Chapter 6.2:
Network Management

NGUYỄN CAO ĐẠT
E-mail:dat@hcmut.edu.vn

Outline

- Network Management Standards
- Network Management Configuration
- Network Operations Center (NOC)

Network Management Standards

- Simple Network Management Protocol
  - SNMP V1, V2, V3
- OSI Model
  - Object-based approach
- TMN Model
  - Just a framework for network management systems
- Web-based Approach

Simple Network Management Protocol

- SNMP
- Application-level protocol
- Part of TCP/IP protocol suite
- Runs over UDP
- From management station, three types of SNMP messages issued
  - GetRequest, GetNextRequest, and SetRequest
  - Port 161
- Agent replies with GetResponse
- Agent may issue trap message in response to event that affects MIB and underlying managed
  - Port 162

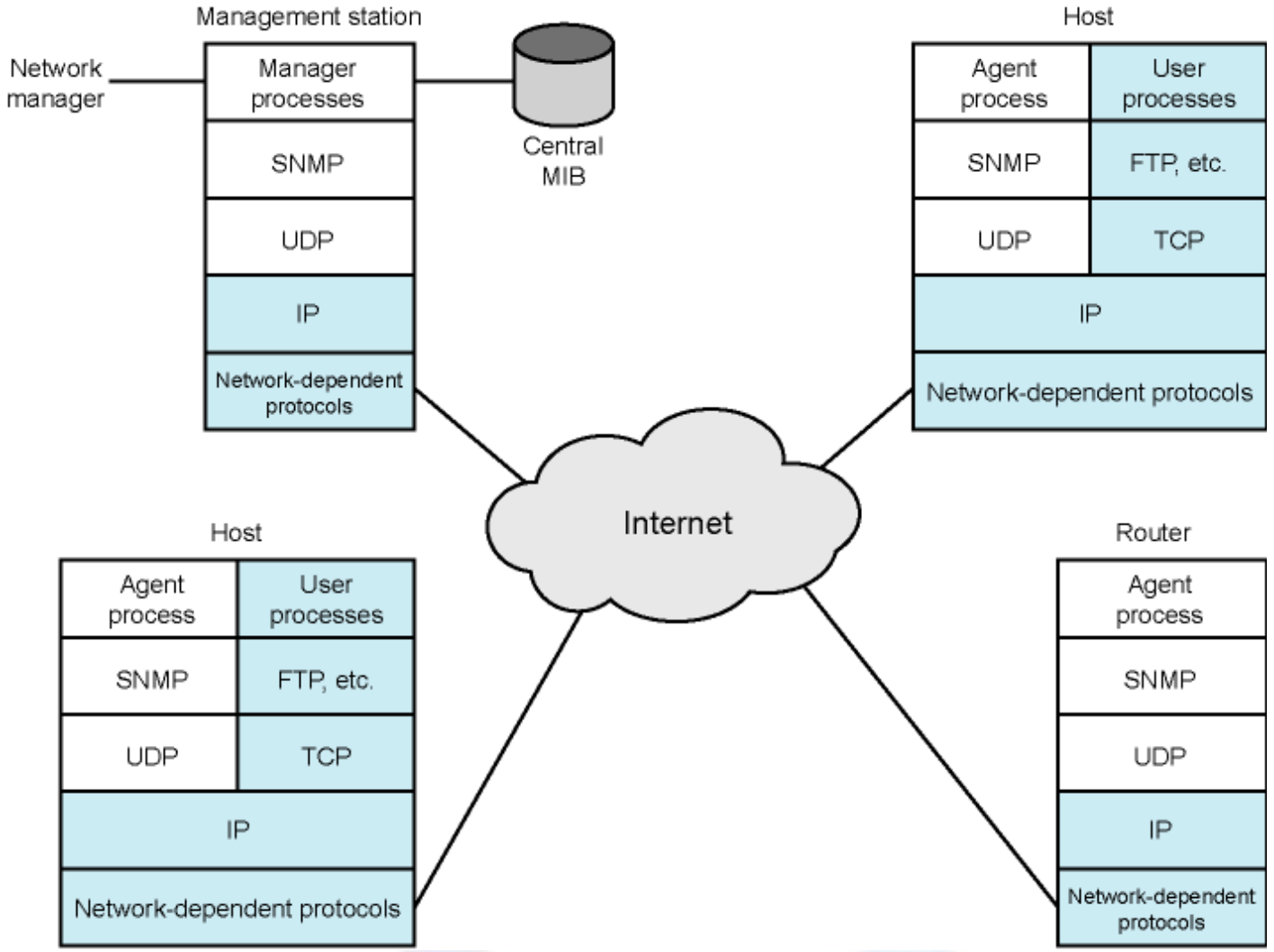
SNMP

- Management Information Base (MIB)
  - Virtual Information Store of MOs
  - Information are stored at MOs using different approaches
  - MIB II added a number of useful variables
- Structure of Management Information (SMI)
  - Framework fot the Definition of SNMP MIBs
  - Object Information Model for Network Management
  - Formal Description of the Structure are Given Using a Subset of ASN.1
- Abstract Syntax Notation 1 (ASN.1)
  - A Standard Object Definition Language
  - A Standard Way to Encode Objects for Transfer Over a Network
  - It's Large,Complex,and not Especially Efficient

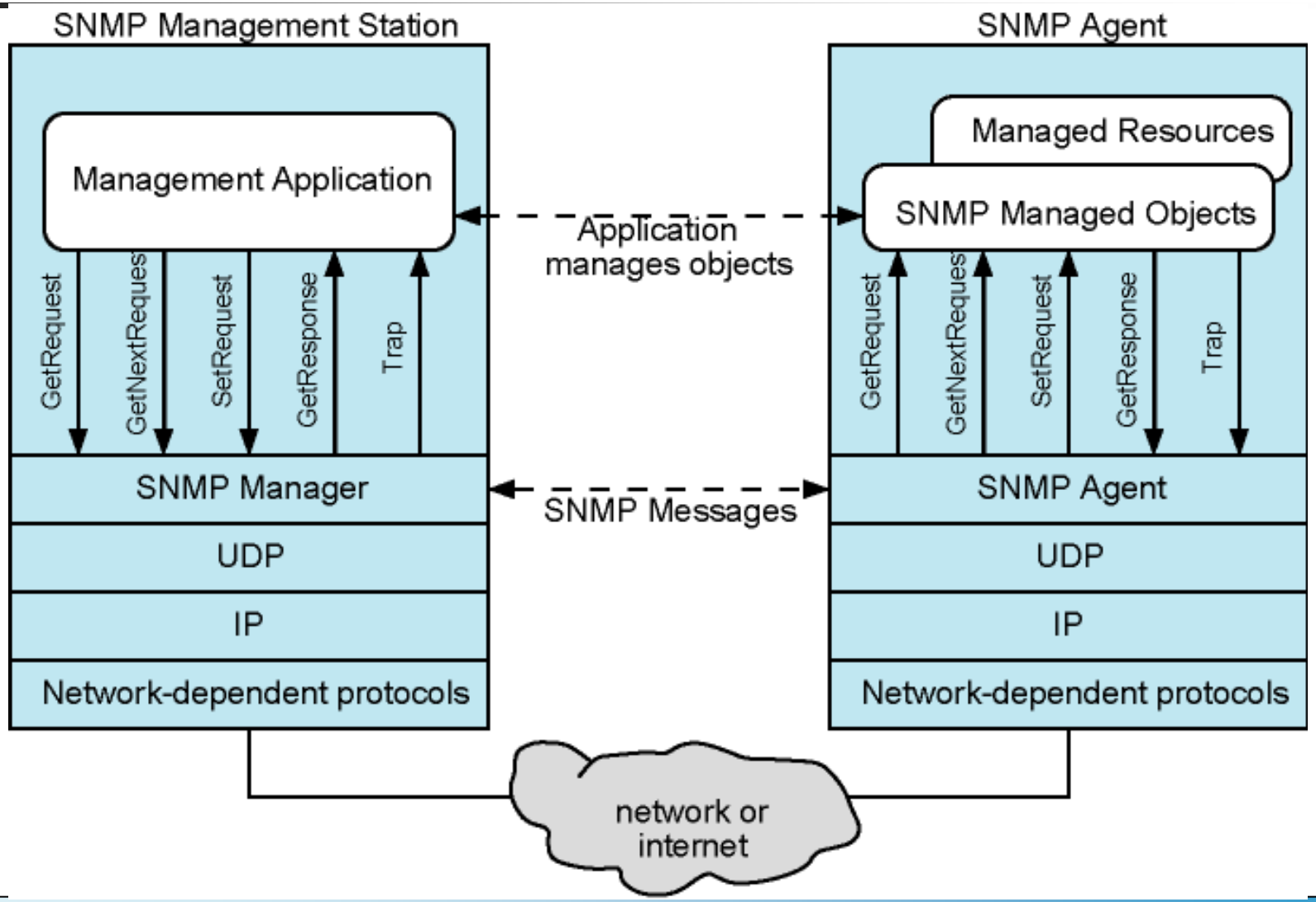
SNMP v1

- August 1988 SNMP specification issued
- Stand alone management stations and bridges, routers workstations etc supplied with agents
- Defines limited, easily implemented MIB of scalar variables and two dimensional tables
- Streamlined protocol
- Limited functionality
- Lack of security
- SNMP v2 1993, revised 1996
  - RFC 1901-1908

SNMPv1 Configuration



The Role of SNMPv1



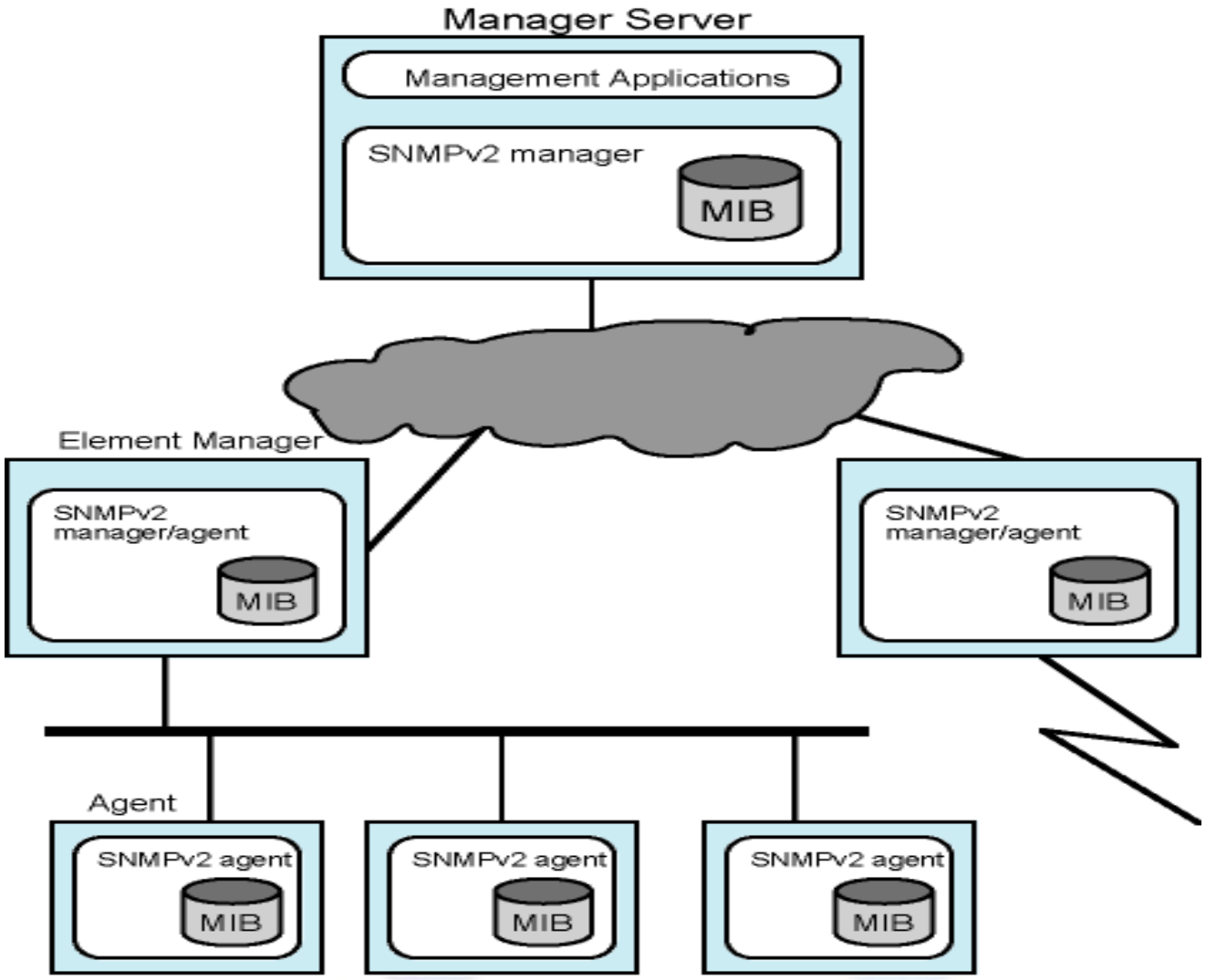
SNMP v2

- Framework on which network management applications can be built
  - e.g fault management, performance monitoring, accounting
- Protocol used to exchange management information
- Each player maintains local MIB
  - Structure defined in standard
- At least one system responsible for management
  - Houses management applications

SNPM v2

- Support central or distributed management
- In distributes system, some elements operate as manager and agent
- Exchanges use SNMP v2 protocol
  - Simple request/response protocol
  - Typically uses UDP
    - Ongoing reliable connection not required
    - Reduces management overhead

SNMPv2 Managed Configuration



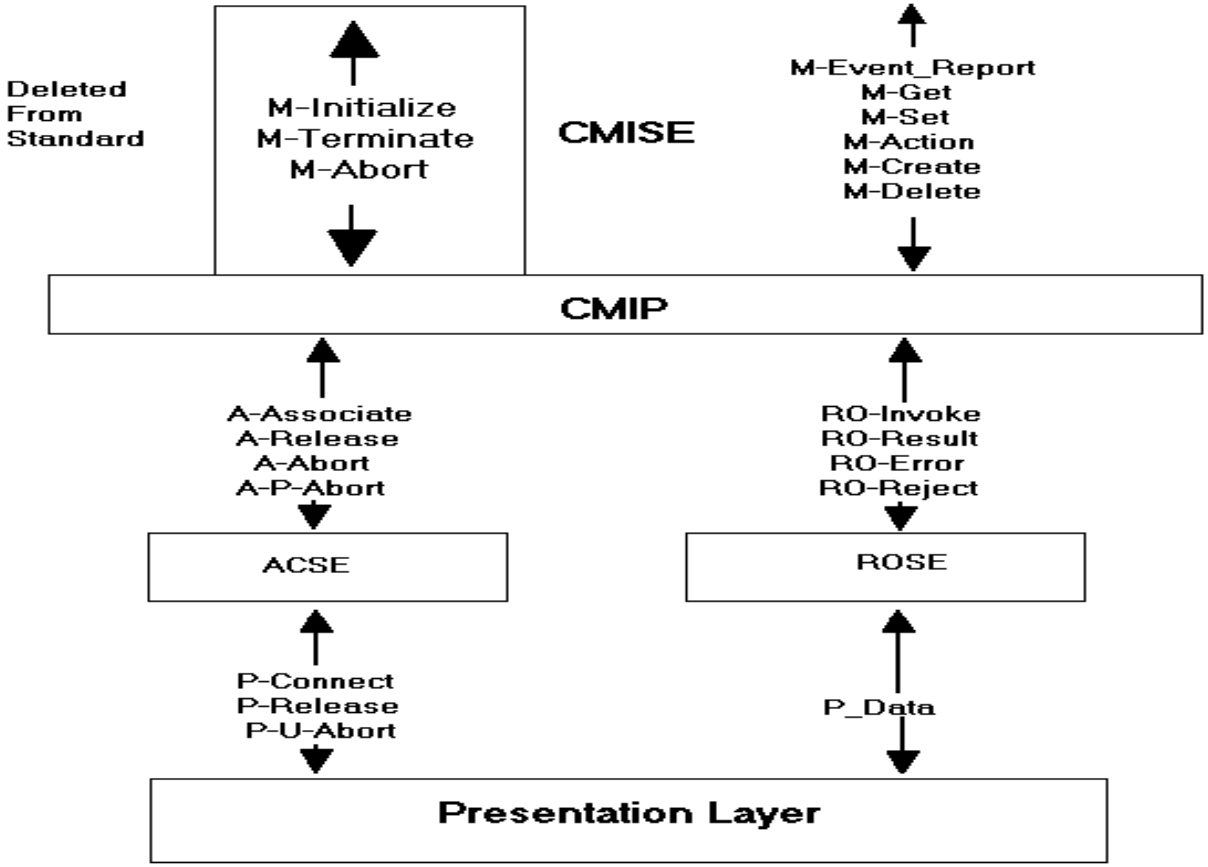
SNMP v3

- Addresses security issues of SNMP v1/2
- RFC 2570-2575
- Proposed standard January 1998
- Defines overall architecture and security capability
- To be used with SNMP v2

SNMP v3 Services

- Authentication
  - Part of User-Based Security (UBS)
  - Assures that message:
    - Came from identified source
    - Has not been altered
    - Has not been delayed or replayed
- Privacy
  - Encrypted messages using DES
- Access control
  - Can configure agents to provide a number of levels of access to MIB
  - Access to information
  - Limit operations

OSI Architecture



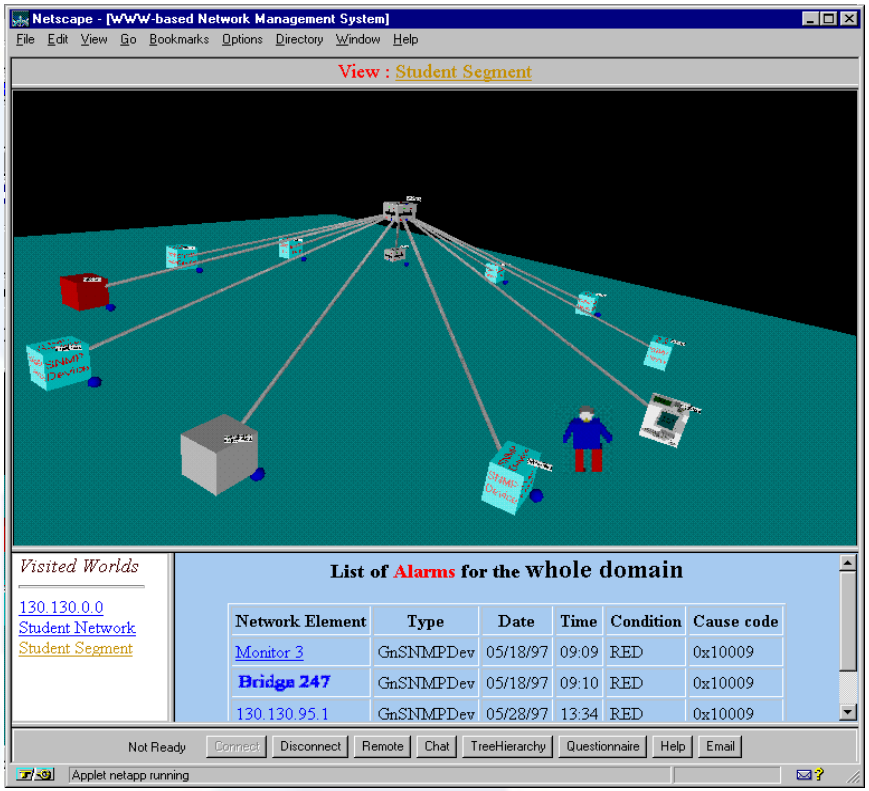
CMISE Service elements with ACSE and ROSE

Telecommunications Management Network

- An Important Framework for Management of Telecommunication Networks
- A Host of Management Functions and Communications
  - Operation
  - Administration
  - Maintenance
  - Provision
- Chosen By Telco's for Managing WANs
- Enables Communication between Operations System(OSs) and Network Elements(NEs) Via a Data Communications Network(DCN)
- Base for ATM network management

Web-based Approaches

- Using HTTP instead of SNMP
  - Web-Based Enterprise Management (WBEM)
  - Java Management API (JMAPI)
- Using Web as an Interface paradigm

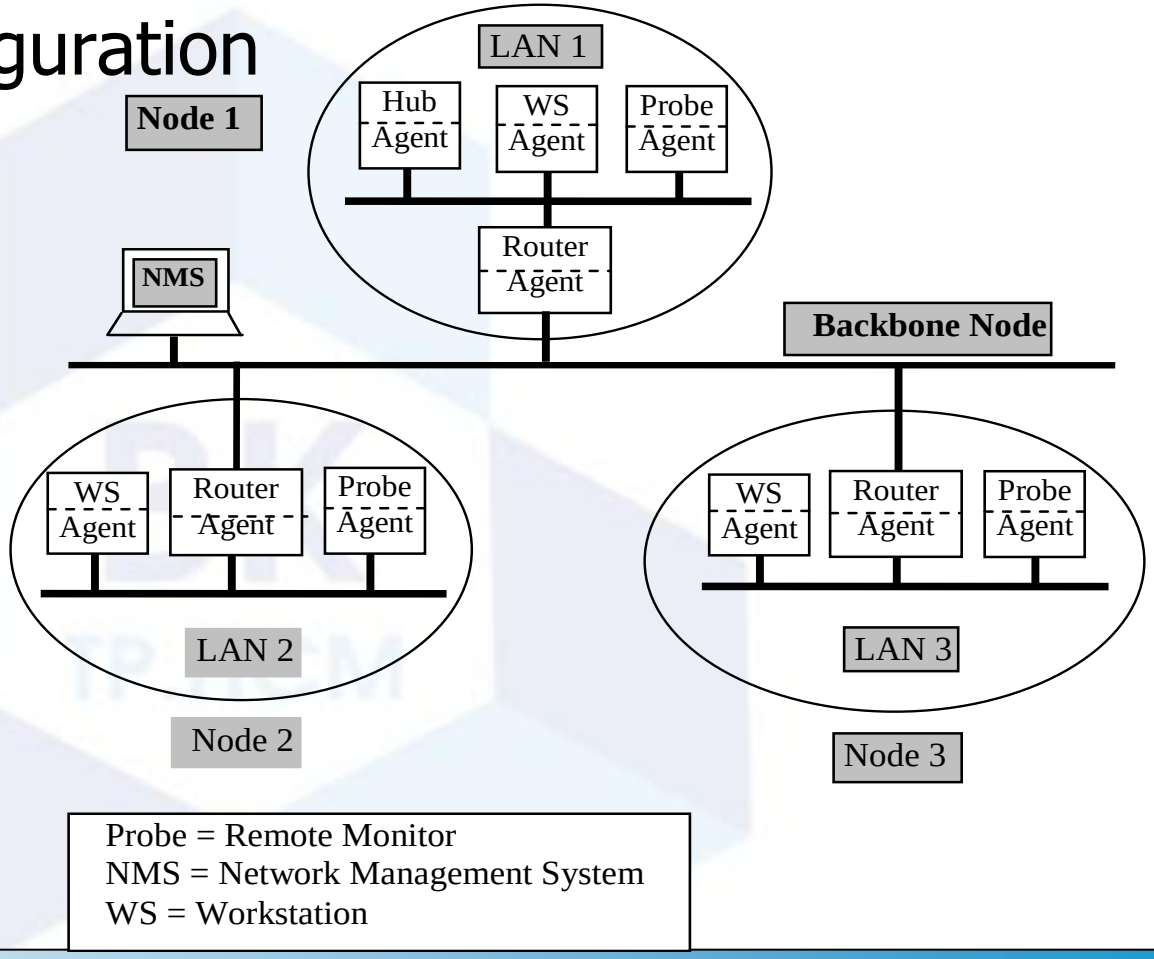


Outline

- Network Management Standards
- Network Management Configuration
- Network Operations Center (NOC)

Network Management Configuration

- Centralized vs distributed
- Centralized configuration

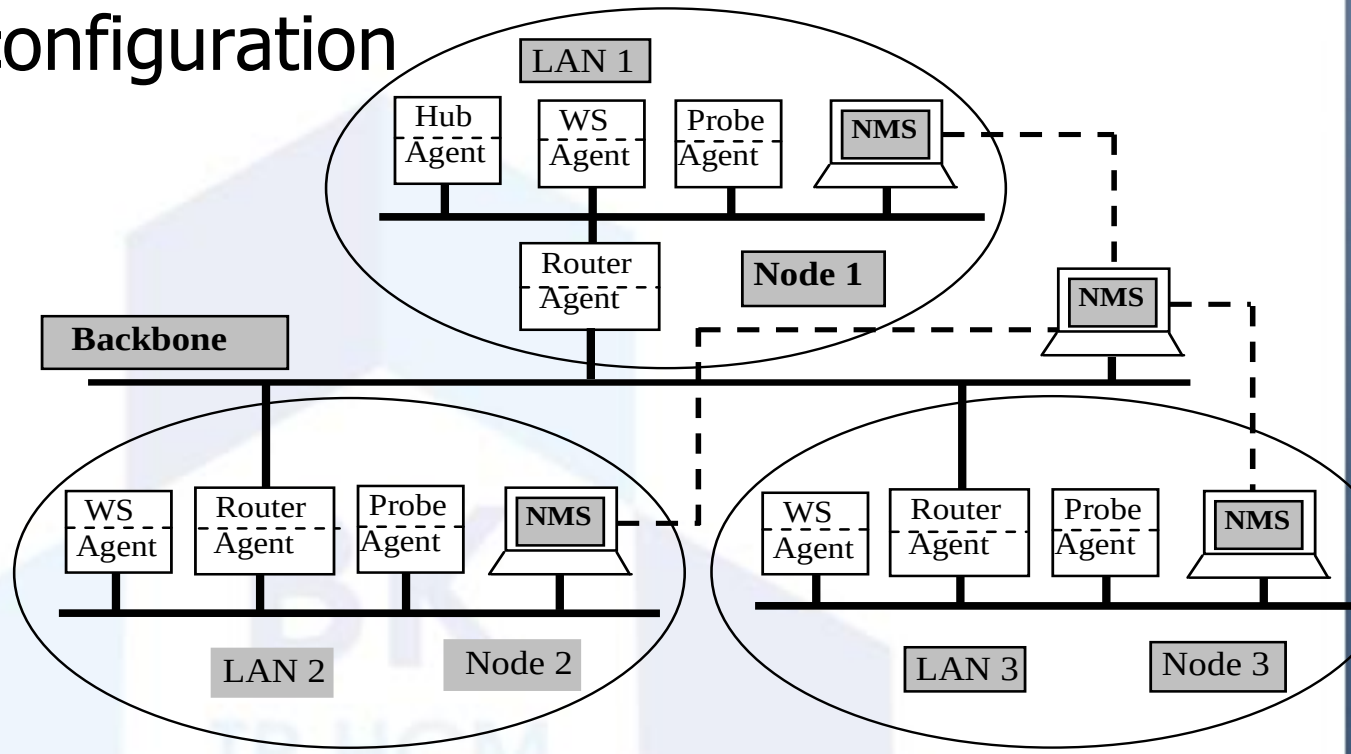


Network Management Configuration

- Centralized configuration
  - One management station hosts NMS
  - Remote monitors/probes on LAN segments
- Advantage: NMS has complete view
- Disadvantage: single point of failure

Network Management Configuration

- Distributed configuration



Probe = Remote Monitor
NMS = Network Management System
WS = Workstation
-------- = In-band or out-of band management communication

Network Management Configuration

- Distributed configuration
  - Each LAN has its own management station and a simple NMS
  - One mgmt station/NMS manages the backbone and coordinates local NMSs
- Advantage: robust in case of failure
- Disadvantage: complexity, coordination

Outline

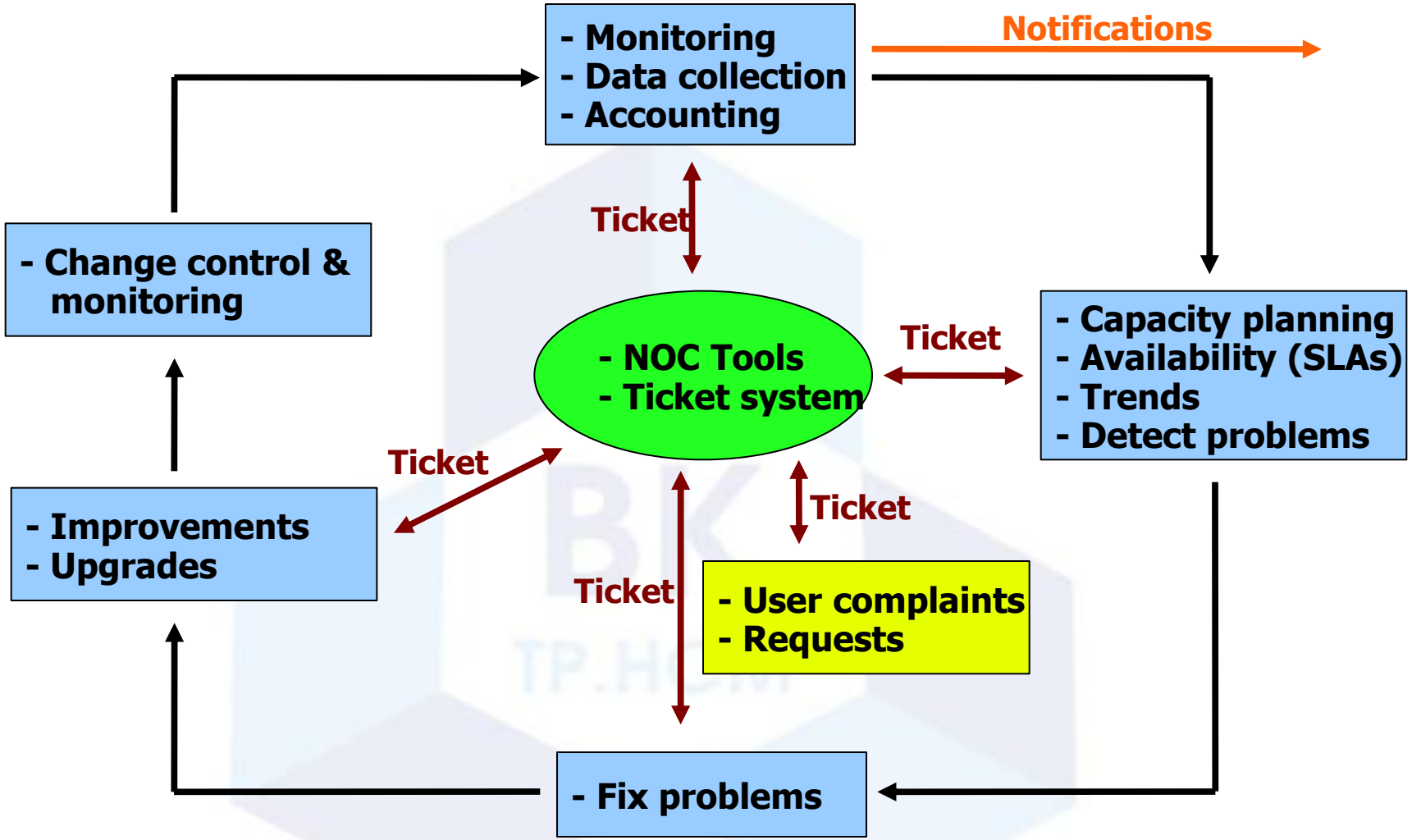
- Network Management Standards
- Network Management Configuration
- Network Operations Center (NOC)

Network Operations Center (NOC)

"Where it all happens"

- Coordination of tasks
- Status of network and services
- Fielding of network-related incidents and complaints
- Where the tools reside ("NOC server")
- Documentation including:
  - Network diagrams
  - database/flat file of each port on each switch
  - Network description
  - Much more as you'll see a bit later.

The Big Picture



A *few* Open Source solutions…

Performance
- Cricket
- IFPFM
- flowc
- mrtg
- netflow
- NfSen
- ntop
- pmacct
- rrdtool
- SmokePing

Ticketing
- RT, Trac, Redmine

Change Mgmt
- Mercurial
- Rancid (routers)
- RCS
- Subversion

Security/NIDS
- Nessus
- OSSEC
- Prelude
- Samhain
- SNORT
- Untangle

Net Management
- Big Brother
- Big Sister
- Cacti
- Hyperic
- Munin
- Nagios*
- Netdisco
- Netdot
- OpenNMS
- Sysmon
- Zabbix

Documentation

Maybe you've asked, "*How do you keep track of it all*?"...

Document, document, document...

Documentation

Basics, such as documenting your switches...

- What is each port connected to?
- Can be simple text file with one line for every port in a switch:
  - health-switch1, port 1, Room 29 – Director's office
  - health-switch1, port 2, Room 43 – Receptionist
  - health-switch1, port 3, Room 100 – Classroom
  - health-switch1, port 4, Room 105 – Professors Office
  - …..
  - health-switch1, port 25, uplink to health-backbone
- This information might be available to your network staff, help desk staff, via a wiki, software interface, etc.
- Remember to label your ports!

Documentation: Labeling

Nice…

Network Documentation

More automation might be needed. An automated network documentation system is something to consider.

- You can write local scripts to do this.
- You can consider some automated documentation systems.
- You'll probably end up doing both.

Network Documentation

There are quite a few automated network documentation systems. Each tends to do something different:

- IPplan:
  http://iptrack.sourceforge.net/
- Netdisco:
  http://netdisco.org/
- Netdot:
  https://netdot.uoregon.edu/

IPplan:

From the IPplan web page:

"IPplan is a free (GPL), web based, multilingual, TCP/IP address management (IPAM) software and tracking tool written in php 4, simplifying the administration of your IP address space. IPplan goes beyond TCPIP address management including DNS administration, configuration file management, circuit management (customizable via templates) and storing of hardware information (customizable via templates)."

Lots of screenshots:

http://iptrack.sourceforge.net/doku.php?id=screenshots

Netdisco:

- Project launched 2003. Version 1.0 released October 2009.
- Some popular uses of Netdisco:
  - **Locate** a machine on the network by MAC or IP and show the switch port it lives at.
  - **Turn Off** a switch port while leaving an audit trail. Admins log why a port was shut down.
  - **Inventory** your network hardware by model, vendor, switch-card, firmware and operating system.
  - **Report** on IP address and switch port usage: historical and current.
  - **Pretty pictures** of your network.

Netdot:

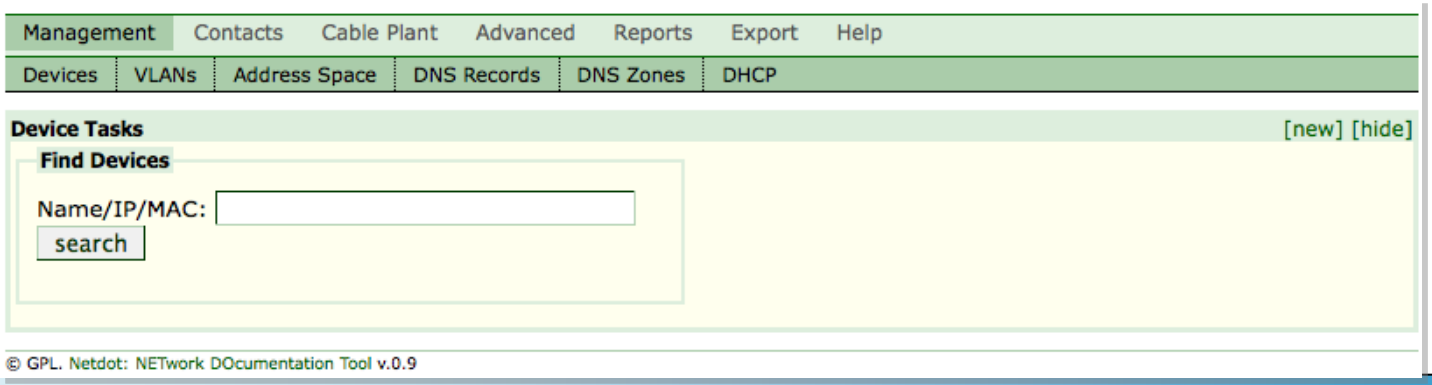
Includes functionality of IPplan and Netdisco and more. Core functionality includes:

- Device discovery via SNMP
- Layer2 topology discovery and graphs, using:
  - CDP/LLDP
  - Spanning Tree Protocol
  - Switch forwarding tables
  - Router point-to-point subnets
- IPv4 and IPv6 address space management (IPAM)
  - Address space visualization
  - DNS/DHCP config management
  - IP and MAC address tracking

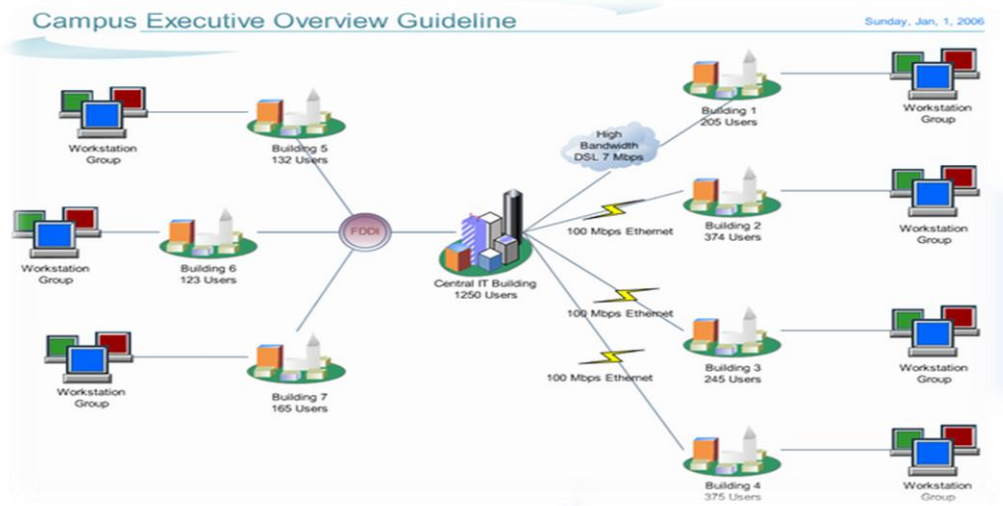
Netdot: {net.} NETwork DOcumentation Tool

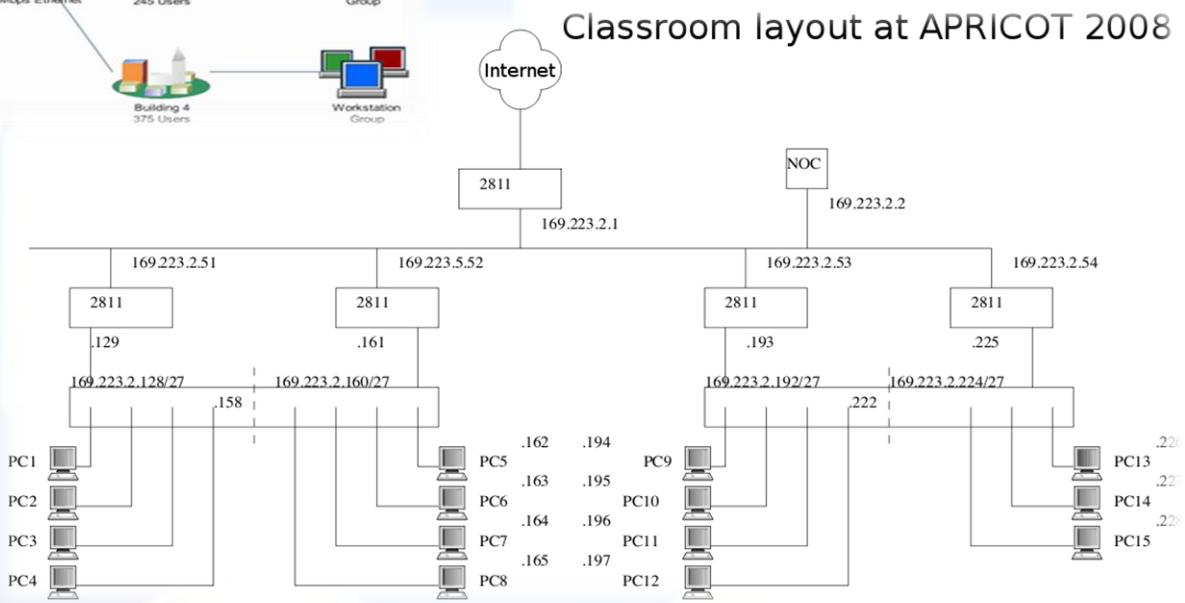
Functionality continued:

- Cable plant (sites, fiber, copper, closets, circuits...)
- Contacts (departments, providers, vendors, etc.)
- Export scripts for various tools (Nagios, Sysmon, RANCID, Cacti, etc)
  - I.E., how we could automate node creation in Cacti!
- Multi-level user access: Admin, Operator, User
- It draws pretty pictures of your network



Documentation: Diagrams





Diagramming Software

Windows Diagramming Software

- Visio:
  http://office.microsoft.com/en-us/visio/FX100487861033.aspx
- Ezdraw:
  http://www.edrawsoft.com/

Open Source Diagramming Software

- Dia:
  http://live.gnome.org/Dia
- Cisco reference icons:
  http://www.cisco.com/web/about/ac50/ac47/2.html
- Nagios Exchange:
  http://www.nagiosexchange.org/

Network monitoring systems & tools

Three kinds of tools

1. **Diagnostic tools** – used to test connectivity, ascertain that a location is reachable, or a device is up – usually active tools
2. **Monitoring tools** – tools running in the background (”daemons” or services), which collect events, but can also initiate their own probes (using diagnostic tools), and recording the output, in a scheduled fashion.
3. **Performance tools** – tell us how our network is handling traffic flow.

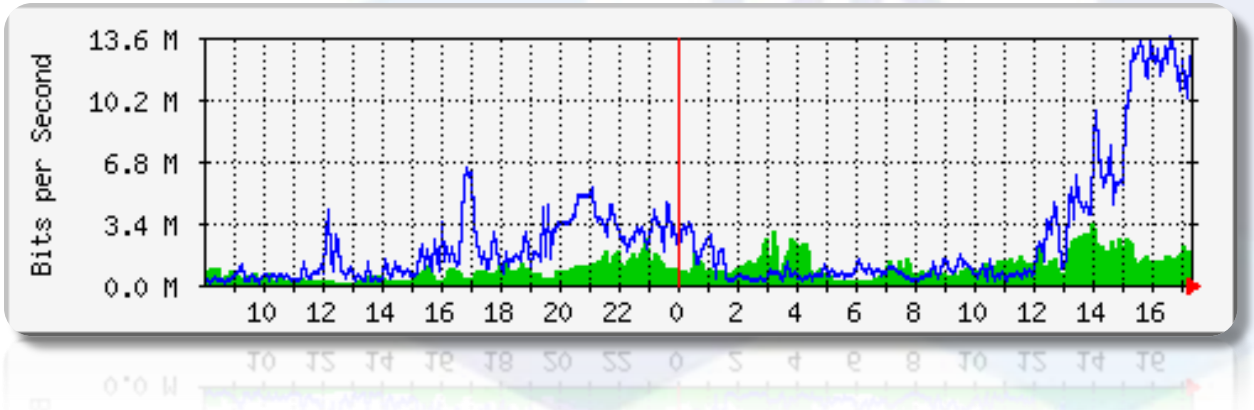
Network monitoring systems & tools

3. Performance Tools

Key is to look at each router interface (probably don't need to look at switch ports).

Two common tools:

- Netflow/NfSen: http://nfsen.sourceforge.net/
- MRTG: http://oss.oetiker.ch/mrtg/



MRTG = "Multi Router Traffic Grapher"

Network monitoring systems & tools

- Active tools
  - Ping – test connectivity to a host
  - Traceroute – show path to a host
  - MTR – combination of ping + traceroute
  - SNMP collectors (polling)
- Passive tools
  - log monitoring, SNMP trap receivers, NetFlow
- Automated tools
  - SmokePing – record and graph latency to a set of hosts, using ICMP (Ping) or other protocols
  - MRTG/RRD – record and graph bandwidth usage on a switch port or network link, at regular intervals

Network monitoring systems & tools

- Network & Service Monitoring tools
  - Nagios – server and service monitor
    - Can monitor pretty much anything
    - HTTP, SMTP, DNS, Disk space, CPU usage, ...
    - Easy to write new plugins (extensions)
  - Basic scripting skills are required to develop simple monitoring jobs – Perl, Shell scripts, php, etc...
  - Many good Open Source tools
    - Zabbix, ZenOSS, Hyperic, OpenNMS ...
- Use them to monitor reachability and latency in your network
  - Parent-child dependency mechanisms are very useful!

Network monitoring systems & tools

- Monitor your critical Network Services
  - DNS/Web/Email
  - Radius/LDAP/SQL
  - SSH to routers
- How will you be notified?
- Don't forget log collection!
  - Every network device (and UNIX and Windows servers as well) can report system events using syslog
  - You MUST collect and monitor your logs!
  - Not doing so is one of the most common mistakes when doing network monitoring

Network management protocols

- SNMP – Simple Network Management Protocol
  Industry standard, hundreds of tools exist to exploit it
  - Present on any decent network equipment
    - Network throughput, errors, CPU load, temperature, ...
  - UNIX and Windows implement this as well
    - Disk space, running processes, ...
- SSH and telnet
  - It is also possible to use scripting to automate monitoring of hosts and services

SNMP tools

- Net SNMP tool set
  - http://net-snmp.sourceforge.net/
- Very simple to build simple tools
  - One that builds snapshots of which IP is used by which Ethernet address
  - Another that builds shapshots of which Ethernet addresses exist on which port on which switch.
  - Query remote RAID array for state.
  - Query server, switches and routers for temperatures.
  - Etc…

Statistics and accounting tools

- Traffic accounting and analysis
  - What is your network used for, and how much
  - Useful for Quality of Service, detecting abuses, and billing (metering)
  - Dedicated protocol: NetFlow
  - Identify traffic ”flows”: protocol, source, destination, bytes
  - Different tools exist to process the information
    - Flowtools, flowc
    - NFSen
    - Many more: http://www.networkuptime.com/tools/netflow/

Fault and problem management

- Is the problem transient?
  - Overload, temporary resource shortage
- Is the problem permanent?
  - Equipment failure, link down
- How do you detect an error?
  - Monitoring!
  - Customer complaints
- A ticket system is essential
  - Open ticket to track an event (planned or failure)
  - Define dispatch/escalation rules
    - Who handles the problem?
    - Who gets it next if no one is available?

Ticketing systems

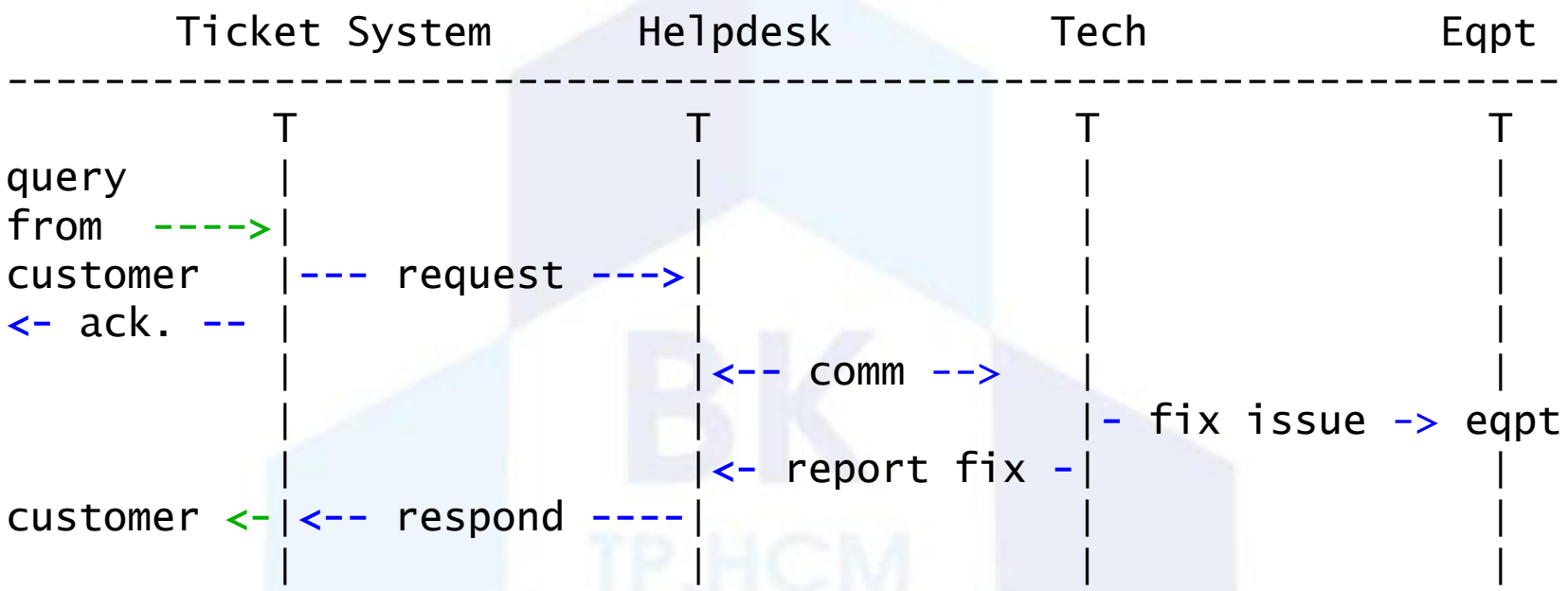
- Why are they important?
  - Track all events, failures and issues
- Focal point for helpdesk communication
- Use it to track all communications
  - Both internal and external
- Events originating from the outside:
  - customer complaints
- Events originating from the inside:
  - System outages (direct or indirect)
  - Planned maintenances or upgrades – Remember to notify your customers!

Ticketing systems

- Use ticket system to follow each case, including internal communication between technicians
- Each case is assigned a case number
- Each case goes through a similar life cycle:
  - New
  - Open
  - ...
  - Resolved
  - Closed

Ticketing systems

Workflow:



Ticketing systems: examples

- rt (request tracker)
  - Heavily used worldwide.
  - A classic ticketing system that can be customized to your location.
  - Somewhat difficult to install and configure.
  - Handles large-scale operations.
- trac
  - A hybrid system that includes a wiki and project management features.
  - Ticketing system is not as robust as rt, but works well.
  - Often used for ”trac”king group projects.
- redmine
  - Like trac, but more robust. Harder to install

Network Intrusion Detection Systems (NIDS)

- These are systems that observe all of your network traffic and report when it sees specific kinds of problems, such as:
  - hosts that are infected or are acting as spamming sources.
- A few tools:
  - SNORT - a commonly used open source tool: http://www.snort.org/
  - Prelude – Security Information Management System https://dev.prelude-technologies.com/
  - Samhain – Centralized HIDS http://la-samhna.de/samhain/
  - Nessus - scan for vulnerabilities: http://www.nessus.org/download/

Configuration mgmt & monitoring

- Record changes to equipment configuration using revision control (also for configuration files)
- Inventory management (equipment, IPs, interfaces)
- Use versioning control
  - As simple as:
    ”cp named.conf named.conf.20070827-01”
- For plain configuration files:
  - CVS, Subversion (SVN)
  - Mercurial
- For routers:
  - RANCID

Configuration mgmt & monitoring

- Traditionally, used for source code (programs)
- Works well for any text-based configuration files
  - Also for binary files, but less easy to see differences
- For network equipment:
  - RANCID (Automatic Cisco configuration retrieval and archiving, also for other equipment types)
- Built-in to Project Management Software like:
  - Trac
  - Redmine
  - And, many other wiki products. Excellent for documenting your network.