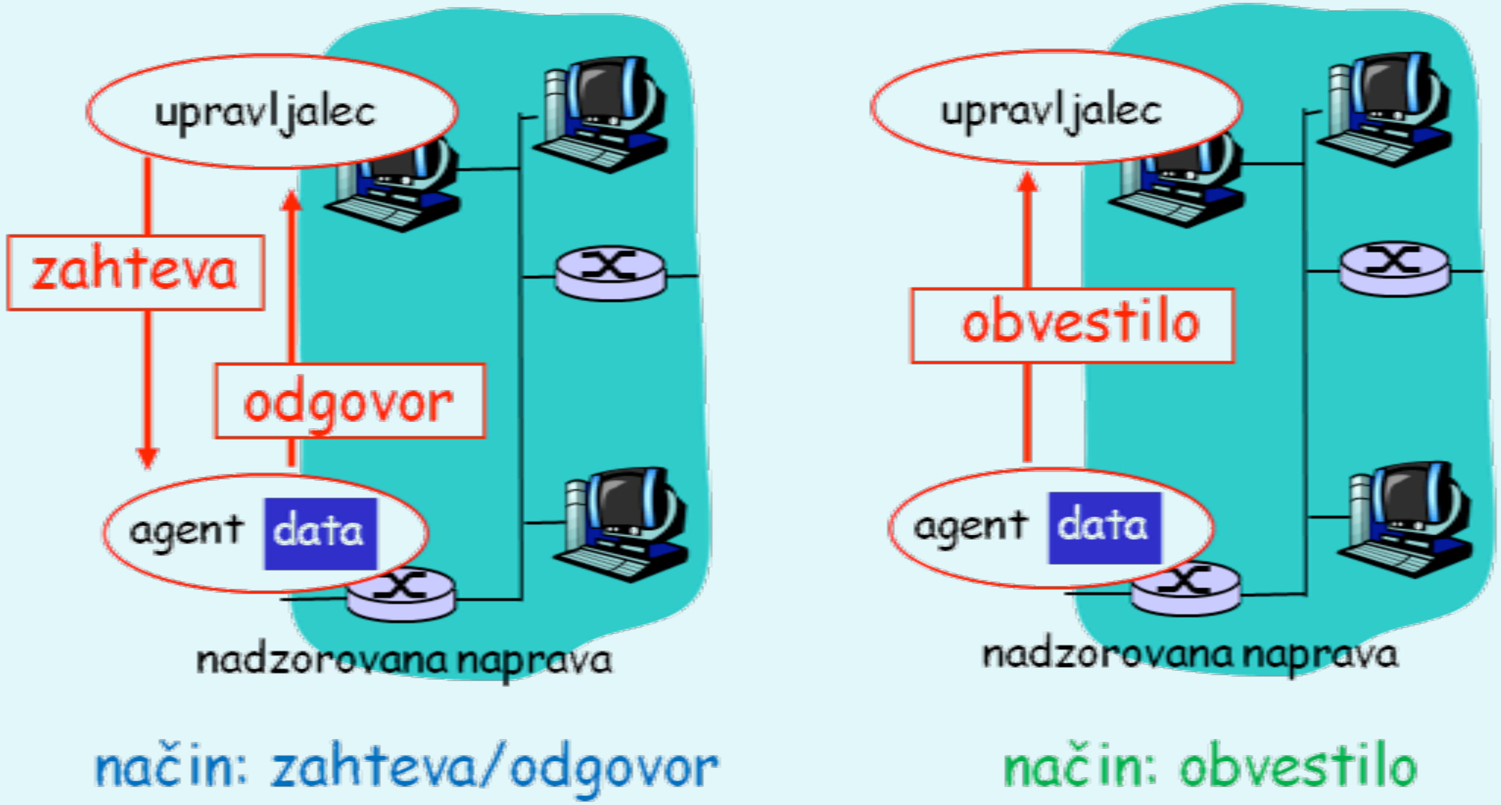
SNMP protocol

- *Simple Network Management Protokol*
- protocol for exchanging control information between the operator and monitored objects.
- information of controlled objects is being transferred between controlled equipment and the operator with accordance to the MIB definition.
- Two operating modes:
  - *request-response*: reading and setting values
  - *trap message*: the device informs the operator about the event



SNMP protocol

- two operating modes



SNMP: message types

Message	Direction	Meaning
GetRequest *GetNextRequest* *GetBulkRequest*	operator -> agent	"give me information" (value, next in list, data block-table)
InformRequest	operator -> operator	mutual transmission of values from MIB
SetRequest	operator -> agent	set the value in MIB
Response	agent -> operator	"here is the value", response to Request
Trap	agent -> operator	notification to operator about the incident

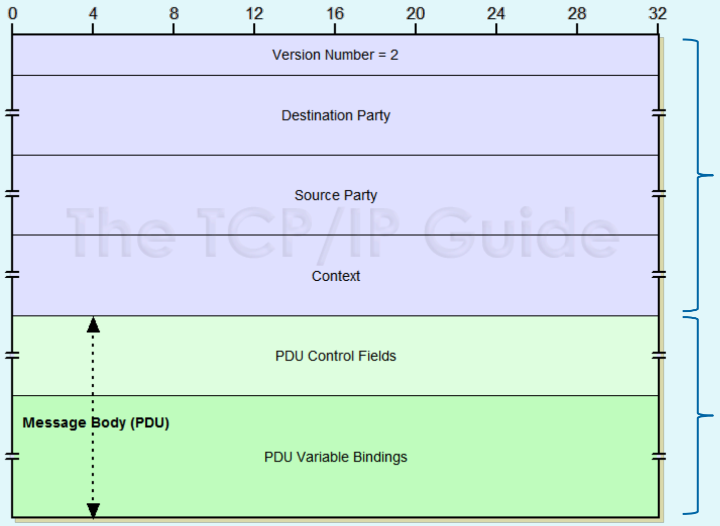
SNMP protocol

- ➢ challenge: find RFC documents about SNMP and find differences between them

- SNMP uses UDP transport protocol
  - port 161: “general" SNMP port, where devices listen for SNMP requests
  - port 162: notifications port (traps), usually where systems listen for control and management of a network

- SNMP implementation must address the following problems:
  - **package size**: SNMP packets can contain extensive information about objects in MIB, UDP on the other hand has an upper limit for the size of the segment (TCP doesn't),
  - **resending**: since UDP is used, delivery and confirmation is not guaranteed. Delivery control should therefore be addressed at a higher OSI level.
  - **problem with lost notifications**: if a notification is lost during transfer, the sender doesn't know anything about it; the recipient also doesn't receive it
    - ➢ challenge: how does SNMPv3 address these problems?

SNMP: message form

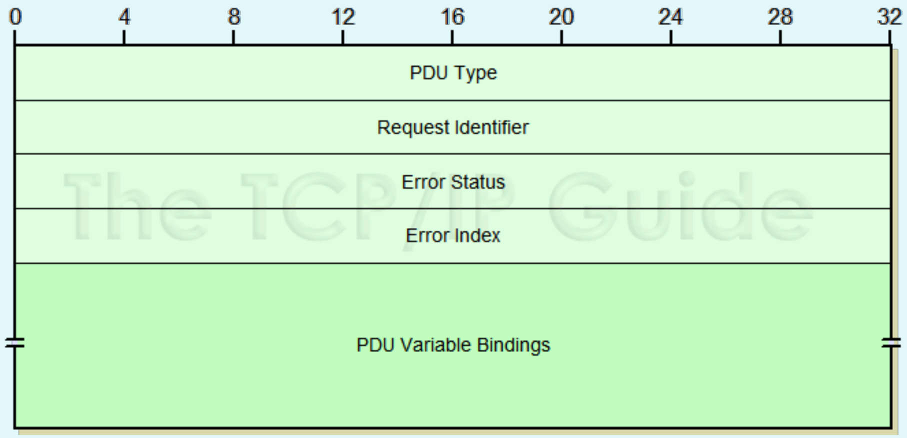


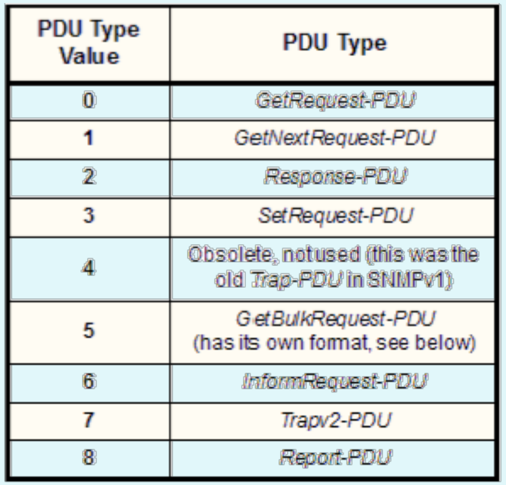
head

PDU(protocol data unit)

Verzija	SNMP protocol version
Destination Party	Recipient identifier
Source Party	Sender identifier
Context	Defines a set of MIB objects that entity can obtain
PDU	Main content of the message, data from the MIB

SNMP: request-response message type

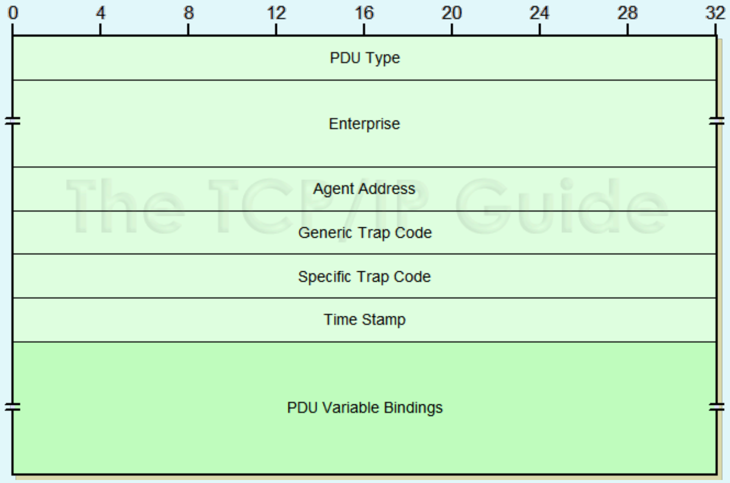




PDU Type Value	PDU Type
0	*GetRequest-PDU*
1	*GetNextRequest-PDU*
2	*Response-PDU*
3	*SetRequest-PDU*
4	Obsolete, not used (this was the old *Trap-PDU* in SNMPv1)
5	*GetBulkRequest-PDU* (has its own format, see below)
6	*InformRequest-PDU*
7	*Trapv2-PDU*
8	*Report-PDU*

Request ID	Integer	Number that relates a request with response. A device that answers, when it stores into a package of Response type. It is also used for artificial control of received packets (SNMP uses UDP transport protocol which doesn't provide this!)
Error Status	Integer	Error code which agent forwards with a Response type package. Value 0 means that there was no error and any other value defines a specific error. ➢ challenge: look at different types of errors
Error Index	Integer	If there was an error, this value is the index of an object that caused the error.
Variable Bindings	Variable	Name-value pairs, that define objects and their values.

SNMP: notification type message



PDU Type	Integer	Value that defines the type of message. Value 4/7 means notification (trap message).
Enterprise	Sequence of Integer	Group identifier.
Agent Address	Network Address	IP address of the agent that generated a notification.
Generic Trap Code	Integer	General error code – from predefined coding.
Specific Trap Code	Integer	Specific error code (depends on the manufacturer equipment)
Time Stamp	TimeTicks	Time since the last time the device initialized. Used for recording.
Variable Bindings	Variable	Name-value pairs that define objects and their values.

Verzije SNMP

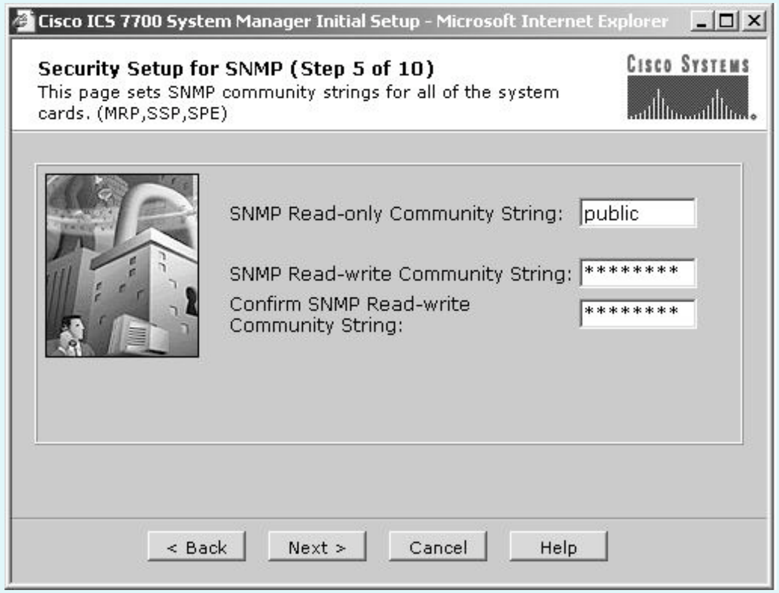
- **SNMPv1**
  - defined in the late 80s
  - turned out to be too weak to implement all the necessary requirements (limited in composition of PDU)

- **SNMPv2**
  - improved SNMPv1 in speed (added GetBulkRequest),safety (but too complex implementation), communication between operators,
  - RFC 1901, RFC 2578
  - uses SMIv2 (improved standard for structuring information)

- **SNMPv3**
  - improved SNMPv2 – added safety mechanisms,
  - enables cryptography, assures safety, integrity, authentication
  - also uses SMIv2

Safety

- Why is it important?
  - SetRequest adjusts controlled devices. Request can be sent at any time?
    - challenge: find 3 more examples of other possible SNMP abuses.
- Safety elements are only introduced in SNMPv3, previous version did not have it. SNMPv3 has built-in security based on user names
  - challenge: read RFC 3414 and find information about which kind of intrusions does SNMPv3 enable protection against. How about Denial of Service attacks and eavesdropping on traffic?



Cisco ICS 7700 System Manager Initial Setup - Microsoft Internet Explorer

Security Setup for SNMP (Step 5 of 10)

This page sets SNMP community strings for all of the system cards. (MRP,SSP,SPE)

SNMP Read-only Community String: public

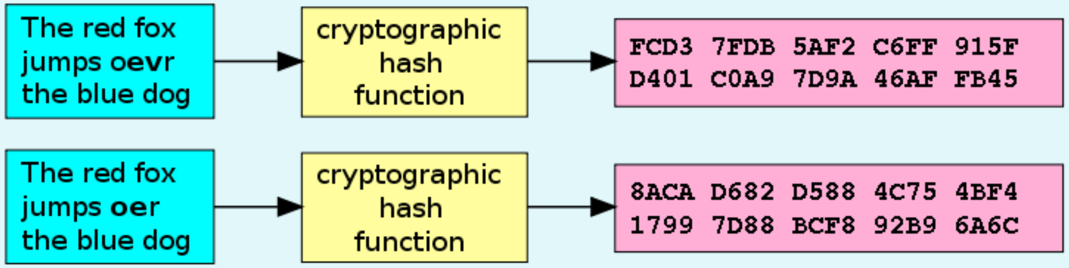
SNMP Read-write Community String: ********

Confirm SNMP Read-write Community String: ********

SNMP. Safety mechanisms

1. **packets content encryption (PDU):** DES is used (exchange of keys is required prior to use)

2. **integrity**: used for message densification with a key which is known to both sender and recipient. With examination of sent densified value we have control over active message counterfeiting

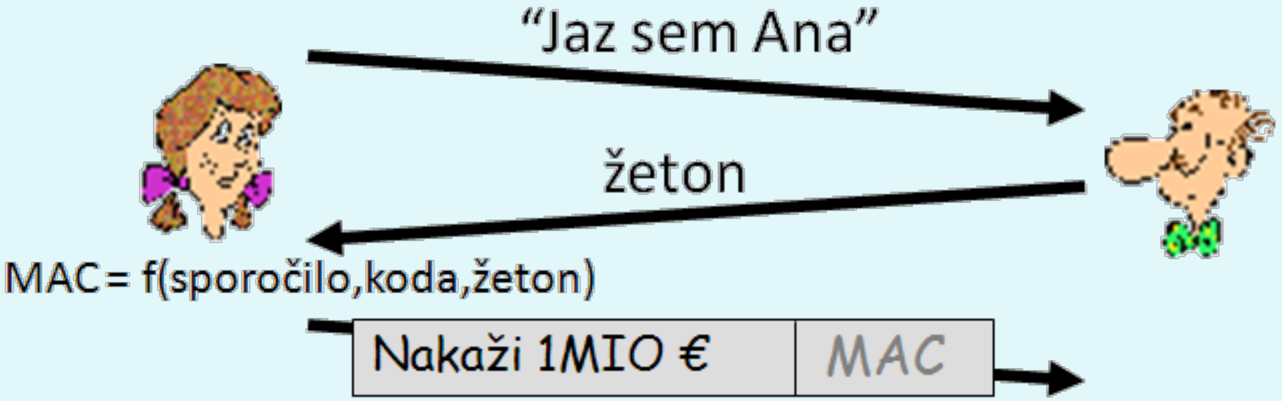


The red fox jumps oevr the blue dog → cryptographic hash function → FCD3 7FDB 5AF2 C6FF 915F D401 C0A9 7D9A 46AF FB45

The red fox jumps oer the blue dog → cryptographic hash function → 8ACA D682 D588 4C75 4BF4 1799 7D88 BCF8 92B9 6A6C

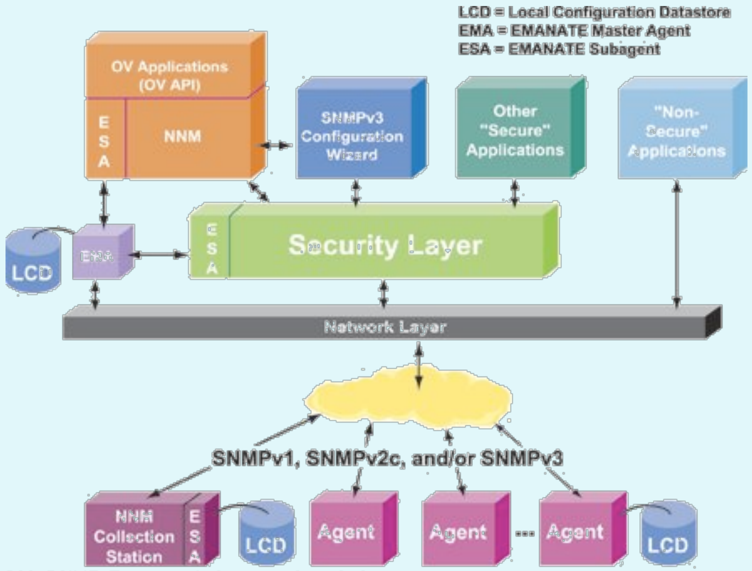
SNMP: Safety mechanisms

3. **protection against repetition of already completed communication (replay attack):** use of one-time chips (*nonce, žeton*): the sender must encode the message according to the nonce which is defined by the receiver (this is usually the number of system start-ups and the time passed since the last start-up)



SNMP: Safety mechanisms

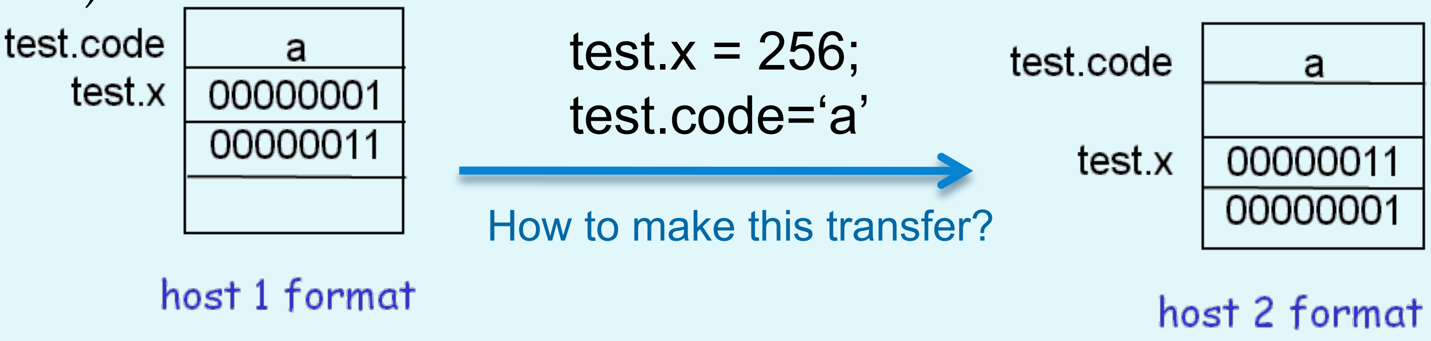
4. **access control:** access control based on user names. The user rights specify which users can read/change which information. User data is stored in *Local Configuration DataStore* database which also contains controlled objects s SNMP!
   - challenge: examine RFC 3415. What is a View-based Access Control Model Configuration MIB?


LCD = Local Configuration Datastore
EMA = EMANATE Master Agent
ESA = EMANATE Subagent
OV Applications (OV API)
ESA
NNM
SNMPv3 Configuration Wizard
Other "Secure" Applications
"Non-Secure" Applications
LCD
EMA
ESA
Security Layer
Network Layer
SNMPv1, SNMPv2c, and/or SNMPv3
NNM Collection Station
ESA
LCD
Agent
Agent
...
Agent
LCD

(C) SNMP Research International, Inc.

Encoding PDU content

- How to encode packet content so that it is understood on all platforms (different data types are of different lengths, thick/thin end)?



test.code a

test.x 00000001

00000011

host 1 format

test.x = 256;

test.code='a'

How to make this transfer?

test.code a

test.x 00000011

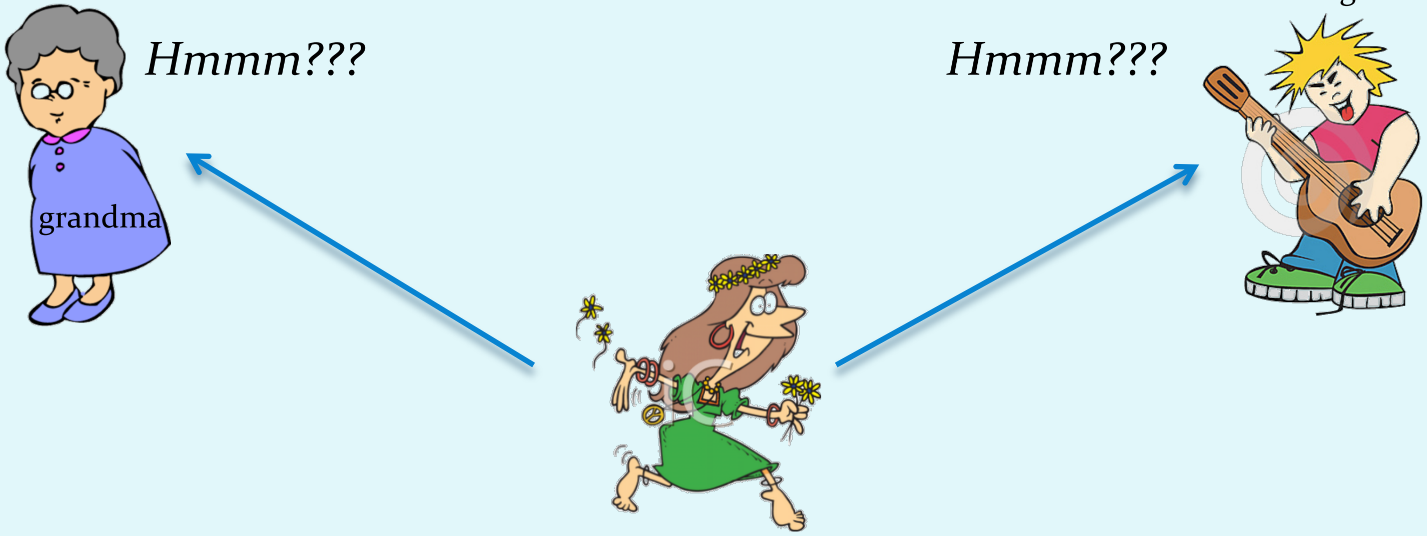
00000001

host 2 format

- we need a uniform coding or some **demonstration level of this data**
  - ASN.1 standard in addition to data types also defines encoding standards.
  - we will see that TLV notation is used for presentation of these operators.

Encoding PDU content

- Similar problem:



teenager

Hmmm???

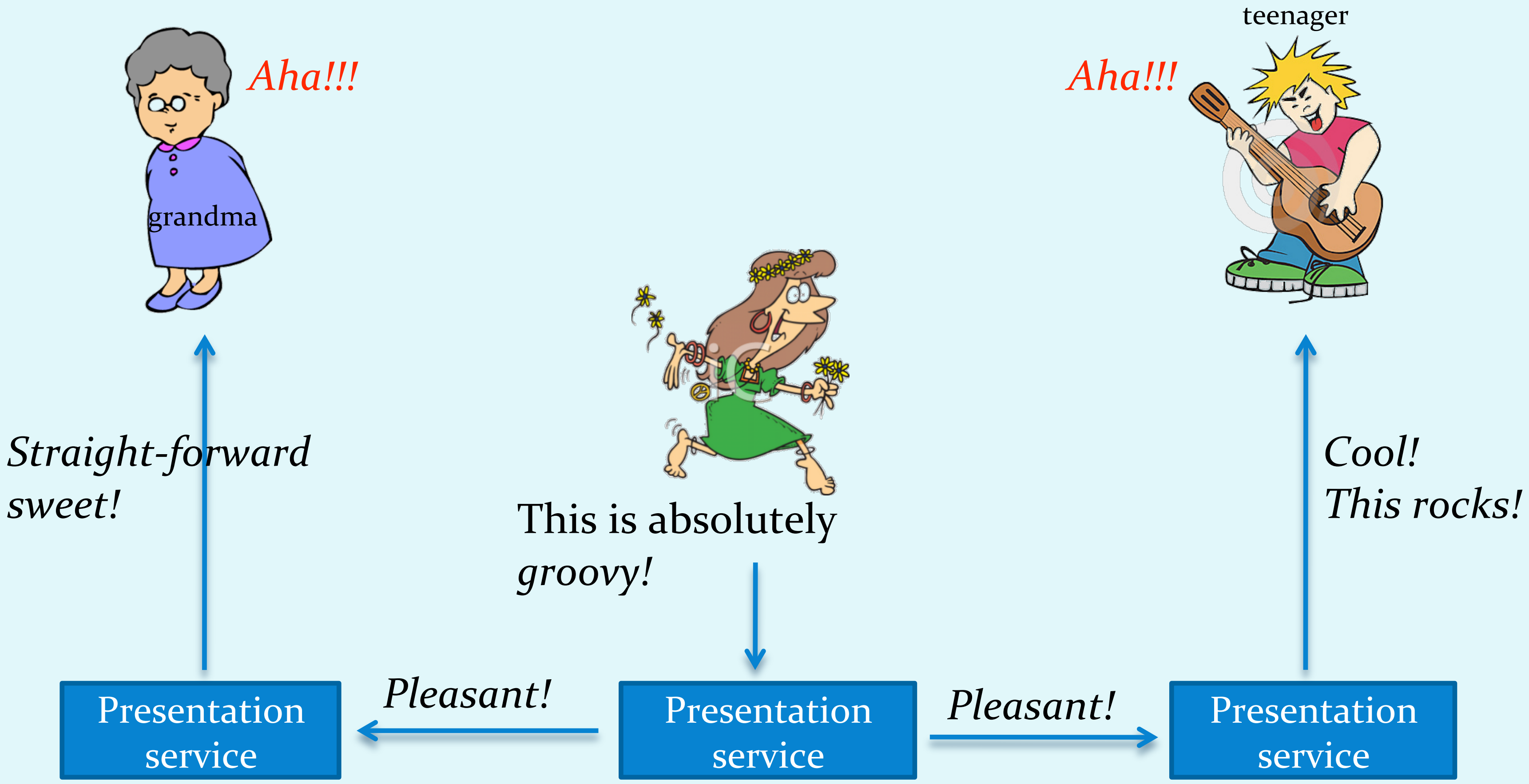
grandma

Hmmm???

This is absolutely *groovy*!

Encoding PDU content

- Similar problem:



teenager

grandma

Aha!!!

Aha!!!

Straight-forward
sweet!

This is absolutely
groovy!

Cool!
This rocks!

Presentation service

Pleasant!

Presentation service

Pleasant!

Presentation service

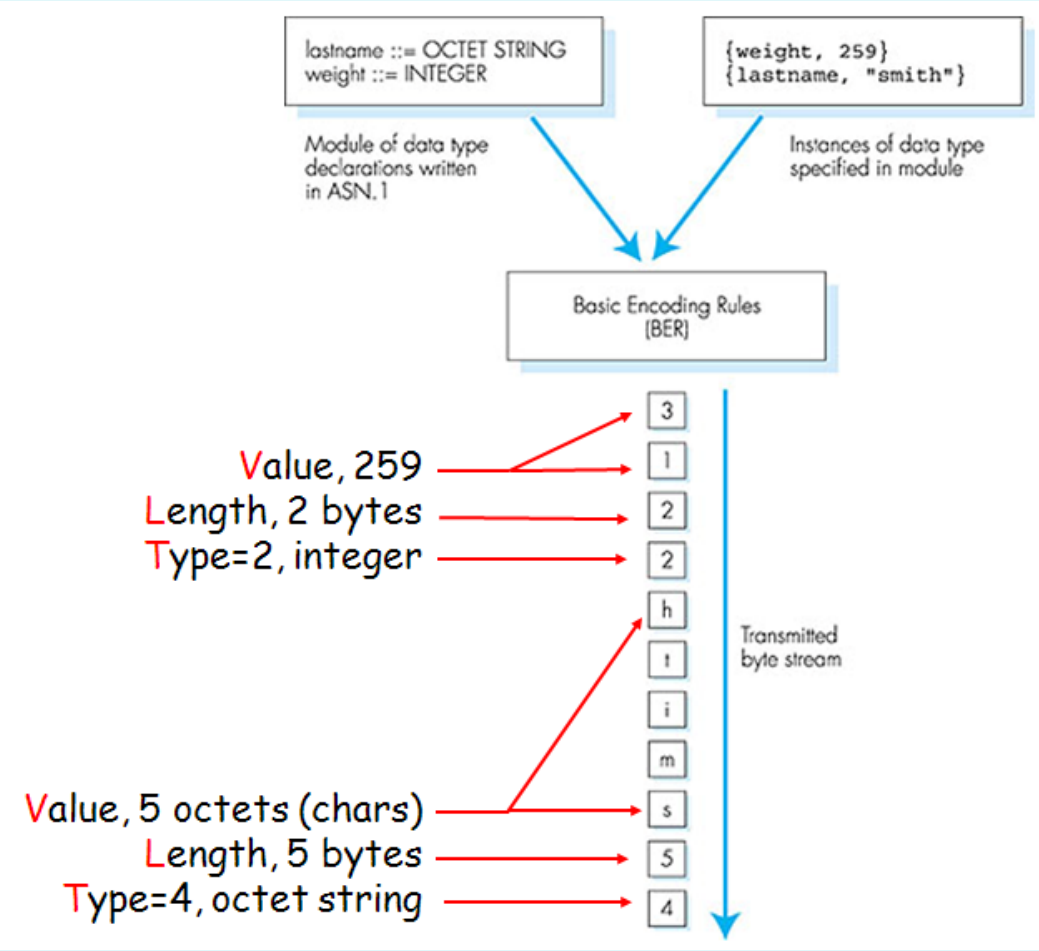
Presentation service: possible solutions

1. Sender accounts the data form used by the recipient: he converts data into the correct form for recipient and only then sends it.
2. sender sends data in his own form, precipient converts into his own form
3. Sender converts into independent form and then sends. Recipient transforms independent form into his own.
   - challenge: what are advantages and disadvantages of these three approaches?

- ASN.1 uses the (3). third solution(independent form).
- BER rules are used when writing types (Binary Encoding Rules). They define the recording of data according to TLV principle (Type, Length, Value).

Example of BER encoding according to TLV principle

Basic ASN.1 data type	Type No.	Use
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



lastname ::= OCTET STRING
weight ::= INTEGER

{weight, 259}
{lastname, "smith"}

Module of data type declarations written in ASN.1

Instances of data type specified in module

Basic Encoding Rules (BER)

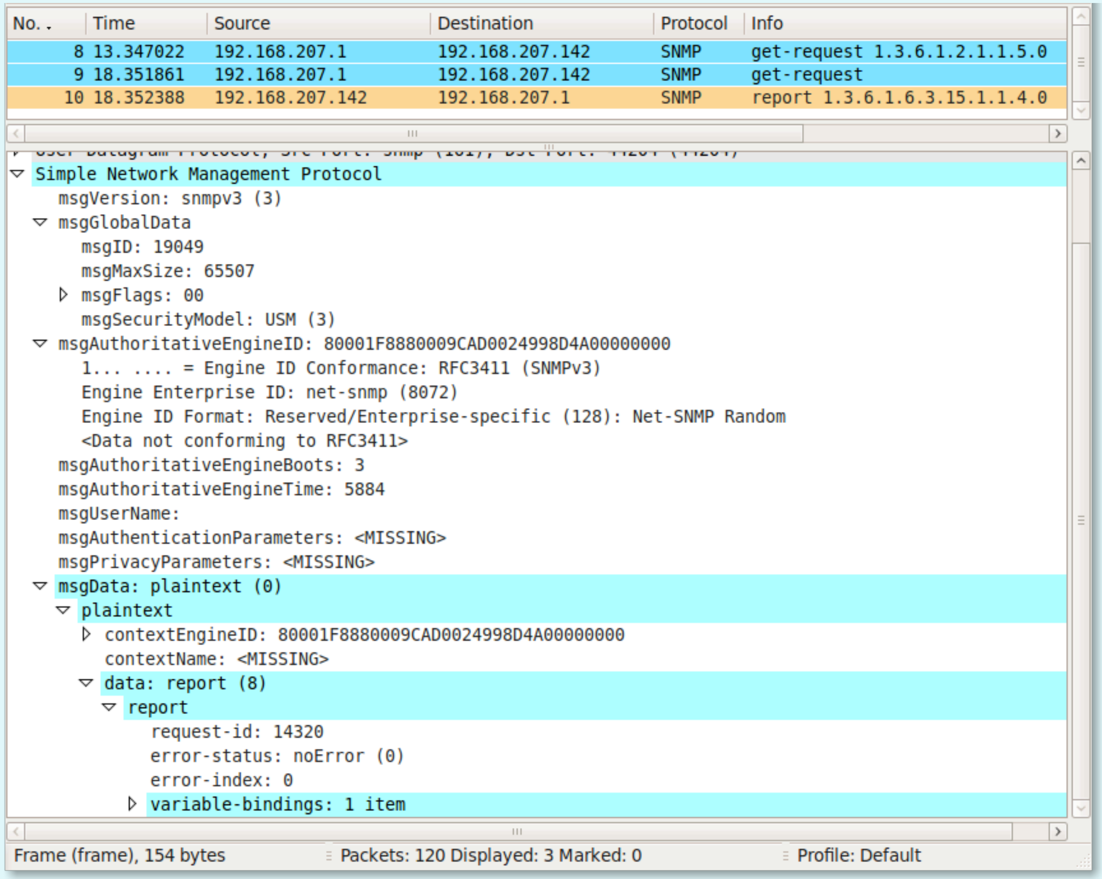
3
1
2
2
h
t
i
m
s
5
4

Transmitted byte stream

Value, 259
Length, 2 bytes
Type=2, integer

Value, 5 octets (chars)
Length, 5 bytes
Type=4, octet string

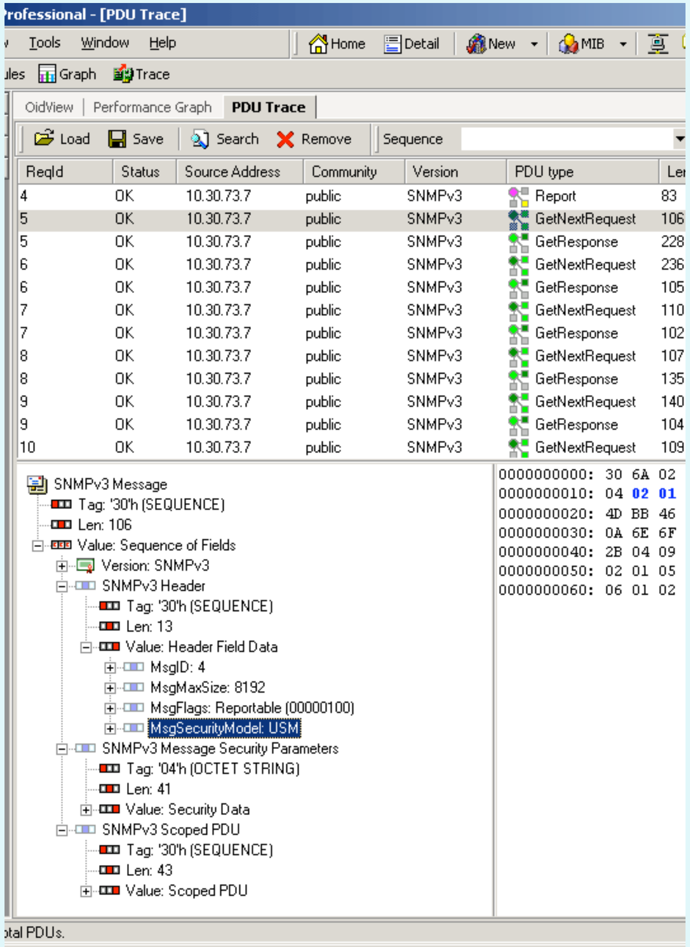
SNMP package capture



```
No. .  Time       Source          Destination      Protocol  Info
    8 13.347022   192.168.207.1   192.168.207.142  SNMP      get-request 1.3.6.1.2.1.1.5.0
    9 18.351861   192.168.207.1   192.168.207.142  SNMP      get-request
   10 18.352388   192.168.207.142 192.168.207.1    SNMP      report 1.3.6.1.6.3.15.1.1.4.0
```

```
▽ Simple Network Management Protocol
    msgVersion: snmpv3 (3)
  ▽ msgGlobalData
      msgID: 19049
      msgMaxSize: 65507
    ▷ msgFlags: 00
      msgSecurityModel: USM (3)
  ▽ msgAuthoritativeEngineID: 80001F8880009CAD0024998D4A00000000
      1... .... = Engine ID Conformance: RFC3411 (SNMPv3)
      Engine Enterprise ID: net-snmp (8072)
      Engine ID Format: Reserved/Enterprise-specific (128): Net-SNMP Random
      <Data not conforming to RFC3411>
    msgAuthoritativeEngineBoots: 3
    msgAuthoritativeEngineTime: 5884
    msgUserName:
    msgAuthenticationParameters: <MISSING>
    msgPrivacyParameters: <MISSING>
  ▽ msgData: plaintext (0)
    ▽ plaintext
      ▷ contextEngineID: 80001F8880009CAD0024998D4A00000000
        contextName: <MISSING>
      ▽ data: report (8)
        ▽ report
            request-id: 14320
            error-status: noError (0)
            error-index: 0
          ▷ variable-bindings: 1 item
```

Frame (frame), 154 bytes   Packets: 120 Displayed: 3 Marked: 0   Profile: Default



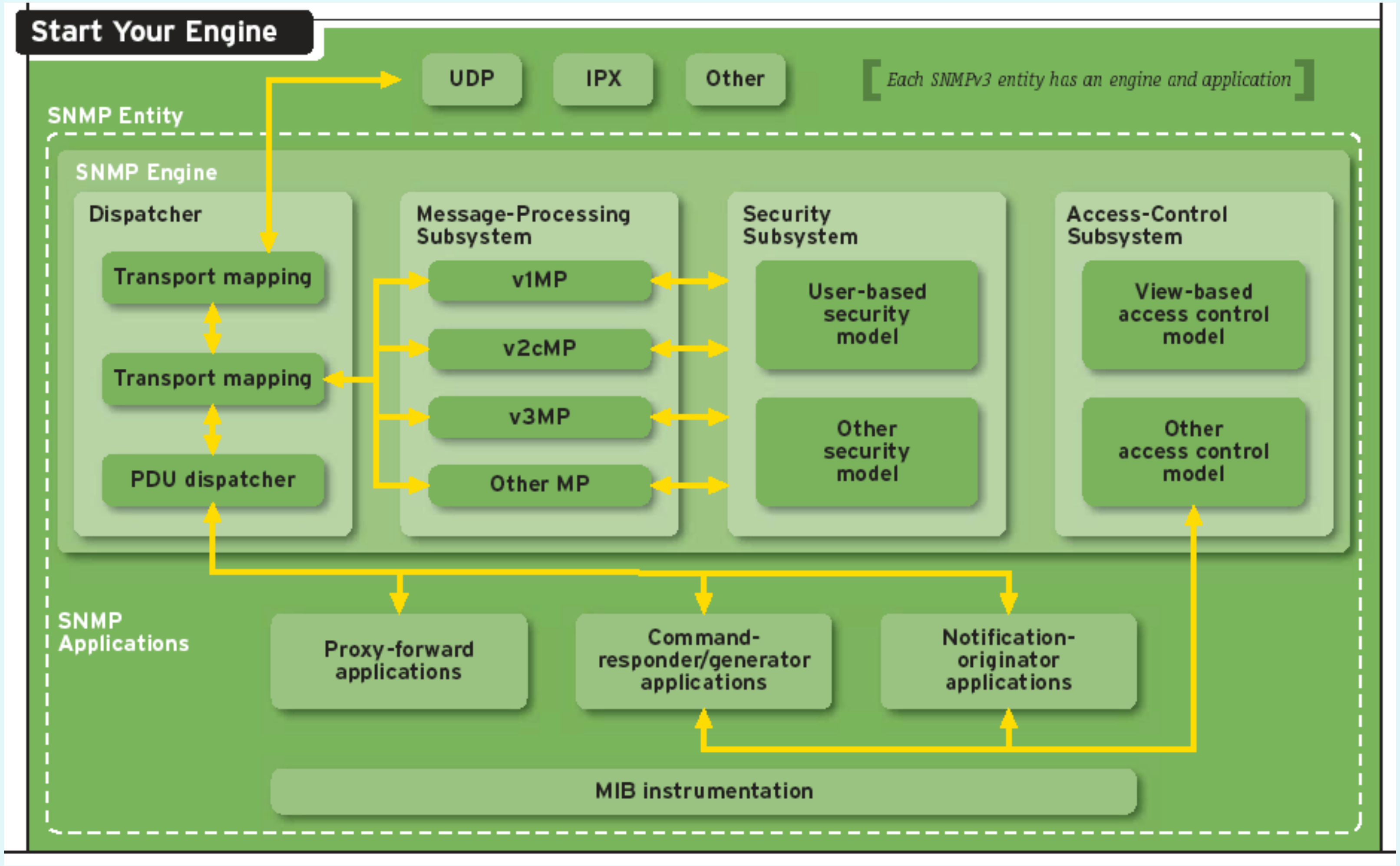
ReqId	Status	Source Address	Community	Version	PDU type	Le
4	OK	10.30.73.7	public	SNMPv3	Report	83
5	OK	10.30.73.7	public	SNMPv3	GetNextRequest	106
5	OK	10.30.73.7	public	SNMPv3	GetResponse	228
6	OK	10.30.73.7	public	SNMPv3	GetNextRequest	236
6	OK	10.30.73.7	public	SNMPv3	GetResponse	105
7	OK	10.30.73.7	public	SNMPv3	GetNextRequest	110
7	OK	10.30.73.7	public	SNMPv3	GetResponse	102
8	OK	10.30.73.7	public	SNMPv3	GetNextRequest	107
8	OK	10.30.73.7	public	SNMPv3	GetResponse	135
9	OK	10.30.73.7	public	SNMPv3	GetNextRequest	140
9	OK	10.30.73.7	public	SNMPv3	GetResponse	104
10	OK	10.30.73.7	public	SNMPv3	GetNextRequest	109

```
SNMPv3 Message
├ Tag: '30'h (SEQUENCE)
├ Len: 106
⊟ Value: Sequence of Fields
  ⊞ Version: SNMPv3
  ⊟ SNMPv3 Header
    ├ Tag: '30'h (SEQUENCE)
    ├ Len: 13
    ⊟ Value: Header Field Data
      ⊞ MsgID: 4
      ⊞ MsgMaxSize: 8192
      ⊞ MsgFlags: Reportable (00000100)
      ⊞ MsgSecurityModel: USM
  ⊟ SNMPv3 Message Security Parameters
    ├ Tag: '04'h (OCTET STRING)
    ├ Len: 41
    ⊞ Value: Security Data
  ⊟ SNMPv3 Scoped PDU
    ├ Tag: '30'h (SEQUENCE)
    ├ Len: 43
    ⊞ Value: Scoped PDU
```

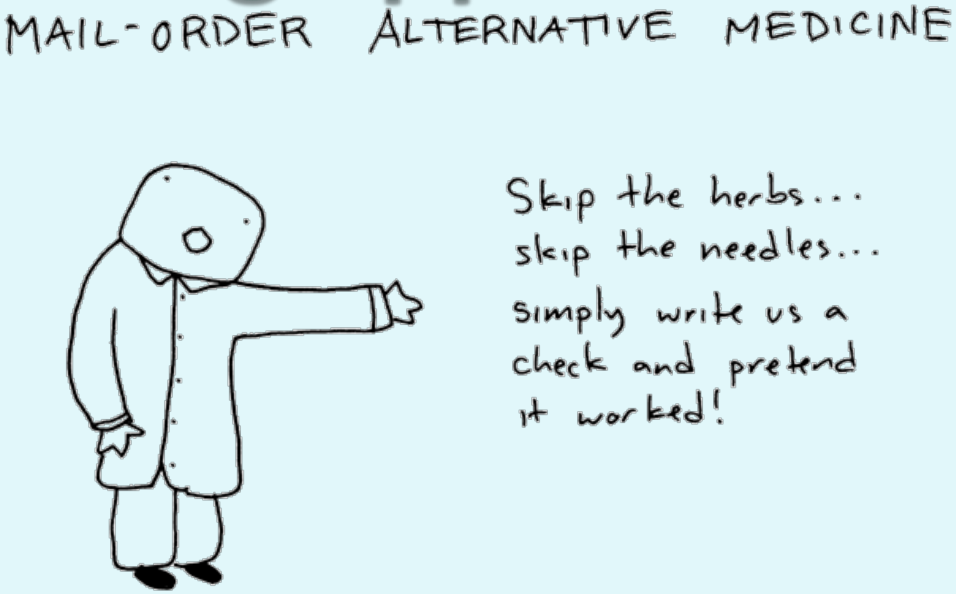
```
0000000000: 30 6A 02
0000000010: 04 02 01
0000000020: 4D BB 46
0000000030: 0A 6E 6F
0000000040: 2B 04 09
0000000050: 02 01 05
0000000060: 06 01 02
```

otal PDUs.

SNMP program structure


Start Your Engine
UDP
IPX
Other
Each SNMPv3 entity has an engine and application
SNMP Entity
SNMP Engine
Dispatcher
Transport mapping
Transport mapping
PDU dispatcher
Message-Processing Subsystem
v1MP
v2cMP
v3MP
Other MP
Security Subsystem
User-based security model
Other security model
Access-Control Subsystem
View-based access control model
Other access control model
SNMP Applications
Proxy-forward applications
Command-responder/generator applications
Notification-originator applications
MIB instrumentation

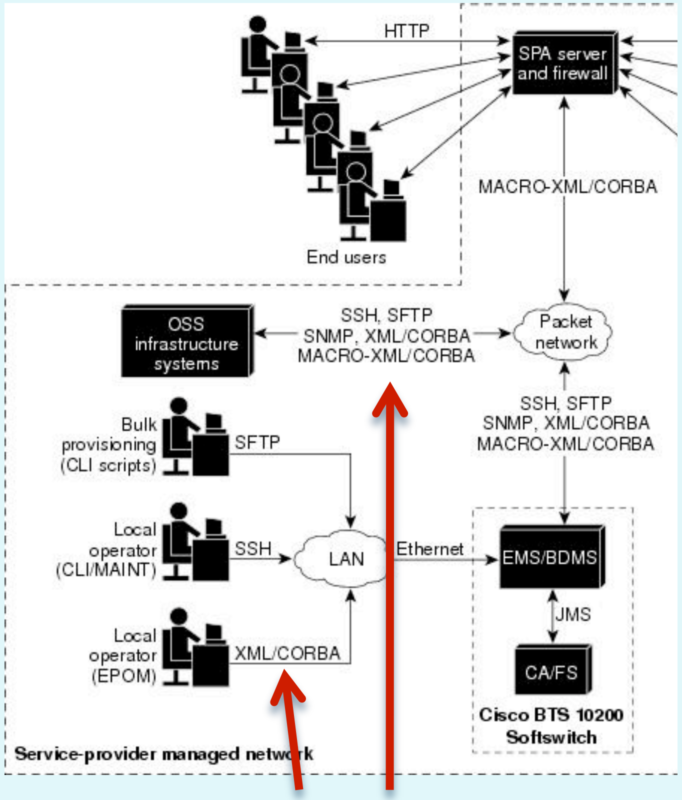
Other monitoring approaches


MAIL-ORDER ALTERNATIVE MEDICINE
Skip the herbs... skip the needles... simply write us a check and pretend it worked!

Alternative boutique solutions

1. XML & SOAP (application level): XML enables graphic and hierarchical way of encoding data which represent elements and content of controlled objects in the network. SOAP is a simple protocol that enables exchange of XML documents in the network.
   - ✓ easy reading and understanding of content on the receiver side.
   - – large overhead compared to binary data encoding

2. CORBA (Common Object Request Broker Architecture) (application level): architecture that defines inter-utility of objects of different programming languages and on different architectures.

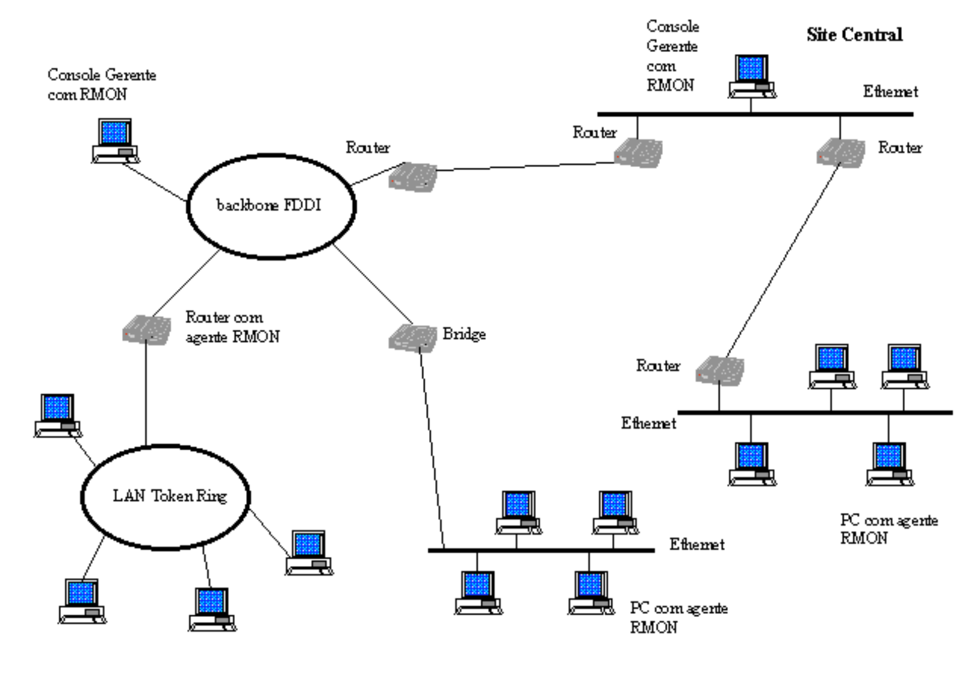


protocol combination!

Event-driven monitoring

RMON (Remote Monitoring) (additional mechanism): Classical SNMP can control the network from a control station. RMON collects and analyses measures locally and sends the results to a remote control station. It has it's own MIB with extensions for different media types.

- ✓ every RMON agent is responsible for local control,
- ✓ sending already completed analysis reduces SNMP traffic between sub-networks
- ✓ It isn't necessary that agents are always visible from the central control system side.
- – longer establishment and installation time of system is required.



fonte: Data Communications Magazine - Maio 1992.

Homework

Assignment for additional points with homework's:

Read RFC 789 which describes a known ARPAnet network failure which happened in 1980.

How could the network failure be avoided or it's recovery time improved if the network administrators would have today's tool for network management and control at their disposal?

Next time we are moving on!

- traffic for applications in real time!