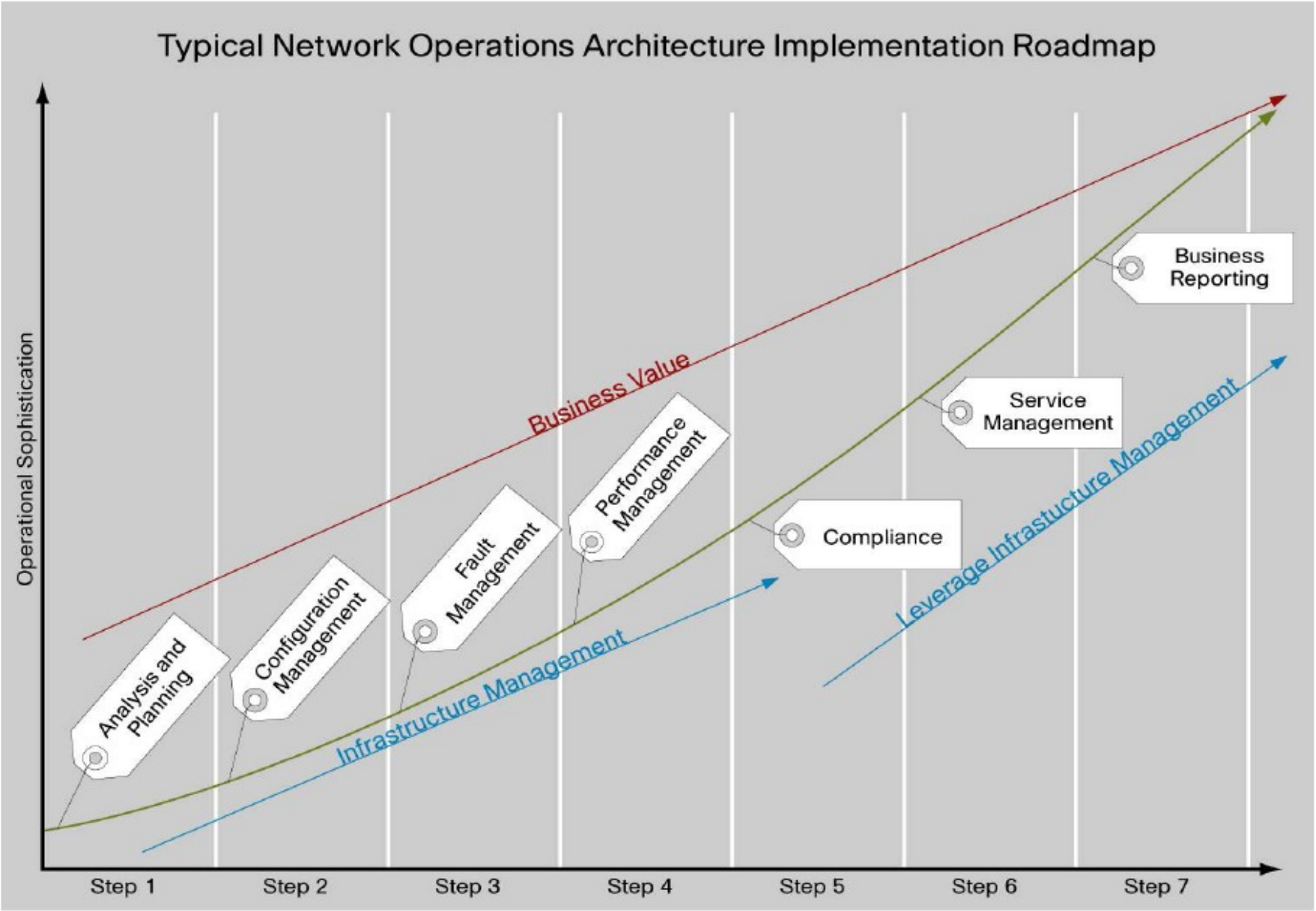
Network Management

Arquitetura de Redes

Mestrado Integrado
Engenharia de Computadores e Telemática
DETI-UA

universidade de aveiro
deti.ua.pt

Network Implementation and Management



Network Management (1)

- Documentation and Diagrams
  - Network documentation and diagrams are critical in a production environment
    - Provide information when troubleshooting network outages; they are, however, static
    - In a dynamic network environment, purely static documentation is not suitable
  - An effective configuration management capability should provide up-to-date and dynamically updated information
    - When combined with static documentation and diagrams, it provides more relevant information to support network operations
- Compliance
  - Compliance is about meeting regulations imposed by government or industry
  - It is not however a matter of buying a product and being compliant; it is about building capabilities to support compliance over time

Network Management (2)

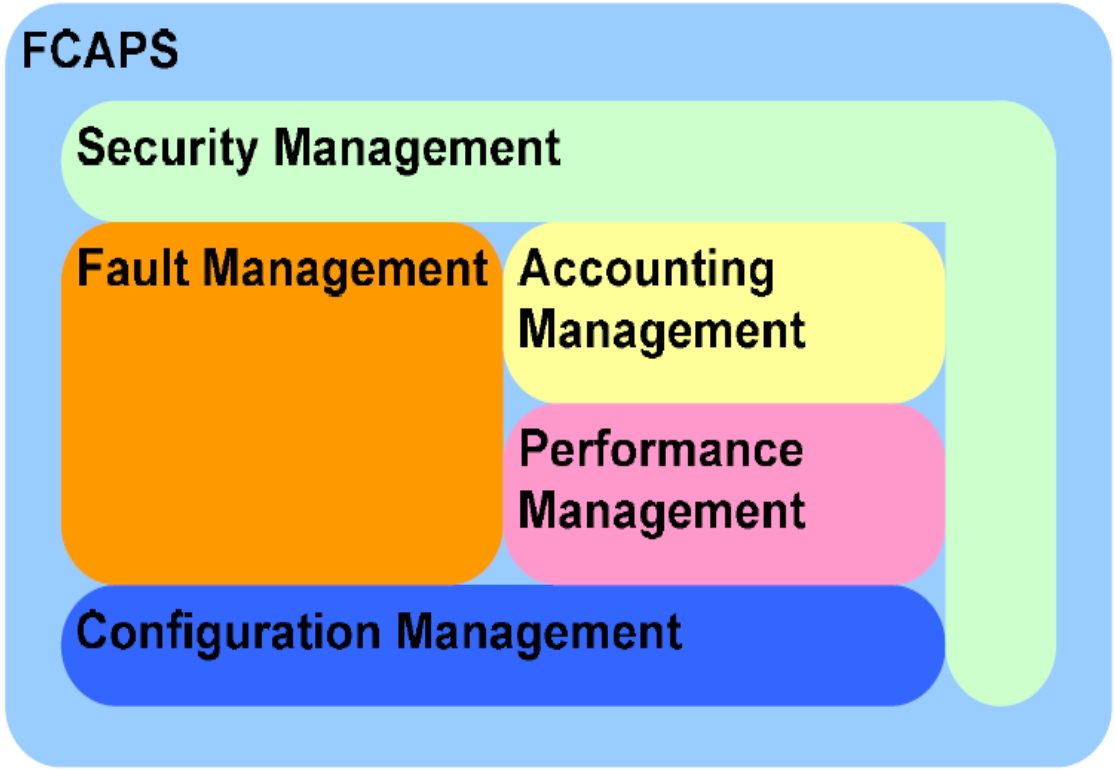
- Managing Risk
  - A key issue with network management is the rapid increase in the number and heterogeneity of network elements
    - The ability to understand risk exposure becomes more difficult
  - The ability to understand exposure is no longer possible without new capabilities in auditing and reporting
  - Requires appropriate supporting processes and operational methodologies so that the risk can be understood and expediently mitigated
- Time to Resolve
  - A key measure in many service levels is incident time to resolution
  - An incident will result from a network outage, and in simple terms, an outage to a production network that is considered stable is caused by one of the following:
    - Layer 1 network failure (leased line, fiber cut, and so on),
    - Physical infrastructure failure, power, air conditioning
    - Hardware failure, power supply, chassis, or module
    - Software failure, due to memory leak or bug
    - Security exploit, causing DOS or software failure
    - A change in configuration, either logical (being a new feature) or physical (being new hardware or connections)
  - Configuration management assists with time to resolution by providing the necessary information to support troubleshooting and decision making. If a network outage is caused by a configuration change, this needs to be eliminated as the root cause in the first instance.

Network Management Models

- FCAPS (Fault, Configuration, Accounting, Performance and Security)
  - Popular conceptual framework for network management
  - Sponsored by ISO
  - For all networks
  - Functions: Fault, Configuration, Accounting, Performance and Security
- TMN (Telecommunications Management Network)
  - Conceptual framework for many Service Provider's network management systems
  - Sponsored by ITU-T
  - For telecommunications networks
  - Functions: Business Management, Service Management, Network Management and Element Management
- OAM&P (Operation, Administration, Maintenance and Provisioning)
  - Widely adopted by large Service Providers in their network management systems
  - Sponsored by service providers
  - For telecommunication networks
  - Functions: Operation, Administration, Maintenance and Provisioning
- TOM (Telecoms Operations Map) and eTOM (enhanced Telecom Operations Map)
  - Designed to replace the OAM&P.
  - Sponsored by TeleManagement Forum
  - For service provider's networks
  - Functions: Network and Systems management, Service development and Operations, Customer care

FCAPS

- Each of the functions interacts with each of the others
- Security has to touch all the functions to be effective
- Configuration is the function that holds the important data for all the functions



FCAPS - Fault Management

- Set of functions that enable the detection, isolation, and correction of abnormal operation of the telecommunication network
- Consists of the following functions
  - Reliability, Availability, and Survivability (RAS) quality assurance
    - Establishes the reliability criteria that guide the design policy for redundant equipment
  - Alarm surveillance
    - Describes the capability to monitor network element failures in near-real time
  - Fault localization
  - Fault correction
  - Testing
    - A network element analyzes equipment functions
    - Active testing of external device components, such as circuits, links, and neighbor devices
  - Trouble administration
    - Transfers trouble reports originated by customers and trouble tickets originated by proactive failure-detection checks

FCAPS - Configuration Management

- Provides functions to identify, collect configuration data from, exercise control over, and provide configuration data to network elements.
- Configuration management supports the following functions
  - Installing the physical equipment and logical configurations
  - Service planning and negotiation
    - Planning for the introduction of new services, changing deployed service features, and disconnecting existing services
  - Provisioning
    - Consists of necessary procedures to bring equipment into service but does not include installation
  - Status and control
    - Provides the capability to monitor and control certain aspects of the network elements
  - Network planning and engineering
    - Functions associated with determining the need for growth in capacity and the introduction of new technologies

FCAPS - Accounting Management

- Provides the procedures to measure the use of network services and determine costs to the service provider and charges to the customer for such use
- Includes the following functions:
- Usage measurement
  - Planning and management of the usage measurement process
  - Network and service usage aggregation, correlation, and validation
  - Usage distribution
  - Usage surveillance
  - Usage testing and error correction
  - Measurement rules identification
  - Usage short-term and long-term storage
  - Usage accumulation and validation
  - Administration of usage data collection
  - Usage generation
- Tariffing and pricing
  - A tariff is used to determine the amount of payment for services usage.
- Collections and finance
  - Functionality for administering customer accounts, informing customers of balances and payment dates, and receiving payments.
- Enterprise control
  - This group supports the enterprise's financial responsibilities, such as budgeting, auditing, and profitability analysis.

FCAPS - Performance Management

- Provides functions to evaluate and report on the behavior of telecommunication equipment and the effectiveness of the network or network element
- Collect and analyze statistical data for the purpose of monitoring and correcting the behavior and effectiveness of the network, network elements, or other equipment, and to aid in planning, provisioning, maintenance, and quality measurement.
- Includes the following functions:
  - Performance quality assurance
    - Includes quality measurements, such as performance goals and assessment functions
  - Performance monitoring
    - Continuous collection of data concerning the performance of the network element.
    - May also be designed to detect characteristic patterns of impairment before the quality has dropped below an acceptable level
  - Performance management control
    - Includes the setting of thresholds and data analysis algorithms and the collection of performance data
    - It has no direct effect on the managed network
    - Includes functions that affect the routing and processing of traffic
  - Performance analysis
    - Collected performance records may require additional processing and analysis to evaluate the entity's performance level
    - Includes functions: Recommendations for performance improvement, Exception threshold policy, Traffic forecasting (trending), Performance summaries (per network and service, and traffic-specific), Exception analysis (per network and service, and traffic-specific), Capacity analysis (per network and service, and traffic-specific) and Performance characterization

FCAPS - Security Management

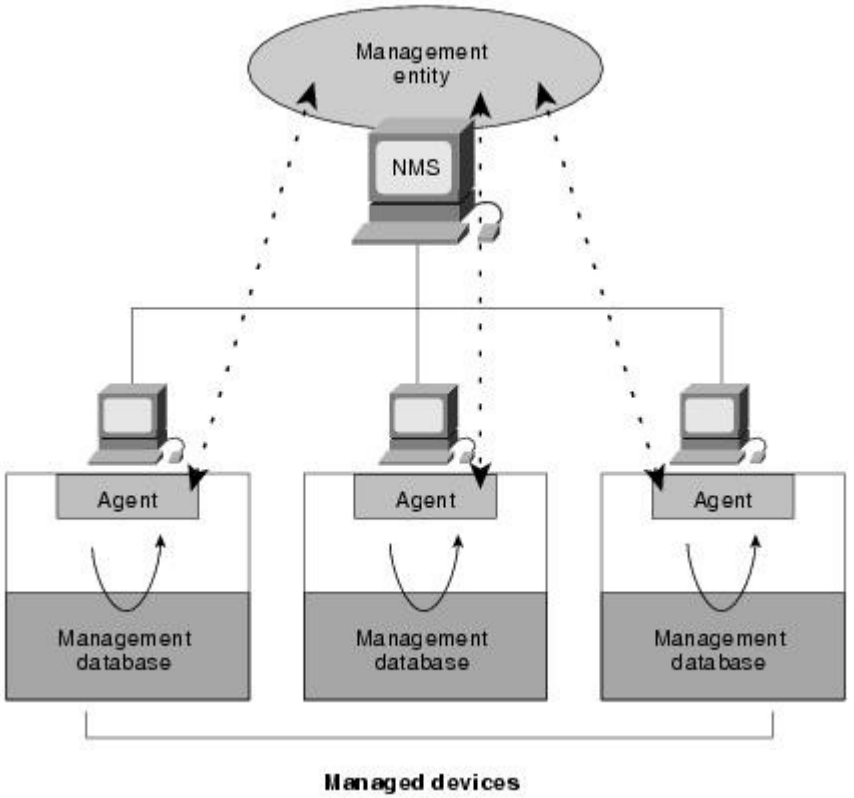
- Security is required for all functional areas.
- Security management consists in providing
  - Services for communications provide authentication, access control, data confidentiality, data integrity, and non-repudiation.
  - Security event detection and reporting reports activities that may be construed as a security violation (unauthorized user, physical tampering with equipment) on higher layers of security applications
- Security management includes the following functions:
  - Prevention
  - Detection
  - Containment and recovery
  - Security administration

SNMP

Simple Network Management Protocol

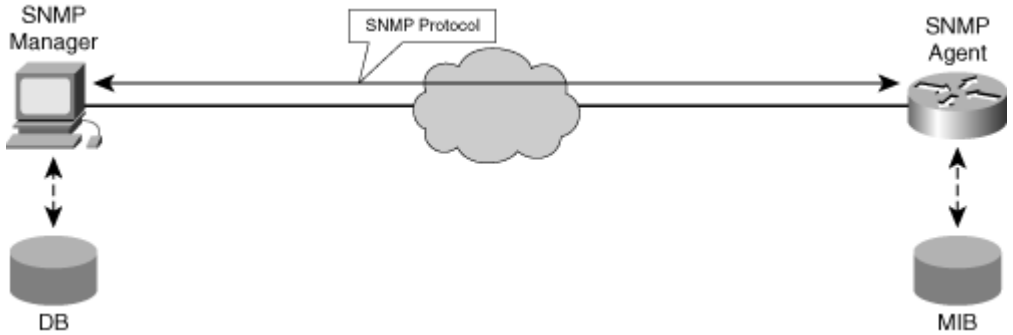
SNMP Basic Components

- An SNMP-managed network consists of three key components:
- Managed devices
  - Network node that contains an SNMP agent.
  - Collect and store management information and make this information available using SNMP.
  - Can be routers and access servers, switches and bridges, hubs, computer hosts, or printers.
- Agents
  - Network-management software module that resides in a managed device.
- Network-management systems (NMSs)
  - Executes applications that monitor and control managed devices.
  - Provide the bulk of the processing and memory resources required for network management.
  - One or more NMSs must exist on any managed network.



Data Collection Protocols: SNMP, SMI, and MIB

- SNMP is an Internet protocol developed by the IETF
- It is designed to facilitate the exchange of management information between network elements



- SNMP agent
  - A software module that resides in network elements; it collects and stores management information specified in the supported MIB modules. The SNMP agent responds to SNMP requests from an NMS station for information and actions. The SNMP agent can send fault notifications pro-actively to the SNMP manager.
- Managed object
  - A representation of something that can be managed.
  - Managed objects differ from variables, which are particular object instances.
- Management Information Base (MIB)
  - A collection of managed objects residing in a virtual information store.
  - A collection of related managed objects is defined in a specific MIB module.
  - A MIB can be considered a local data store at the network element.
- Syntax notation
  - A language used to describe managed objects in a machine-independent format
  - SNMP-based management systems use a subset of the International Organization for Standardization's (ISO) Open System Interconnection (OSI) Abstract Syntax Notation 1 (ASN.1, International Telecommunication Union Recommendation X.208) to define both the packets exchanged by the management protocol and the objects that are to be managed.
- Structure of Management Information (SMI)
  - Defines the rules for describing management information (the MIB). The SMI is defined using ASN.1.

SNMP Basic Commands

- Managed devices are monitored and controlled using four basic SNMP commands: read, write, trap, and traversal operations.
  - The **read** command is used by an NMS to monitor managed devices. The NMS examines different variables that are maintained by managed devices.
  - The **write** command is used by an NMS to control managed devices. The NMS changes the values of variables stored within managed devices.
  - The **trap** command is used by managed devices to asynchronously report events to the NMS. When certain types of events occur, a managed device sends a trap to the NMS.
  - Traversal operations are used by the NMS to determine which variables a managed device supports and to sequentially gather information in variable tables, such as a routing table.

SNMP: Polling

- Manager periodically asks the agent for new information

☺ Advantage: Manager completely controls the equipment, and knows all network details

☹ Disadvantage: Delay between event and its entry in the system, and unnecessary communication overhead:

  - Slow polling, slow answer to the events
  - Quick polling, quick reaction, but large bandwidth waste

SNMP: Traps

- There is an event → trap is sent
- Trap contains appropriate information

  equipment name, time instant of event, type of event

☺ Advantage: information only generated when required

☹ Disadvantage:

- ☹ More resources required in the managed equipment
- ☹ Traps can be useless
  - If many events occur, bandwitdh can be wasted with all traps (thresholds can solve)
  - Since the agent has only a limited scope of the network, NMS may already know about the events.

- Traps&Polling
  - Event occurs → trap is sent
  - Manager performs polling to obtain the rest of information
  - Manager also performs periodic polling, as backup

SNMP Versions

Model	Level	Authentication	Encryption	What Happens
v1	noAuthNoPriv	Community String	No	Uses a community string match for authentication.
v2c	noAuthNoPriv	Community String	No	Uses a community string match for authentication.
v3	noAuthNoPriv	Username	No	Uses a username match for authentication.
v3	authNoPriv	MD5 or SHA	No	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithm.
v3	authPriv	MD5 or SHA	DES or AES	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides DES 56-bit or CFB128-AES-128 encryption in addition to authentication based on the CBC-DES (DES-56) standard.

SNMPv1: security and authentication

- In its initial version, authorization and authentication were based on the notion of “SNMP community string”
- The “words of community” identify the permissions of the machine accessing the agent: read-only ou read-write
- By default, all systems are configured with the community strings:
  - public (read-only)
  - private (read-write)
- The words are case sensitive.

SNMPv2c and SNMPv3 versions

- SNMPv2 extensions
  - Structure of management information (SMI)
  - Manager-Manager capacity
  - New protocol operations
- SNMPv3 extensions
  - New message format
  - Message security
  - Access control

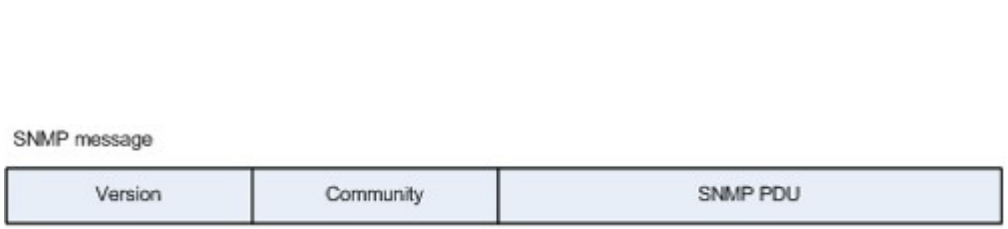
SNMPv3: Security

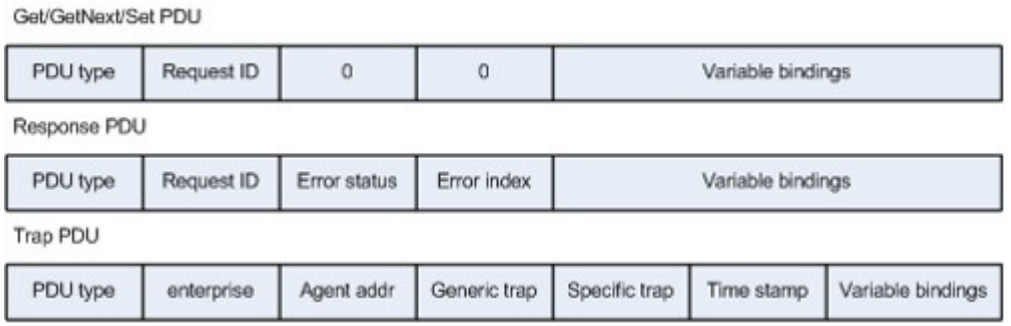
- Notion of “access control dependent on the user”
  - The agent mantains access rights information (policies) to different users in a data base
- Authentication: shared secret key
  - MD5 or SHA authentication passphrase hashes
- Privacy
  - Packet data may now be DES encrypted (future use allows additional encryption)
  - Passphrase defaults to authentication passphrase
  - Allows for unique Privacy passphrase
- Protection against replays: resort to nounces*

*arbitrary number used only once in a cryptographic communication

SNMPv1 Message

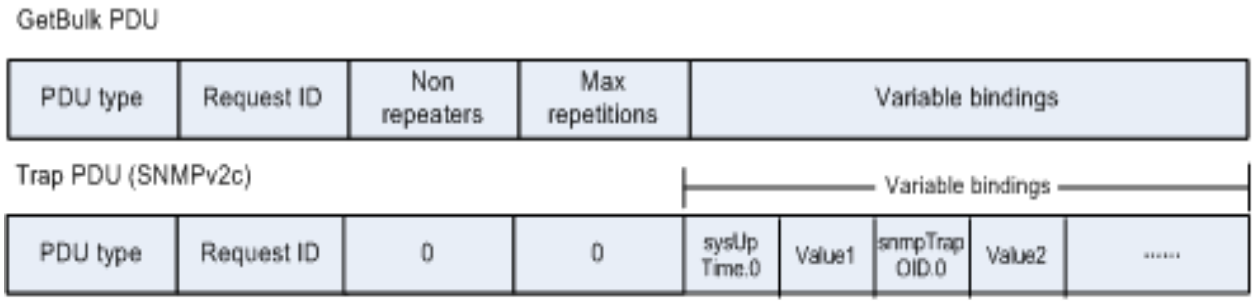
- Version: SNMP version.
- Community: Community name, used for the authentication between an agent and the NMS.
  - In Get or GetNext operations, read community name is used for authentication;
  - In Set operation, write community name is used for authentication.
- Request ID: It is used to match a response to a request.
  - SNMP assigns a unique ID to each request.
- Error status: It is used in a response to indicate the errors when the agent processes the request
  - noError, tooBig, noSuchName, badValue, readOnly, and genErr.
- Error index: Provides the information of the variables that caused the error when an error occurs.
- Variable bindings: It is composed of a variable name and value.
- Enterprise: Type of the device that generates traps.
- Agent addr: Address of the device that generates traps.
- Generic trap: It includes coldStart, warmStart, linkDown, linkup, authenticationFailure, egpNeighborLoss and enterpriseSpecific.
- Specific trap: Specific trap information of a vendor.
- Time stamp: The amount of time between the time when the SNMP entity sending this message reinitialized and the time when traps were generated, that is, the value of sysUpTime.



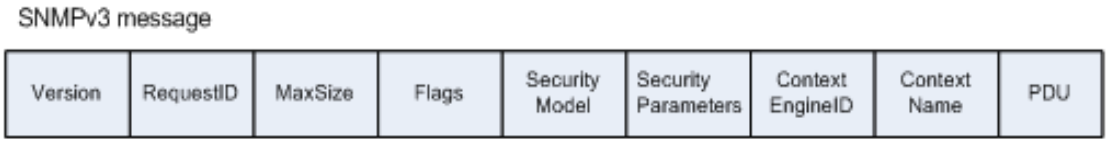


SNMPv2c Message

- Compared with SNMPv1, GetBulk packets are added in SNMPv2c.
  - GetBulk operation corresponds to GetNext operation.
  - In a GetBulk operation, the setting of Non repeaters and Max repetitions parameters enables NMS to obtain data of many managed objects from an agent.
- In SNMPv2c, trap message format is different from that in SNMPv1.
  - SNMPv2c trap PDU adopts the format of SNMPv1 Get/GetNext/Set PDU, and sysUpTime and snmpTrapOID are used as variables in variable bindings to create a packet.



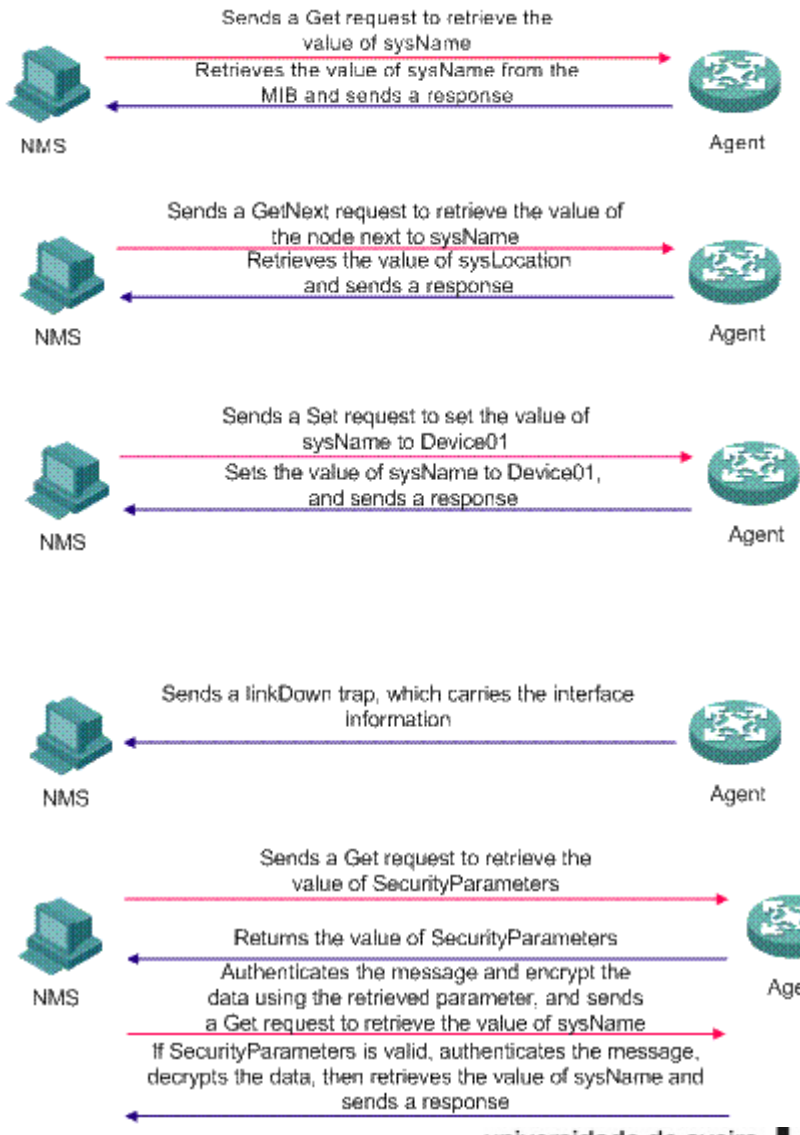
SNMPv3 Message



- SNMPv3 message format is modified, but the PDU format is the same as that in SNMPv2c.
- The entire SNMPv3 message can be authenticated, and EngineID, ContextName, and PDU are encrypted.
- RequestID, MaxSize, Flags, SecurityModel and SecurityParameters form the SNMPv3 message header.
- Fields:
  - RequestID
  - MaxSize: The maximum size of the message that the sender of the message can receive.
  - Flags: Message flag which occupies one byte. Only the lowest three bytes are valid. 0x0 indicates no authentication no privacy, 0x1 indicates authentication without privacy, 0x3 indicates authentication with privacy, and 0x4 indicates to send a report PDU.
  - SecurityModel: Message security model, in the range 0 to 3. 0 indicates any model, 1 indicates SNMPv1 security model, 2 indicates SNMPv2c security model, and 3 indicates SNMPv3 security model.
  - SecurityParameters includes the following fields:
    - AuthoritativeEngineID: Specifies the snmpEngineID of the authoritative SNMP engine involved in the exchange of the message, used for identification, authentication and encryption for an SNMP entity. This field refers to the source for a trap, response, or report, and to the destination for a Get, GetNext, GetBulk, or Set operation.
    - AuthoritativeEngineBoots: Specifies the snmpEngineBoots value at the authoritative SNMP engine involved in the exchange of the message. It indicates the number of times that this SNMP engine has initialized or reinitialized itself since its initial configuration.
    - AuthoritativeEngineTime: Specifies the snmpEngineTime value at the authoritative SNMP engine involved in the exchange of the message. It is used for time window check.
    - UserName: Specifies the user (principal) on whose behalf the message is being exchanged. Usernames configured on NMS and Agent must be the same.
    - AuthenticationParameters: A key used in authentication calculation. If no authentication is performed, this field is null.
    - PrivacyParameters: A parameter used in privacy calculation.
  - ContextEngineID: Uniquely identifies an SNMP entity. For a message received, this field decides how this message will be processed; for a message sent, this field is provided by the sender.
  - ContextName: Identifies a context. Must be unique within an SNMP entity.

SNMP Operations

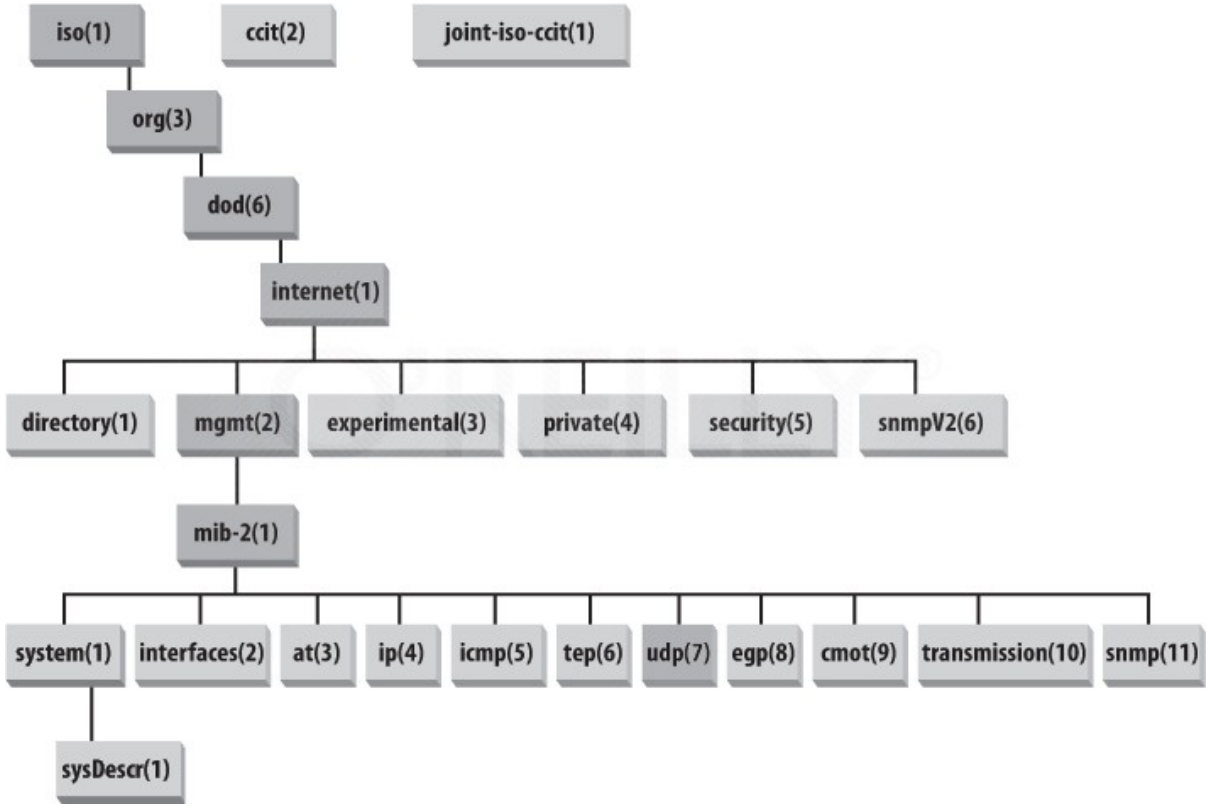
- SNMP provides the following five basic operations:
  - Get operation
    - Request sent by the NMS to the agent to retrieve one or more values from the agent.
  - GetNext operation
    - Request sent by the NMS to retrieve the value of the next OID in the tree.
  - Set operation
    - Request sent by the NMS to the agent to set one or more values of the agent.
  - Response operation
    - Response sent by the agent to the NMS.
  - Trap operation
    - Unsolicited response sent by the agent to notify the NMS of the events that occurred.
- In SNMPv3 get operations are performed using authentication and encryption.



Structure of Management Information (SMI)
&
Management Information Base (MIB)

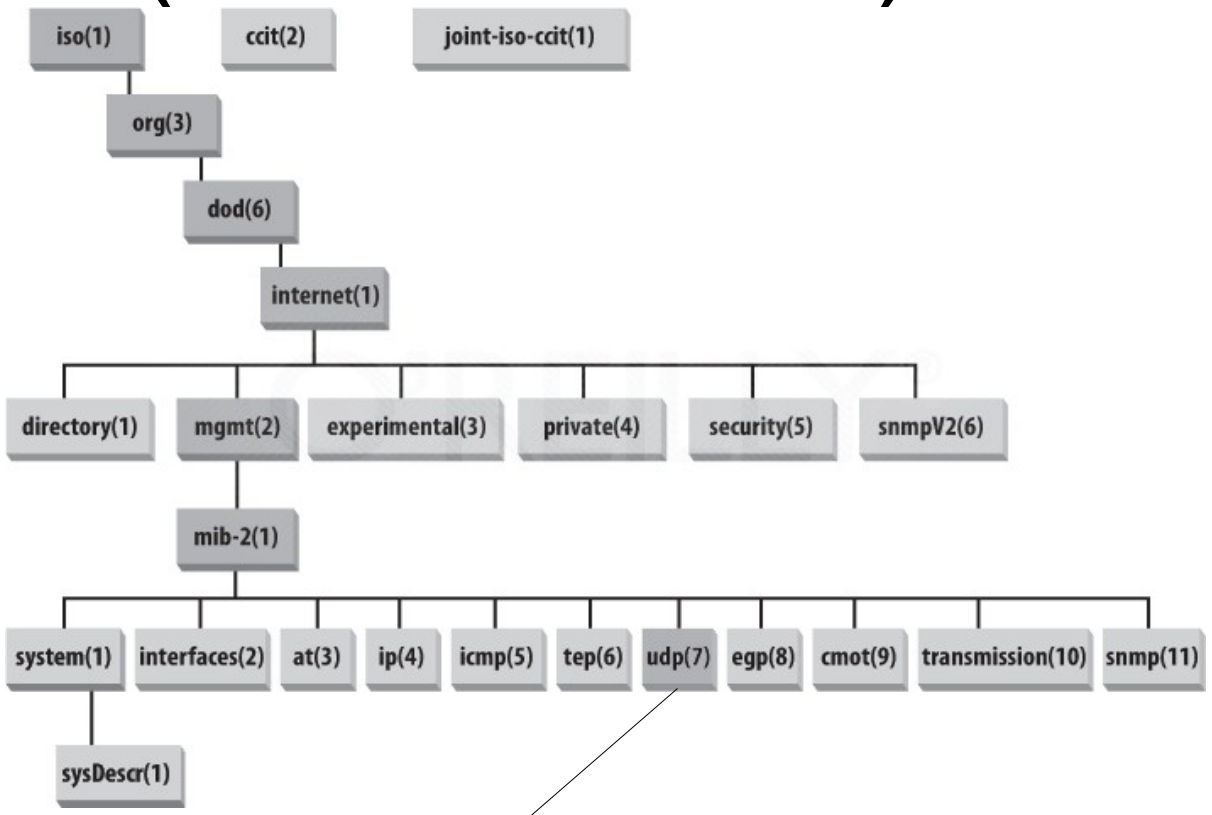
MIB Modules and Object Identifiers

- An SNMP MIB module is a specification of management information on a device
- The SMI represents the MIB database structure in a tree form with conceptual tables, where each managed resource is represented by an object
- Object Identifiers (OIDs) uniquely identify or name MIB variables in the tree
  - Ordered sequence of nonnegative integers written left to right, containing at least two elements
  - For easier human interaction, string-valued names also identify the OIDs
    - MIB-II (object ID 1.3.6.1.2.1)
    - Cisco private MIB (object ID 1.3.6.1.4.1.9)
- The MIB tree is extensible with new standard MIB modules or by experimental and private branches
  - Vendors can define their own private branches to include instances of their own products



SNMP Names (numbers/OID)

- To nominate all possible objects (protocols, data, etc.) an ISO Object Identifier (OID) tree is used:
  - Hierarchic nomenclature of objects
  - Each leaf of the tree has a name and number



1.3.6.1.2.1.7.1

ISO
ISO-ident. Org.
US DoD
Internet

udpInDatagrams
UDP
MIB2
management

SNMP MIBs

- Management Information Base (MIB): set of managed objects, used to define information from equipments, and created by the manufacturer
- Example: UDP module

Object ID	Name	Type	Comments
1.3.6.1.2.1.7.1	UDPInDatagrams	Counter32	Number of UDP datagrams delivered to users.
1.3.6.1.2.1.7.2	UDPNoPorts	Counter32	Number of received UDP datagrams for which there was no application at the destination port.
1.3.6.1.2.1.7.3	UDPInErrors	Counter32	The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.
1.3.6.1.2.1.7.4	UDPOutDatagrams	Counter32	The total number of UDP datagrams sent from this entity.

SMI: Data language definition

- Well-defined sintax and semantics of management information
  - Type of basic data
    - INTEGER, Integer32, Unsigned32, OCTET, STRING, OBJECT IDENTIFIED, IPaddress, Counter32, Counter64, Guage32, Tie Ticks,Opaque...
  - Type of object
    - Type of data, status, semantic of the managed object
  - Module identification
    - Collection of objects inter-related in the MIB

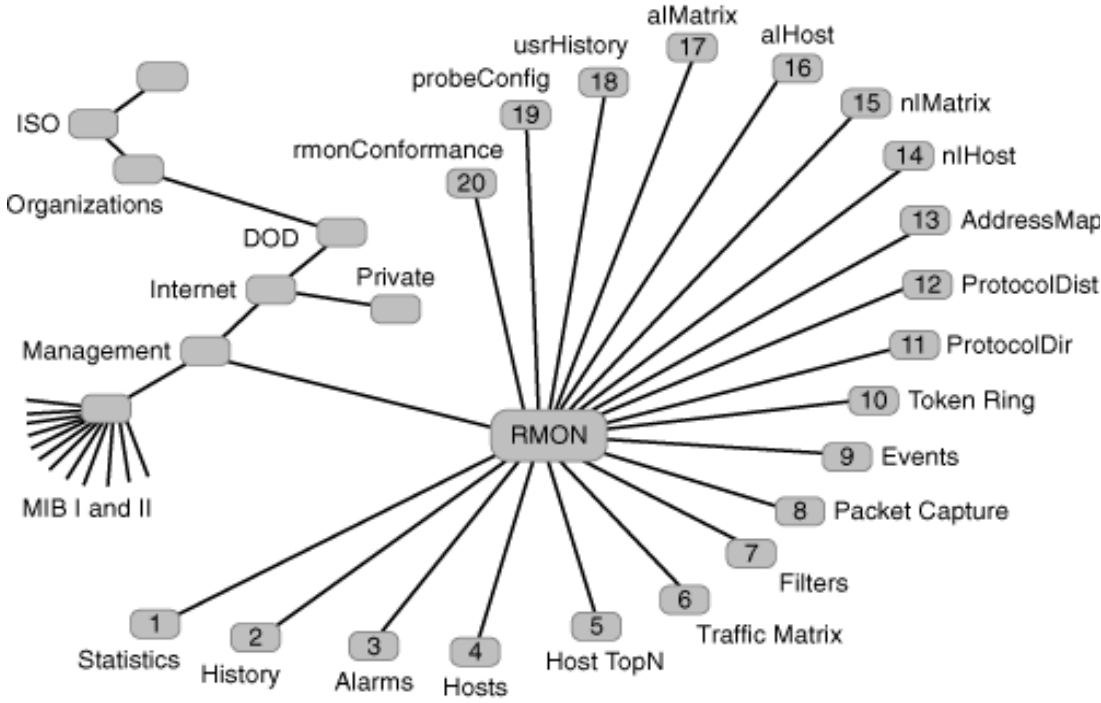
SMI: Data Types for Scalars

	SMIv1	SMIv2
SIMPLE TYPES:	INTEGER	INTEGER
	OCTET STRING	OCTET STRING
	OBJECT IDENTIFIER	OBJECT IDENTIFIER
	-	Integer32
APPLICATION-WIDE TYPES:	-	Unsigned32
	Gauge	Gauge32
	Counter	Counter32
	-	Counter64
	TimeTicks	TimeTicks
	IpAddress	IpAddress
	Opaque	Opaque
	NetworkAddress	-
PSEUDO TYPES:	-	BITS

Remote Network MONitoring (RMON)

RMON

- RMON is a set of standardized MIB variables that monitor networks
  - All previously defined MIBs monitored only nodes
- RMON has 9 groups
  - Statistics, History, Alarm, Host, HostTopN, Matrix, Filter, Packet Capture, and Event
- The term RMON now is often used to refer to the concept of remote monitoring and to the entire series of RMON MIB extensions
- The main RMON MIB extensions are:
  - RMON 1 and RMON 2 MIBs - Remote Monitoring MIB versions 1 and 2
  - DSMON MIB - Remote Monitoring MIB Extensions for Differentiated Services
  - SMON MIB - Remote Network Monitoring MIB Extensions for Switched Networks
  - APM MIB - Application Performance Measurement MIB



RMON Statistics

- Provides data for fault analysis, configuration and performance
- Measurements obtained per interface
- Measured statistics:
  - Packets, bytes, broadcasts, multicasts, collisions, errors
  - Packet distribution length (several levels)
    - 65 - 127 bytes
    - 128 - 255 bytes
    - 256 - 511 bytes
    - 512 - 1023 bytes
    - 1024 - 1518 bytes
  - Reports errors

RMON History

- Periodically stores statistic RMON values to further analysis
  - Configurable in terms of what can be monitored (parameters and interfaces) and monitoring periodicity
- Very useful for performance management
- Uses a circular buffer, whose lenght can be configured

RMON Alarm

- Useful for faults and performance management
- Defines thresholds (along time) and generates notifications
- Works based on
  - Absolute and relative values (deltas)
  - Alarms to increase, decrease, or both

RMON Host and HostTopN

- RMON Host
  - Monitors objects per host, in each probe segment
  - Uses addresses, source and destination, creation time instant
  - Useful for configuration, performance and accounting management
  - Information:
    - IN / OUT, PACKETS / OCTETS, BROADCASTS, MULTICASTS, ERRORS
- RMON HostTopN
  - Uses RMON Host objects to prepare reports about sets of hosts, in a specified period
  - Reports made for NMS requested values

RMON Matrix

- Object tables that maintain traffic statistics between a pair of addresses
- Determines traffic patterns in a network segment
- Used for performance management, security (determines attackers), and accounting
- Data is monitored
  - For each destination and source address
    - Packets, bytes and errors

RMON Filter, Packet Capture and Events

- RMON Filter
  - Used to configure probes to packet analysis
  - Used in fault management and security
- RMON Packet Capture
  - Defines buffering schemes for packets in the filtering group
  - Allows the counting of packets as a function of specific patterns
  - Enables packets to be captured after they flow through a channel.
    - Size of buffer for captured packets, full status (alarm), number of captured packets.
- RMON Events
  - Defines events, creates logs and/or generates traps
  - May eliminate resort to constant “polling”
  - Used for fault management, performance and security

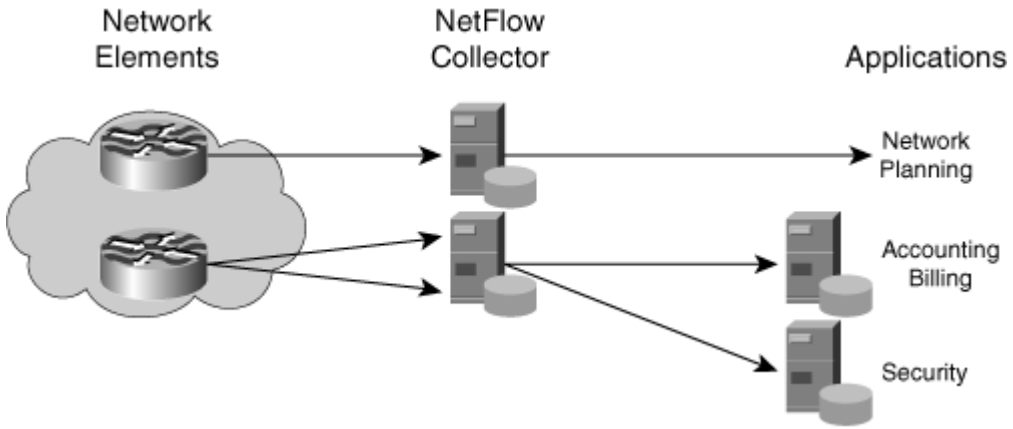
RMON 2

- RMON 2 also contains these groups:
  - Protocol Directory: list of protocols the probe can monitor
  - Protocol Distribution: traffic statistics for each protocol
  - Address Map: maps network-layer (IP) to MAC-layer addresses
  - Network-Layer Host: layer 3 traffic statistics, per host
  - Network-Layer Matrix: layer 3 traffic statistics, per source/destination pairs of hosts
  - Application-Layer Host: traffic statistics by application protocol, per host
  - Application-Layer Matrix: traffic statistics by application protocol, per source/destination pairs of hosts
  - User History: periodic samples of user-specified variables
  - Probe Configuration: remote configure of probes
  - RMON Conformance: requirements for RMON2 MIB conformance
- RMON: used to analyze network segments.
- RMON 2: used in network backbones.

Network Awareness

Data Collection Protocols: NetFlow and IPFIX Export Protocols

- Cisco IOS NetFlow services give network administrators access to information about IP flows within their networks
  - An IP flow is defined as a unidirectional sequence of packets between given source and destination endpoints
  - IP flows are highly granular; flow endpoints are identified by IP address and by transport layer application port numbers
- NetFlow flow records are exported to an external device, a NetFlow collector
  - Can be used for a variety of purposes, including network management and planning, enterprise accounting, departmental chargeback, ISP billing, data warehousing, user monitoring and profiling, combating denial of service (DoS) attacks, and data mining for marketing purposes



- The IETF IPFIX stands for "IP Flow Information eXport," is an IETF effort to standardize an export protocol similar to NetFlow
  - A protocol that exports flow-related information
  - IPFIX protocol specifications are largely based on the NetFlow version 9 export protocol

Data Collection Protocols: PSAMP

- The Packet Sampling (PSAMP) working group history started immediately after the IPFIX working group creation
- There was a clear need to define a standard set of capabilities for network elements to sample subsets of packets by statistical and other methods
  - Specifically, on the high-end routers where monitoring every packet was practically impossible
- The focus of the working group was to
  - Specify a set of selection operations by which packets are sampled
  - Specify the information that will be made available for reporting on sampled packets
  - Describe protocols by which information on sampled packets is reported to applications
  - Describe protocols by which packet selection and reporting are configured
- For export of PSAMP packet information, the IPFIX protocol is used

Monitoring and Management Tools

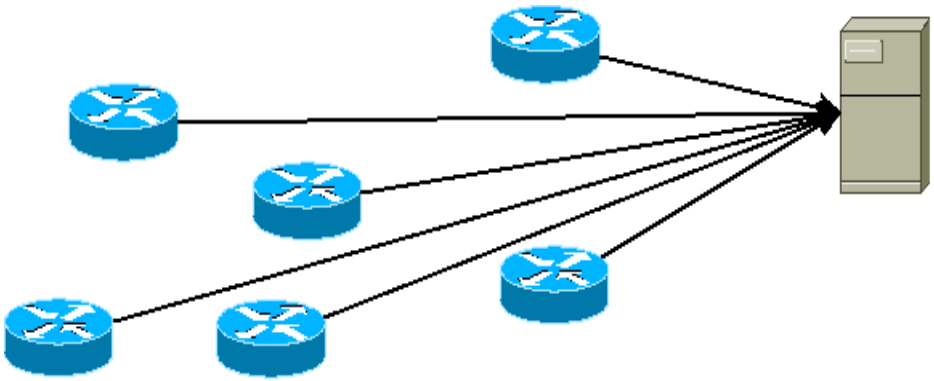
- Integrated Monitoring & Management
  - CiscoWorks
    - SNMP and Cisco Discovery Protocol (CDP) based
  - Allows equipment reconfiguration and firmware update
- Monitoring (and Alert)
  - Link usage, flow analysis, traffic matrices, protocol usage
  - SNMP and/or pcap lib based tools
    - Multiple proprietary tools
    - Open source/freeware
      - Cacti, Nagios, NTOP, OpenNMS
  - Netflow based tools
- Management
  - Console/scripting based tools
- In Research (advanced traffic capture and processing capabilities)
  - Pcap lib based tools
    - TCPdump, Wireshark, Tshark, etc...
  - DAG technology (cards+software)

Network Awareness

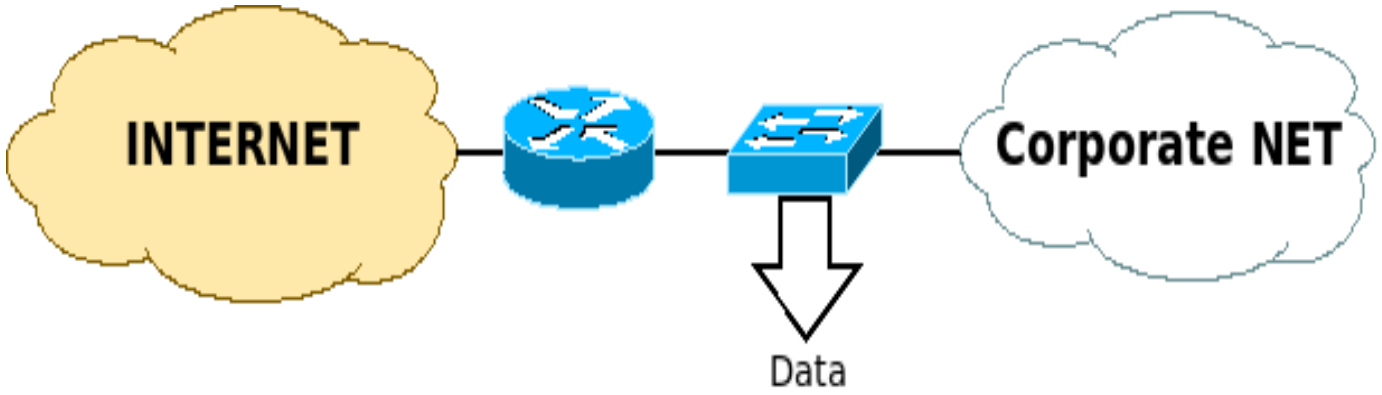
- Acquiring knowledge on current Users, Services, Traffic and Network profiles/behaviors/interactions
- Acquire knowledge about the network at ALL LEVELS
  - Users
    - Location and movement
    - Applications' preferences
    - Usage profiles / Hourly behavior
  - Applications
    - Characteristic signatures
    - Relation with the network
  - Traffic
    - Packets and flow level statistics
  - Network response
    - QoS
- Infer CURRENT situation to determine FUTURE network/service scenarios
  - Multi-level knowledge of the network, users and services characteristics
  - Multi-level and time correlations
  - Inputs from other (business) management levels
    - Administration, Marketing and Commercial departments
  - Technological/Sociological Trends
    - Small-scale to world-scale expectations

Network Monitoring

- In the past

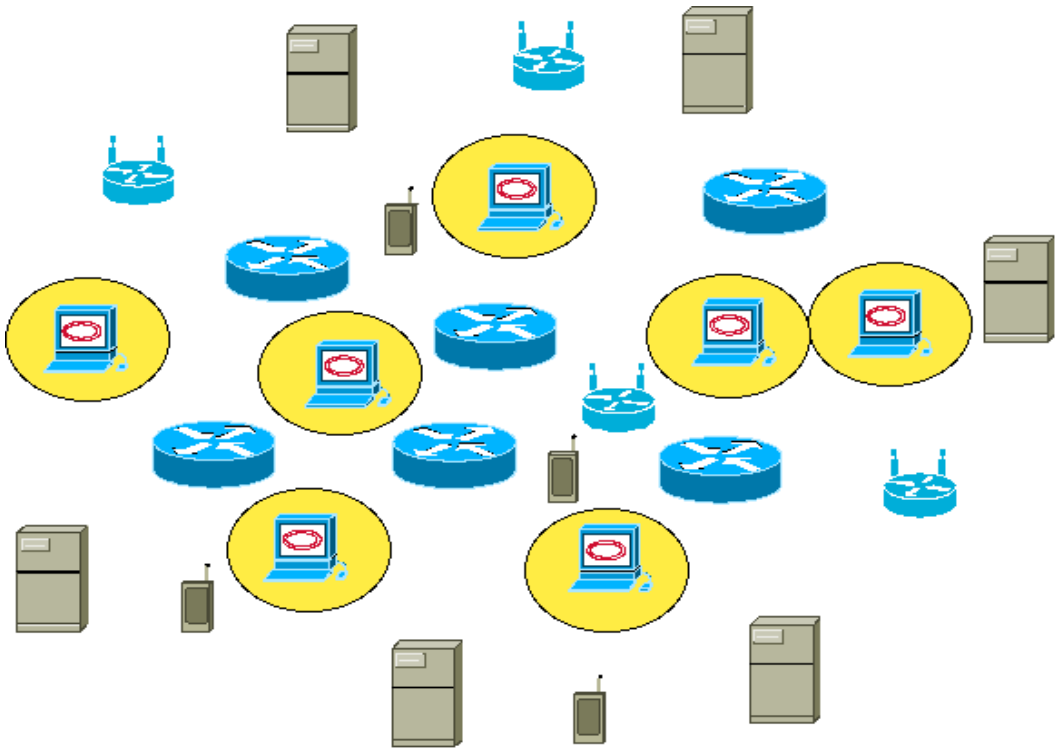


- Simple data from network nodes
- Single-point traffic monitoring



Distributed, heterogeneous, and intelligent Monitoring

- Currently and future



- Distributed probes
- Monitoring
  - Wired and Wireless network devices
  - Wired and Wireless network terminals
  - Servers
- Capturing
  - Users' behaviors
  - Traffic
  - Service stats
  - Equipment logs
- Doing
  - Distributed data processing
  - Distributed archive