LECTURE 13

Network management. SNMP.

Assoc. Prof. Rosen Radkov PhD

Network management goals

- IT infrastructure consists of components of different types: servers, workstations, switches, routers, wireless devices, communication lines, software, protocols, etc.

- They are configured in different ways

- In order to ensure the system's operability for a long period of time, it is necessary to monitor whether the current state of the devices corresponds to the expected values

Network management goals

- The information obtained gives an opportunity:

- Monitor real-time events and respond appropriately to prevent unplanned downtime and assess error rates

- Develop capacity management plans based on trends (daily, weekly, monthly)

- To improve traceability of network events - events and anomalies

Network management goals

- To prevent security breaches
- To monitor traffic
- Monitor SLA compliance
- To monitor the status of the hosts
- To monitor the performance of the systems
- ....

Network management model by ISO

- **Configuration management** – review and manage the configuration of devices in the managed network, in order to maintain the necessary versions of hardware and software;
- **Fault Management** – immediate detection, logging and response to network failures and anomalies;
- **Performance management** – quantitative measurement, evaluation, reporting and analysis of network components;

Network management model by ISO

- **Security management** – managing access to network resources according to imposed policies;

- **Accounting management** – allows IT managers to set, report and manage user and device access to the network, as well as define quotas for their usage.

NETWORK ADMINISTRATION

What is network management?

„Network management includes the deployment, integration and coordination of the hardware, software and human elements to monitor, test, poll, configure, analyze, evaluate and control the network and element resources to meet the real-time, operational performance, and Quality of Service requirements at a reasonable cost.“

T. Saydam and T. Magedanz 1996г

Assoc. Prof. Rosen Radkov PhD

Network Management System (NMS)

- A set of tools
- Simple interface
- A powerful set of commands
- A minimum set of additional equipment
- The IT infrastructure is presented in a unified way

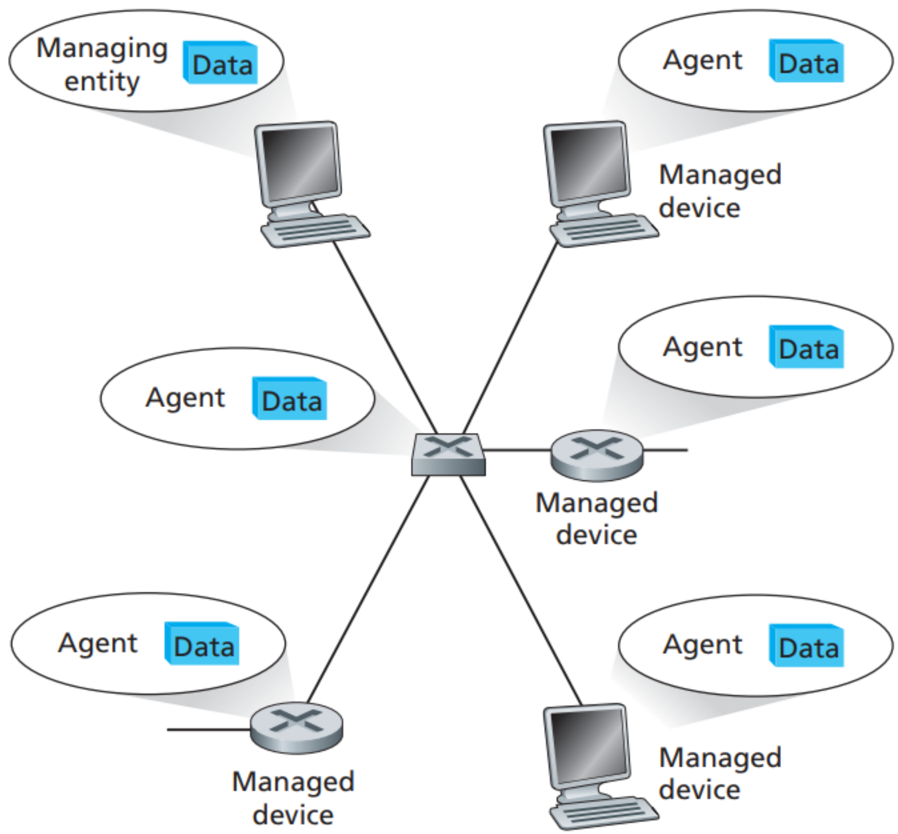
NETWORK ADMINISTRATION

Basic components of NMS

- ➢ Management station(MS)

- ➢ Managed devices
  - Managed objects
  - Agents
  - Management Information Base (MIB)

- ➢ Network protocol



Assoc. Prof. Rosen Radkov PhD

Management station

- A standalone system or part of a system
- Easy-to-use interface (in many cases with automated operations)
- Creates and maintains a database of managed devices (*asset management*)
- Implements policy requirements for component monitoring and management
- Enables keyword search

Agents

- Software that is part of the device OS (computer, router, switch, printer, etc.)
- Provides the MS with the requested information
- Executes requests to change parameters
- Provides MS with urgent, unrequested information

Management Information Base (MIB)

- Management Information Base, MIB, can be thought of as a virtual information store, holding managed objects whose values collectively reflect the current “state” of the network. Represents each network component as a set of objects with a unique identifier ObjectID (Abstract Syntax Notation One – ASN.1 ISO X.680 2002). The MIB can be represented as an index to access some parts of the configuration. This index is a tree composed of the child object's position among other objects from the same parent node. MIB objects are described according to a data definition language known as Structure of Management Information (SMI) - RFC 2578; RFC 2579; RFC 2580. It describes the data type, the object model and how the rules are constructed, ie. the format of the data being exchanged

Structure of management Information (SMI)

- Data type (RFC 2578)

Data Type	Description
INTEGER	32-bit integer, as defined in ASN.1, with a value between -2^{31} and $2^{31}-1$ inclusive, or a value from a list of possible named constant values.
Integer32	32-bit integer with a value between -2^{31} and $2^{31}-1$ inclusive.
Unsigned32	Unsigned 32-bit integer in the range 0 to $2^{32}-1$ inclusive.
OCTET STRING	ASN.1-format byte string representing arbitrary binary or textual data, up to 65,535 bytes long.
OBJECT IDENTIFIER	ASN.1-format administratively assigned (structured name); see Section 9.3.2.
IPaddress	32-bit Internet address, in network-byte order.
Counter32	32-bit counter that increases from 0 to $2^{32}-1$ and then wraps around to 0.
Counter64	64-bit counter.
Gauge32	32-bit integer that will not count above $2^{32}-1$ nor decrease beyond 0 when increased or decreased.
TimeTicks	Time, measured in 1/100ths of a second since some event.
Opaque	Uninterpreted ASN.1 string, needed for backward compatibility.

Structure of management Information (SMI)

- High-level constructs of SMI

- OBJECT-TYPE - The OBJECT-TYPE construct is used to specify the data type, status, and semantics of a managed object. Collectively, these managed objects contain the management data that lies at the heart of network management. There are more than 10,000 defined objects in various Internet RFCs [RFC 3410]. The OBJECT-TYPE construct has four clauses. :

✓ SYNTAX
✓ MAX-ACCESS
✓ STATUS
✓ DESCRIPTION

Structure of management Information (SMI)

- Example:

```
ipSystemStatsInDelivers OBJECT-TYPE
SYNTAX Counter32
MAX-ACCESS read-only
STATUS current
DESCRIPTION
        "The total number of datagrams successfully
        delivered to IPuser-protocols (including ICMP).
        When tracking interface statistics, the counter
        of the interface to which these datagrams were
        addressed is incremented. This interface might
        not be the same as the input interface for
        some of the datagrams.
        Discontinuities in the value of this counter can
        occur at re-initialization of the management
        system, and at other times as indicated by the
        value of ipSystemStatsDiscontinuityTime."
::= { ipSystemStatsEntry 18 }
```

Structure of management Information (SMI)

- High-level constructs of SMI

- MODULE-IDENTITY - The MODULE-IDENTITY construct allows related objects to be grouped together within a “module.” In addition to containing the OBJECT-TYPE definitions of the managed objects within the module, the MODULE-IDENTITY construct contains clauses to document contact information of the author of the module, the date of the last update, a revision history, and a textual description of the module.

Structure of management Information (SMI)

- Example:

```
ipMIB MODULE-IDENTITY
       LAST-UPDATED "200602020000Z"
       ORGANIZATION "IETF IPv6 MIB Revision Team"
       CONTACT-INFO
              "Editor:
              Shawn A. Routhier
              Interworking Labs
              108 Whispering Pines Dr. Suite 235
              Scotts Valley, CA 95066
              USA
              EMail: <sar@iwl.com>"
       DESCRIPTION
              "The MIB module for managing IP and ICMP
              implementations, but excluding their
              management of IP routes"
```

……..

Structure of management Information (SMI)

- High-level constructs of SMI

- NOTIFICATION-TYPE - used to specify information about SNMPv2-Trap and InformationRequest messages generated by an agent or management entity.

- MODULE-COMPLIANCE - defines the set of managed objects within a module that the agent must implement;

- AGENT-CAPABILITIES - defines the capabilities of agents with respect to object and event notification definitions.

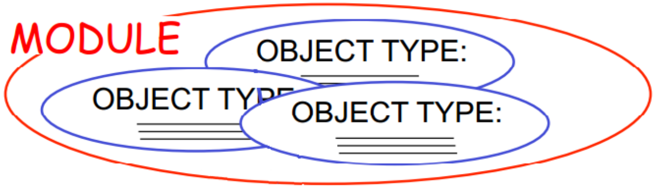
SMI: an example for Module and Object definition

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 4}
```

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}
```



Management Information Base (MIB)

- Each object has a value that represents a particular characteristic of the component—name, location, IP address, Ethernet contention counter, and so on. and others.;

- Components of the same type have the same MIB;

- Standard component descriptions are defined by categories: routers, switches, etc.;

Network Management Protocol

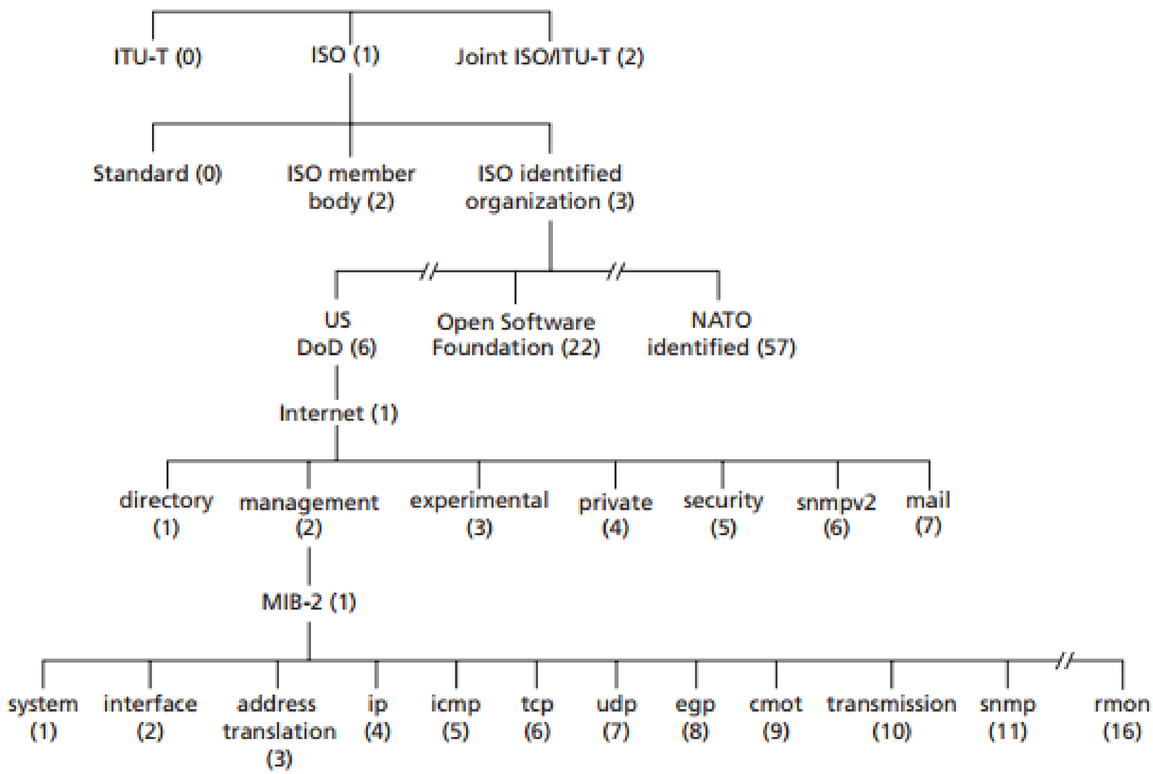
- It is intended for the exchange of messages between the MS and the agents

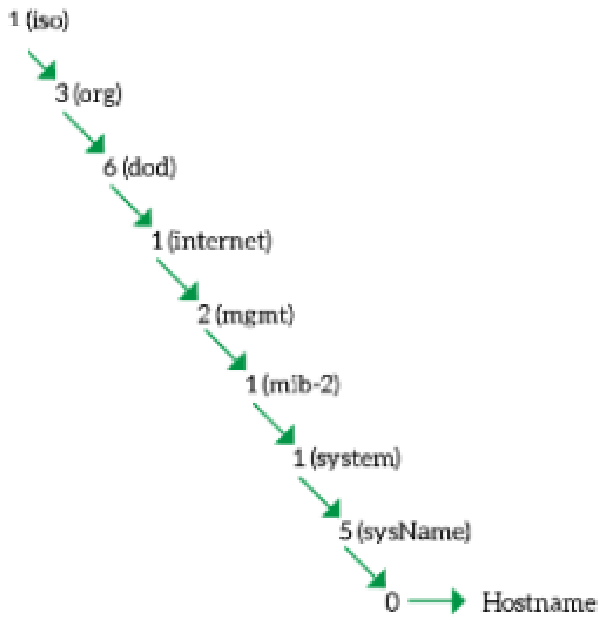
- TCP/IP model use Simple Network Management Protocol (SNMP)
  - limited capabilities, but easy to apply
  - the most commonly used protocol

- OSI use *Common Management Information Protocol* (*CMIP*)
  - many possibilities, but complicated to apply
  - used in large telecommunication companies

- SNMPv2 – also applicable to OSI and TCP/IP

Management Information Base (MIB)

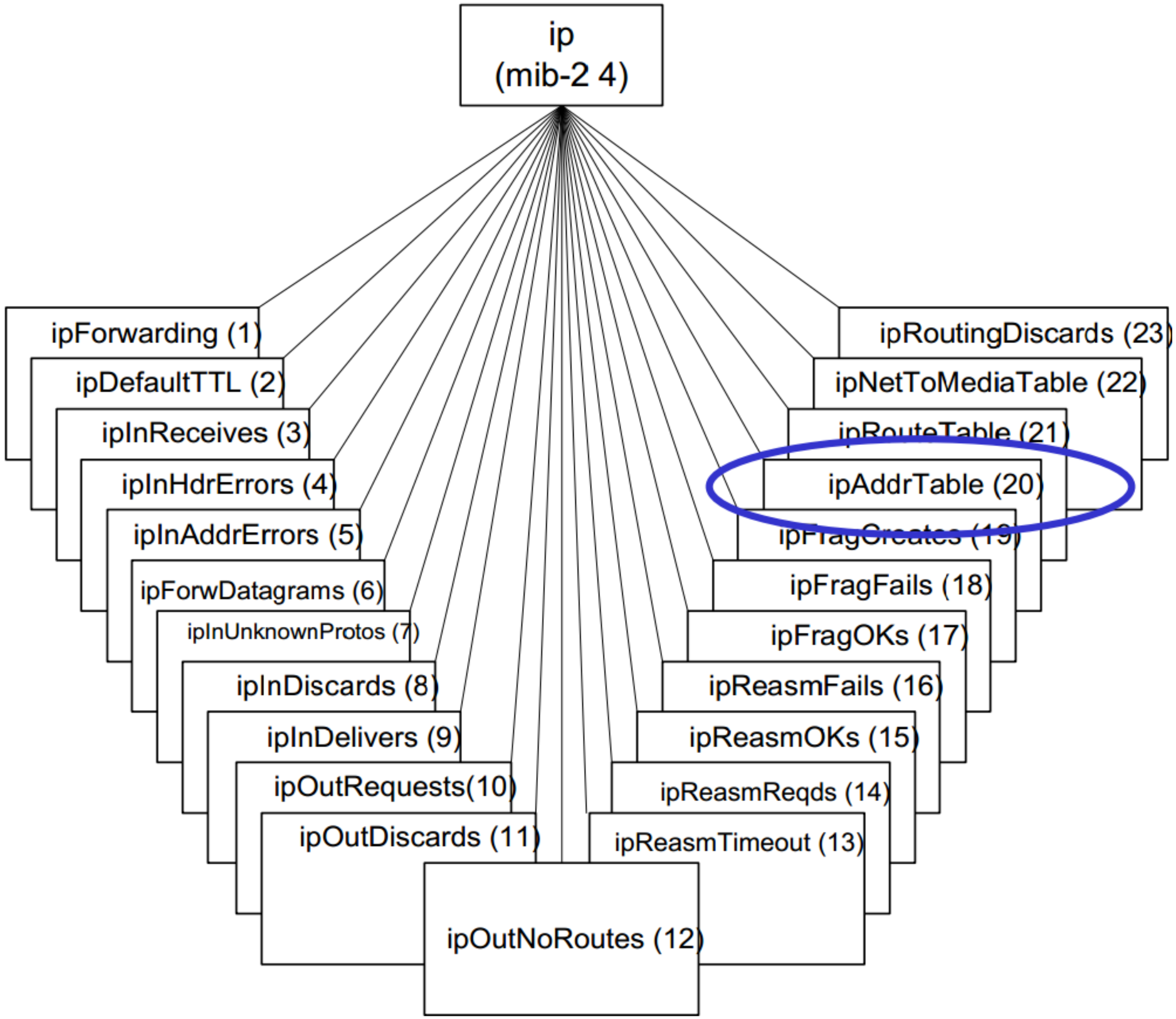




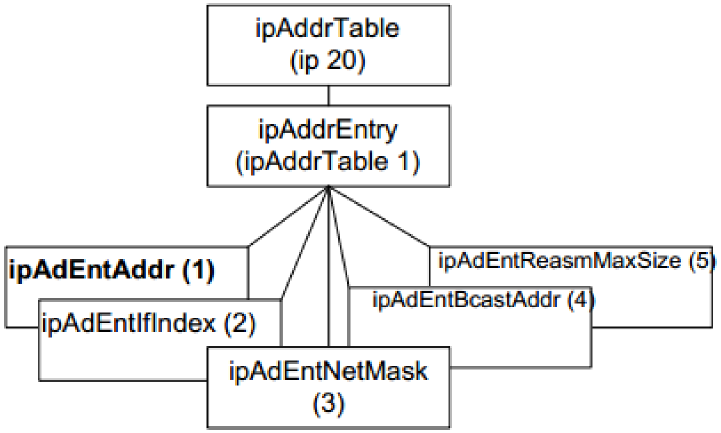
Numeric positions are written by separating them with a period, e.g. the full identifier for the hostname is 1.3.6.1.2.1.1.5.0

Management Information Base (MIB)

- ✓ IP Address Table: table of host IP addresses;
- ✓ IP Route Table: record for each route
- ✓ IP network-to-Media Table: a table containing the translation of IP addresses to physical addresses



Management Information Base (MIB)



Entity	OID	Description (brief)
ipAddrTable	ip 20	Table of IP addresses
ipAddrEntry	IpAddrTable 1	One of the entries in the IP address table
ipAdEntAddr	IpAddrEntry 1	The IP address to which this entry's addressing information pertains
ipAdEntIfIndex	IpAddrEntry 2	Index value of the entry, same as ifIndex
ipAdEntNetMask	IpAddrEntry 3	Subnet mask for the IP address of the entry
ipAdEntBcastAddr	IpAddrEntry 4	Broadcast address indicator bit
ipAdEntReasmMaxSize	IpAddrEntry 5	Largest IP datagram that can be reassembled on this interface

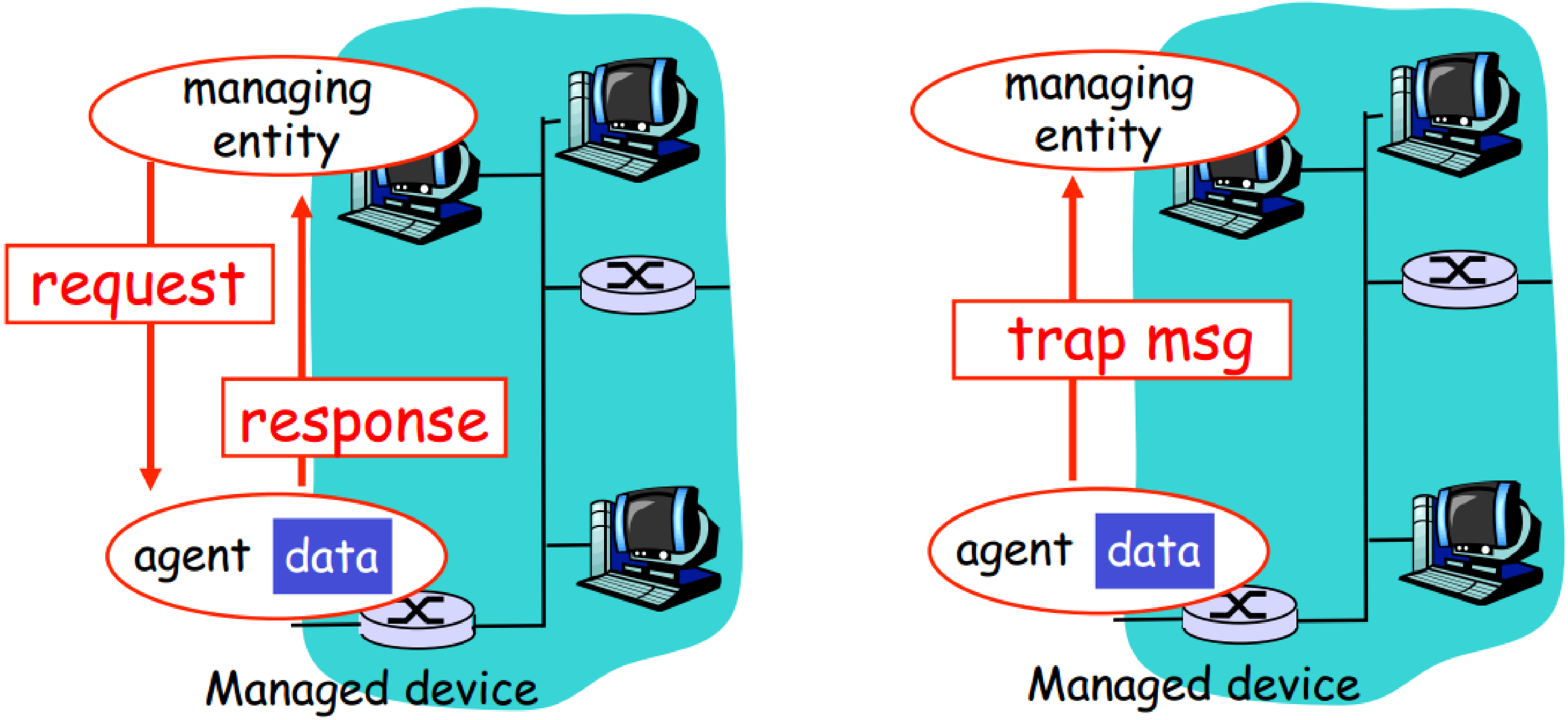
Management Information Base (MIB)

Object Identifier	Name	Type	Description (from RFC 1213)
1.3.6.1.2.1.1.1	sysDescr	OCTET STRING	"Full name and version identification of the system's hardware type, software operating-system, and networking software."
1.3.6.1.2.1.1.2	sysObjectID	OBJECT IDENTIFIER	Vendor-assigned object ID that "provides an easy and unambiguous means for determining 'what kind of box' is being managed."
1.3.6.1.2.1.1.3	sysUpTime	TimeTicks	"The time (in hundredths of a second) since the network management portion of the system was last re-initialized."
1.3.6.1.2.1.1.4	sysContact	OCTET STRING	"The contact person for this managed node, together with information on how to contact this person."
1.3.6.1.2.1.1.5	sysName	OCTET STRING	"An administratively assigned name for this managed node. By convention, this is the node's fully qualified domain name."
1.3.6.1.2.1.1.6	sysLocation	OCTET STRING	"The physical location of this node."
1.3.6.1.2.1.1.7	sysServices	Integer32	A coded value that indicates the set of services available at this node: physical (for example, a repeater), data link/subnet (for example, bridge), Internet (for example, IP gateway), end-to-end (for example, host), applications.

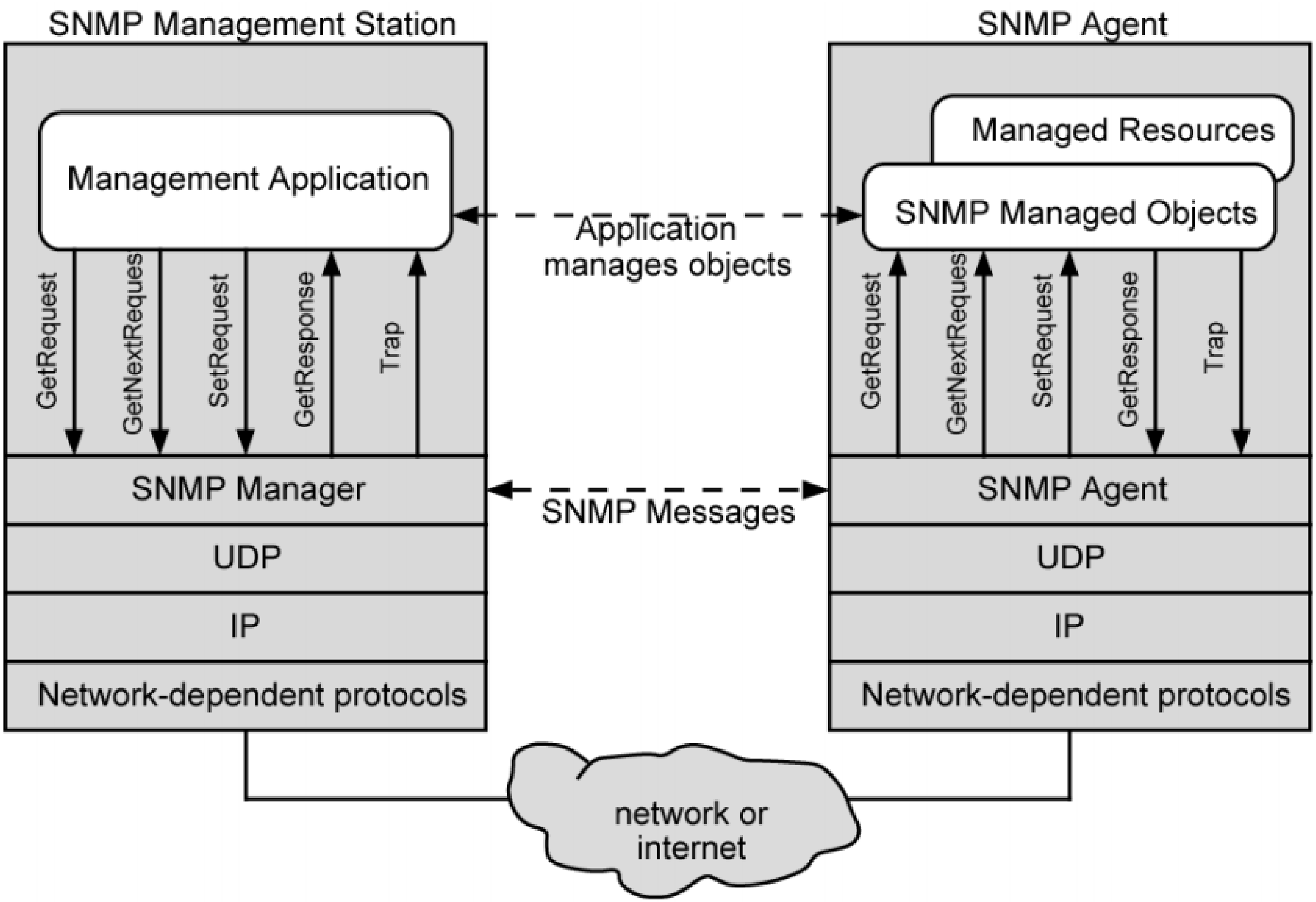
SNMPv1 architecture (RFC1067-1212)

- Application protocol
- Use UDP as transport protocol
- It uses the following messages exchanged through the port161
  - *GetRequest*
  - *GetNextRequest*
  - *SetRequest*
- Agent response with *GetResponse*
- Agent can send the *trap message* (UDP port 162), in case an event has occurred that affects the MIB and management accordingly

SNMPv1 architecture



SNMPv1 architecture



SNMPv1 architecture

- If a router has the following table

status	IpAdEntAddr	IpAdEntIfIndex	IpAdEntBcastAddr	IpAdEntReasmMaxSize
1	123.45.2.1	1	0	12000
1	123.45.3.4	3	1	12000
1	165.8.9.25	2	0	10000
1	9.96.8.138	4	0	15000

- To obtain the *maximum reassembly size* value for interface 3, the MS must send the following command:

- *get_request(1.3.6.1.2.1.4.20.1.5.123.45.3.4)*

- The agent's response will be:

- *get_response(1.3.6.1.2.1.4.20.1.5.123.45.3.4=12000)*

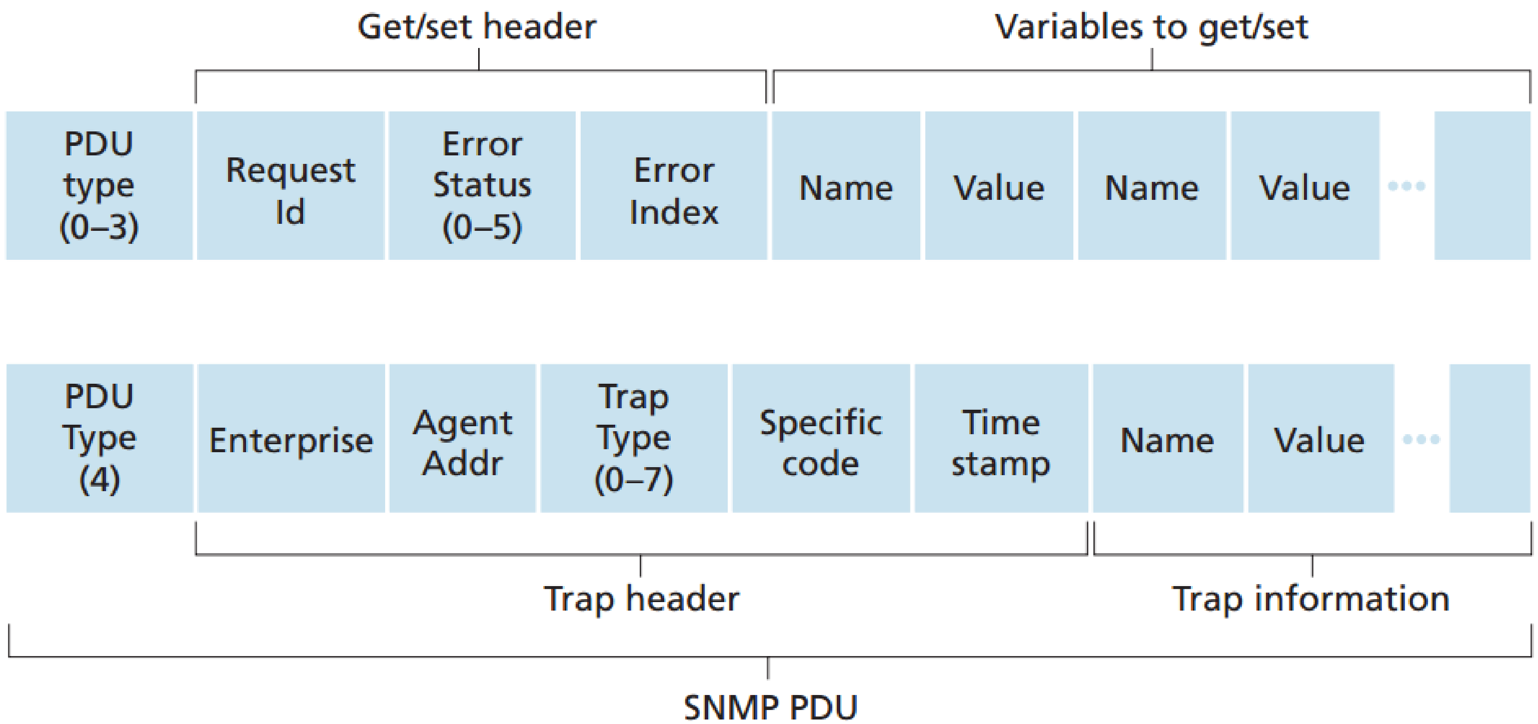
Innovations in SNMPv2 (RFC1146-1452) and SNMPv3 (RFC2571)

- Bulk data transfer
- Message exchange manager-to-manager
- SMIv2
- Create and delete rows in a table
- Add communication protection
  - **NoAuthNoPriv** (no authentication, no privacy) - The network device does not authenticate the MS.
  - **AuthNoPriv** (authentication, no privacy) - MS authenticates using a shared secret.
  - **AuthPriv** (authentication and privacy) – MS authentication, but also encryption of SNMP traffic.
- Defining an SNMP engine (SNMPv3)

SNMPv2 PDU types

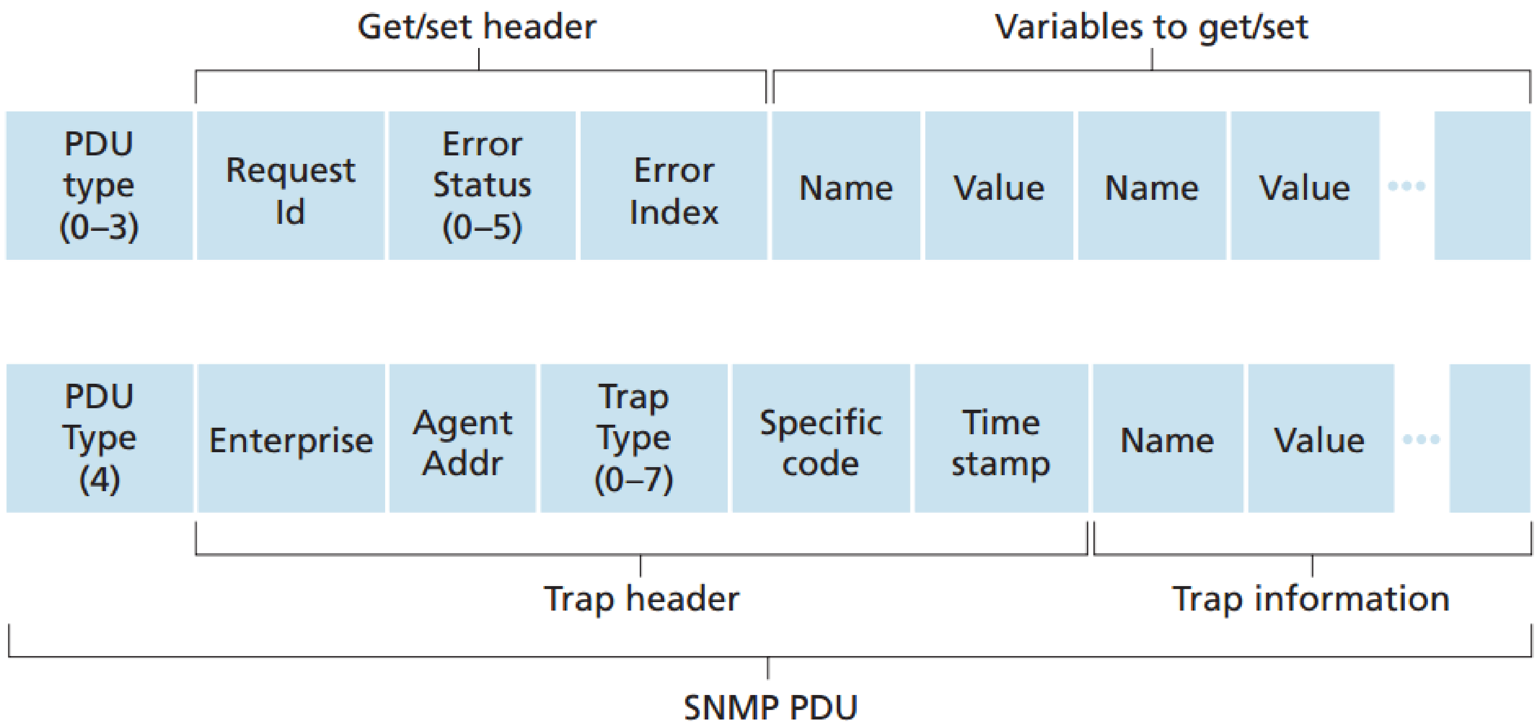
SNMPv2 PDU Type	Sender-receiver	Description
`GetRequest`	manager-to-agent	get value of one or more MIB object instances
`GetNextRequest`	manager-to-agent	get value of next MIB object instance in list or table
`GetBulkRequest`	manager-to-agent	get values in large block of data, for example, values in a large table
`InformRequest`	manager-to-manager	inform remote managing entity of MIB values remote to its access
`SetRequest`	manager-to-agent	set value of one or more MIB object instances
`Response`	agent-to-manager or	generated in response to
	manager-to-manager	`GetRequest,`
		`GetNextRequest,`
		`GetBulkRequest,`
		`SetRequest PDU`, or
		`InformRequest`
`SNMPv2-Trap`	agent-to-manager	inform manager of an exceptional event

SNMPv2 PDU format



Error Status field:
0 – noError – there is no mistake
1 – noError – the answer cannot be placed in a single message
2 – noSuchName – non-existent variable
3 – badValue – an invalid value or syntax was used in a Set command
4 – readOnly – read-only value
5 – genErr – unknown error

SNMPv2 PDU format



Trap type field:

0 – coldStart – set initial state

1 – wannStart – restore the initial state

2 – linkDown

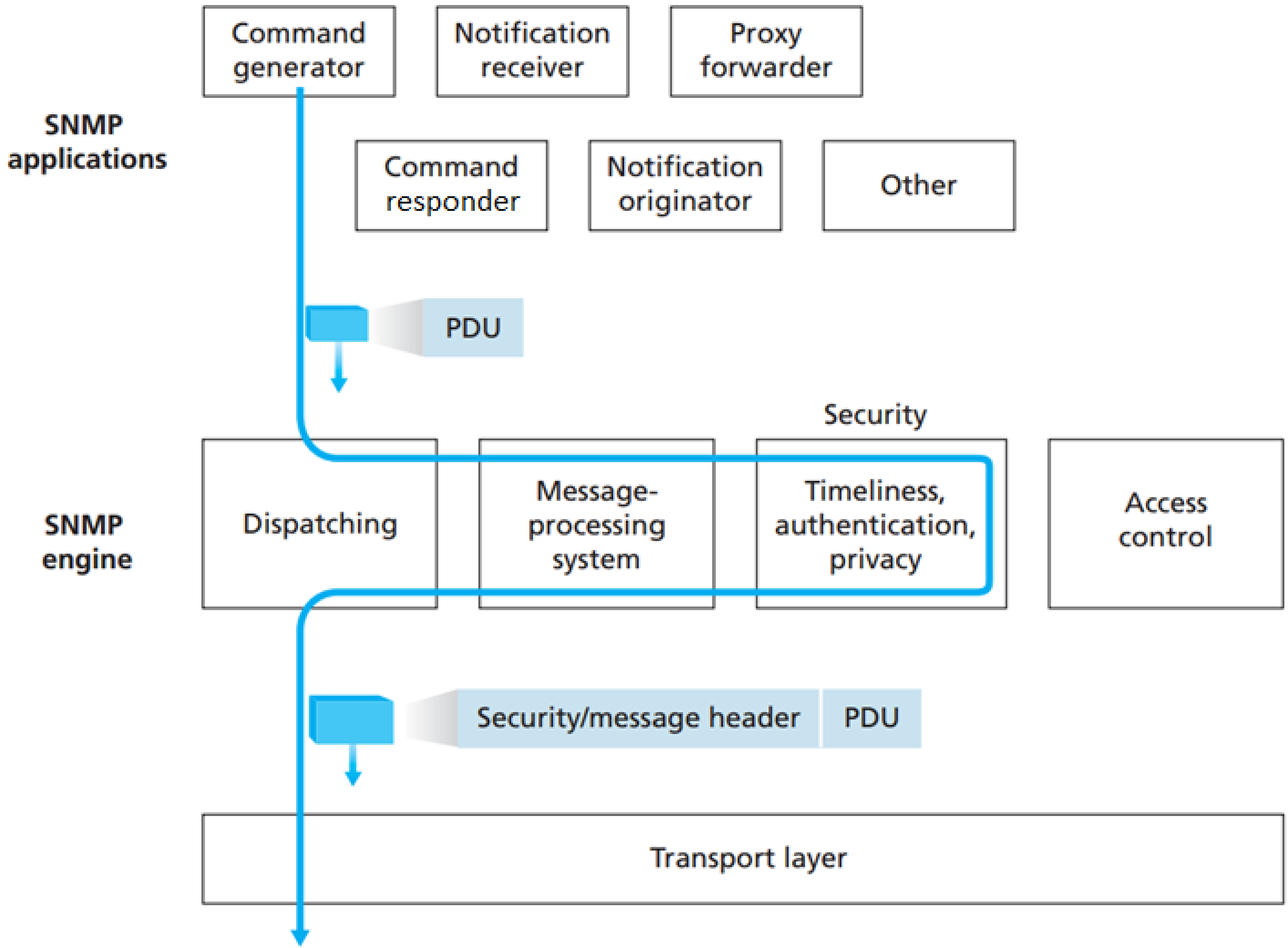
3 – linkUp

4 – authenticationFailure

5 – egpNeighborLoss

6 – entrpriseSpecific –*trap* info is included in *Specific code* field

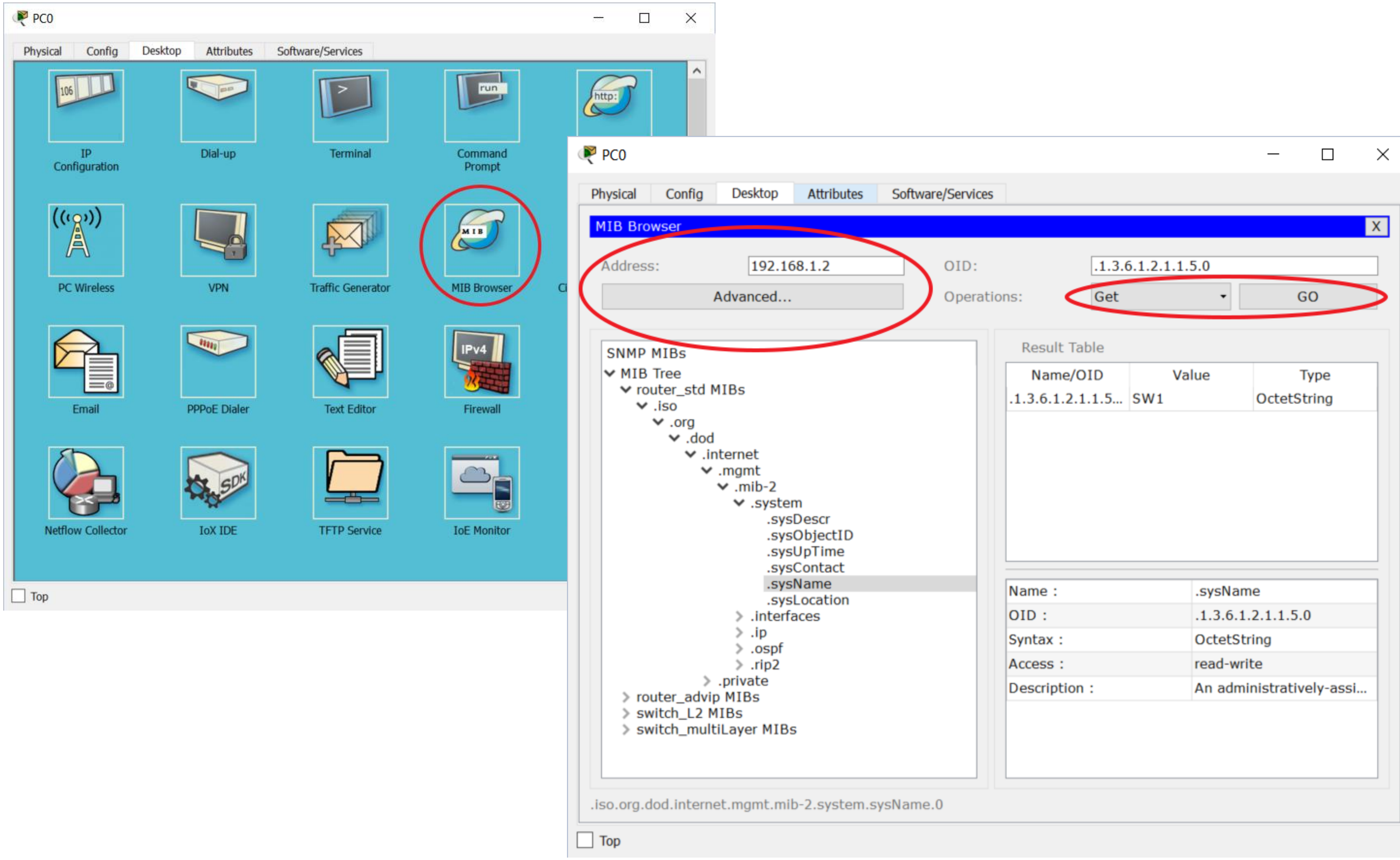
SNMPv3 engine



Assoc. Prof. Rosen Radkov PhD

NETWORK ADMINISTRATION

Read MIB using Cisco Packet Tracer



Assoc. Prof. Rosen Radkov PhD

THANK YOU FOR THE ATTENTION!

Assoc. Prof. Rosen Radkov PhD