CS2505: Network Management

Outline

- Introduction to network management
  - motivation
  - major components
- Internet network management framework
  - MIB: management information base
  - SMI: data definition language
  - SNMP: protocol for network management
  - NETCONF/YANG

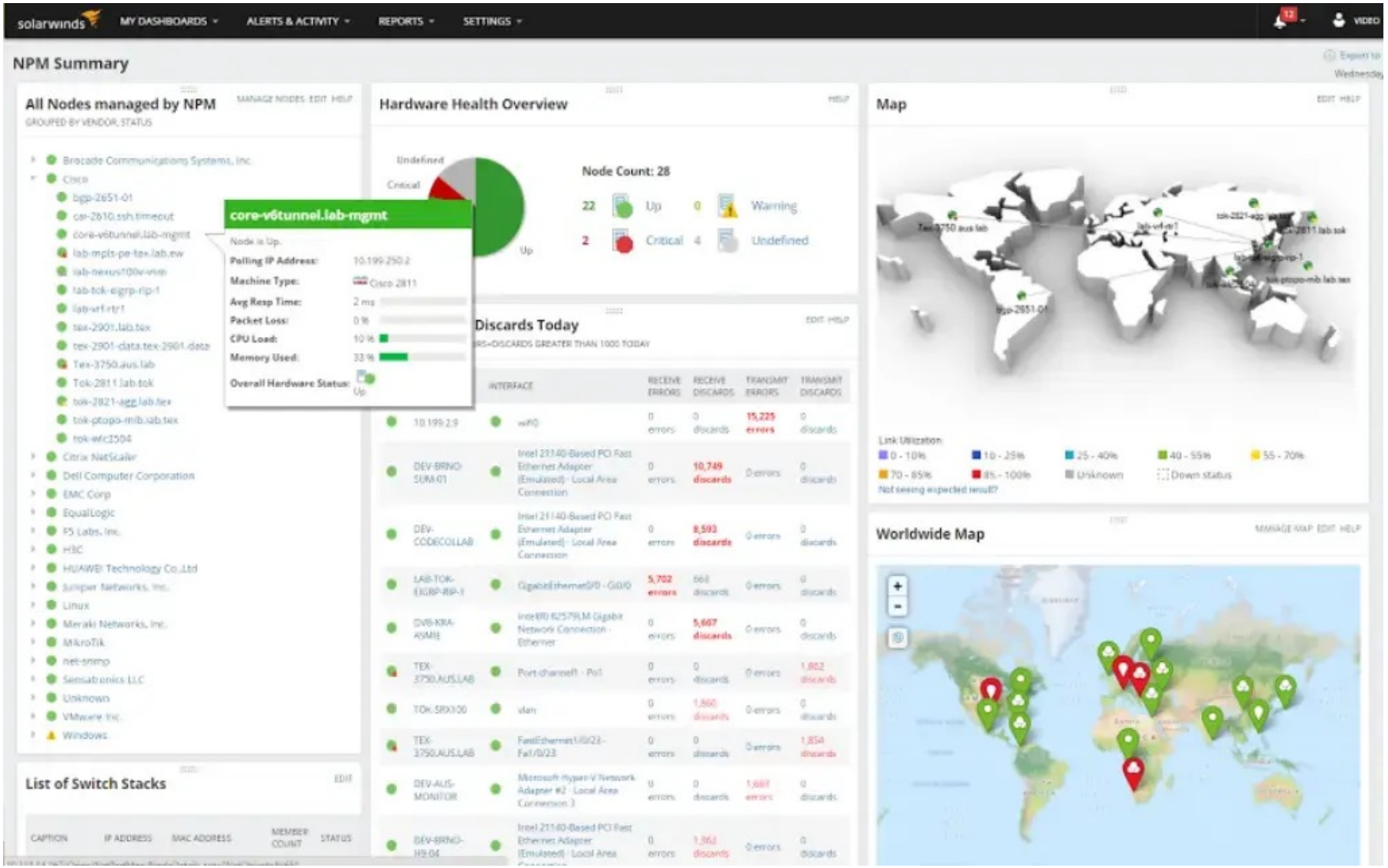
What is network management?

- autonomous systems (aka "network"): 100s or 1000s of interacting hardware/software components
- other complex systems requiring monitoring, control:
  - jet airplane
  - nuclear power plant
  - others?

"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."

Network Operations Centre

Images show AT&T's global network operations centre (NOC)

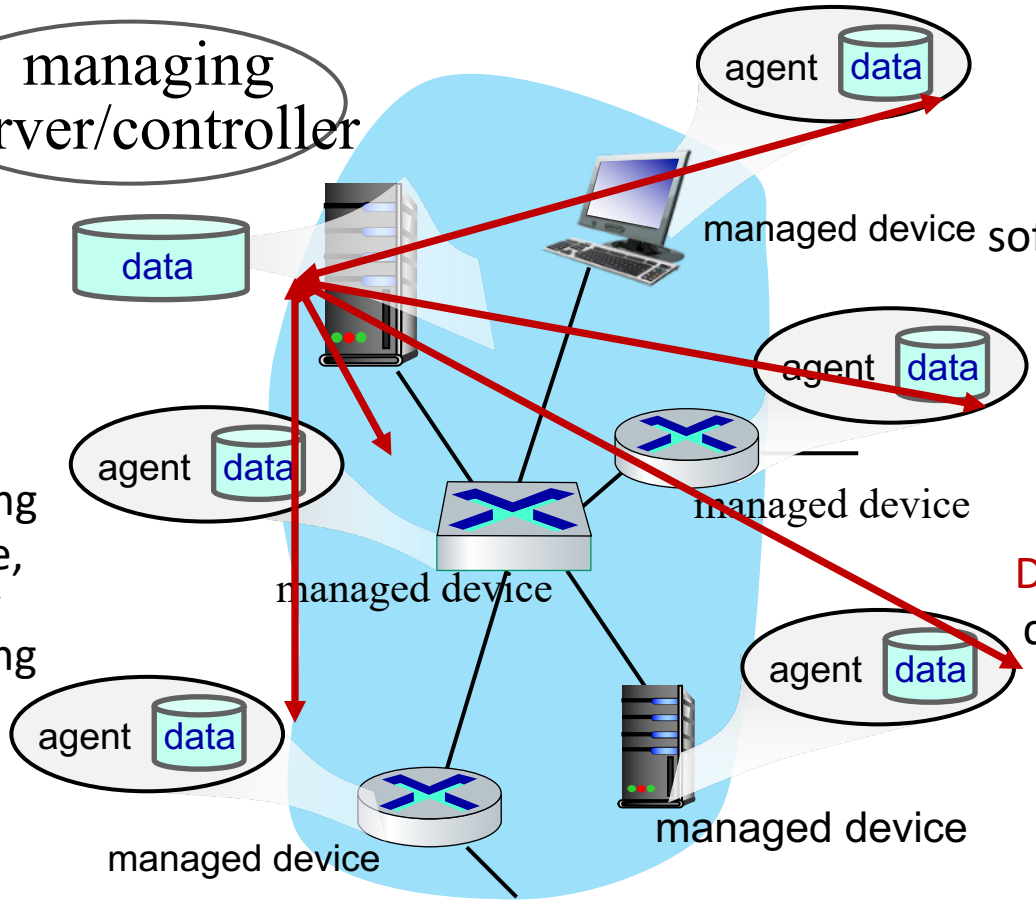


Example: SolarWinds Network Performance Monitor

Infrastructure Components

Managing server: application, typically with network managers (humans) in the loop

Network management protocol: used by managing server to query, configure, manage device; used by devices to inform managing server of data, events.



Managed device: equipment with manageable, configurable hardware, software components

Data: device "state" configuration data, operational data, device statistics

Popular Approaches

- CLI (Command Line Interface)
  - operator issues (types, scripts) direct to individual devices (e.g., vis ssh)
- SNMP/MIB
  - operator queries/sets devices data (MIB) using Simple Network Management Protocol (SNMP)
- NETCONF/YANG
  - communicate actions/data to/from/among remote devices
  - expressed using YANG data modelling language

Outline

- Introduction to network management
  - motivation
  - major components
- Internet network management framework
  - MIB: management information base
  - SMI: data definition language
  - SNMP: protocol for network management
  - NETCONF/YANG

SNMP overview: 4 key parts

- Management information base (MIB):
  - distributed information store of network management data
- Structure of Management Information (SMI):
  - data definition language for MIB objects
- SNMP protocol
  - convey manager<->managed object info, commands
- security, administration capabilities
  - major addition in SNMPv3

SMI: data definition language

Purpose: syntax, semantics of management data well-defined, unambiguous

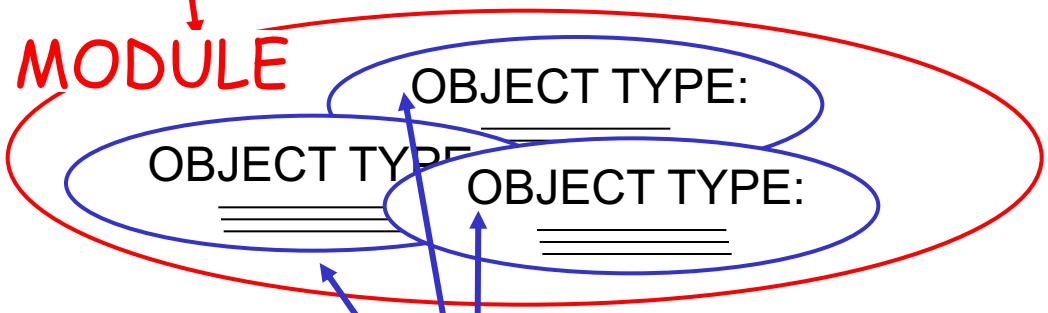
- base data types:
  - straightforward, boring
- OBJECT-TYPE
  - data type, status, semantics of managed object
- MODULE-IDENTITY
  - groups related objects into MIB module

Basic Data Types

INTEGER
Integer32
Unsigned32
OCTET STRING
OBJECT IDENTIFIED
IPaddress
Counter32
Counter64
Guage32
Time Ticks
Opaque

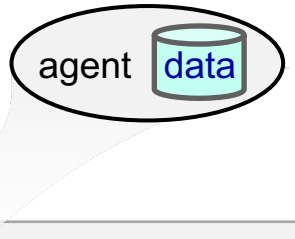
SNMP MIB

MIB module specified via SMI
MODULE-IDENTITY
(100s of standardized MIBs, many more vendor-specific)



objects specified via SMI
OBJECT-TYPE construct

Example MIB for UDP



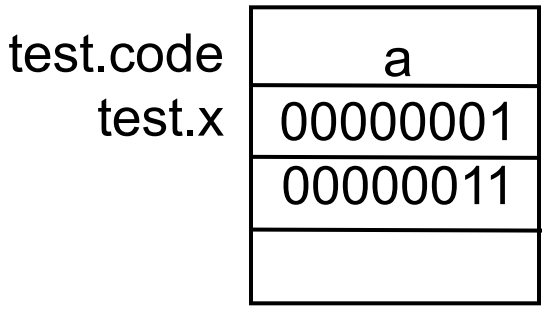
Object ID	Name	Type	Comments
1.3.6.1.2.1.7.1	UDPInDatagrams	32-bit counter	total # datagrams delivered
1.3.6.1.2.1.7.2	UDPNoPorts	32-bit counter	# undeliverable datagrams (no application at port)
1.3.6.1.2.1.7.3	UDInErrors	32-bit counter	# undeliverable datagrams (all other reasons)
1.3.6.1.2.1.7.4	UDPOutDatagrams	32-bit counter	total # datagrams sent
1.3.6.1.2.1.7.5	udpTable	SEQUENCE	one entry for each port currently in use

- SNMP uses ISO Object ID standard, X.660
  - a hierarchy for naming "objects"
  - also used for many other systems

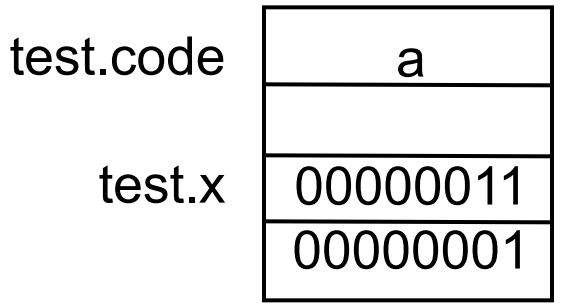
The presentation problem

- SNMP agents and manager may have different ways of representing data, leading to misinterpretation of message contents

```
struct {
   char code;
    int x;
    } test;
test.x = 256;
test.code='a'
```



host 1 format



host 2 format

Presentation problem: potential solutions

1. Sender learns receiver's format. Sender translates into receiver's format. Sender sends.
   - real-world analogy?
   - pros and cons?
2. Sender sends. Receiver learns sender's format. Receiver translate into receiver-local format
   - real-world-analogy
   - pros and cons?
3. Sender translates host-independent format. Sends. Receiver translates to receiver-local format.
   - real-world analogy?
   - pros and cons?

ASN.1: Abstract Syntax Notation 1

- ISO standard X.680
  - used extensively in Internet and telco networks
- defined data types, object constructors
  - like SMI
- BER: Basic Encoding Rules
  - specify how ASN.1-defined data objects to be transmitted
  - each transmitted object has Type, Length, Value (TLV) encoding

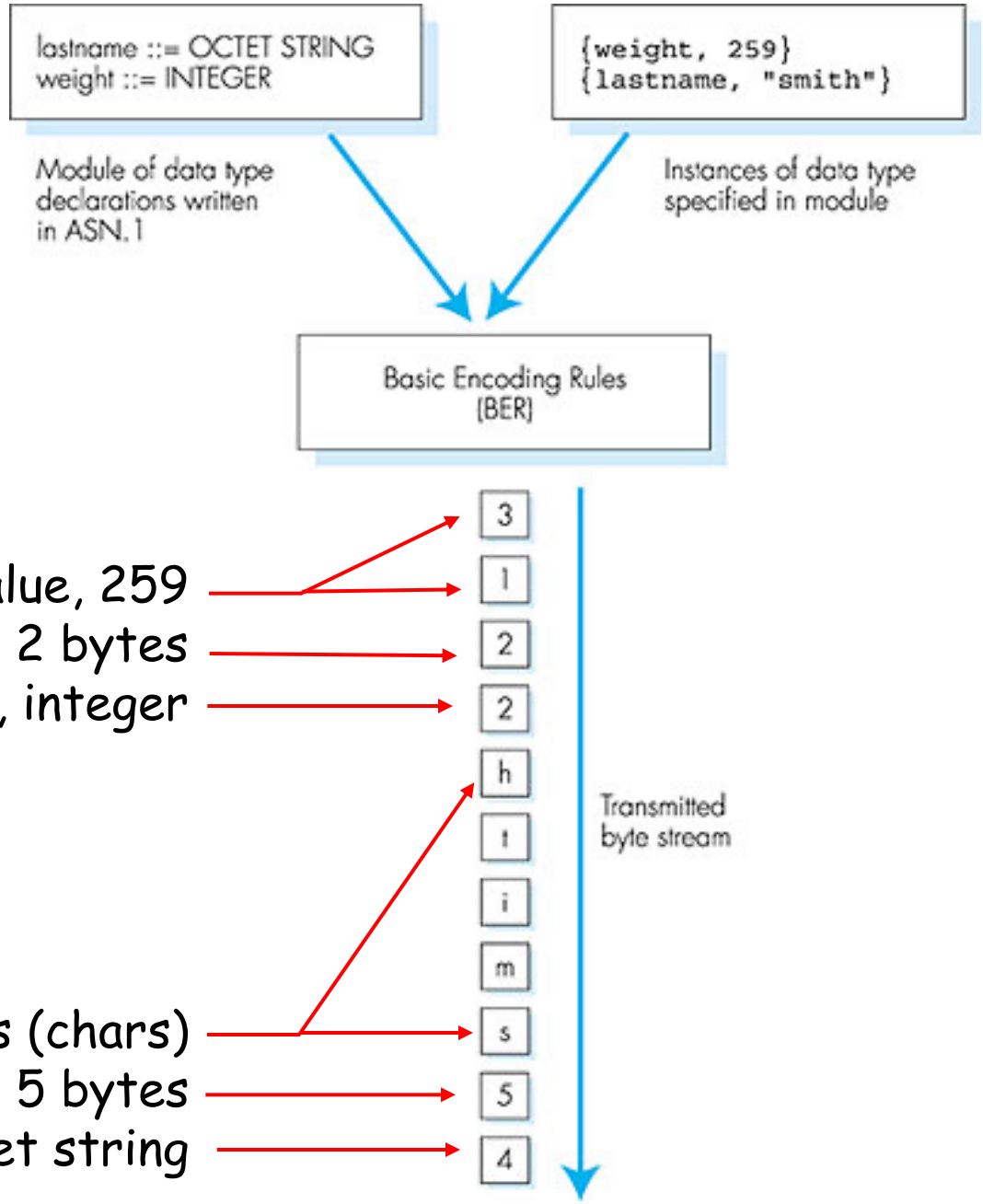
TLV Encoding

Idea: transmitted data is self-identifying

- T: data type, one of ASN.1-defined types
- L: length of data in bytes
- V: value of data, encoded according to ASN.1 standard

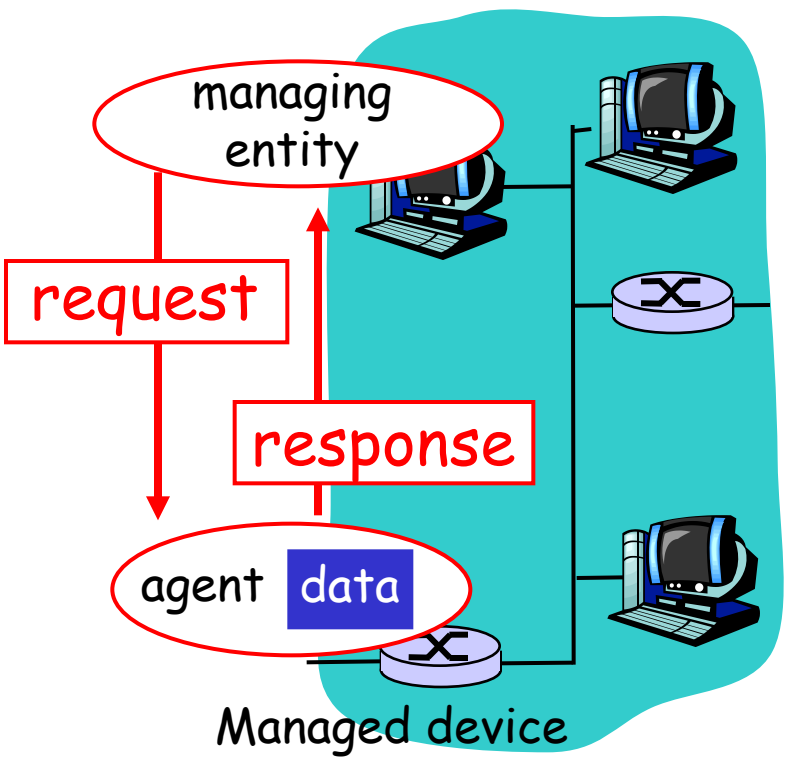
Tag Value	Type
1	Boolean
2	Integer
3	Bitstring
4	Octet string
5	Null
6	Object Identifier
9	Real

TLV encoding: example

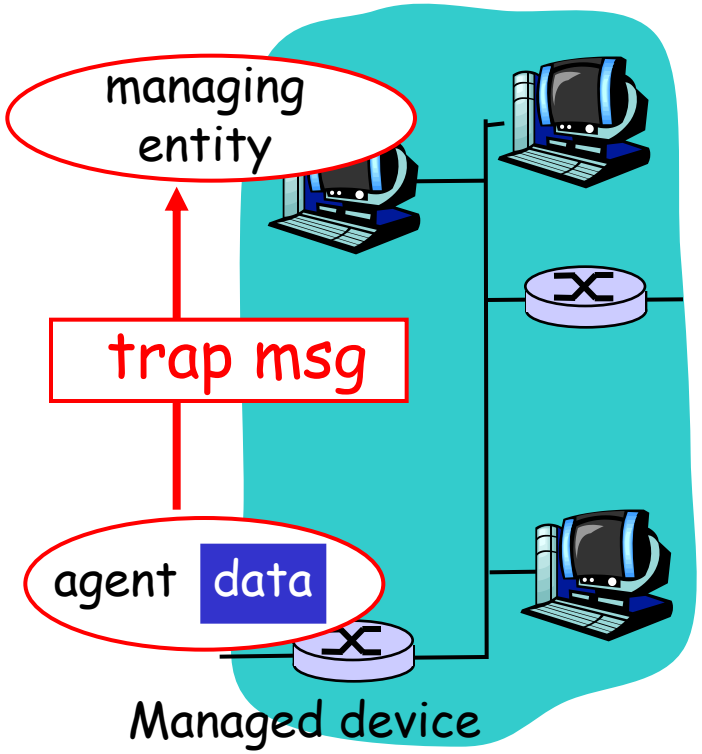


SNMP protocol

Two ways to convey MIB info, commands:



request/response mode

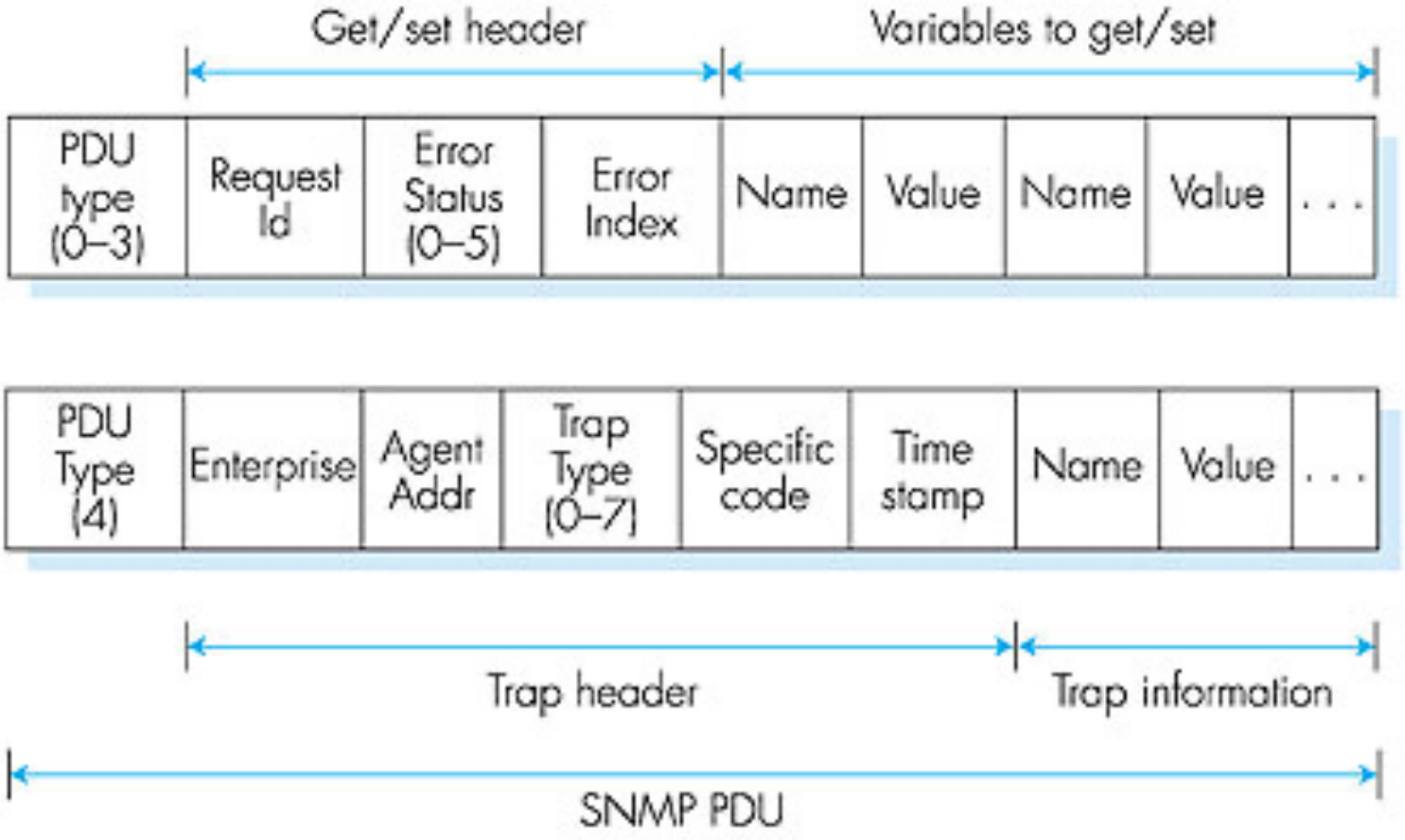


trap mode

SNMP protocol: message types

Message type	Function
GetRequest GetNextRequest GetBulkRequest	Mgr-to-agent: "get me data" (instance,next in list, block)
InformRequest	Mgr-to-Mgr: here's MIB value
SetRequest	Mgr-to-agent: set MIB value
Response	Agent-to-mgr: value, response to Request
Trap	Agent-to-mgr: inform manager of exceptional event

SNMP protocol: message formats



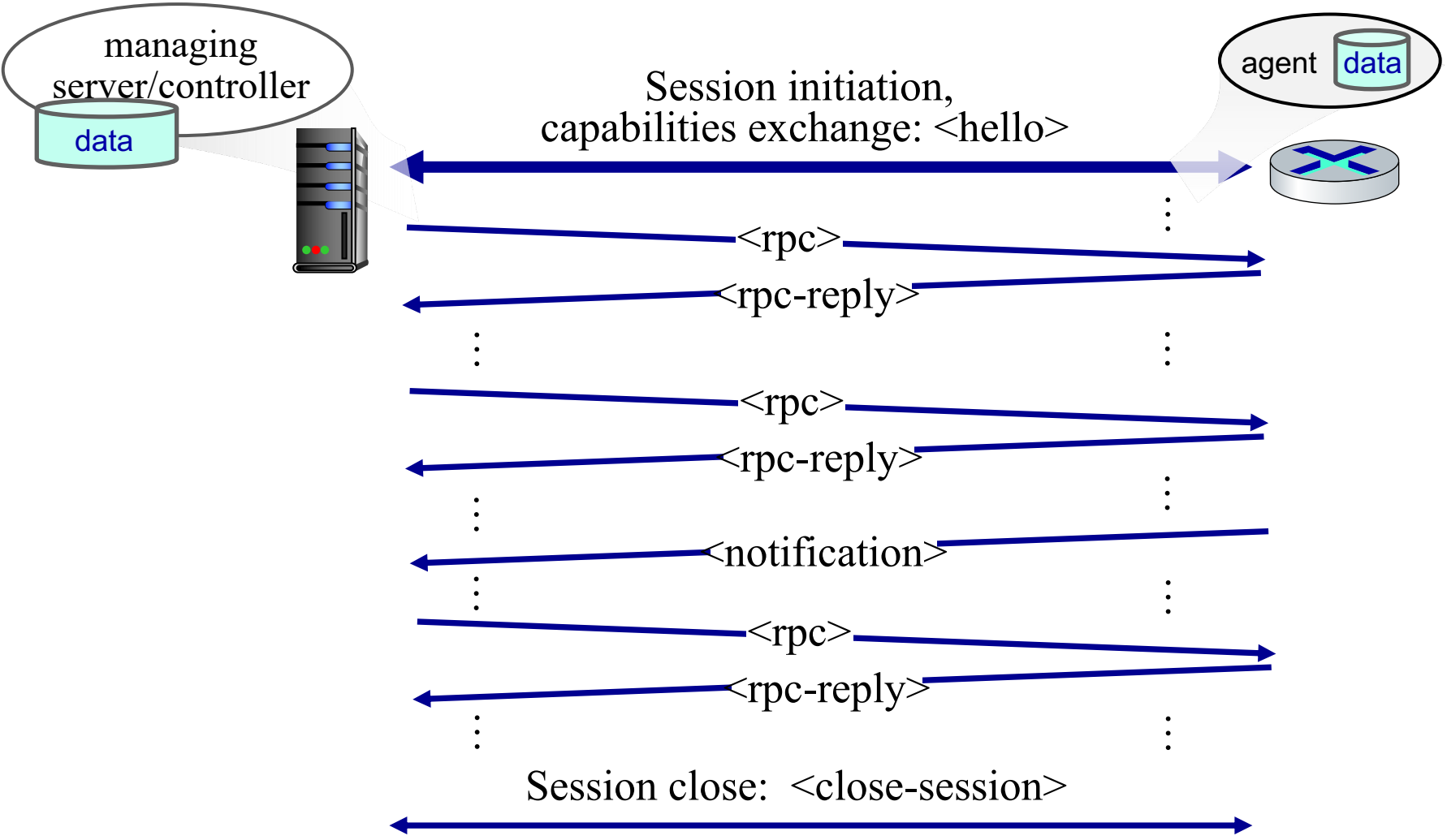
SNMP security and administration

- encryption: DES-encrypt SNMP message
- authentication: compute, send MIC(m,k): compute hash (MIC) over message (m), secret shared key (k)
- protection against playback: use nonce
- view-based access control
  - SNMP entity maintains database of access rights, policies for various users
  - database itself accessible as managed object!

NETCONF Overview

- Goal: actively manage/configure devices network-wide
- Operates between managing server and managed network devices
  - actions: retrieve, set, modify, activate configurations
  - atomic-commit actions over multiple devices
  - query operational data and statistics
  - subscribe to notifications from devices
- Remote procedure call (RPC) paradigm
  - NETCONF protocol messages encoded in XML
  - exchanged over secure, reliable transport (e.g., TLS) protocol

NETCONF initialization, exchange, close



Selected NETCONF Operations

NETCONF Ooeration	Description
<get-config>	Retrieve all or part of a given configuration. A device may have multiple configurations.
<get>	Retrieve all or part of both configuration state and operational state data.
<edit-config>	Change specified (possibly running) configuration at managed device. Managed device <rpc-reply> contains <ok> or <rpcerror> with rollback.
<lock>, <unlock>	Lock (unlock) configuration datastore at managed device (to lock out NETCONF, SNMP, or CLIs commands from other sources).
<create-subscription>, <notification>	Enable event notification subscription from managed device

Sample NETCONF RPC Message

```
01 <?xml version="1.0" encoding="UTF-8"?>
02 <rpc message-id="101"
03   xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
04   <edit-config>
05     <target>
06       <running/>
07     </target>
08     <config>
09       <top xmlns="http://example.com/schema/
         1.2/config">
10         <interface>
11           <name>Ethernet0/0</name>
12           <mtu>1500</mtu>
13         </interface>
14       </top>
15     </config>
16   </edit-config>
17 </rpc>
```

note message id

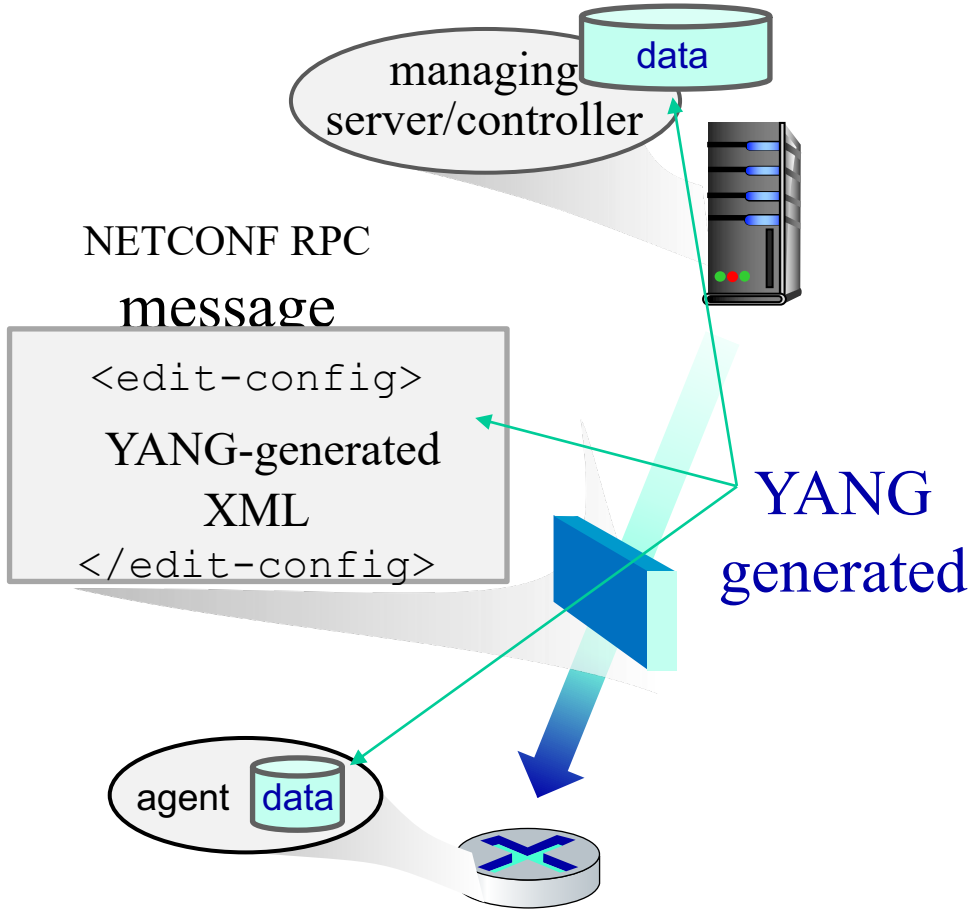
change a configuration

change the running configuration

change MTU of Ethernet 0/0 interface to 1500

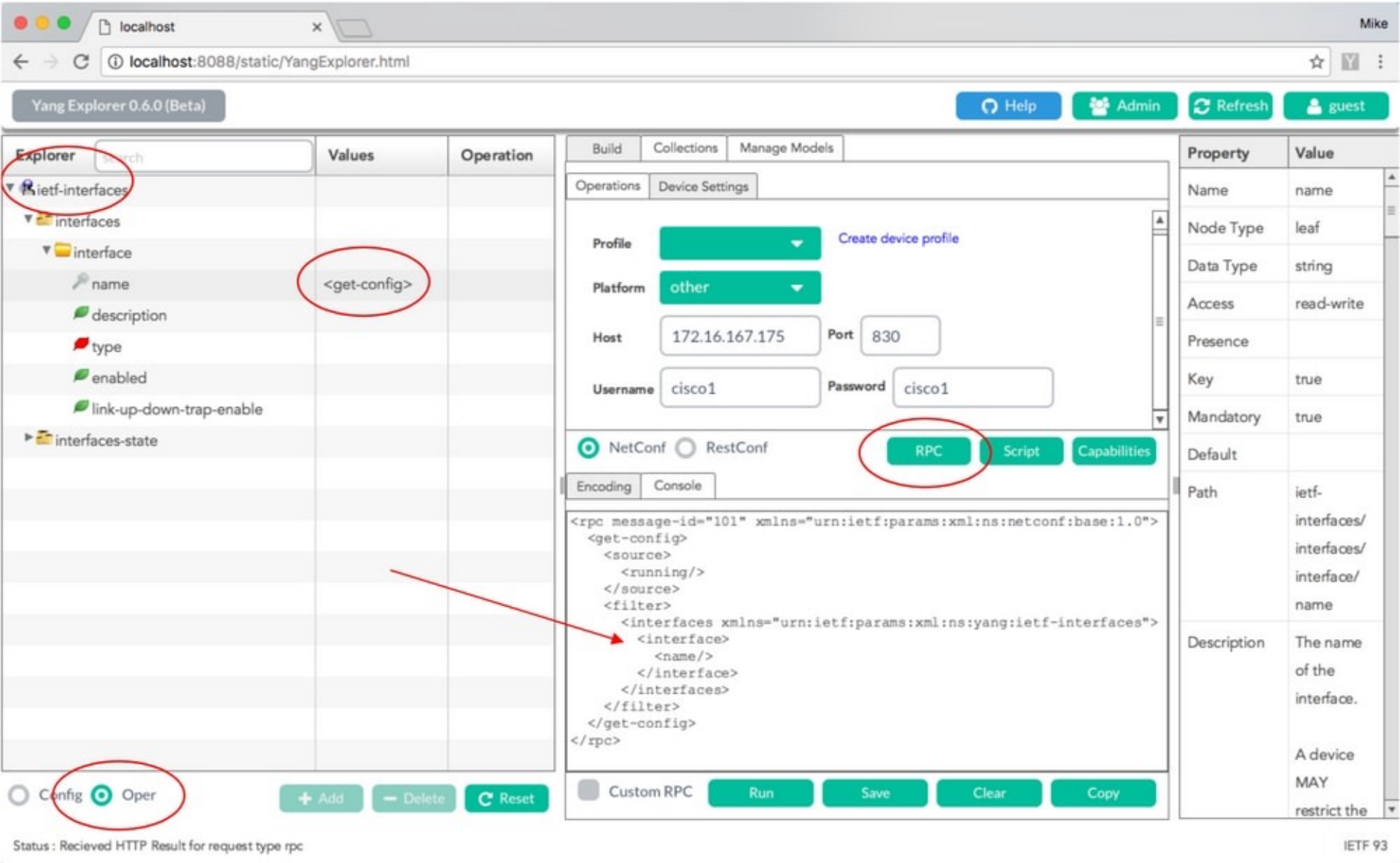
YANG

- Yet Another Next Generation (YANG) data modelling language
- Used to specify structure, syntax, semantics of NETCONF network management data
  - built-in data types, like SMI



YANG

- XML document describing device, capabilities can be generated from YANG description
- can express constraints among data that must be satisfied by a valid NETCONF configuration
  - ensure NETCONF configurations satisfy correctness, consistency constraints



Example from Cisco of requesting a list of network interface names

Comparing SNMP & NETCONF

- NETCONF designed to monitor and configure networks while SNMP was for devices
  - Transactions (set of related actions) across multiple devices
  - Supports the shift towards network automation
- YANG considered to be more expressive and easier to use than SMI
  - XML widely used and human-readable
- NETCONF uses secure and reliable end-to-end transport (TLS and TCP) unlike SNMP which uses UDP

Network Management: summary

- network management key points:
  - extremely important: significant portion of network "cost" (operational expenditure OPEX)
  - SNMP protocol as a tool for conveying information
  - NETCONF/YANG
- Network management as a tool, but:
  - what to measure/monitor?
  - how to respond to failures?
  - alarm correlation/filtering

Role for machine learning in data analysis