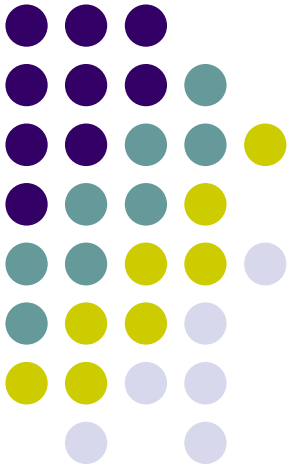
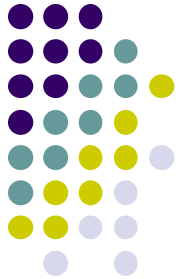
Network Management Model (Part-2)

Lecture-7

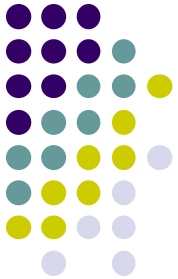


ISO Network Management Categories



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

Performance Management

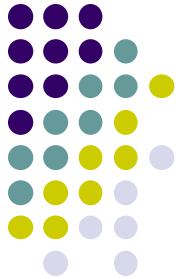


- Concerned with
  - Response time
  - Utilization
  - Error rates, etc.
- Must collect and analyze data
  - Number and type of packets
  - Might also rely on simulations

Performance Management Sub-Categories

Collecting Baseline Utilization Data	• Measuring link utilization using a probe • Counting packets received/transmitted by a specific device • Measuring device processor usage • Monitoring device queue lengths • Monitoring device memory utilization • Measuring total response times
Collecting a History of Utilization Data	• Measuring utilization and **response times at different times** of the day • Measuring utilization and **response times on different days** over an extended period
Capacity Planning	• Manually graphing or using a **network management tool to graph utilization** as a function of time to detect trends • Preparing **trend reports** to document **projected need for and the cost** of network expansion.
Setting Notification Thresholds	• Having a network management tool poll devices for values of critical parameters and graphing these values as a function of time • Setting polling intervals • **Setting alarms/alerts** on those parameters when the threshold is reached or a percentage of it is reached • Initiating an action when the threshold is reached such a **sending a message to the network manager.**
Building Databases	• Having the **network management tool create a database of records containing device name, parameter, threshold and time for off-line** analysis. • Using the database to extract time dependence of utilization • Using the time dependence of parameters to decide when network upgrades will be necessary to maintain performance
Running Network Simulations	• Using a simulation tool to develop a model of the network • Using the model's parameters and utilization data to optimize network performance
Latency	• Query/Response time interval

Fault Management

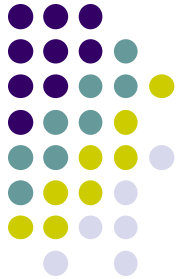


- Preventions, detection and isolation of abnormal behavior
  - May be caused by malfunction, cable issue etc.
- Traffic, trends, connectivity, etc.
  - SNMP polls
  - **Alarms** for automatic fault detection
  - Monitor statistics
  - Timeliness, etc.

Fault Management Sub-categories

Prioritization	• Identify which fault events should cause messages to be sent to the manager • Identify which devices should be polled and at what intervals • Identify which device parameter values should be collected and how often • Prioritize which messages should be stored in the manager's database • Prioritize faults in the order in which they should be addressed
Timeliness Required	• Management Station is passive and only receives event notifications • Management Station is active and polls for device variable values at required intervals • Application periodically requests a service from a service provider
Physical Connectivity Testing	• Using a cable tester to check that links are not broken
Software Connectivity Testing	• Using an application that makes a request of another device that requires a response. ❑ The most often application for this is **Ping**. It calls the Internet Control Message Protocol (ICMP) which sends periodic Echo Request messages to a selected device on a TCP/IP network ❑ Application on one device makes a request of an application on another device
Device Configuration	• Devices are configured conservatively to minimize chances of dropped packets.
SNMP Polls	• Devices are periodically polled to collect network statistics
Fault Reports Generated	• Thresholds configured and alarms generated • Text media used for report • Audio media used for report • A color graphical display used to show down devices • Human manager is notified by pager
Traffic Monitored	• Remote Monitors used • Protocol analyzers used • Traps sent to Network Management Station • Device statistics monitored
Trends	• Graphical trends generated to identify potential faults

Configuration Management



- Device configuration
  - May be done locally or remotely
- Network configuration
  - Sometimes called “capacity mgmt”
  - Critical to have sufficient capacity
- Desirable to automate as much as possible
  - For example, DHCP and DNS
- Extensions to SNMP MIB

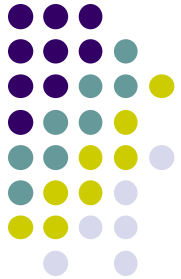
Configuration Management Sub-categories

Configuration (Local)	• Choice of medium access protocol • Choice of correct cabling and connectors • Choice of cabling layout • Determining the number of physical interfaces on devices • Setting device interface parameter values ❑ Network layer addresses (e.g. IP, NetWare, etc) • Configuration of multiport devices (e.g. hubs, switches and routers) • Use of the Windows Registry • Comparing current versus stored configurations • Checking software environments • SNMP service
Configuration (Remote)	• From the network management station • Disabling device ports • Redirecting port forwarding • Disabling devices • Comparing current versus stored configurations • Configuring routing tables • Configuring security parameters such as community strings and user names • Configuring addresses of management stations to which traps should be sent • Verifying integrity of changes

Configuration Management Sub-categories

Configuration (Automated)	• Using the Dynamic Host Configuration Protocol (DHCP) to configure IP addresses • Using Plug and Play enabled NICs for automatic selection of interrupts and I/O addresses • Domain Name Services (DNS) addresses • Trap/alert messages from agents
Inventory (Manual)	• Maintaining records of cable runs and the types of cables used • Maintaining device configuration records • Creating network database containing for each device: • Device types ❑ Software environment for each device ❑ operating systems ❑ utilities • drivers • applications ❑ versions ❑ configuration files (.ncf, .ini, .sys) • vendor contact information • IP address • Subnet address
Inventory (Automated)	• Auto-discovery of devices on the network using an NMS • Auto-determination of device configurations using an NMS • Creation of a network database • Auto-mapping of current devices to produce a network topological map • Accessing device statistics using an NMS and the Desktop Management Protocol

Security Management

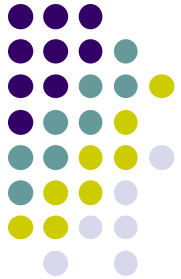


- Control access to network/resources
  - Authentication: who goes there?
  - Authorization: are you allowed to do that?
  - Firewalls
  - Intrusion detection systems (IDS)
  - Notification of (attempted) breaches, etc.
- Critical to always authenticate participants
- SNMPv1 has very little security
- SNMPv3 has lots of security built in

Security Management Sub-categories

Applying Basic Techniques	• Identifying hosts that store sensitive information • Management of passwords • Assigning user rights and permissions • Recording failed logins • Setting remote access barrier codes • Employing virus scanning • Limiting views of the Enterprise network • Tracking time and origin of remote accesses to servers
Identifying Access Methods Used	• Electronic Mail • File Transfer • Web Browsing • Directory Service • Remote Login • Remote Procedure Call • Remote Execution • Network Monitors • Network Management System
Using Access Control Methods	• Encryption • Packet filtering at routers • Packet filtering at firewalls • Source host authentication • Source user authentication
Maintenance	• Audits of the activity at secure access points • Executing security attack programs (Network Intrusion Detection) • Detecting and documenting breaches
Accessing Public Data Networks	• No restrictions - hosts are responsible for securing all access points • Limited access - only some hosts can interface with the Public Data Network using a proxy server
Using an Automated Security Manager	• Queries the configuration database to identify all access points for each device. • Reads event logs and notes security-related events. • Security Manager shows a security event on the network map. • Reports of invalid access point attempts are generated daily for analysis

Accounting Management

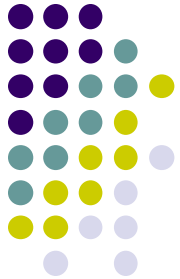


- Measuring the usage of network resources in order to distribute costs and resources
- E.g., monitoring the use of a server by users in a specific department and charging the department accordingly

Accounting Management Sub-categories

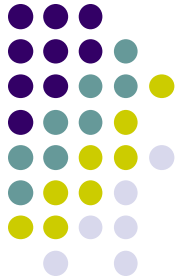
Gather Network Device Utilization Data	• Measure usage of resources by cost center • Set quotas to enable fair use of resources • Site metering to track adherence to software licensing
Bill Users of Network Resources	• Set charges based on usage. • Measure one of the following ❑ Number of transactions ❑ Number of packets • Number of bytes • Set charges on direction of information flow
Use and Accounting Management Tools	• Query usage database to measure statistics versus quotas • Define network billing domains • Implement automatic billing based on usage by users in the domain • Enable billing predictions • Enable user selection of billing domains on the network map
Reporting	• Create historical billings trends • Automatic distribution of billing to Cost Centers • Project future billings by cost center

Management Tools



Company	Product	URL	Comments
Apptitude (HiFn)	Meterware/ Analyzer	http://www.hifn.com	NMS used in this book. Is a complete SNMPv1 tool. It is only available with the book. Apptitude was a leader in SNMP management software and hardware for many years. HiFn develops integrated circuits for encryption.
SNMP Research International	• EnterPol • CIAgent • SNMPv3 Wizard	http://www.snmp.com/index.html	EnterPol is a NMS. CIAgent is an agent. CIAgent is a free download. SNMPv3 Wizard is an agent configuration tool. The company has many other products. The company has been a leader in the SNMP field
Castlerock	SnmpC	http://www.castlerock.com/	The Work Group Edition 5.1 is appropriate for small networks It supports SNMPv3, as does the Enterprise edition that provides other capabilities. Cost of the Work Group Edition is $995.00 The company has been a leader in the SNMP field
Solar Winds	Engineers Edition	http://solarwinds.net/	Provides a number of management tools ranging in price from $145 to $1995. The $1995.00 package is Web-enabled. The Engineers Edition at $995.00 looks like the most attractive for users of this book in that it contains most of the features of the HiFn Ama;uzer.
MG-SOFT	Net Inspector Lite	http://www.mg-soft.si/	Net Inspector Lite is $495.00. It looks like a good choice for readers of this book. MG-SOFT provides many other more comprehensive products and products can be enhanced by proxy front-end modules. There are also products that support SNMPv3

Management Tools



Triticom	LANdecoder SNMP Manager	http://www.triticom.com/	LANdecoder SNMP Manager is a simple, easy to use SNMP Manager for Microsoft Windows environment. With it, you can query and control any SNMP-capable device on your network. It can operate standalone or be integrated with Triticom's LANdecoder 32 V 3.2., a network analyzer. The price of LANdecoder SNMP manager is $995.00
Finisar	Shomiti Surveyor	http://www.finisar-systems.com/	Shomiti Systems is now part of Finisar. The Surveyor product is a comprehensive network hardware manager. A free download is available.
Acterna	Link View Classic 7.2	http://www.acterna.com/	A software based network analyzer at a price of $995.00. Includes a traffic generator. Excellent graphics Also available is Advanced Ethernet Adapter which provides promiscuous capture of packets. Price is then $2700.00.

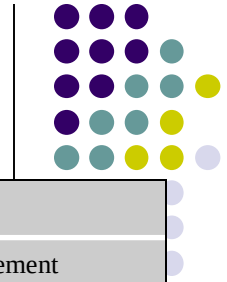
Management Tools

Company	Product	URL	Comments
Network Instruments	Observer 8	http://www.netinst.com/html/observer.html	Supports Ethernet, Token Ring, FDDI, GigaBit and Windows 98/ME and NT/2000/XP. Includes capture for protocol analysis. Price is $995.00
Precision Guesswork	LANwatch32 v6.0	http://www.guesswork.com/snmptool.html	Described to be an easy-to-use command-line application that allows you to GET a variable, SET a variable, get the NEXT variable, or even get all the variables. Provides programs for receiving ALERTS, as well as a simple monitoring program that allows you to tell if your hosts are SNMP reachable, IP reachable, or not reachable. Allows you to remotely monitor, gather and change networking information from hosts on your network. Enables you to diagnose existing problems on the network, predict where problems are likely to occur, pinpoint faulty routers and interfaces, and, in general, exert control over your network.
Cisco	Small Network Management LAN Management	http://www.cisco.com/warp/public/cc/pd/wr2k/wrsnms/ http://www.cisco.com/warp/public/cc/pd/wr2k/lnmn/	Cisco produces many network management products. These products seem most appropriate for audience of this book.

Management Tools

3COM	Network Supervisor 3.5	http://www.3com.com/products/en_US/detail.jsp?tab=features&pathtype=purchase&sku=3C15100C	This free package can be downloaded from this site. Other packages are available from this site also.
Computer Associates	Unicenter Network and Systems Manager 3.0	http://www3.ca.com/Solutions/SubSolution.asp?ID=2846	This is the basic network infrastructure management package. There are add-on applications available such as a performance application
Enterasys	NetSight Element Mgr. NetSight Policy Mgr.	http://www.enterasys.com/products/items/NS-EM/ http://www.enterasys.com/products/items/NETSIGHT-PM/	Element Manager is the basic network management package. Policy Manager incorporates the business model into the management process
Sunrise Telecom	LAN Explorer	http://www.sunrisetelecom.com/lansoftware/lanexplorer.shtml	A comprehensive NMS, comparable to Analyzer but also containing packet capture and analysis capabilities. $799.00 per license.

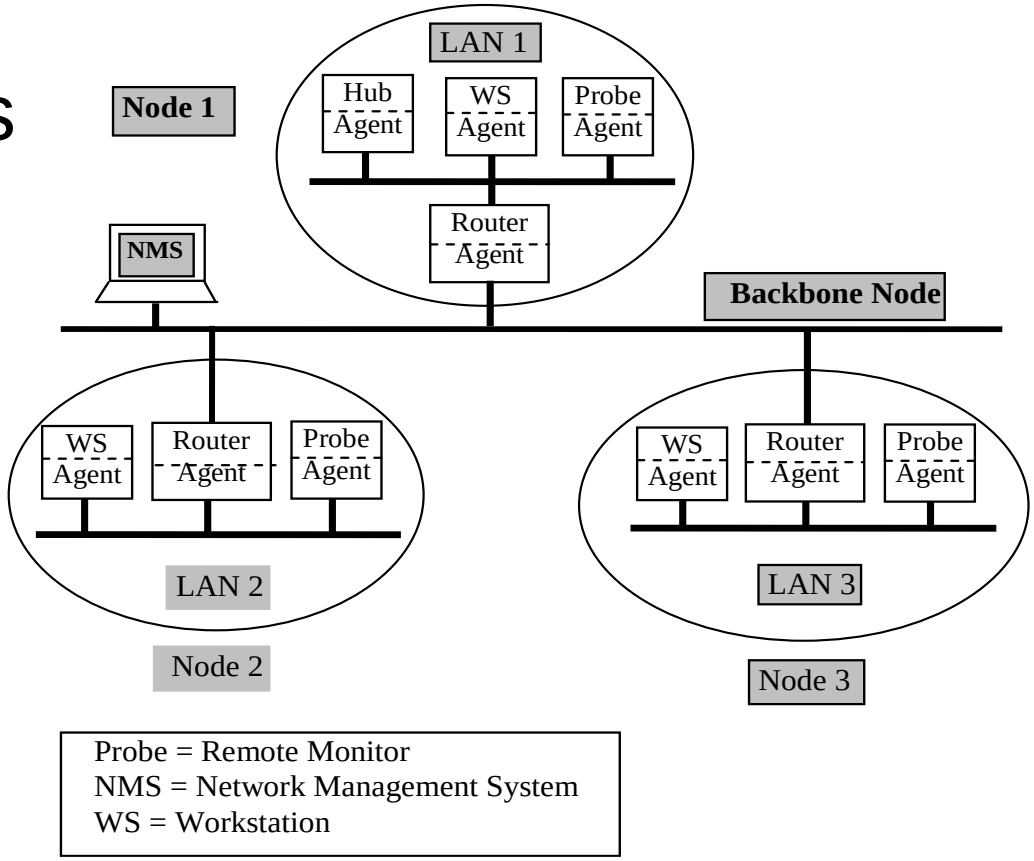
Management Tools



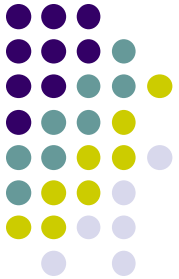
Company	Product	URL	Comments
HP	Toptools	http://www.hp.com/toptools/prodinfo/overview.intro.html	Toptools is a comprehensive hardware management product. It has many plug-ins for specific hardware. All its features can be integrated into your enterprise management platforms such as hp OpenView Network Node Manager, Microsoft SMS, CA Unicenter TNG, IBM Tivoli Enterprise Management and Tivoli NetView
IBM	Tivoli Netview 7.1	http://www.tivoli.com/products/index/netview/	This comprehensive management product also correlates and manages events for systematic management of faults.
Groupe Bull S. A. EVIOIAN (A Bull Company)	Openmaster SLM	http://www.bull.com/	Monitoring and control functions encompass systems management, network management, and application management, and it can manage software configurations, hardware assets and batch production. It also works at a higher level, addressing the underlying business needs in a business-oriented way, to provide measurable business value.
Compuware	Network Vantage	http://www.compuware.com/products/vantage/networkvantage/	Formerly called Ecoscope, monitors network performance by monitoring protocol and application traffic. Par of a suite called Vantage
NetScout	nGenius Real Time Monitor	http://www.netscout.com/products/rtm.htm	Real time voice, video and data traffic. Part of the nGenius Suite.
Nortel	Optivity 6.0 Network Management System	http://www.nortelnetworks.com/products/01/optivity/net_mgmt/index.html	Optivity Network Management System is a comprehensive network management solution. Its key features include fault management, performance analysis, reporting, and access level security
BGS	Patrol Connect SNMP	http://www.bgs.com/products/proddocview.cfm?id=7263	There are many Patrol products by BGS. Connect SNMP seems the most appropriated for this book. BGS products cover all aspects of network management.

Network Management Configuration

- Centralized vs distributed
- Centralized configuration



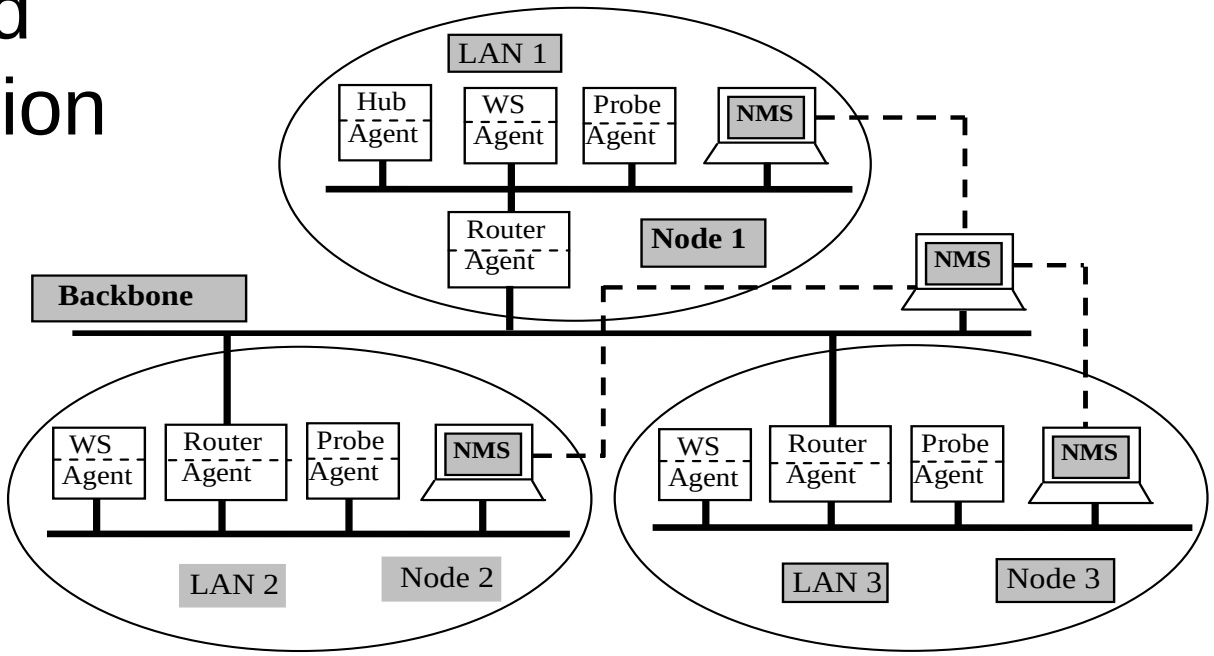
Network Management Configuration



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

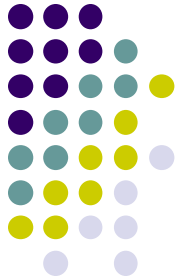
Network Management Configuration

- 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

References

- J. Richard Durke, *Network Management, Concepts and Practice: A Hands-on Approach*, Prentice Hall, 2004.
- J. F. Kurose and K. W. Ross, *Computer Networking: A Top-Down Approach Featuring the Internet,* 3nd Edition, Prentice Hall, 2005.