

COSC 301

Network Management and Security

Lecture 19: Management Tools and Protocols

What is Network Management?

Monitoring, testing, configuring, and trouble-shooting network components to meet a set of requirements defined by an organization.

These requirements include the smooth, efficient, operation of the network that provides the predefined quality of service to users.

ITS Service Outage:

Why we Manage?

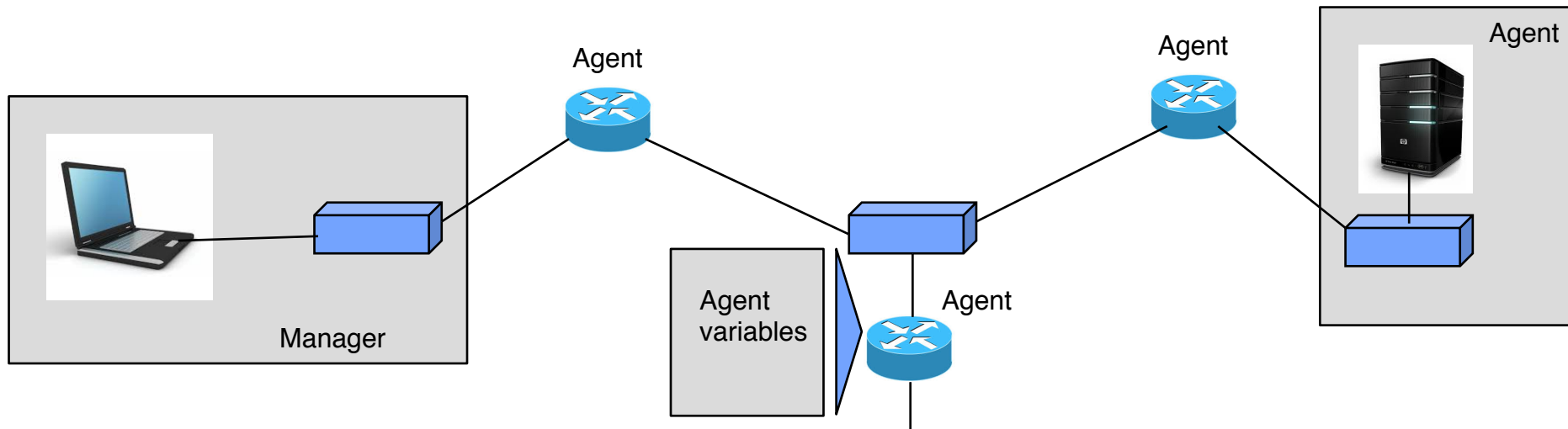
- **Maintaining**
 - Configure the resources properly
- **Monitoring**
 - Improve visibility of the network
- **Early Warning**
 - Aim to preempt causes of downtime, find anomaly.
 - Imminent failure: changes in rate of errors
- **Planning**
 - Trend analysis & capacity planning
 - Daily, weekly, yearly graphs.
 - Statistical tools

Areas of Network Management

- Configuration Management
 - Reconfiguration and documentation
 - Hardware, software, user-account
- Fault Management
 - Reactive: detect, isolate, correct, and record
 - Proactive: tries to avoid faults from happening
- Performance Management
 - Capacity, traffic, throughput, and response time
- Security Management
- Accounting Management
 - Control user's access to network resources through charges

SNMP (1)

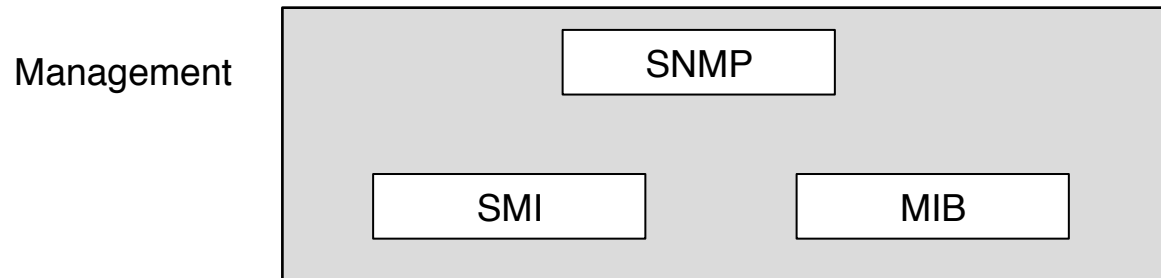
- Simple Network Management Protocol
 - A framework for managing devices in an internet using the TCP/IP protocol suite
 - Provides a set of fundamental operations for monitoring and maintaining an internet
 - Use the concept of manager and agent
 - Agent: a managed station (router or host) that runs SNMP server program
 - Manager: a host that runs the SNMP client program



SNMP (2)

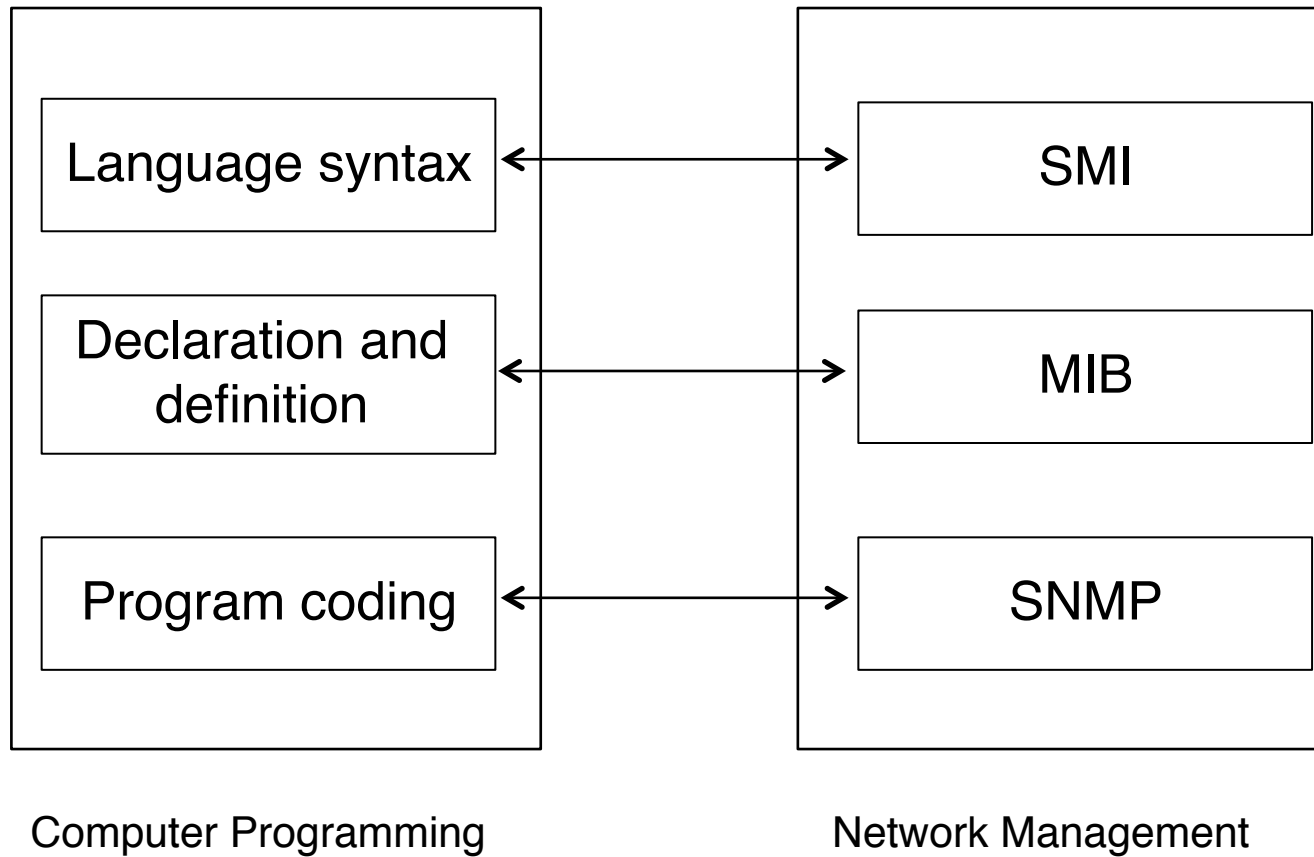
- Basic ideas for management with SNMP
 - “client pull” model
 - Each agent (server) keeps performance information in a database.
 - A manager (client) “pulls” data from the agent
 - A manager forces an agent to perform a task by resetting values in the agent database
 - “server push” model
 - An agent (server) “pushes” out a trap message to the manager process (client) by warning the manager of an unusual situation

Management Components



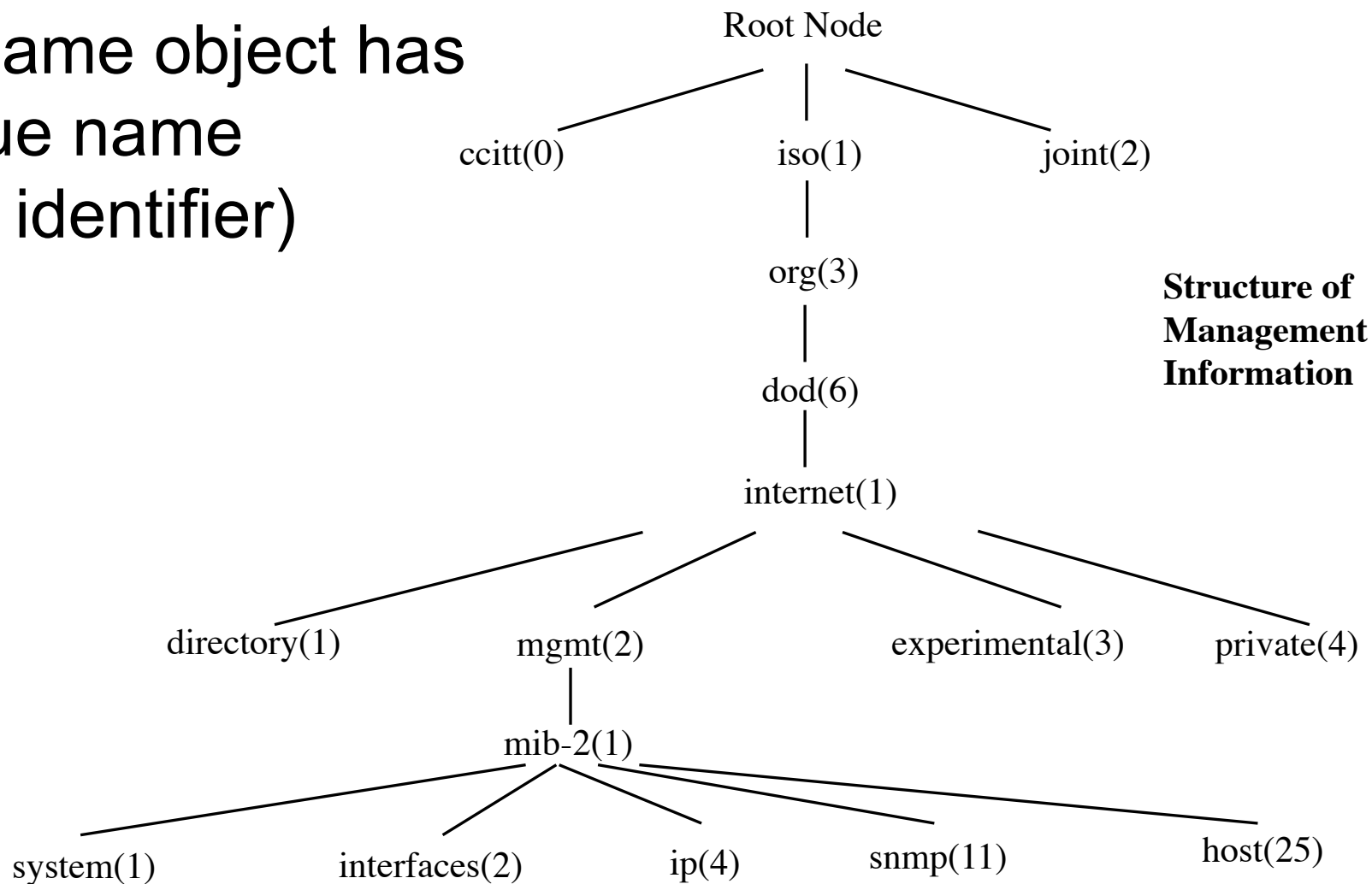
- **SMI (Structure of Management Information)**
 - Defines rules for naming objects, defining object types, and showing how to encode objects and values
- **MIB (Management Information Base)**
 - Creates a collection of named objects, their types, and their relationship to each other
- **SNMP**
 - Defines the format of packets exchanged between a manager and an agent
 - It reads and changes the status of objects in SNMP packets

An Analogy



SMI Tree

- Each name object has a unique name (object identifier)



Tree Pointing (OIDs)

- Each object can be defined using a sequence of integers separated by dots (used in SNMP)
- Each object can also be defined using a sequence of textual names separated by dots (used by people)

iso.org.dod.internet.mgmt.mib-2 <--> 1.3.6.1.2.1

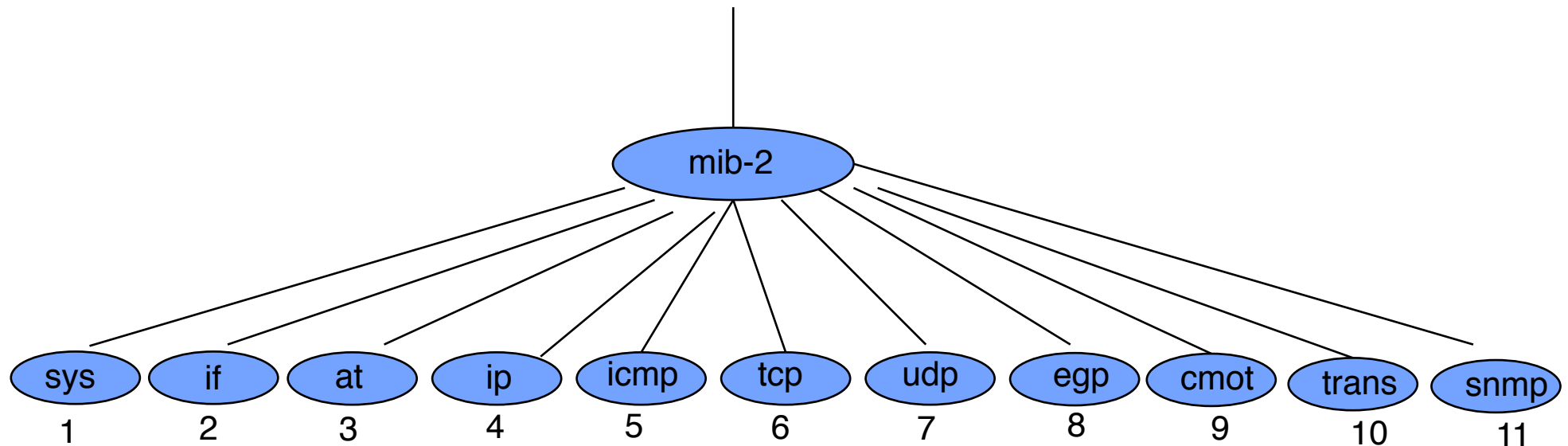
- The objects that are used in SNMP are located under the mib-2 object. So their identifiers always start with 1.3.6.1.2.1

Object Data Types

- Simple data types
 - INTEGER, OCTET STRING, IPAddress, Counter32, TimeTicks, ...
- Structured type
 - **Sequence**: a combination of simple data types, not necessarily of the same type, Similar to a struct in C.
 - **Sequence of**: a combination of simple data types all of the same type or a combination of sequence data types all of the same type. Similar to an array in C.

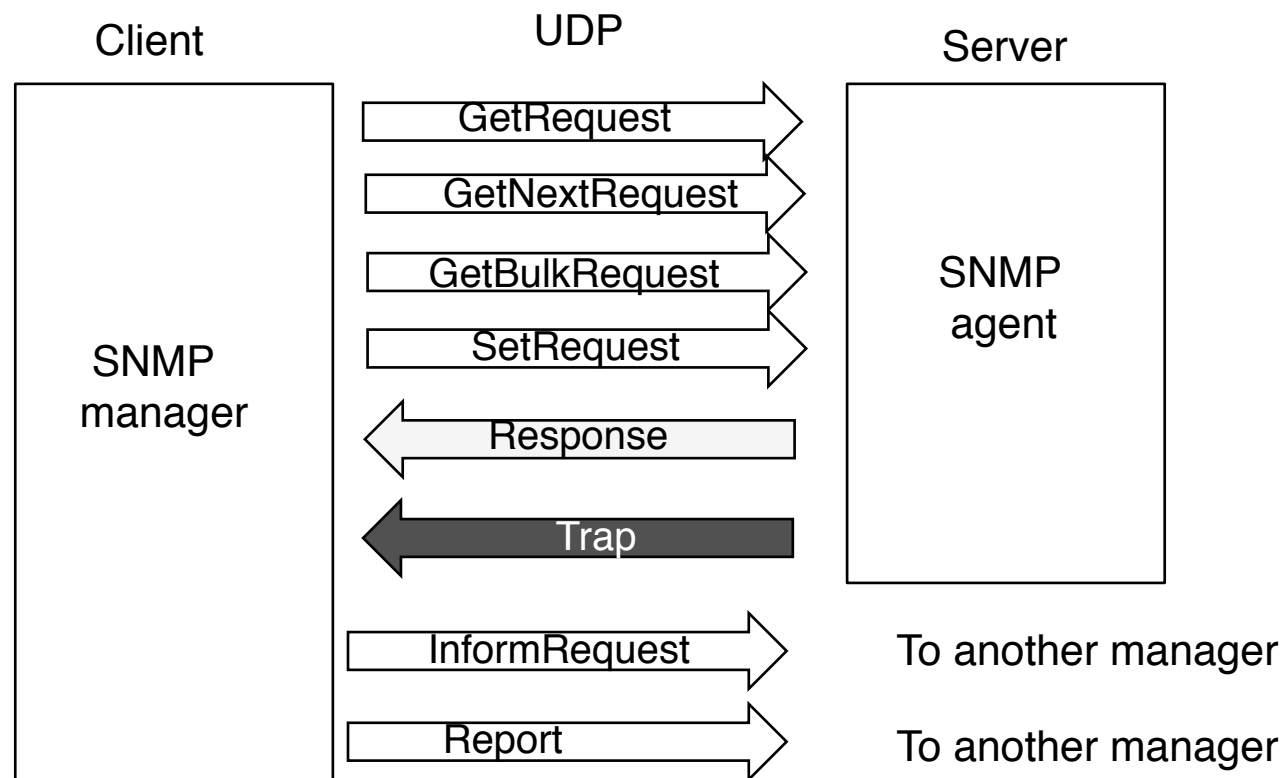
MIB

- Each agent has its own MIB, which is a collection of all the objects that the manager can manage
- The objects in MIB are categorized into several groups



SNMP

- Uses both SMI and MIB
- Uses UDP protocol on port 161 (agent) and port 162 (manager)
- Defines eight types of protocol data units

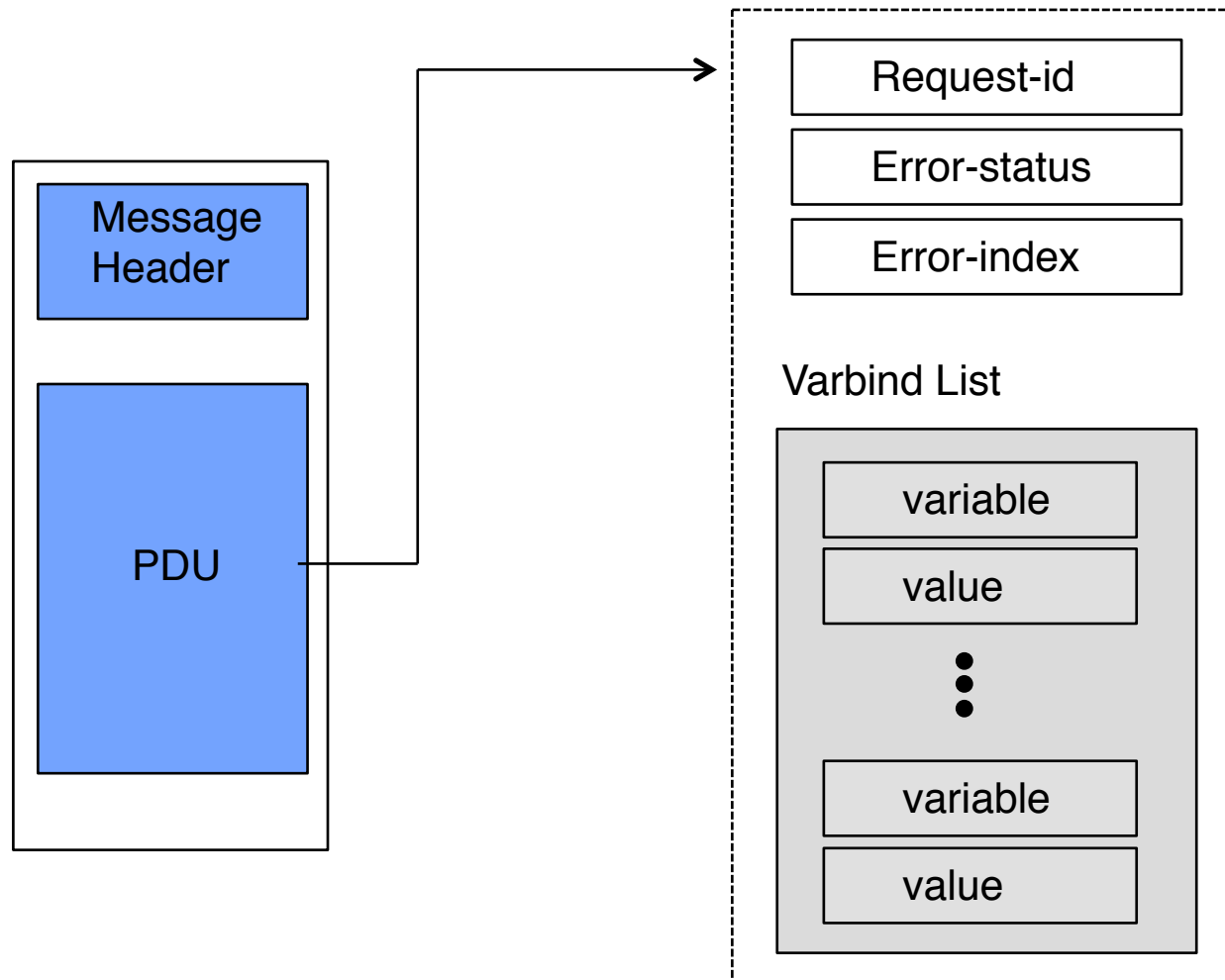


Trap

- Asynchronous notification from agent to network management station
 - When an interface changes state (up/down/testing)
 - Some threshold is exceeded (e.g error rate)
 - Authentication failure

Can we trust SNMP Trap?

SNMP Message

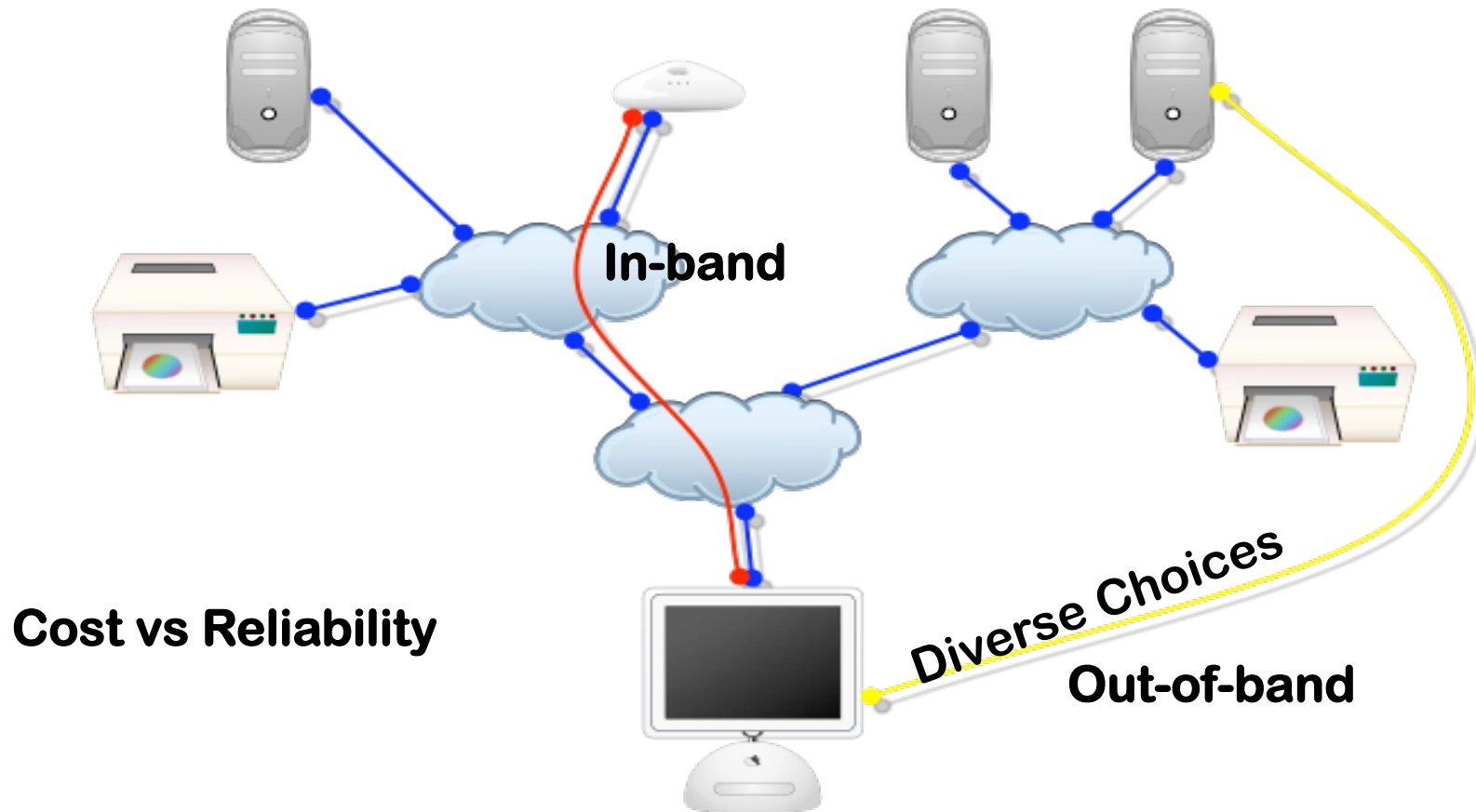


SNMP Versions

- **Version 1**
 - Very simple
 - No encryption.
- **Version 2**
 - Introduced bulk operations
 - Still no encryption
- **Version 3**
 - No changes to the protocol
 - Primarily added security and remote configuration enhancements
 - Changed architecture to user/view based access control with payload encryption.

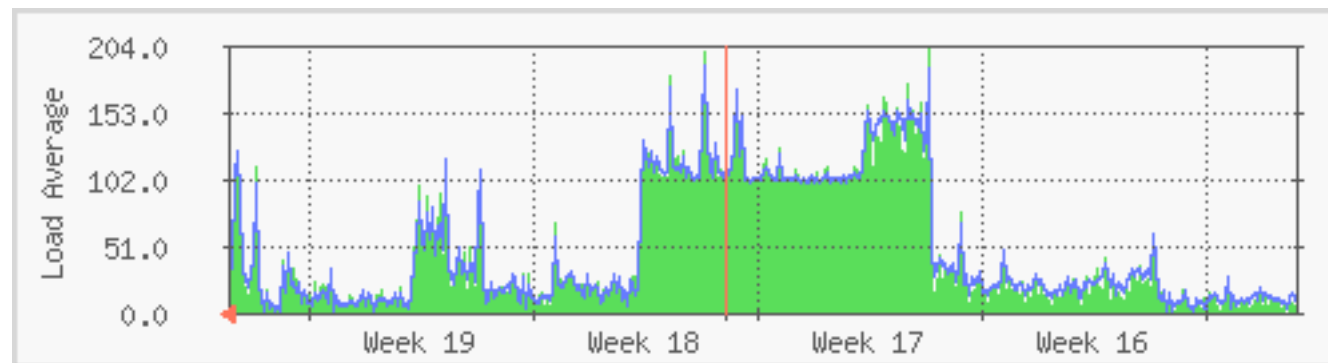
NMS Architecture

- In-band or Out-of-band?
 - *Failover?*
 - *Cost?*

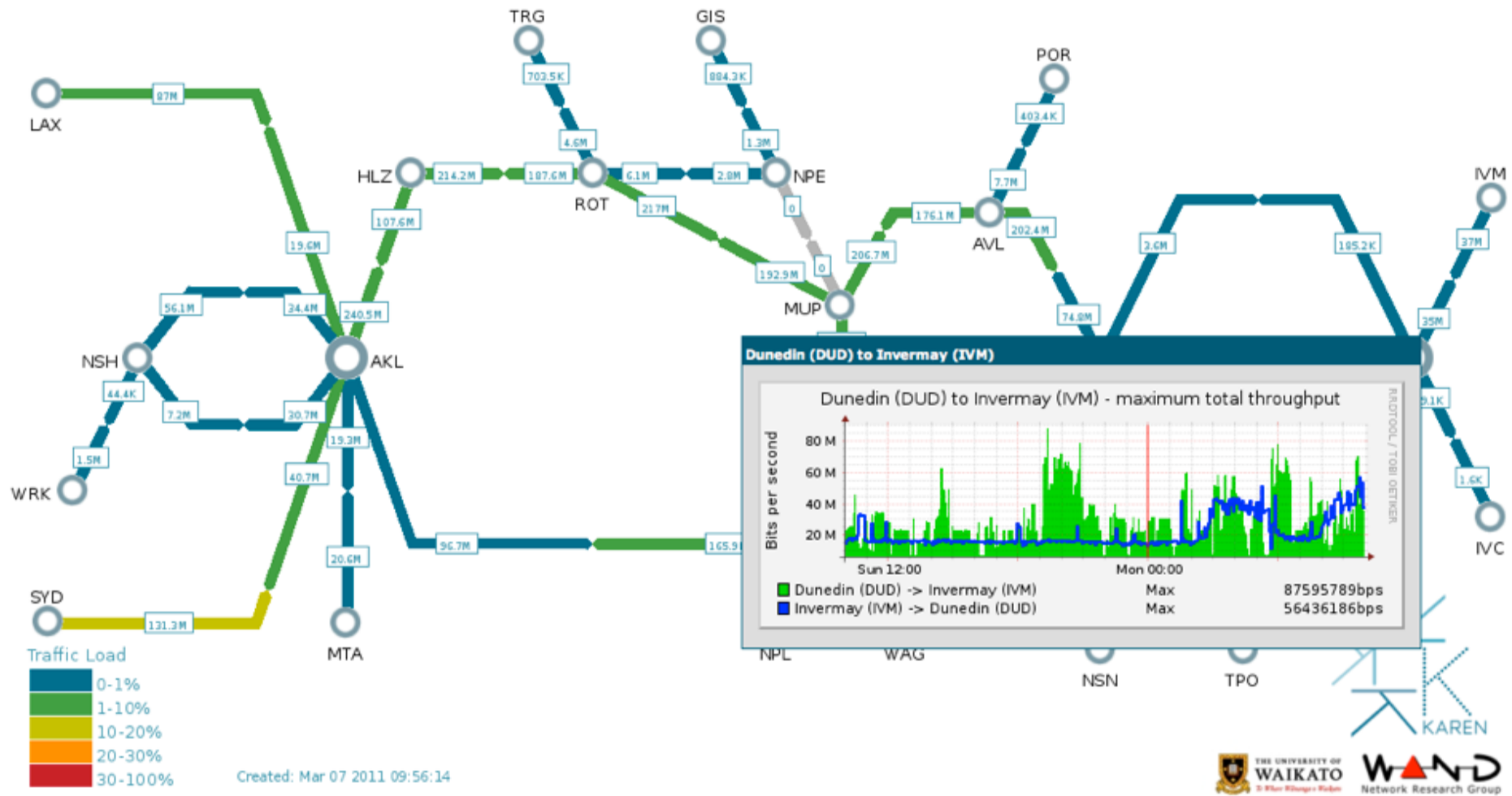


NMS Applications

- **NMS Suites**
 - database storage, visualization, alerts, trend analysis
- **Element managers**
 - generally configuration software that comes with the device, e.g. network printer admin utility
- **Trend analysis**
 - graphs, forecasting, weather maps



Example (PHP Weathermap)



Live KAREN Weathermap

Summary

- What is SNMP? How many ways to collect information? Push, pull, trap
- What is NMS (Network Management System)?
 - An application for managing network components and network trend analysis.
 - Based on SNMP