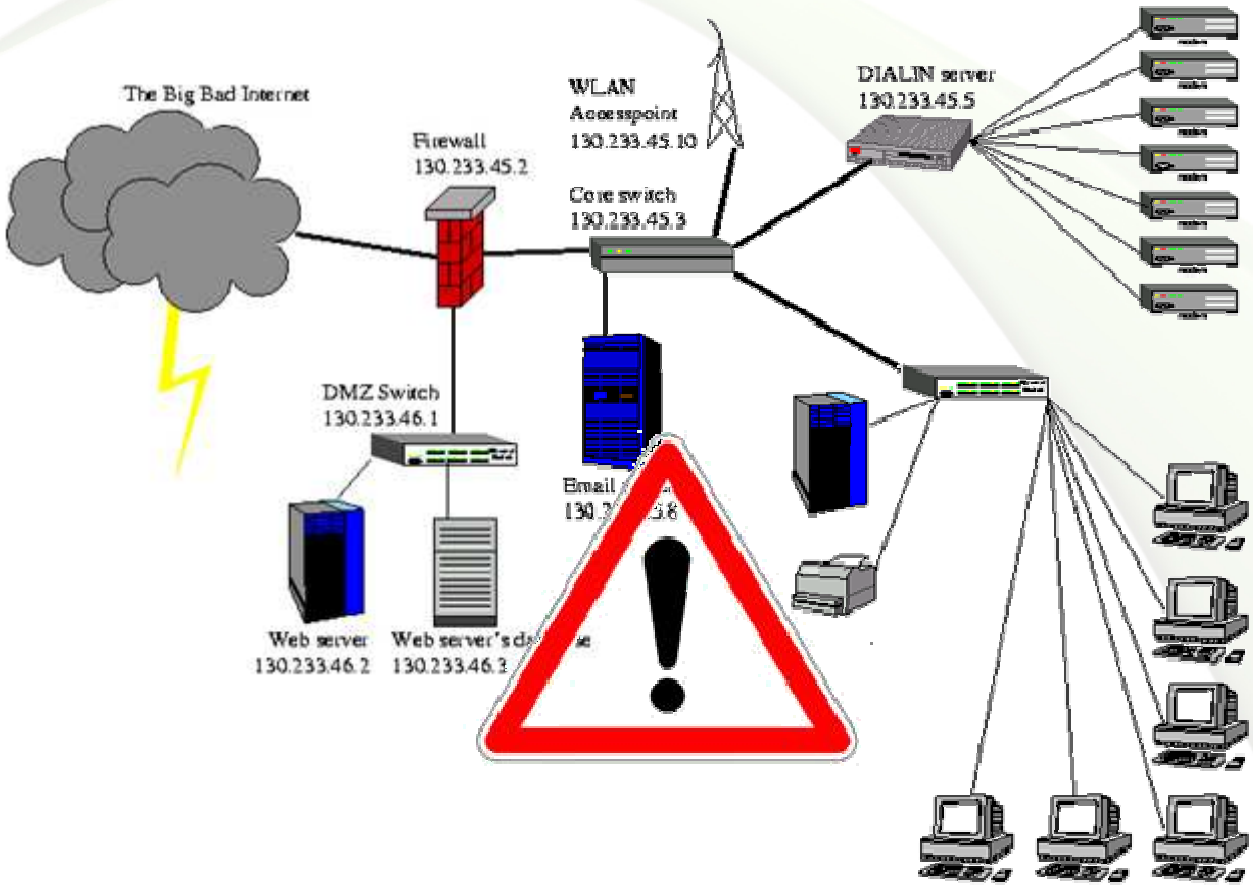
esprit
Ecole Supérieure Privée d'Ingénierie et de Technologies

Network Management & SNMP

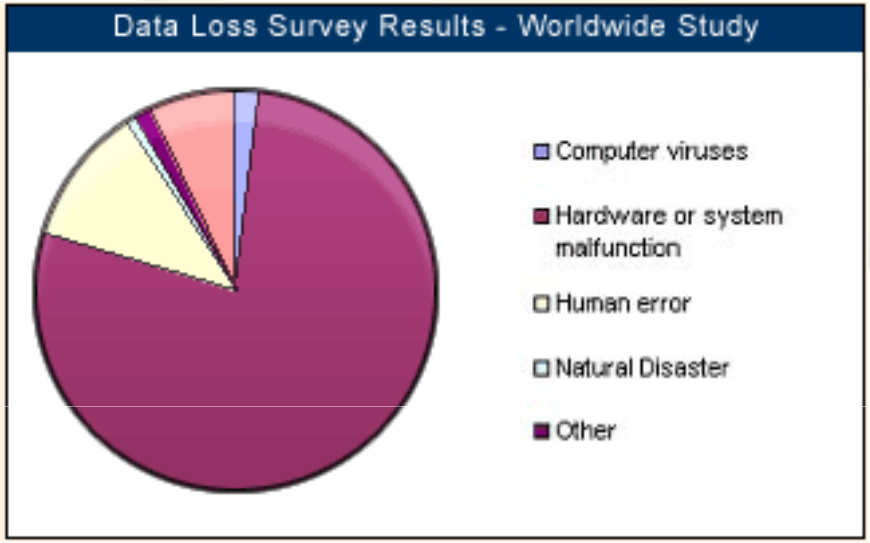
Elaborated by:
Mrs Hana BOUAFIF

Academic Year: 2009/2010

The enterprise Network



Data Loss Statistics - How much will data loss affect your business?



(Source: http://www.rbs2000.com)

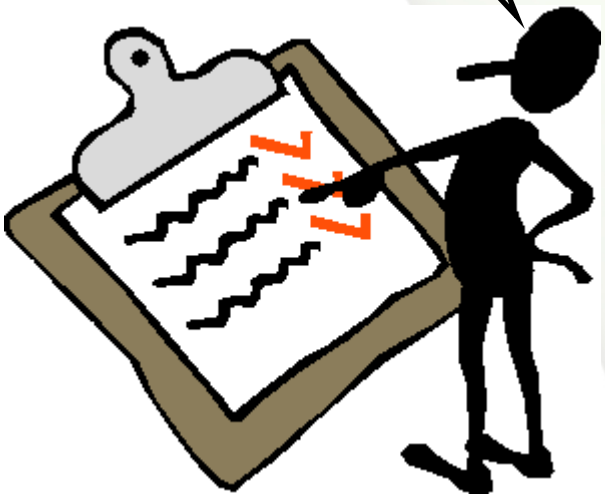
- The average company spends between $100,000 and $1,000,000 in total ramifications per year for desktop-oriented disasters (both hard and soft costs.) (Source: 7th Annual ICSA Lab's Virus Prevalence Survey, March 2002)
- Americanbusiness lost more than $7.6 billion as a result of viruses during first six months of 1999. (Research by Computer Economics)

Network & Business

Our networks are surrounded by threats, this will lead to **downtime**, **loss of data**
We shall then ensure the **availability** of our networks!!

Network administrator (anxious and desperate)

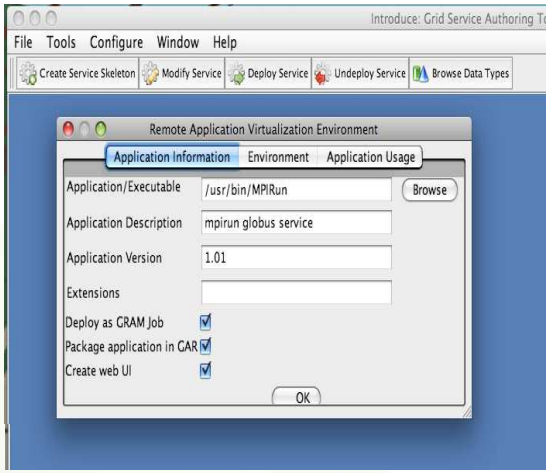
✓Our network has become evolving!!
✓Our credibility is decreasing though
✓ I'm really worried about my **BUSINESS**!!



Boss (not satisfied)

The enterprise points of failure (1)

Employees



Application / Informations

Lost productivity and missed deadlines.

☹

The enterprise points of failure (2)

Customers

Transactions online

Lost revenues and damaged credibility ☹

The enterprise points of failure (3)

No collaboration / No communication

It harms the relationship and affects their goals.

☹

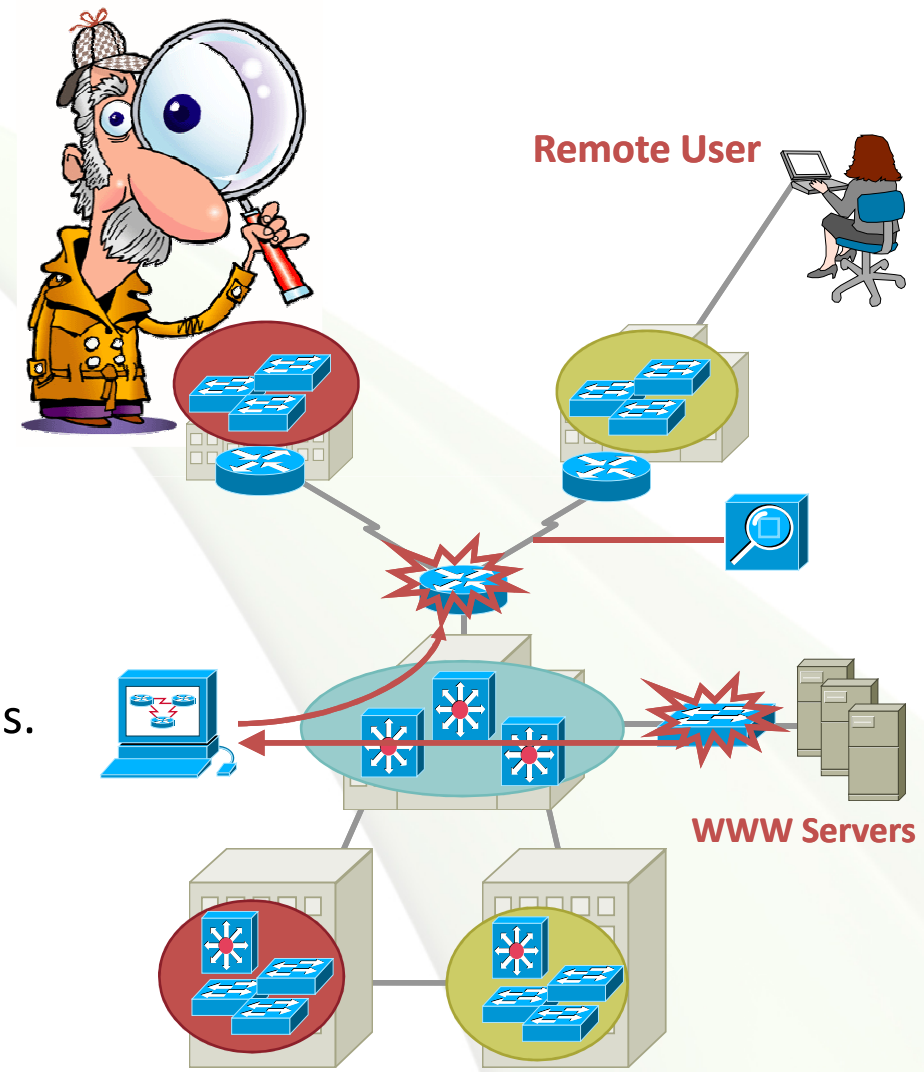
Network Monitoring & Control

Network monitoring :

- Real-time alerts,
- Historical information,
- Performance ,
- Device, application, and data status.

Network Control:

- Security
- Configuration



Solution : Network management

Network Management

Network Monitoring

Network Control

- Configuration Management
- Performance Management
- Fault Management
- Accounting Management
- Security Management

Outline

- Functional Areas of Network Management
- Network Management Architecture
- Network Management Protocols
- SNMP Protocol
- Demonstration
- Conclusion

Functional Areas of Network Management
Network monitoring

- **Performance Management** :

  Indicators : Availability, Response Time, Accuracy, Throughput, Utilization…

- **Fault Management :**
  - Detect the fault
  - Determine exactly where the fault is
  - Isolate the rest of the network from the failure so that it can continue to function
  - Reconfigure or modify the network in such a way as to minimize the impact
  - Repair or replace the failed components

  – Tests: connectivity, data integrity, response-time, ….

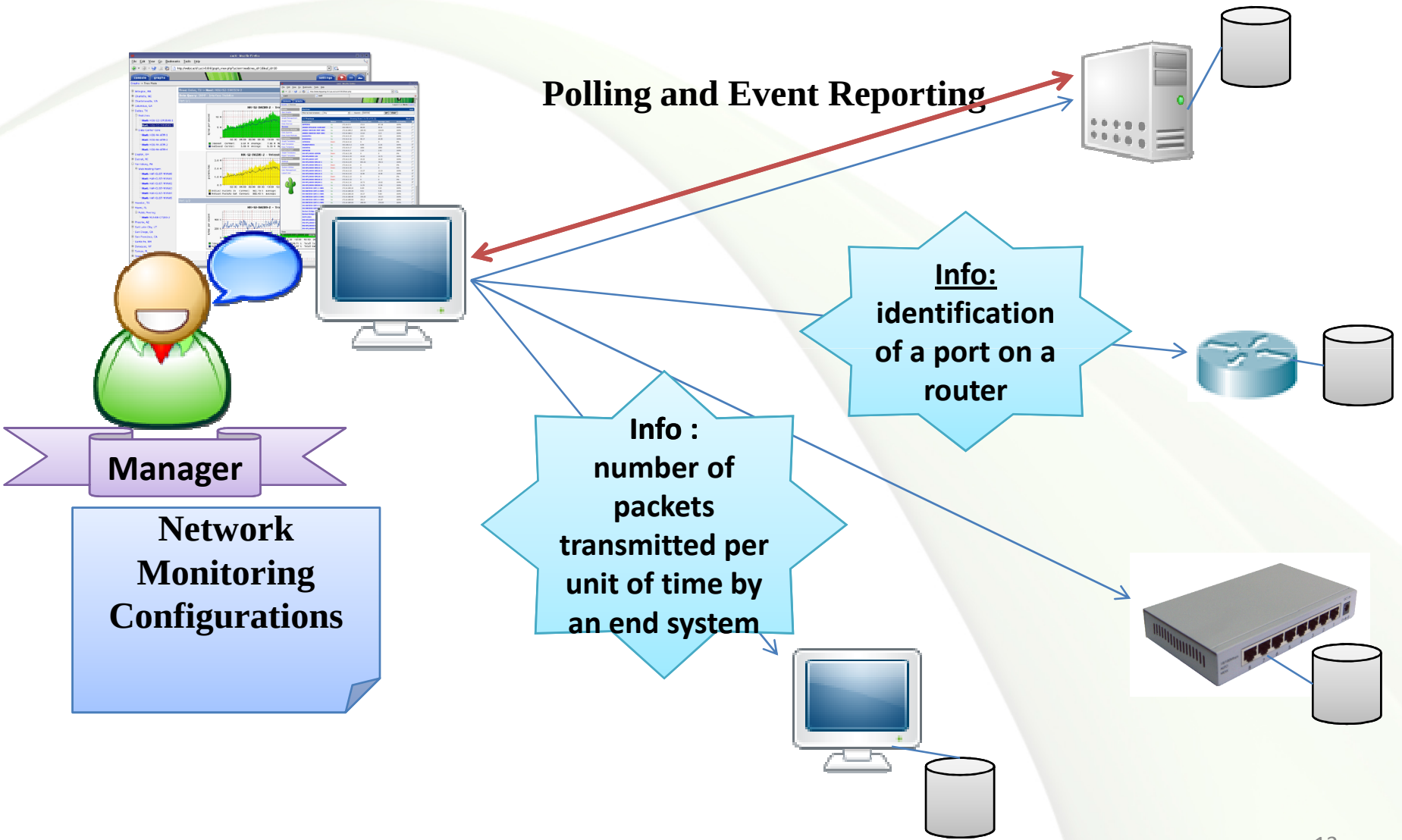
- **Accounting Management :**
  – Keeping the track of the usage of the network resources by the users.
  – Indicators: CPU , Memory , Bandwidh, disk space …

Functional Areas of Network Management
Network control

- **Security Management:**
  - Security services: generating, distributing, storing of encryption keys for services
  - Exception alarm generation, detection of problems
  - Backups, data security
  - Security logging

- **Configuration Management:**
  - Installation of new hardware/software
  - Tracking changes in control configuration
  - Change management
  - Configuration audit

Network Management Architecture



Network Management Protocols

- ***1987 :***OSI approach:
  - **CMIP** - common management information protocol, and **CMOT** (CMIP over TCP)
  - **CMIS** - common management information service (user interface)

- ***1989 :***Internet approach: **SNMP** Simple Network Management Protocol

SNMP protocol

- SNMP is an IETF application layer protocol that facilitates the exchange of management information between network devices.

- **SNMPv1** : RFC 1155 1156 1157 (1990)
  - Very simple protocol
    - Easy to implant
    - Simple messages
    - Little additional cost

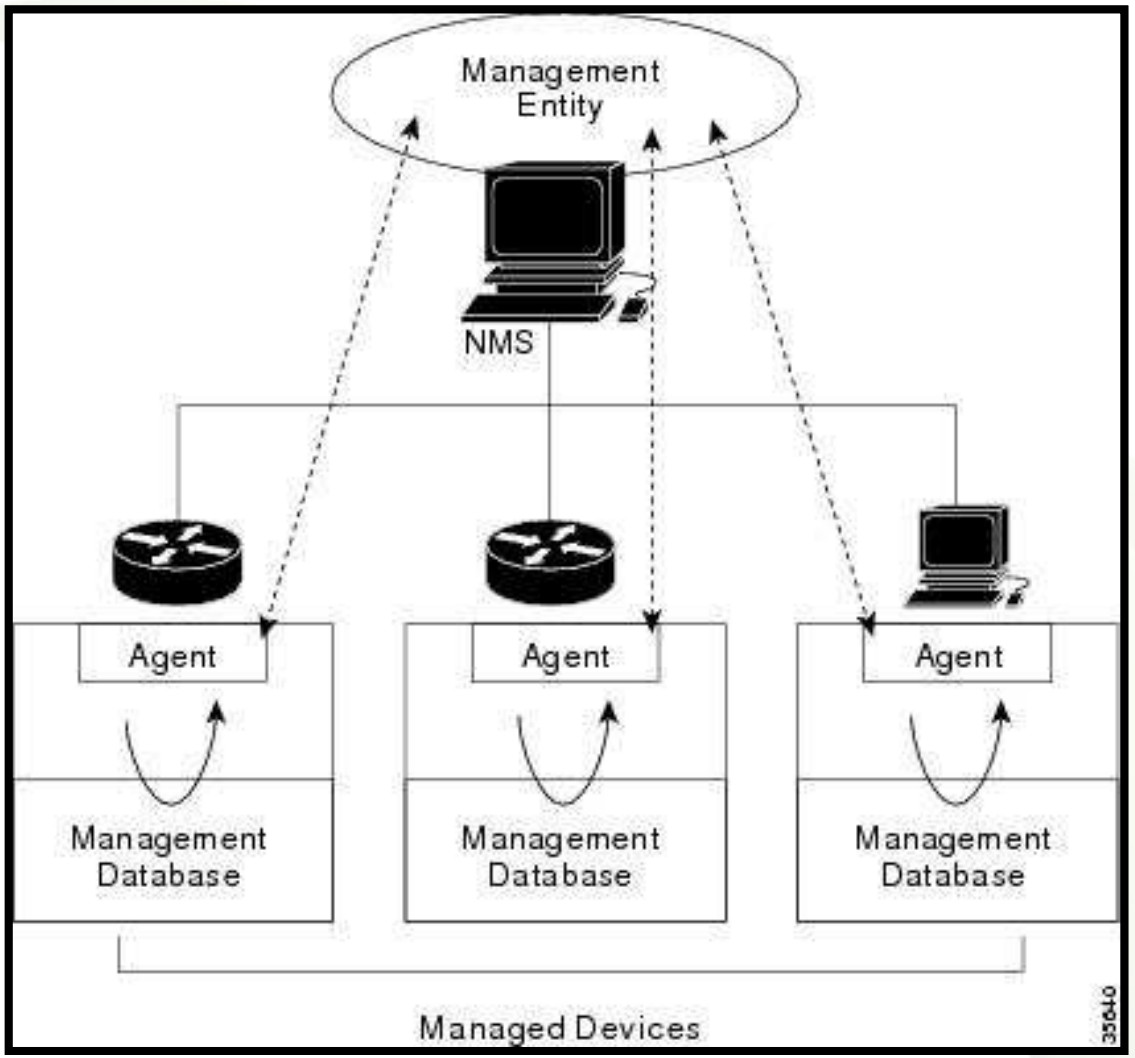
- **SNMPv2** : RFC 1902 1903 1904 1905 1906 1907 (1996)
  - Structure of Management Information – (MIBs).
  - Protocol operations.
  - Security : Access Control Polic y

- **SNMPv3** : RFC 3411, 3412, 3413, 3414, 3415, 3416, 3417, 3418 (2002)
  - Add security: authentication, Integrity and Confidentiality of data

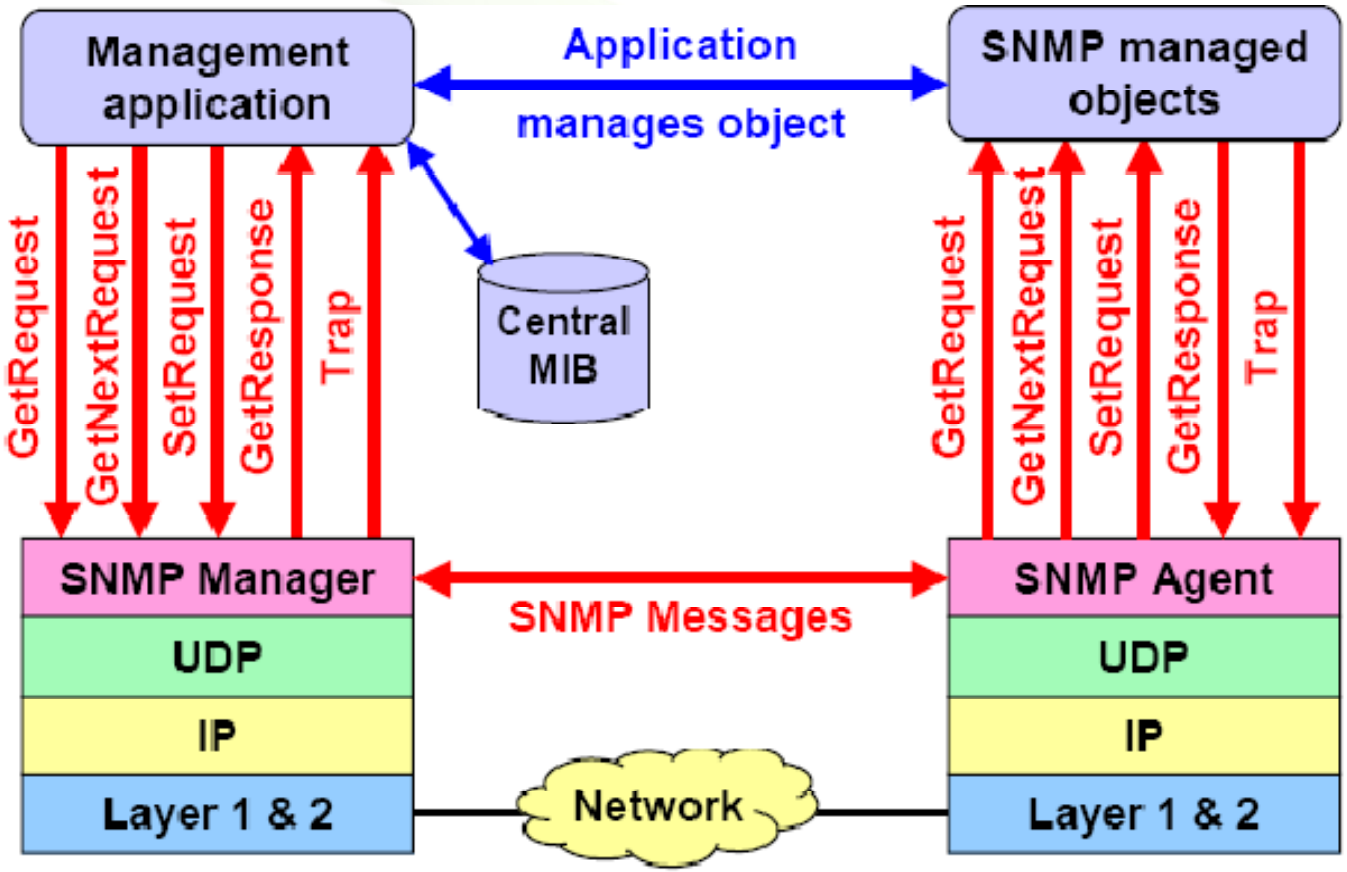
Basic Components of SNMP

- **NMS (Network Management Station)**
  - Run applications that monitor and control managed devices. NMS provide resources required for network management
- **Managed Devices**
  - Contain an SNMP agent and reside on a managed network.
  - Collect and store management information and make it available to NMS by using SNMP.
  - Include routers, access servers, switches, bridges, hubs, hosts, or printers.
- **Agents**
  - A network-management software module, that resides in a managed device. An agent has local knowledge of management information and makes that information available by using SNMP.
- **MIB (Management Information Base)**

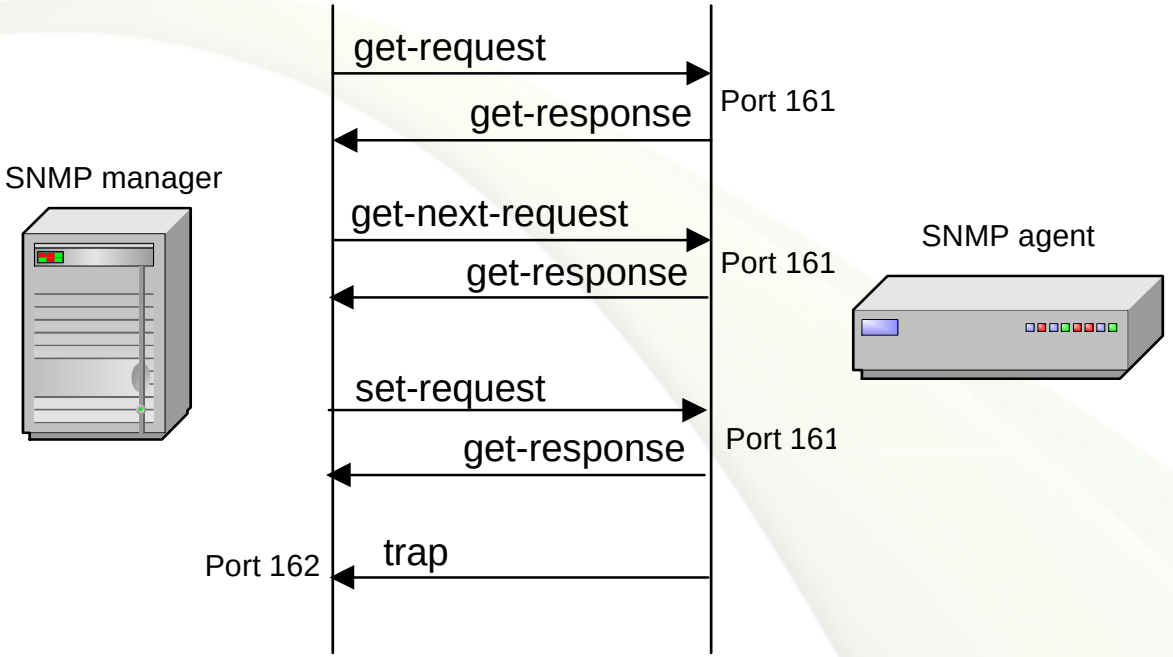
An SNMP-Managed Network



Network Level Architecture



SNMP Messages



- **GetRequest**: request values of variables from device
- **GetNextRequest**: request value of variable following the one supplied
- **GetResponse**: return values
- **SetRequest**: instruct device to set values of variables
- **Trap**: from device - notify monitor / manager of value change

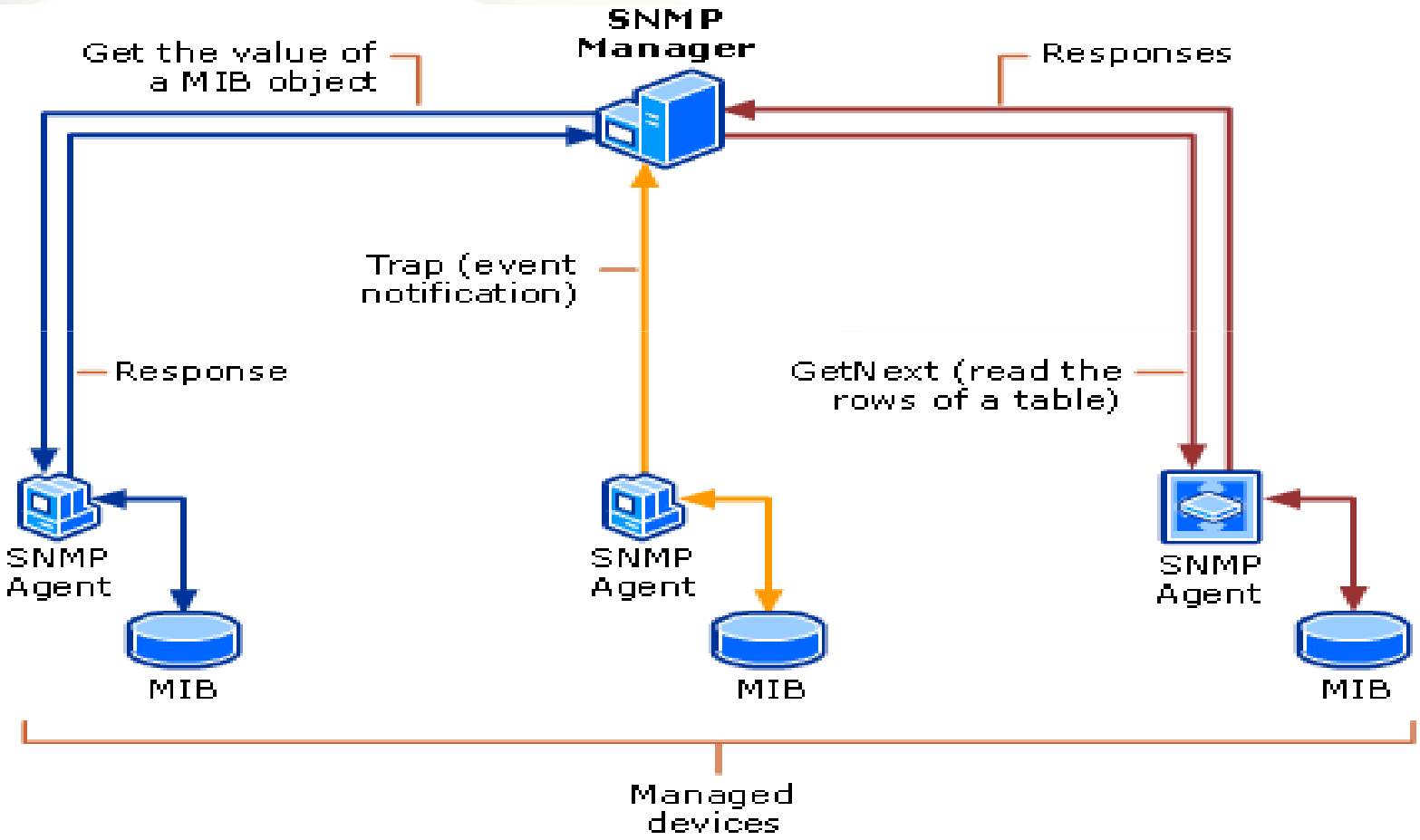
Ports & UDP

- SNMP uses User Datagram Protocol (UDP) as the transport mechanism for SNMP messages

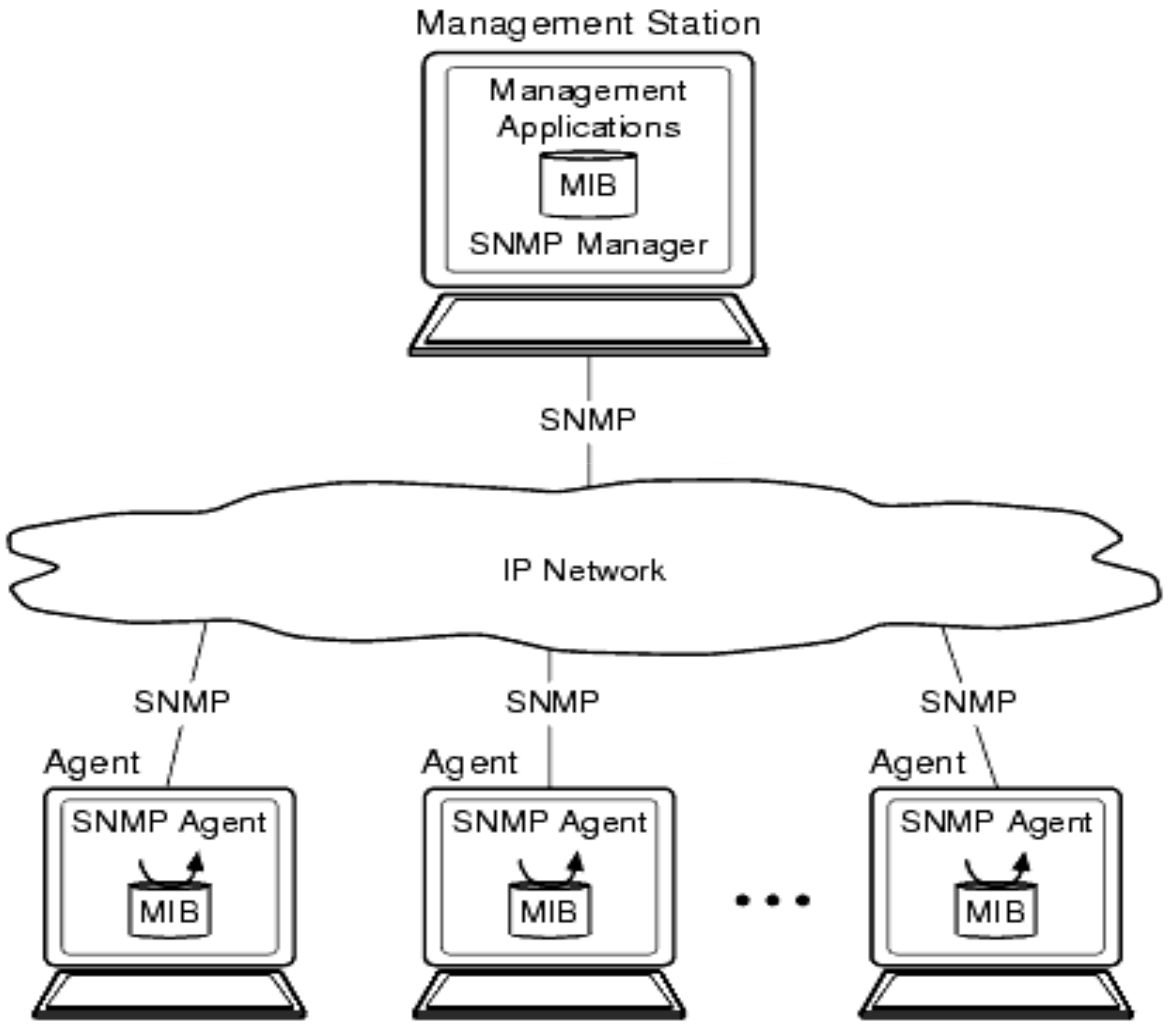
SNMP uses two well-known ports to operate:

- **UDP/TCP Port 161** – SNMP Request/Response Messages
- **UDP/TCP Port 162** - SNMP Trap Messages

Messages exchanging scenario



Management Information Base



MIB Structure

- Every management station or an agent in an SNMP architecture maintains a local database having information related to the network management.
- This virtual information store is called MIB- objects database
- An SNMP MIB contains definitions and information about the properties of managed resources and the services that the agents support. The manageable features of resources, as defined in an SNMP MIB, are called managed objects

Managed objects

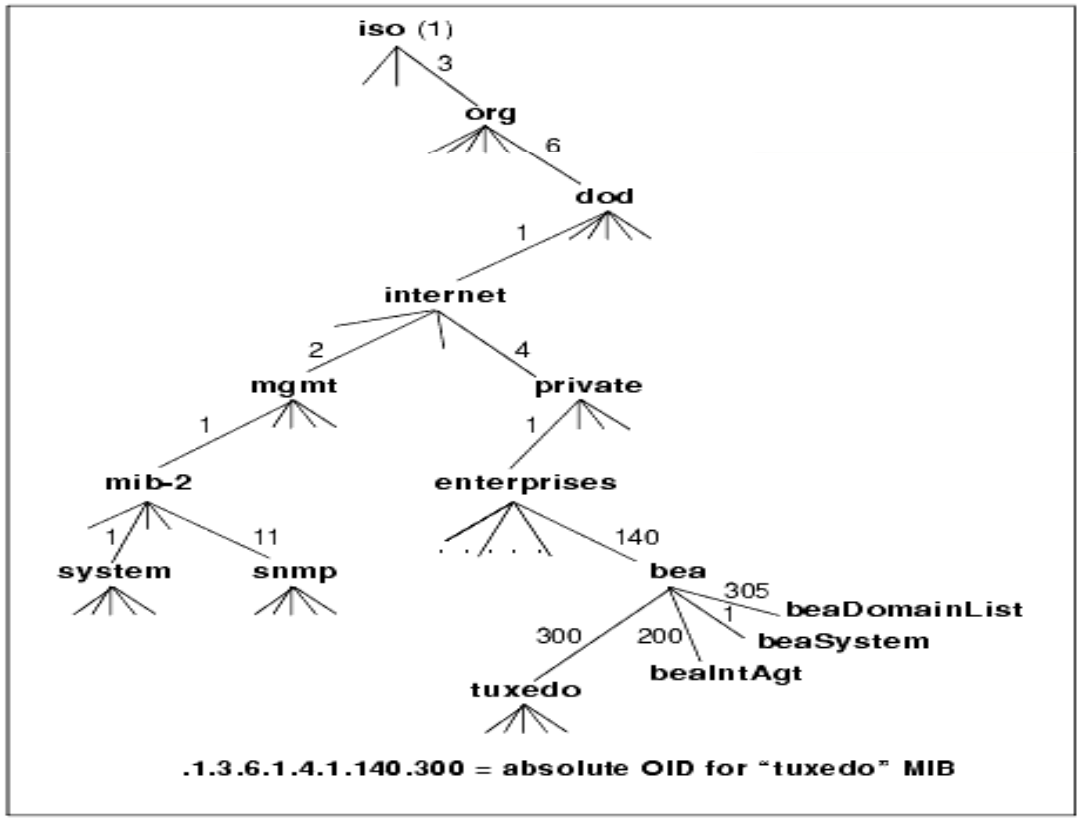
- Each managed object is assigned an *object identifier (OID)*
- The OID is specified in a MIB file.

- An OID can be represented as a sequence of integers separated by decimal points or by a text string:

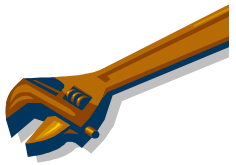
  Example:
  - *1.3.6.1.2.1.4.6.*
  - i*so.org.dod.internet.mgmt.mib-2.ip.ipForwDatagrams*

Object Identifier

- Object Identifier (OID):
  - Global identifier for a particular object type.
  - An OID consists of a sequence of integers, which specify the position of the object in the global object identifier tree.



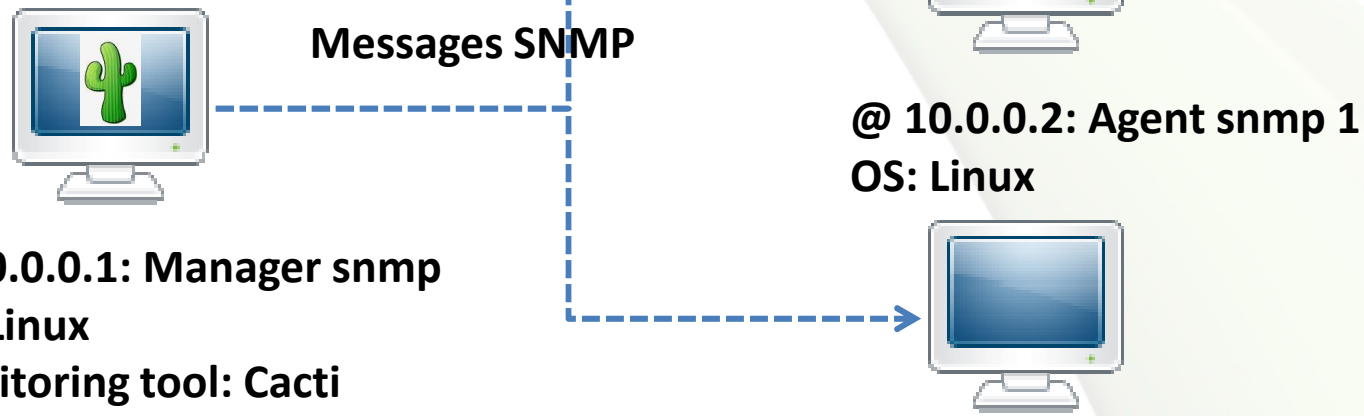
Network Management Tools



- Health status of the network.
- It provides information about collected data and the analysis of such raw data with a view to using scarce or limited resources effectively.
- Examples:
    - HP OpenView
    - SunNet Manager
    - Ciscoworks
    - Nagios
    - cacti

Demonstration

- Management Entity :MIB browser
- Monitoring tool: Cacti



Conclusion

- Your network is your business.
- Network management helps you to stay in business.
- SNMP is a standard protocol that has wide acceptance in the industry and is flexible enough to describe almost anything.
- The network monitoring application should be easy to use, quick to deploy, a proven solution that you can depend on to have an available network.

References

- http://www.dpstele.com
- http://www.debuntu.org
- http://www.commentcamarche.net
- http://en.wikipedia.org/wiki/SNMP

Thank for your attention

“Looking at one map and knowing it represents every piece of equipment you're monitoring in the field… that's pretty good peace of mind."