Network Management

Andrea Bianco
Telecommunication Network Group
firstname.lastname@polito.it
http://www.telematica.polito.it/

Acknowledgements

- Part of this material taken from
  - Chapter 9, Network Management, of the book Jim Kurose, Keith Ross, Computer Networking, A Top Down Approach, Addison Wesley
  - Fabio Baroncelli (Scuola Superiore Sant'Anna) slides on SNMP
  - Rachida Dssouli: Advanced Network Management

Network management definition?

- Difficult to find a definition
- Due to the complexity of today networks, automated network management tools become essential
  - Standardization also become fundamental to guarantee interoperability
- A network management system is a set of tools for network monitoring and control
- Network management includes the deployment, integration and coordination of the hardware, software and human elements to test, poll, configure, analyze, evaluate and control the network and element resources to meet the real time, operational and QOS requirements……
  - From:Saydam, Magendaz "From Networks and Network Management into Services and Service Management". J. of Network ans System Management

Network management definition?

- Network management refers to the activities, methods, procedures and tools that pertain to the operation, administration, maintenance, and provisioning of networked systems
- Operation deals with keeping the network up (and the service provided by the network)
- Administration involves keeping track of network resources and of their assignments
- Maintenance is concerned with performing repairs and upgrades
  - But also to adjust device configuration to improve network performance
- Provisioning means resource configuration to enable a given service
- Sometimes a distinction is made between
  - Network management
  - System management
  - Application management
  - Service management

Network Management: is it important?

- Cost are essentially depending on
  - Equipment costs (CAPEX, Capital Expenditures)
    - Amortized over several years
  - Costs to operate the network (OPEX, Operational Expendirtures)
    - Operating personnel, electricity, physical space (if rented),
- Often OPEX become dominant
- Network management directly affects OPEX, which are in many scenarios dominant
- Not easy to quantify the cost benefits of management
- Need to track problems
  - Users may be willing to verify SLAs
  - ISPs need to control, maintain, upgrade, forecast

Management and control operations

- The Network Management framework is often divided in five areas (ISO) :
  - Configuration Management (connection management and format adaptation) [A1]
  - Performance monitoring and management [A2]
  - Security management [A3]
  - Accounting management (pricing) [A4]
  - Safety/fault management [A5]

Functional model of the control and management plane

- Network Elements (NE): network components which need to be controlled (links, terminals, interfaces, switches, routers, ADMs, OXCs, …)
- Each NE is managed by an Element Management Systems (EMS)
  - Each EMS manages more NEs
  - Each NE internally has an "Agent" which communicates with the respective EMS
- Network Management System (NMS): managing (centralized) system controlling the EMSs
- NMS, EMS and Agent communicate through a (data) control network (called Data Communication Network – DCN) using proper signaling protocols.

Network management

- Normally the network is managed in a centralized way
- A distributed solution can be necessary both to allow the network to scale to a large number of nodes and to achieve high performance (e.g., SONET can recover from a fault in 50 ms)
- The Internet exploits for management operations the Simple Network Management Protocol (SNMP) and uses distributed database infrastructures called Management Information Bases (MIB)
- Key question: at which layer? at all layers?

Network management

- The (telco) service providers are converging toward a system called Telecommunication Management Network (TMN) which uses the OSI management protocols (Common Management Information Protocol – CMIP) and object oriented model for databases
- The diffusion of the OSI protocols is usually limited, while operators tend to standardize interfaces between proprietary systems and the NMS using the Common Object Request Broker (CORBA) model which is industrial standard

Configuration management [A1]

- Allow a network manager to track which devices are on the network and their HW and SW configurations
- Equipment management:
  - Inventory of the different devices and components building the network
    - Gather and maintain infos on network components
  - Installation of new software releases
- Connection management:
  - Set up and release of connections, VCs, lightpaths, etc
- Adaptation management:
  - Signal conversion (wavelength, frame, power, modulation format conversion)
  - Add/drop of the header/padding fields
  - Policing of the different signals according to the Service level agreement (SLA)
- Modify the network configuration (re-configuration) when needed
  - May be triggered by
    - performance evaluation analysis
    - required network upgrades
    - fault recovery
    - security checks

Performance management [A2]

- Quantify, measure, report, analyze and control the performance of network components (routers, host, end-to-end paths)
- Try to ensure a certain level of performance according to the targeted quality
- Two main issues
  - Monitoring
  - Control
- Parameters
  - Throughput
  - Delays
  - Utilization
  - Loss rates
  - Bit error rates
  - Availability
- Related to fault management and alarm triggering in case of faults

Security management [A3]

- Control access to network resource according to a defined policy
- Identify sensitive information (e.g. network management info) and protect it
- At which layer?
  - Physical (encryption)
  - Network (packet filters)
  - Application (authentication)
  - Firewalls, VPNs, intrusion detection systems (NIDS)
- Includes alarm generation, problems detection, backups, data security, security logging

Accounting management [A4]

- Specify, log and control user and device access to network resource
- Exploits quotas, usage-based charging, allocation of resource-access privileges
- Accounting reports generated periodically
- Check for violations
- Billing

Fault management [A5]

- Log, detect and respond to fault conditions in the network
- "Immediate" handling of transient network failures (links, hosts, routers hardware, power outage, software outages)
- Fault is an abnormal condition and requires an action to repair the fault
- Examples of procedures for fault management
  - detection, isolation, reconfiguration, repair, reconfiguration

Network management in the Internet

Network management in the Internet

- Two main aspects
  - Network monitoring
  - Device management
- Network monitoring
  - Active monitoring (ping, traceroute, pathchar, iperf)
    - Requires additional traffic generation
  - Passive monitoring (HW or SW probes, sniffers)
    - Packet based
    - Flow based
- Device management
  - SNMP, MIB, ASN.1
- Relies also on lower layer management techniques (e.g. SONET/SDH protection and restoration)

Network monitoring in the Internet

- Ping test host reachability
  - Exploits ICMPs echo (request and reply) messages
  - Measures the average round trip time

```
PING www.ietf.org (64.170.98.32) 56(84) bytes of data.
64 bytes from mail.ietf.org (64.170.98.32): icmp_seq=0 ttl=66 time=169 ms
64 bytes from mail.ietf.org (64.170.98.32): icmp_seq=1 ttl=66 time=172 ms
64 bytes from mail.ietf.org (64.170.98.32): icmp_seq=2 ttl=66 time=174 ms
64 bytes from mail.ietf.org (64.170.98.32): icmp_seq=3 ttl=66 time=177 ms

--- www.ietf.org ping statistics ---

4 packets transmitted, 4 received, 0% packet loss, time 3008ms
rtt min/avg/max/mdev = 169.290/173.427/177.398/2.994 ms, pipe 2
```


Network monitoring in the Internet

- Traceroute detects the path (intermediate routers) followed to reach a target host
  - Send IP packets with increasing TTL
  - Routers send TTL time exceeded ICMP messages

```
 1  130.192.7.17 (130.192.7.17)  5.676 ms  0.607 ms  0.626 ms
 2  192.168.255.206 (192.168.255.206)  0.645 ms  0.603 ms  0.528 ms
 3  192.168.255.10 (192.168.255.10)  0.798 ms  0.678 ms  0.617 ms
 4  192.168.255.14 (192.168.255.14)  0.937 ms  1.189 ms  0.884 ms
 5  130.192.227.254 (130.192.227.254)  4.637 ms  11.700 ms  22.441 ms
 6  mz-c-polfi (130.192.232.60)  5.759 ms  21.303 ms  5.959 ms
 7  c7200 (130.192.232.254)  5.893 ms  6.036 ms  6.146 ms
 8  ru-polito-rt-to1.to1.garr.net (193.206.132.33)  6.179 ms  6.371 ms  6.414 ms
 9  rt-to1-rt-mi2.mi2.garr.net (193.206.134.41)  9.005 ms  9.136 ms  9.464 ms
10  rt-mi2-rt1-mi1.mi1.garr.net (193.206.134.189)  11.519 ms  4.213 ms  4.616 ms
11  so-5-0-0.ar2.LIN1.gblx.net (67.17.210.157)  36.865 ms  4.501 ms  4.517 ms
12  te1-4-10G.ar3.DAL2.gblx.net (67.16.143.134)  217.643 ms  316.401 ms  212.964 ms
13  151.164.251.161 (151.164.251.161)  128.657 ms  129.028 ms  133.934 ms
14  151.164.95.82 (151.164.95.82)  167.274 ms  167.678 ms  166.669 ms
15  AMS-1152322.cust-rtr.swbell.net (75.61.192.10)  173.937 ms  168.103 ms  168.303 ms
16  mail.ietf.org (64.170.98.32)  173.586 ms  174.903 ms  169.267 ms
```

Measuring network throughput

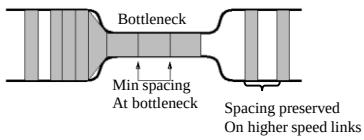
- Several tools available
- E.g. iperf
  - Requires installation of client and server (needs cooperation)
  - Client generates UDP or TCP packets
  - Server receives and collect measurements sent back to the client
  - Allows selection of
    - Port, maximum window size, duration, packet size, Mbyte to send, number of parallel streams

Path characterization

- Pathchar, Clin, pchar
- Idea
  - Rtt=propagation delay + queueing delay + packet_size/link_bw
  - sends multiple packets of varying sizes to each router along route
  - measures minimum round trip time (to cancel queueing delay)
  - plot min RTT vs packet size to get bandwidth
  - repeats the measurements for several hops (exploits increasing TTLs)
  - can take a long time and requires many packets

Bottleneck capacity estimation

- The Packet Pair (PP) technique measures the bottleneck capacity of a path.
- When two packets are sent one after the other (back-to-back), they will be received at the end of the path spaced in time
- If there is no cross-traffic, the spacing (or dispersion) between the packets is inversely proportional to the capacity of the bottleneck link.
- Bprobe, Nettimer, pathrate, CapProbe



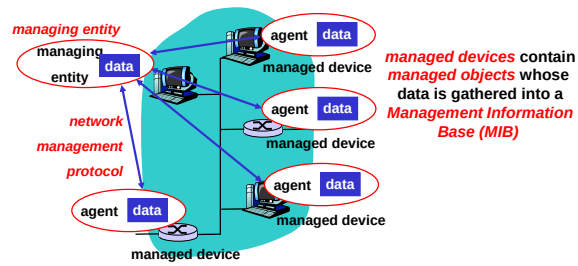
Bottleneck capacity estimation

- Packet trains
  - similar to packet pair
  - send L back-to-back packets of fixed size and measure at the receiver the Average Dispersion Rate (ADR), the time between the arrival of the first and the last packet of the train.
  - if no cross-traffic is present, the dispersion of the train will be due solely to the bottleneck link
- pathrate, pathload
- Compared to PP, ADR is
  - more robust to outliers and less sensitive to errors and timestamp granularity (the dispersion is measured over more packets)
  - but the probability that a cross-traffic packet interferes with the train of probe packets is higher

Device management in the Internet

- Key elements
  - SNMP (RFC1067)
  - MIB (RFC 1213)
  - SMI (RFC 1155)
- SNMP (Simple Network Management Protocol) is an application layer protocol that permits to exchange management information between managers and agents
- MIB (Managed Information Base) is the information set that each manageable device stores to reflect its status
  - Is a tree-structured database of objects
  - Objects can be counters (discarded IP datagrams or number of coillision in Ethernet), descriptive infos (software version) or complex structures (routing path)
- SMI (Structure of Management Information) is a data representation
  - It defines the syntax (ASN.1 formal language) that permits to formally define the MIB content

Architecture for device management

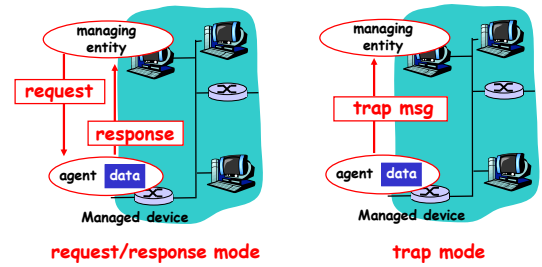


SNMP

- SNMP agents run on manageable network devices where device infos (MIBs) are stored
- An SNMP manager contacts SNMP agents to query or modify the MIB
- SNMP is the application layer protocol used by SNMP managers and agents to communicate
  - Three SNMP protocol versions were defined
- Runs on top of UDP
  - Port 161 SNMP messages
  - Port 162 Trap messages
- Permits to manage device remotely (via Internet)
  - Relies on Internet connectivity
- Instead of defining many commands (reboot, add route, delete route, disable interface ..) it simply allows to write and read MIB variables
  - Writing variables may trigger actions
  - Simple to add new functions: add new variables
  - Operations must be atomic

SNMP protocol

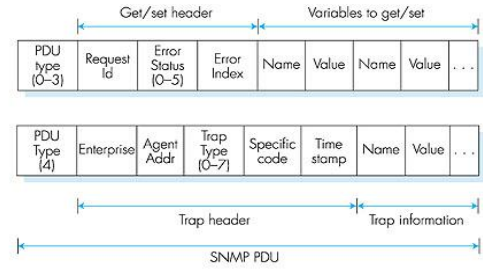
Two ways to convey MIB info, commands:



SNMP commands

- GET_REQUEST (GET_NEXT_REQUEST, GET_BULK_REQUEST)
  - Issued by the manager to monitor devices
  - An Object value or instance (next object in list, block of objects) in the MIB is read by the manager
- SET_REQUEST
  - Issued by the manager to modify device configuration and/or behaviour
  - Object values in the MIB are written by the manager
- INFORM_REQUEST
  - Manager to manager to exchange MIB infos
- RESPONSE
  - Issued by the agent to answer to GETREQUEST, GET_NEXT_REQUEST, GET_BULK_REQUEST, SET_REQUEST, INFORM_REQUEST
- TRAP
  - Issued by agents to asynchronously report (exceptional) events to the manager

SNMP protocol: message formats



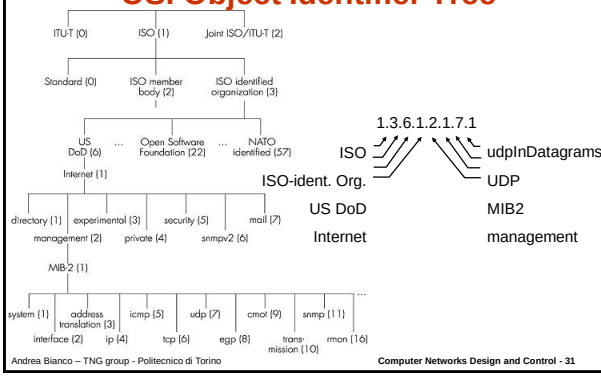
SNMP use

- Network monitoring
  - Periodic polling of devices to detect device status
  - Implies trade off between frequency of polls (higher frequencies imply more precise infos) and generated management traffic
- Failure detection
  - SNMP trap help in identifying exceptional events (not fully reliable and not fast)
  - May adapt pollign frequency on the basis of trap reception
- Long term statistical analysis and reporting
- Remote device configuration and control

Object naming, representation and encoding

- How to specify object names?
  - ISO Object Identifier tree:
    - Hierarchical naming of all objects
- How to formally define object types?
  - ASN.1 formal language (similar to SMI representation)
- How to transfer object values from agent to managers?
  - Cannot relay on memory to menory copy given the heterogeneity of devices
  - Different data format, different storage conventions, …
- How to map objects in sequence of bits?
  - Each device may use its own internal format, but a common device-independent format is defined
  - Encoding rules

OSI Object Identifier Tree



Management Information Base

- Main categories
  - System
  - Interfaces
  - IP
  - TCP
  - UDP
  - ICMP
  - EGP
- Examples of variables
  - sysUptime (system): time since last device reboot
  - ifNumber (interfaces): number of netowrk interfaces
  - ifMtu (interfaces): MTU of a specific interface
  - ipDefaultTTL (ip): default value of TTL
  - ipInReceives (ip): number of received IP datagrams
  - ipRoutingTable (ip): IP routing table
  - tcpMaXConn (tcp): Maximum number of TCP connections

MIB example: UDP module

Object ID	Name	Type	Comments
1.3.6.1.2.1.7.1	UDPInDatagrams	Counter32	total # datagrams delivered at this node
1.3.6.1.2.1.7.2	UDPNoPorts	Counter32	# underliverable datagrams no app at portl
1.3.6.1.2.1.7.3	UDInErrors	Counter32	# undeliverable datagrams all other reasons
1.3.6.1.2.1.7.4	UDPOutDatagrams	Counter32	# datagrams sent
1.3.6.1.2.1.7.5	udpTable	SEQUENCE	one entry for each port in use by app, gives port # and IP address

Object types

- ASN.1 formal language defines
  - Primitive data types
  - Complex constructed data types
  - Macros data type
- Primitive data types
  - INTEGER
  - OCTECT STRING (use to represent hex data such as MAC adddresses)
  - OBJECT IDENTIFIER (string of numbers used to identify objects)
  - ENUMERATED (set of integers)
  - BOOLEAN
  - COUNTER (non negative integer increasing modulo a value)
  - GAUGE (non negative integer increasing and decreasing, stuck at maximuim)
  - IPADDRESS
  - NETWORKADDRESS
  - TIMETICKS

Object types

- ASN.1 constructors
  - SEQUENCE: an ordered list of datatypes
  - SEQUENCE OF: an ordered list of objects of the same type
- Examples

iso.org.dod.internet.mgmt.mib.ip.ipAddrTable or 1.3.6.1.2.1.4.20

```
ipAddrTable :== SEQUENCE OF IpAddrEntry

ipAddrEntry :== SEQUENCE {
  ipAdEntAddr          IPADDRESS,
  ipADDEntIfIndex      INTEGER,
  ipAdEntNetMask       IPADDRESS,
  ipAdEntBcastAddr     IPADDRESS,
  ipAdEntReasmMaxSize  INTEGER
  }
```


Object types

- Templates are used to obtain complete information on objects in the MIB (not only the value)
  - OBJECT IDENTIFIER
  - OBJECT TYPE
  - OBJECT CONSTRAINTS
  - OPERATION ALLOWED
  - OBJECT DESCRIPTION
- ipAdEntReasmMaxSize OBJECT-TYPE

  SYNTAX INTEGER (0..65535)

  ACCESS read-only

  STATUS mandatory

  DESCRIPTION " The size of the largest IP datagram which this entity can re-assemble from incoming IP fragmented datagrams received on this interface."

  ::= { ipAddrEntry 5}

Macro template example

- The OBJECT IDENTIFIER for ipAdEntReasmMaxSize is {ipAddrEntry 5}, or 1.3.6.1.2.1.4.20.1.5.
- The SYNTAX for the value of ipAdEntReasmMaxSize is a variable INTEGER that belongs to the [0, 65535] range.
- ACCESS defines types of operations that can be performed. Only reading allowed, not updating.
- STATUS set to mandatory states that this variable must be supported.
- The DESCRIPTION describes that the value of this variable is the size of the largest datagram that can be reassembled from fragments at the interface.

BER: Basic Encoding Rules

- Set of rules to serialize ASN.1 messages in binary data
- TLV (Type Length Value) encoding
  - Type is one of ASN.1 types
    - 1 Boolean
    - 2 Integer
    - 3 Bitstring
    - 4 Octectstring
    - ……
  - Length is the data length in byte
  - Value of data according to ASN.1
- Transmitted data are self-identifying
- Solves problems of
  - Variable data length
  - Extensibility (add new T values)

TLV example

- Suppose we want to transmit a module of data type declared via ASN.1 as:

  lastname :== OCTECT STRING

  weight :== INTEGER
- Suppose the instance has values {smith, 259}
- The BER rules state we should send Value=259, Length=2, Type=2 (INTEGER), Value=smith, Length=5, Type =4 (OCTET STRING)
- Sequence of transmitted bytes
  - 3 1 2 2 h t i m s 5 4