Network Management

Things a network manager needs to be able to do

- Remotely:
  - Detect problems in network devices (NICs, routers, links…)
  - Monitor traffic for resource allocation
  - Monitoring performance vs. Service Level Agreements (SLAs)
  - Detect intrusions
Network Management Software

- As networks grew, lost ability to manage by hand (or by vendor)
- Widely recognized in '80s that a universal system was needed
  - ISO → Common Management Information Protocol (CMIP)
  - IETF → Simple Network Management Protocol (SNMP)

ISO’s areas of network management

- Performance management
- Fault management
- Configuration management
- Accounting management
- Security management
Performance management

- Objective: monitor and control performance of network devices and channels – Ensure that the network provides acceptable performance for the long-term
  - Utilization
  - Throughput
  - Congestion
  - …

Fault management

- Objective: detect and respond to faults in the network
  - Detection / Isolation / Resolution
  - Router hardware failures
  - Router software errors
  - Link failures
  - Host failures (?)
Configuration management

- Objective: Allow the manager to track the devices in the network and their configurations
  - Hardware
  - Software

Accounting management

- Objective: Allows manager to control and track usage of network resources
  - Usage quotas
  - Charging
  - Privileges
Security management

- Objective: Control access to network resources
  - Security policy
  - Key distribution
  - Certification authorities
  - Firewalls
  - ...

SNMP
Components of a network management infrastructure

- Managing entity – central control point
- Managed device – network hw/sw
  - Managed objects – individually-managed parts of a device
  - Management Information Base (MIB) – managed data (in a common db format)
  - Management agent – local management process
- Management protocol – defines the interaction between Managing Entity and Managed Devices

Simple Network Management Protocol (SNMP)

- Most widely used network management protocol (Internet)
- RFC 2570
- First released in early ’90s
Elements of the SNMP operational model

- Data definition language (SMI)
- Definitions of management information (MIB)
- Protocol definition (SNMP)
- Security and admin capabilities

SNMP operation

Managing entity
Manager sw
Manager sw
MIB Schema
Get
Get-next
Set
Response
Trap
Managed device
Agent sw
Agent sw
MIB Data
Get – retrieve a value from a specified variable
Get-Next -- retrieve the next value
Set -- set a variable to a specified value
Trap -- Alert from Agent
SNMP transport

- SNMP messages normally carried by UDP
- SNMP does not specify a re-transmission policy (although there is no prohibition on building one in)
Traps

• To minimize polling, SNMP uses Traps to allow managed device to alert managing entity to events

• Trap messages contain:
  – Network device name
  – Time of event
  – Type of event:
    • Unexpected restart
    • Expected restart
    • Link failure
    • Link just came up
    • Authentication failure
    • Neighbor down
    • User-specified

Problems with traps

• Use resources on network device
• “Big” events may tie up network with trap messages
• Many trap messages report things the manager already knows

• So polling usually used as complement
Managing Network Data

Data definition language

- “Structure of Management Information” (SMI)
- Defines the management information residing in a managed entity (the “MIB”)
SMI data types

- Integer32 (32 bit integer)
- Unsigned32 (unsigned 23-bit integer)
- Octet String (byte string up to 64KB long)
- Object Identifier (structured name)
- IPAddress
- Counter32, Counter64 (wrapping counters)
- Gauge32 (non-wrapping counter)
- TimeTicks (1/100ths of a sec since some event)

The SMI OBJECT-TYPE construct

- OBJECT-TYPE
  - Objects that contain the management data
  - Specifies data type, status and semantics of a managed object
  - Different OBJECT-TYPES are standard, defined in RFCs

- Clauses of OBJECT-TYPE
  - SYNTAX – basic data type of the object
  - MAX-ACCESS – permissions
  - STATUS – validity of object definition
  - DESCRIPTION – plaintext describing the object
An example OBJECT-TYPE

ipInDelivers OBJECT-TYPE
SYNTAX Counter32
MAX-ACCESS read-only
STATUS current
DESCRIPTION "The total number of input datagrams successfully delivered to IP user protocols (including ICMP)"
::= {ip 9}

(from RFC 2011)

The SMI MODULE-IDENTITY construct

- Groups related objects together (e.g., all of the IP-related objects are in the “ipMIB” module – RFC 2011)
- Some module types:
  - IP (RFC 2011)
  - TCP (RFC 2012)
  - UDP (RFC 2013)
Management Information Base (MIB)

- A virtual database that holds the managed modules/objects at a managed device (collectively, for the entire network)

IDs for modules and objects

- Every module/object is assigned a hierarchical number
- Numbering defined by ISO Abstract Syntax Notation – One (ASN.1)
ASN.1

- An ISO framework intended to give a unique identifier to every object type in a network

ASN.1 hierarchy

```
sysDescr ID = 1.3.6.1.2.1.1.1
```

Example MIB objects

- 1.3.6.1.2.1.1.3 (sysUpTime) -- system up time in 1/100th of a sec
- 1.3.6.1.2.1.1.6 (sysLocation) – physical location of this node
- 1.3.6.1.2.1.7.4 (udpInErrors) – number of received UDP datagrams that could not be delivered

Security
SNMP Security

• “Security’s Not My Problem”
• Early version (v1) had weak security
  – Weak authentication
    • IP address “white lists” – easily spoofed
    • “community strings” – not secret
  – No privacy
    • All messages in plaintext – easily intercepted and spoofed
• Present version (v3) improves

SNMPv3 security

• Each user has secret key
• All messages protected by hash code
• Message encryption available (Privacy)
Remote Monitoring (RMON)

- HW/SW “probes” that provide specific info about network devices
  - Statistics about device operation
  - History of statistics
  - Thresholds for alarms
  - Identity of hosts on the network
  - Statistics about hosts on the network
  - Traffic between two addresses
  - Detection of specific packets
  - Events to log, trap on
Web-based management

- The idea: HTTP carries the management information, user interfaces through a web browser
- Not (yet) a replacement for the entire SNMP operational model
  - SNMP = instrumentation and control
  - HTTP+browser = universally-available transport and display mechanism
- Advantages:
  - Accessibility from any point
  - Needs less proprietary SW
  - Platform independence
  - Easier deployment, maintenance, training…
- Examples:
  - Internet Traffic Report (www.internettrafficreport.com)
  - DNS response time (www.caida.org/cgi-bin/dns_perf/main.pl)
  - Quest IP Statistics (http://stat.qwest.net/index_flash.html)