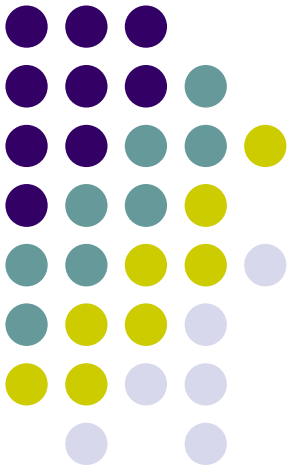
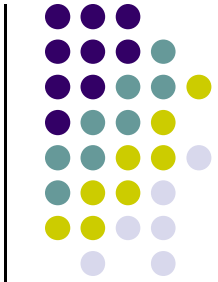
Network Management

Network Management Model

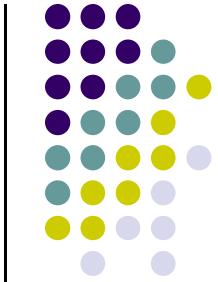


Outline



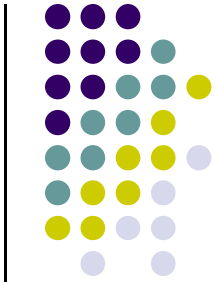
- What is network management?
- Network management vocabulary
- Evolution of network management
- Network implementation design
- ISO network management categories
- Management tools

What is network management?



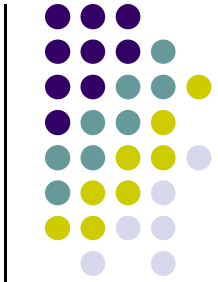
- In the early days, network was small and local
- Network manager's job includes
  - Installation: attach PCs, printers, etc. to LAN
  - Configuration: NICs, protocol stack, user app's shared printers, etc.
  - Testing: Ping was sufficient to "manage" network
  - More devices: bridge, router
- Job was manageable

What is network management?



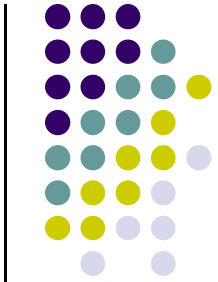
- Above only deals with configuration
- Ongoing maintenance issues
  - How to optimize performance?
  - How to handle failures and network changes?
  - How to extend network capacity?
  - How to account for network usages?
  - How to solve network security issues?

What is network management?



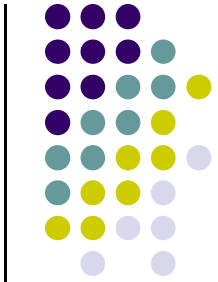
- In the past, the network manager might take all the responsibilities
- Today the task has divided into specialties:
  - Server admin
  - System admin
  - Network admin
  - Security specialist
  - Different certifications for these
    - Cisco, Novell, Microsoft, Sun, $(ISC)^2$, etc.

What is network management?



- Today, networks are larger and more complicated, so more demands on network manager
- How to monitor and control the network effectively and timely?
  - Management tools are needed
- Network-based management tools: use the network to manage the network (remotely)
  - To control
    - Simple Network Management Protocol (SNMP)
    - Management Information Base (MIB)
    - Network Management System (NMS)
  - To monitor
    - Remote Monitor (RMON1)

What is network management?



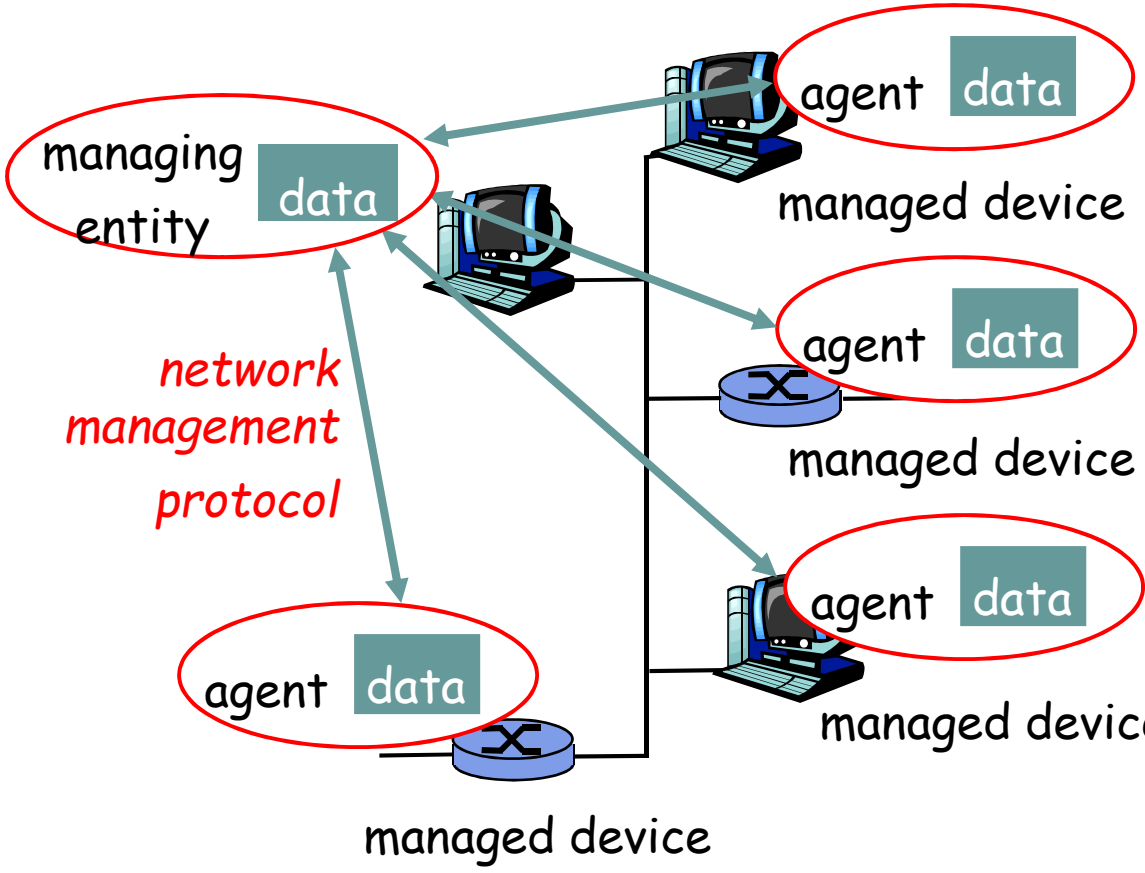
Definition by Saydam (in Journal of Networks and System Management, published in Dec. 1996):
Network management includes the deployment, integration and coordination of the hardware, software, and human elements to monitor, test, poll, configure, analyze, evaluate, and control the network and element resources to meet the real-time, operational performance, and Quality of Service requirements at a reasonable cost.

In brief:

Network management is mostly a combination of local and remote configuration and management with software.

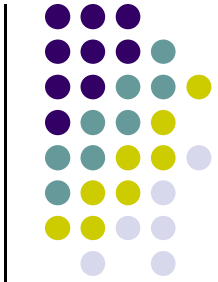
Remote network management is accomplished when one computer is used to monitor, access, and control the configuration of other devices on the network.

Network management vocabulary



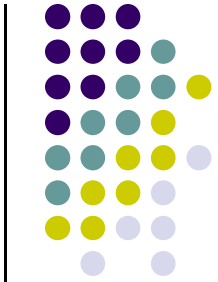
managed devices contain *managed objects* whose data is gathered into a *Management Information Base (MIB)*

Network management vocabulary



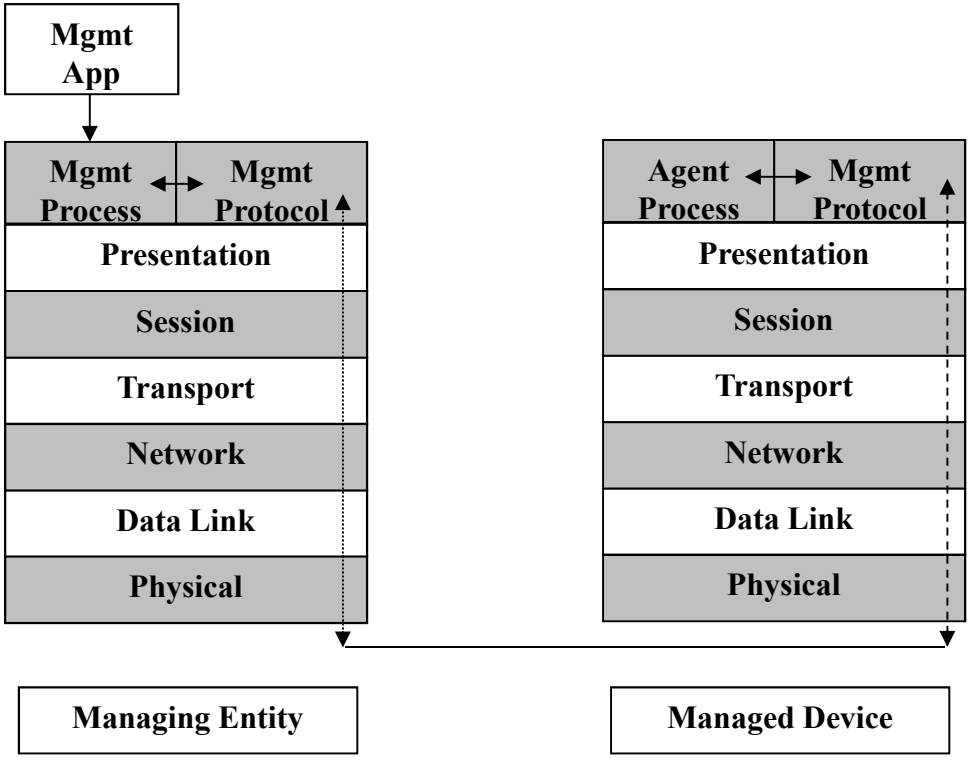
- Managed Device
  - Devices to be monitored/controlled, e.g., router, switch, hub, bridge, workstation.
  - A managed device may have several managed objects to be managed
  - A software (agent) is installed to provide **access** to information/parameters (data) about the device, which is called Management Information Base (MIB)
- Managing Entity
  - Used by the manager/Admin to do network management
  - PC, notebook, terminal, etc., installed with a software called Network Management System (NMS)
  - NMS displays/analyzes data from management agents

Network management vocabulary

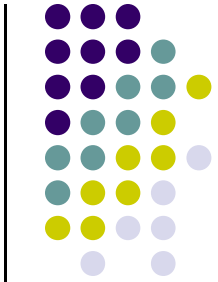


- Network Management Protocol
  - Runs between the managing entity and the managed devices
  - The managing entity can query the status of the managed devices and take actions at the devices via its agents
  - Agents can use the protocol to inform the managing entity of exceptional events
  - E.g., SNMP: Simple Network Management Protocol
- Managing agents located at managed devices are periodically queried by the managing entity through a network management protocol.

Network management example

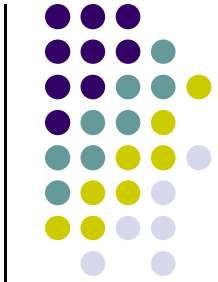


Network management example



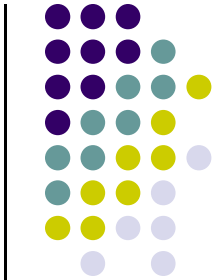
- To get value of MIB variable from mgmt agent
  1. Mgmt app (part of NMS) on managing entity passes request to mgmt process
  2. Mgmt process calls network mgmt protocol (e.g., SNMP)
  3. SNMP constructs Get-Request packet and sent it to the managed device through the network
  4. Mgmt agent on managed device receives Get-Request
  5. Agent process accesses requested value
  6. SNMP constructs Get-Response packet and sent it to managing entity through the network
  7. Mgmt process on managing entity receives response
  8. Mgmt process passes data to mgmt app

Network Management Overhead



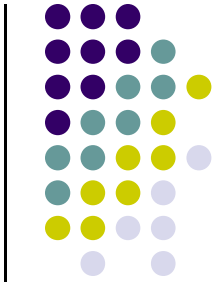
- There is overhead in terms of
  - CPU cycles to generate and process information/packets
    - May require dedicated Managing Entity
  - Bandwidth usage for sending request and receiving responses
- A tradeoff between cost and benefit

Additional Network Management Capabilities



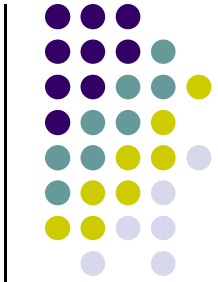
- For efficiency, multiple values can be constructed in a single Get-Response packet
- Can traverse MIB in logical order
- Mgmt agent can send unsolicited mssages
  - These are known as **traps**
  - E.g., if a device goes down
- Can request info from probes or remote monitors (RMON)
  - Monitoring activity (traffic) on a network segment

Evolution of Network Management



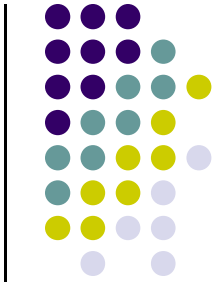
- In 1977 International Organization for Standards (ISO) began work on Open Systems Interconnection (OSI) reference model
  - Purpose was to “provide a common basis for the coordination of standards developments for the purpose of system interconnection, while allowing existing standards to be placed in perspective within the overall Reference Model”
- OSI model published in 1984 (7 years!)

Evolution of Network Management



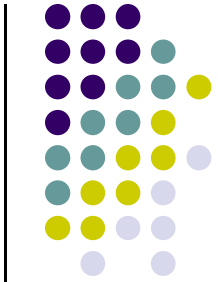
- In March 1987, effort to develop Simple Gateway Monitoring Protocol (SGMP)
  - SGMP out by November 1987
  - Could “get” and “set” variable values
- About same time Common Mgmt Information Protocol (CMIP) developed for OSI model
  - CMIP is roughly SNMP for the OSI model
- Effort to develop CMIP Over TCP (CMOT) as alternative to SGMP

Evolution of Network Management



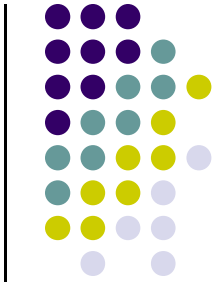
- CMIP uses Remote Operations Services Elements (ROSE)
  - ROSE is for communication with distributed apps in OSI model
- OSI mgmt process is richer and more comprehensive than that provided by SNMP
- But OSI approach is more complex and took longer to develop
  - SNMP: “keep it simple”, and it’s good enough
  - So SNMP won out in practice

Evolution of Network Management



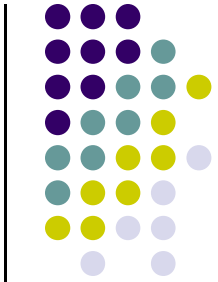
- Due to controversy/delays in OSI approach, Internet Activities Board (IAB) held meeting in 1988
  - Decided to pursue both CMOT and SGMP
  - Eventually abandoned CMOT (complexity)
- Eventually, three RFCs resulted…
- The three RFCs
  - Structure of Management Information (SMI), uses Abstract Syntax Notation One (ASN.1)
  - Management Information Base (MIB), the data structure on the mgmt agent
  - Simple Network Management Protocol (SNMP)
- By 1989, SNMP was the *de facto* standard for management of TCP/IP networks

Evolution of Network Management



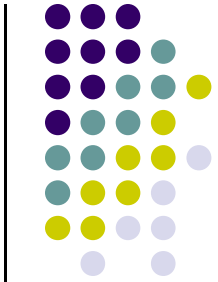
DATE	EVENT	REFERENCE
1968	ARPA funds development of packet switching networks	1. RFC 1120 Internet Activities Board. V. Cerf. Sep-01-1989. (Obsoleted by RFC 1160) 2. RFC 1160 Internet Activities Board. V. Cerf. May-01-1990. (Obsoletes RFC 1120)
1974	TCP/IP concept proposed	Cerf V., and R. Kahn, "A Protocol for Packet Network Interconnection", IEEE Trans. on Communications, Vol. COM-22, No. 5, pp. 637-648, May 1974. [Ref 26]
1976	Ethernet Developed	Metcalfe, R., and D. Boggs, "Ethernet: Distributed Packet for Local Computer Networks", Communications of the ACM, Vol. 19, No. 7, pp. 395-404, July 1976.
1978	OSI Reference Model Development Initiated	

Evolution of Network Management

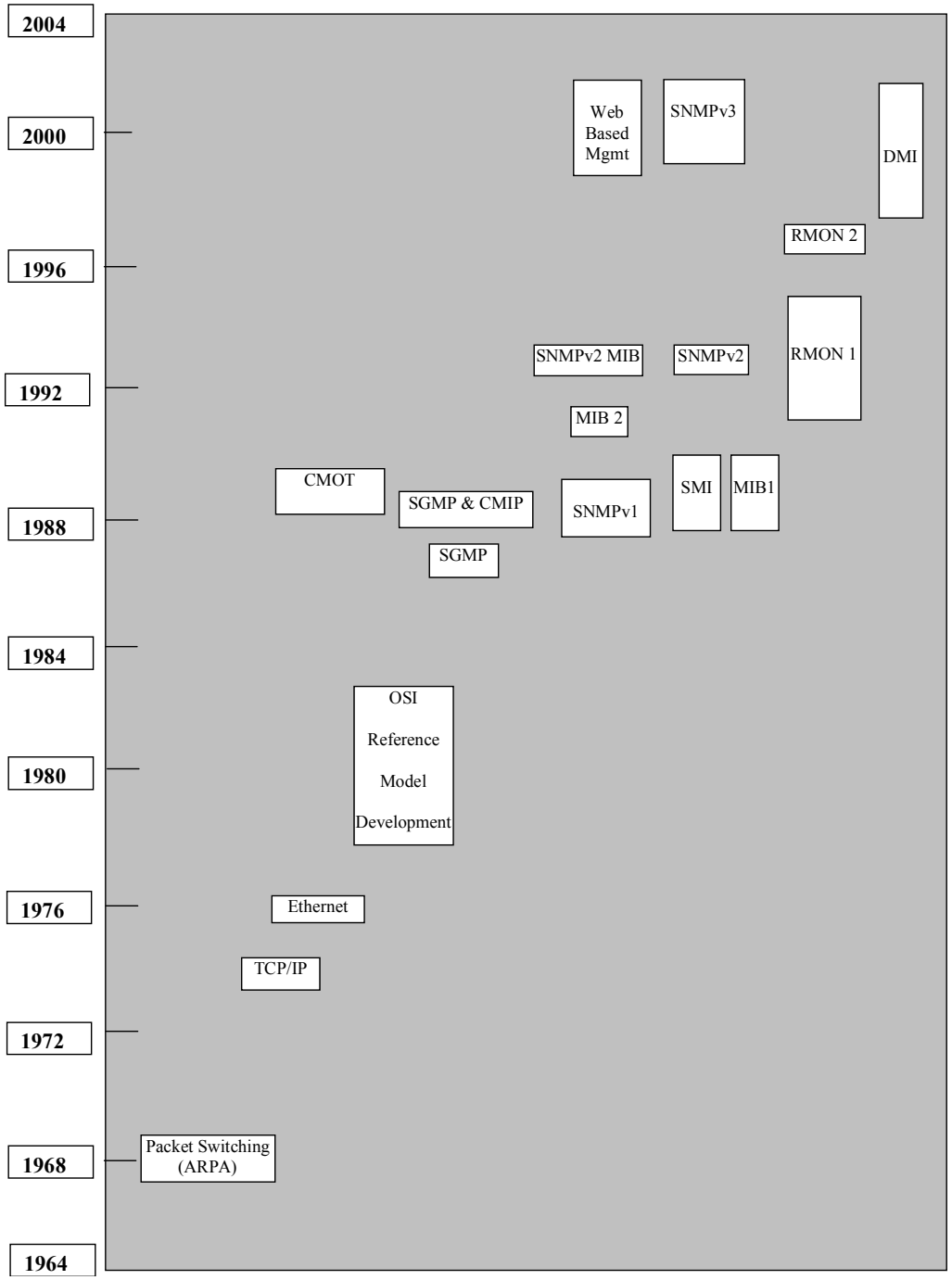


1983	OSI Reference Model becomes international standard	ISO/IEC 7498 (CCITT X.200) [Ref 1]
1987	SGMP development started ASN.1 developed	[Ref 24] ISO 8824, Parts 1-4
1988	IAB initiates study of SGMP and CMIP SNMPv1 becomes Interim Draft Standard SNMPv1 becomes Draft Standard IAB initiates development of Internet Standard Network Management Framework (SMI) Draft Standard MIB I developed	Interim RFC 1028 (SNMPv1) Draft RFC 1098 (SNMPv1) Draft RFC 1065 (SMI) Draft RFC 1066 (MIB I) [Ref 10]
1989	CMOT approach abandoned SNMP becomes the defacto standard for TCP/IP management	
1990	SMI becomes Recommended Standard SNMPv1 becomes Recommended Standard MIB I becomes Recommended Standard	RFC 1165 (SMI) RFC 1157 (SNMP) [Ref 3] RFC 1156 (MIB I) [Ref 11]
1991	MIB II RMON1	RFC 1213 (MIB II) RFC 1271 (RMON I) [Ref 12]

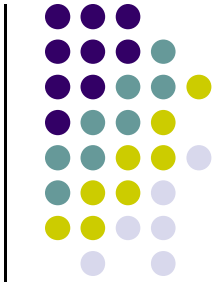
Evolution of Network Management



1993	SNMPv2 Proposed SNMPv2 Security SNMPv2 MIB SNMPv2 SMI	RFC 1441(SNMPv2 Management Framework RFC 1446(SNMPv2 Security Protocols RFC 1450 (SNMPv2 MIB) RFC 1442 SNMPv2 Structure of Management Information
1995	RMON I	RFC 1757 [Ref 13]
1997	RMON II	RFC2021
1998	Desktop Management Interface (DMI) Specification v 2.0s Web-based Management Initiative	1. http://www.dmtf.org/sped/dmis 2. Network Computing, Feb 2001, p57 http://www.dmtf.org/standards/standard_wbem.php
1999	SNMPv2 Management Frameworks SNMPv3 Security	RFC 2571 RFC 2574 (User-based Security Model)
2002	SNMP Management Frameworks SNMPv3 Security SNMP VACM SNMP MIB	RFC 3411, STD 62 RFC 3414 (User-based Security Model), STD 62 RFC 3415 (View-based Access Control Model), STD 62 RFC 3418, STD 62

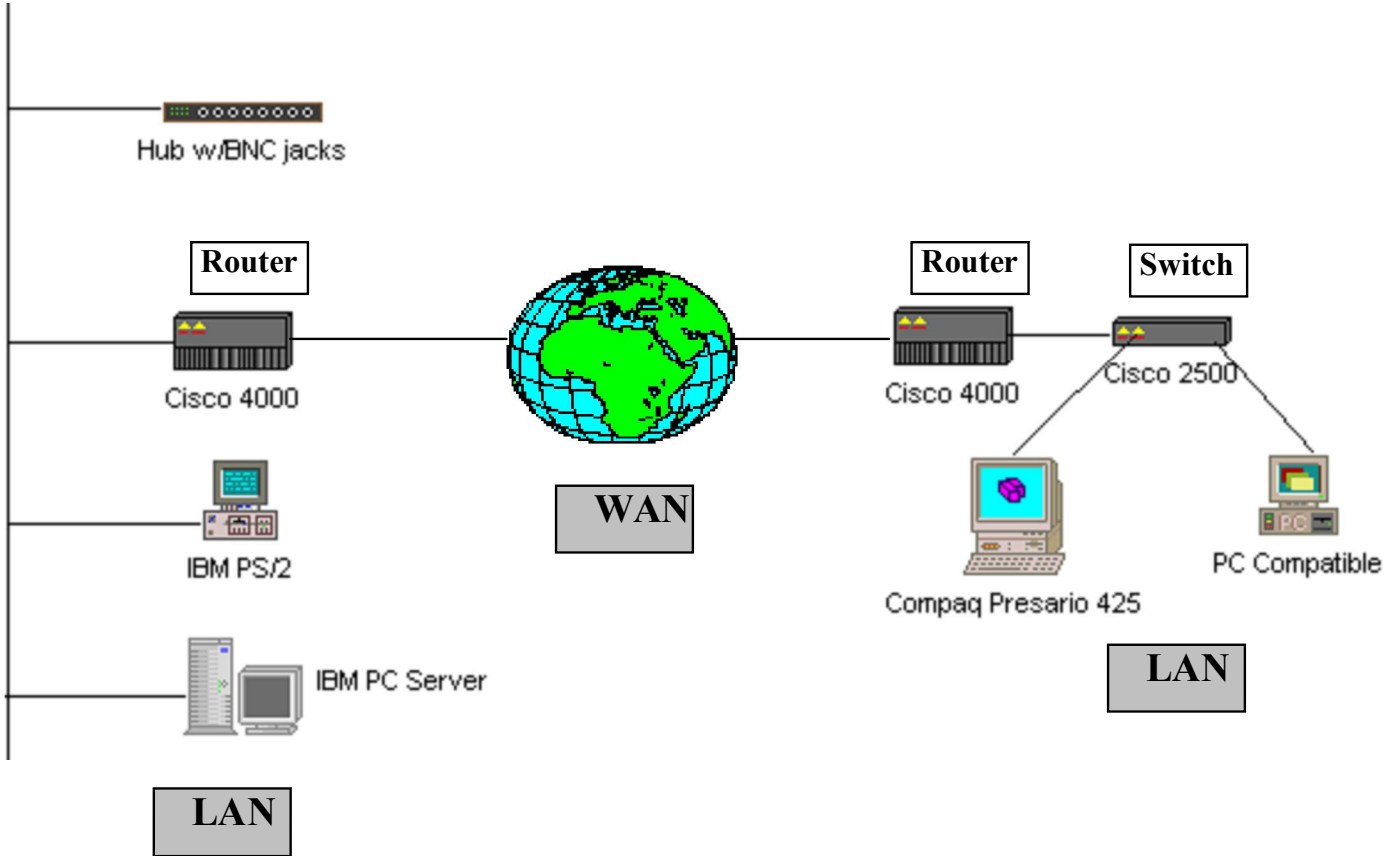

2004
2000
1996
1992
1988
1984
1980
1976
1972
1968
1964
Web Based Mgmt
SNMPv3
DMI
RMON 2
RMON 1
SNMPv2 MIB
SNMPv2
MIB 2
CMOT
SGMP & CMIP
SNMPv1
SMI
MIB1
SGMP
OSI Reference Model Development
Ethernet
TCP/IP
Packet Switching (ARPA)

Network Implementation Strategy Design

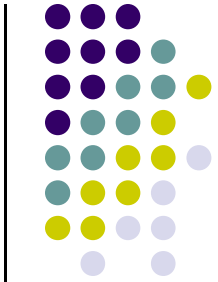


- ISO defines five network management categories
- Network implementation design is “like a 6th category”
  - Good design makes management easier
- Small network: a single LAN
  - For example, CS dept at HKBU
- Medium network: a few LANs
  - E.g., the campus network of HKBU
- Large network: geographically distributed
  - Wide-area network

Network Implementation Strategy Design

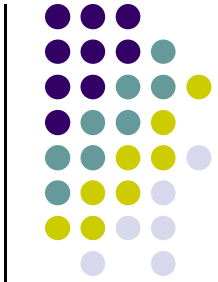


Network Implementation Strategy Design



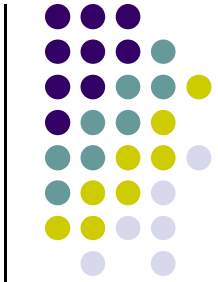
Category	Issues
Geographical Distribution	1. Office • Subnets • LAN 1. Department (many offices) • Subnets • LAN 1. Division (many departments) • LAN • WAN 1. Organization (many divisions) • Local ❑ LAN ❑ MAN ❑ WAN • National ❑ WAN • Global • WAN

Network Implementation Strategy Design



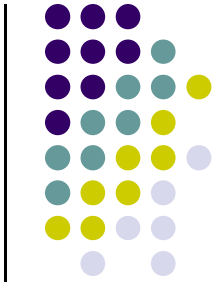
Subnets	• How many • Connectivity ❑ Bridges ❑ Switches ❑ Routers • Ethernet • Wireless • Number of receivers • 10BASET • Location of hub(s) • 10BASE2 • 10BASE5 • How many IP addresses ❑ Static addresses ❑ Addresses supplied by DHCP

Network Implementation Strategy Design



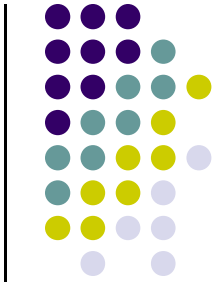
LAN	1.How many 2.Domain names 3.DNS (Domain Name Service) configuration 4.Network address 5.Subnets •How many 1.Connectivity •Switched Ethernet •Router 1.Ethernet 2.Token Ring 3.FDDI (Fiber Distributed Data Network)
MAN (Metropolitan Area Network)	1.Connectivity between LANs ❑FDDI ❑SONET(Synchronous Optical Network) ❑LAN ❑ATM ❑SMDS (Switched Multi-megabit Data Service) ❑DQDB (Dual Queue Dual Bus) ❑Ethernet

Network Implementation Strategy Design



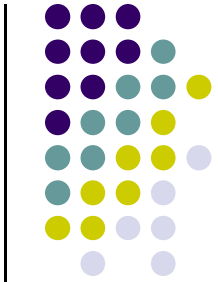
WAN	1. Connectivity between LANs or MANs ❑ PSTN ❑ X.25 ❑ TI-T3 ❑ SONET ❑ Frame Relay ❑ SMDS ❑ ATM ❑ Distribution of services

Network Implementation Strategy Design



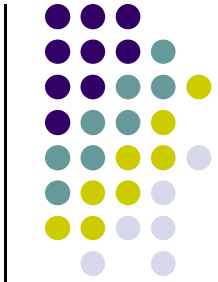
Bandwidth Requirements	1. Video Bandwidth • Constant • Time Dependent • Bandwidth on Demand 1. Audio Bandwidth • Constant • Time Dependent • Bandwidth on Demand 1. Teleconferencing Bandwidth
Media Requirements	1. Cable 2. Wireless 3. Microwave 4. Satellite 5. Optical Fiber
Technology	1. What is available now 2. Minimum required for the job 3. Technology improvements during next 5 years 4. Required to support expected growth

Network Implementation Strategy Design



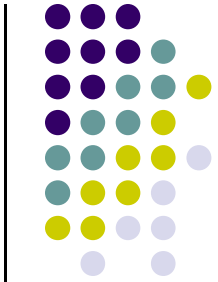
Service Level Agreements (SLA)	1. Specified bandwidth available at any time 2. Specified bandwidth available during specified time periods 3. Bandwidth on demand
Security Requirements	1. Location of firewalls 2. Firewall capabilities 3. Location of proxy servers 4. Encryption and authentication needs 5. Network Intrusion Detectors (NID)
Budget	1. To support resources of optimum network 2. To support resources of minimum network

Network Management Categories



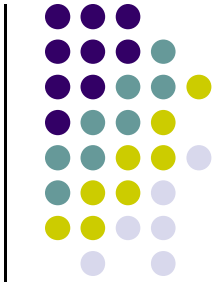
CATEGORY	METRICS
Reliability	• Transmission error rates • Dropped packets • Link failures
Faults	• Proactive prevention • Detection • Location • Correction time
Availability	• Mean time between failures (MTBF) of network
Performance	• Time to provide a response to the user ❑ Processor total use ❑ Processor interrupts/sec ❑ Processor queue length ❑ Transmit packet lengths

Network Management Categories



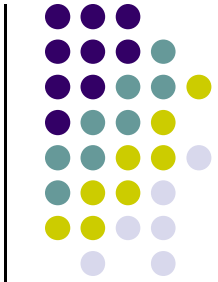
Throughput	• Bytes per second that a user can expect to transmit reliably. • Guaranteed throughput based on Service Level Agreement (SLA)
Data	• Packet throughput
Voice	• Ordered packet throughput
Video	• Link bandwidth • Bandwidth on demand
Use	• Packets/sec • Transactions/sec
Resource Use	• Application software • Network devices • Services • Permanent storage • CPU

Network Management Categories



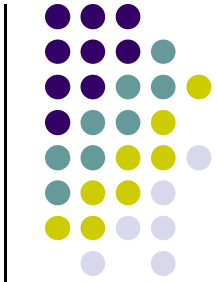
CATEGORY	METRICS
Policies	• Traffic • What's Critical • How many network control packets • Which threshold alarms • Alerts on what events • What's Non-critical • Backup-what and how often • Application testing • Software upgrades-how often • Administration • Type of service availability required • Security level required • Firewall protection requirements • Network Intrusion Detection needs • Number of Software License requirements • User rights requirements and how distributed among which users.
Redundancy	• Number of redundant systems required • Critical alternate paths
User Support	• Automatic responses to user questions about procedures • Automatic responses to user questions about network problems • Automatic reporting of problems and solutions to users and to a database

ISO Network Management Categories



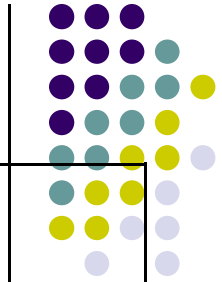
- Performance Management
- Fault Management
- Configuration Management
- Security Management
- Accounting Management

Performance Management



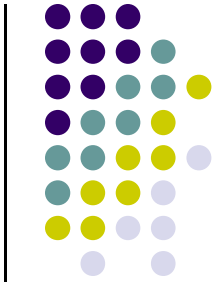
- Concerned with
  - Response time
  - Utilization
  - Error rates, etc.
- Must collect and analyze data
  - Number and type of packets
  - Might also rely on simulations

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

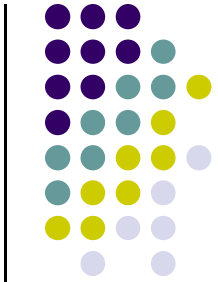


- Preventions, detection and isolation of abnormal behavior
  - May be caused by malfunction, cable issue, the janitor, etc.
- Traffic, trends, connectivity, etc.
  - SNMP **polls**
  - **Alarms** for automatic fault detection
  - Monitor statistics
  - Timeliness, etc.

Fault Management Sub-categories

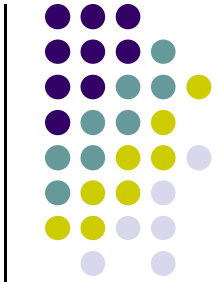
Prioritization	• Prioritize faults in the order in which they should be addressed • Use in-band management packets to learn about important faults • Identify which fault events should cause messages to be sent to the manager • Identify which devices should be polled and at what intervals • Identify which device parameter values should be collected and how often • Prioritize which messages should be stored in the manager's database
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.Exe. 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



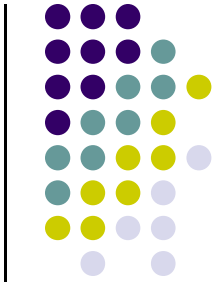
- Device configuration
  - May be done locally or remotely
- Network configuration
  - Sometimes called “capacity mgmt”
  - Critical to have sufficient capacity
- Desirable to automate as much as possible
  - For example, DHCP and DNS
- Extensions to SNMP MIB

Configuration Management Sub-categories



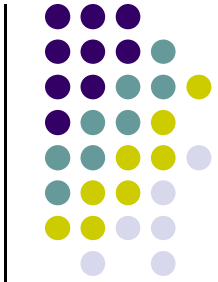
Configuration (Local)	• Choice of medium access protocol • Choice of correct cabling and connectors • Choice of cabling layout • Determining the number of physical interfaces on devices • Setting device interface parameter values ❑ Interrupts ❑ I/O Addresses ❑ DMA numbers ❑ Network layer addresses (e.g. 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



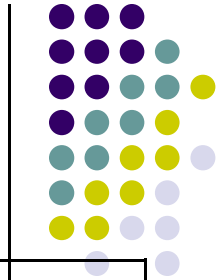
Configuration (Automated)	• Using the Dynamic Host Configuration Protocol (DHCP) to configure IP addresses • Using Plug and Play enabled NICs for automatic selection of interrupts and I/O addresses • Domain Name Services (DNS) addresses • Trap messages from agents
Inventory (Manual)	• Maintaining records 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



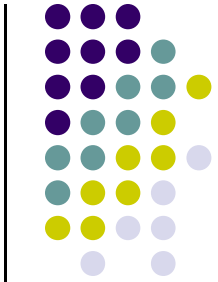
- Control access to network/resources
  - Authentication: who goes there?
  - Authorization: are you allowed to do that?
  - Firewalls
  - Intrusion detection systems (IDS)
  - Notification of (attempted) breaches, etc.
- Critical to always authenticate participants
- SNMPv1 has very little security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

Security Management Sub-categories



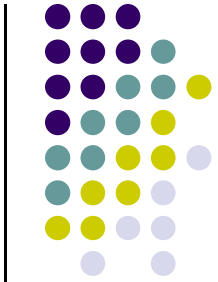
Applying Basic Techniques	• Identifying hosts that store sensitive information • Management of passwords • Assigning user rights and permissions • Recording failed logins • Setting remote access barrier codes • Employing virus scanning • Limiting views of the Enterprise network • Tracking time and origin 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 should be able to present network maps. • Reports of invalid access point attempts are generated daily for analysis

Accounting Management



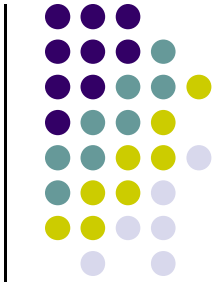
- Measuring the usage of network resources in order to distribute costs and resources
- E.g., monitoring the use of a server by users in a specific department and charging the department accordingly

Accounting Management Sub-categories



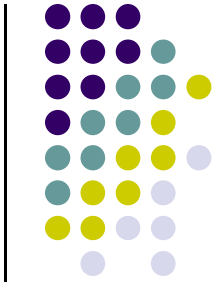
Gather Network Device Utilization Data	• Measure usage of resources by cost center • Set quotas to enable fair use of resources • Site metering to track adherence to software licensing
Bill Users of Network Resources	• Set charges based on usage. • Measure one of the following ❑ Number of transactions ❑ 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



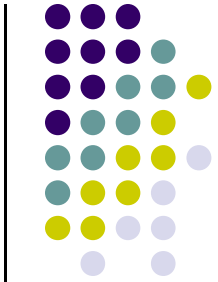
Company	Product	URL	Comments
Apptitude (HiFn)	Meterware/ Analyzer	http://www.hifn.com	NMS used in this book. Is a complete SNMPv1 tool. It is only available with the book. Apptitude was a leader in SNMP management software and hardware for many years. HiFn develops integrated circuits for encryption.
SNMP Research Internation al	• 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



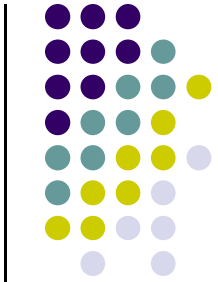
Triticom	LANdecoder SNMP Manager	http://www.triticom.com/	LANdecoder SNMP Manager is a simple, easy to use SNMP Manager for Microsoft Windows environment. With it, you can query and control any SNMP-capable device on your network. It can operate standalone or be integrated with Triticom's LANdecoder 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



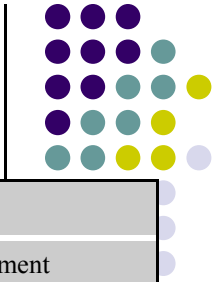
Company	Product	URL	Comments
Network Instruments	Observer 8	http://www.netinst.com/html/observer.html	Supports Ethernet, Token Ring, FDDI, GigaBit and Windows 98/ME and NT/2000/XP. Includes capture for protocol analysis. Price is $995.00
Precision Guesswork	LANwatch32 v6.0	http://www.guesswork.com/snmptool.html	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.

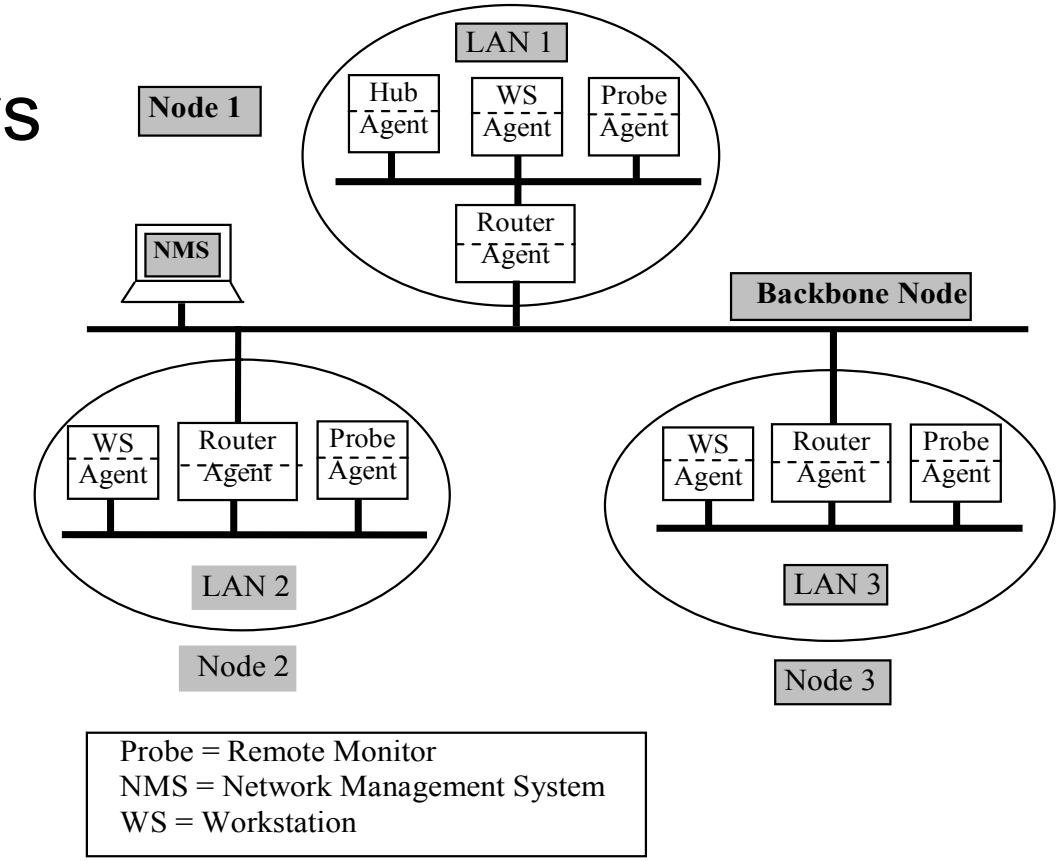
Management Tools



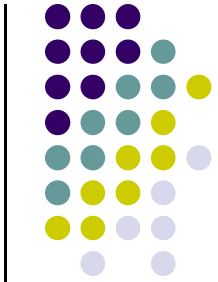
Company	Product	URL	Comments
HP	Toptools	http://www.hp.com/toptools/prodinfo/overview.intro.html	Toptools is a comprehensive hardware management product. It has many plug-ins for specific hardware. All its features can be integrated into your enterprise management platforms such as hp OpenView Network 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



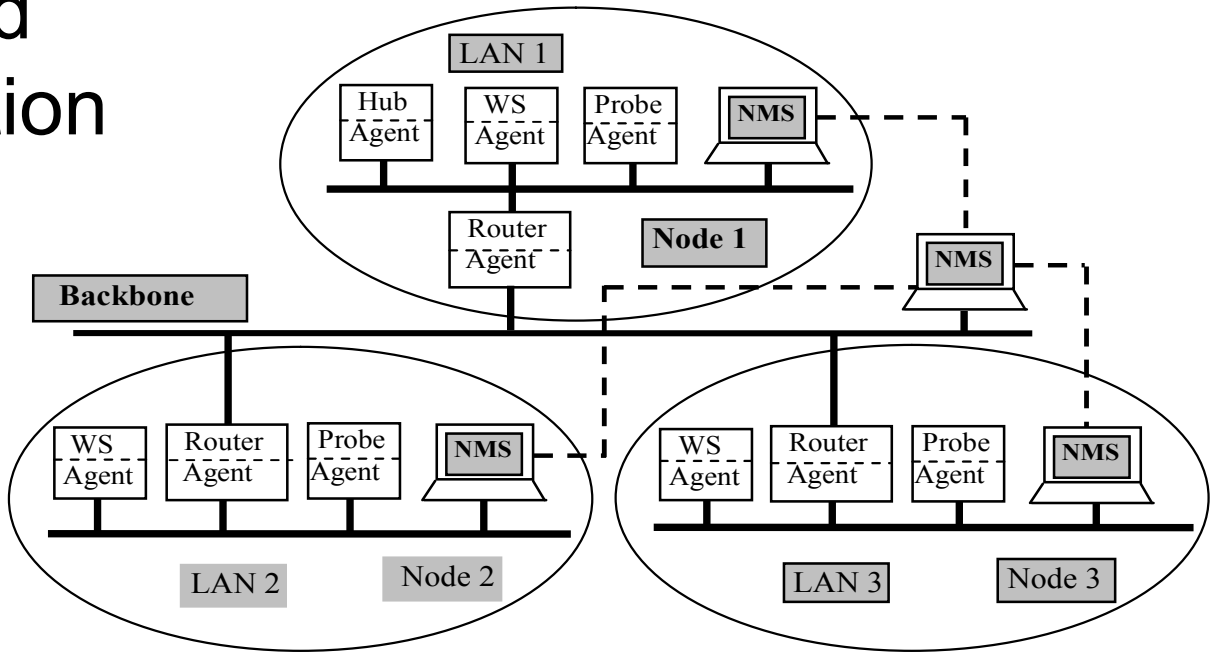
Network Management Configuration



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

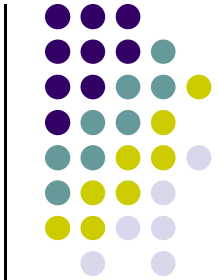
Network Management Configuration

- Distributed configuration



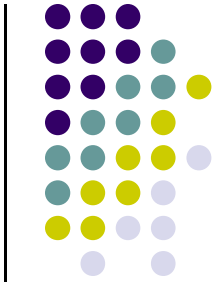
Probe = Remote Monitor
NMS = Network Management System
WS = Workstation
-------- = In-band or out-of band management communication

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.