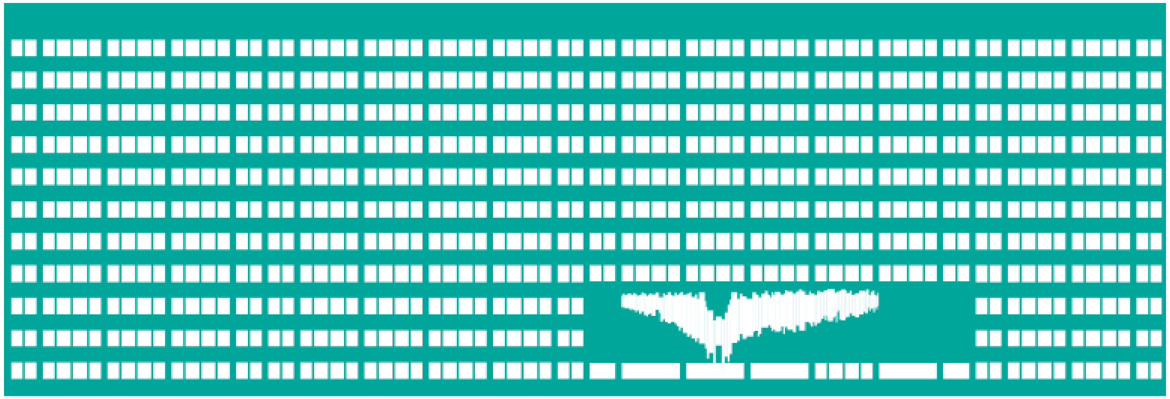
VSB TECHNICAL UNIVERSITY OF OSTRAVA | FACULTY OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCE | DEPARTMENT OF COMPUTER SCIENCE

Introduction to Network Management



Computer Networks
Lecture 14

Network Management

- A discipline dealing with operating, monitoring and managing (computer) networks
- **FCAPS** ISO model and framework (since 1980s):
  - **F**ault Management – to recognize, isolate, correct and log faults
  - **C**onfiguration Management
  - **A**ccounting Management
  - **P**erformance Management
  - **S**ecurity management
- Network management station (NMS) – monitors and controls network elements using specific applications

Simple Network Monitoring – SNMP

- ICMP is not suitable for everything, multiple protocols existed during 1980s (SGMP, HEMS, CMIP)
- SNMP was meant as short-term solution based on TCP/IP stack in 1988, with very simple protocol – just 5 message types in SMNPv1
    - Defined by IETF (RFC 1098, 1901, 3410-3417,…)
- For performance, issues detection/diagnostics and baselines for network growth
- Developed remote monitoring capability
- But SNMPv1 was not secured, only community strings (R/O, R/W), SNMPv3 adds cryptography

SNMP Structure

- 3 primary elements:
  - SNMP Agents – software modules in managed devices talking to Managers
    - Translate local info to MIB info
  - SNMP Managers – Network Management Stations which receive messages from Agents, do reporting, can even execute programs.
  - Management Information Base – MIB – collection of definitions of device management information organised by OIDs (Object IDs)
    - There is actually no explicit root of the tree of OIDs, one is for ISO(1), another for CCIT(2), …

Management Information Base – MIB

- Represents resources as objects, each having one or more variables, the OID is a unique object ID
- Variables represent one aspect of managed agent (e.g. number of TX frames on Ethernet Interface)
  - Scalar and tabular types – integer, octet string, OID, NULL, sequence + application-based (e.g. IP address). Access to a single cell for tabular type
- What information should actual networking elements provide to NMS. Extended in MIB II.
- Numeric identifiers, with a proprietary manufacturer-based extension possible
  - iso.org.dod.internet.private.enterprises (1.3.5.1.4.1)
- Structure of Management Information (SMI) for MIB – (RFC 1065) uses ASN.1 syntax to define objects

SNMPv1

- 5 basic messages (PDUs)
  - Get Request – polls agent for information
  - GetNext Request – requests next item in a dataset
  - Set Request – requests a change to a value
  - Response – sends a response to the Manager
  - Trap – informs a NMS of an event occurring
- No authentication
- R/O community string is "public" by default
  - Different community strings for different authorization
- Set is typically disabled for security reasons

SNMPv2

- Development became fragmented into several branches (SNMPv2c, SNMPv2u, SNMPv2*)
- Mainly addressing security issues and introducing new datatypes (e.g. 64-bit integers, gauges, counters, unsigned ints)
- GetBulk command added
- Inform Request – command to forward information from Trap between managers
- Better error handling

Never really took off due to disagreements and security concerns

SNMPv3

- Design became security-centric
  - Users and user groups
    - MIB views for groups of users – read view, write view, notify view containing lists of OIDs
    - Access policies for groups of users
    - Notifications (TRAP messages) for groups of users
- Cryptographic algorithms have been added
  - Authentization, message integrity, message digests
  - Optional message encryption
  - Message format had to be modified
- Consolidates best features of different v2 branches

Remote Monitoring – RMON

- Central network management of a internetwork consisting of several LANs
  - Adds a remote monitoring MIB supplementing MIB-II
  - Provides a significant expansion of SNMP functions
  - Distributes the management system
- Oriented on Ethernet (and in past on Token-Ring)
- A special extension of MIB – RMON MIB
- Defines standard network-monitoring functions and interfaces for communicating between SNMP-based management consoles and remote monitors
- Remote network probes for local statistics, trends, communication matrices, even packet capture

Remote Monitoring Design Goals

- Off-line operation – routine polling from Network Managers not needed
- Problem detection and reporting
- Proactive monitoring – running diagnostics+logging
- Multiple managers – better reliability, specialization
- Analyses specific to the data collected on its subnetwork, e.g. hosts generating a lot of traffic
- Providing RMON probes implementing RMON MIBs
  - Just SNMP agents with these extra features
- RMON1 monitors LANs or captures traffic on L2
- RMON2 can analyse network/transport-layer protocols – extension for higher ISO-OSI layers

RMON1 statistics groups

- Ethernet Statistics (1) – for individual interfaces
- History Control (2) – periodic collection of values
  - Ethernet History – recording of periodically collected values
- Alarm (3) – generates events (TRAP) on crossing of the thresholds (with hysteresis support)
- Host (4) – statistics associated with each host identified by its MAC address
- HostTopN (5) – table of the most active hosts based on their statistics
- Matrix (6) – matrix of communication between hosts
- Filter (7) – matching PDUs to filter equation for capture or event generation
- Packet Capture (8) – buffer for packet cap. based on a filter
- Event (9) – generation and notification of events from the device, including logging