

Towards Self-Managed Networks

**Computer Networks and
Internet Engineering (CNIE)
Division**

C-DAC, Electronics City
Bangalore

- Conventional Network Management
- Network Management Overheads
- Need for Self-Management
- C-DAC's approach towards self-managing networks
- Call for Participation..

- Refers to activities, methods, procedures, and tools that pertain to the operation, administration, maintenance, and provisioning of networked systems.
- Some possible strategies
 - Centralized management
 - Distributed management
 - Self-managed networks

- OSI overview of Network management includes
 - Fault Management
 - Configuration Management
 - Accounting
 - Performance Management
 - Security Management

Need for Network Management



- Network planning
- Administering the network
- Gathering statistics
- Monitoring network performance
- Generation of regular reports
- Security monitoring
- Troubleshooting
- Routine tasks should be automated

- Hosts are the computers on the network
- Routers/gateway, bridges and repeaters network them
- Modems link them to the PSTN/leased lines
- Terminal Servers, hubs etc. provide network access to hosts and users

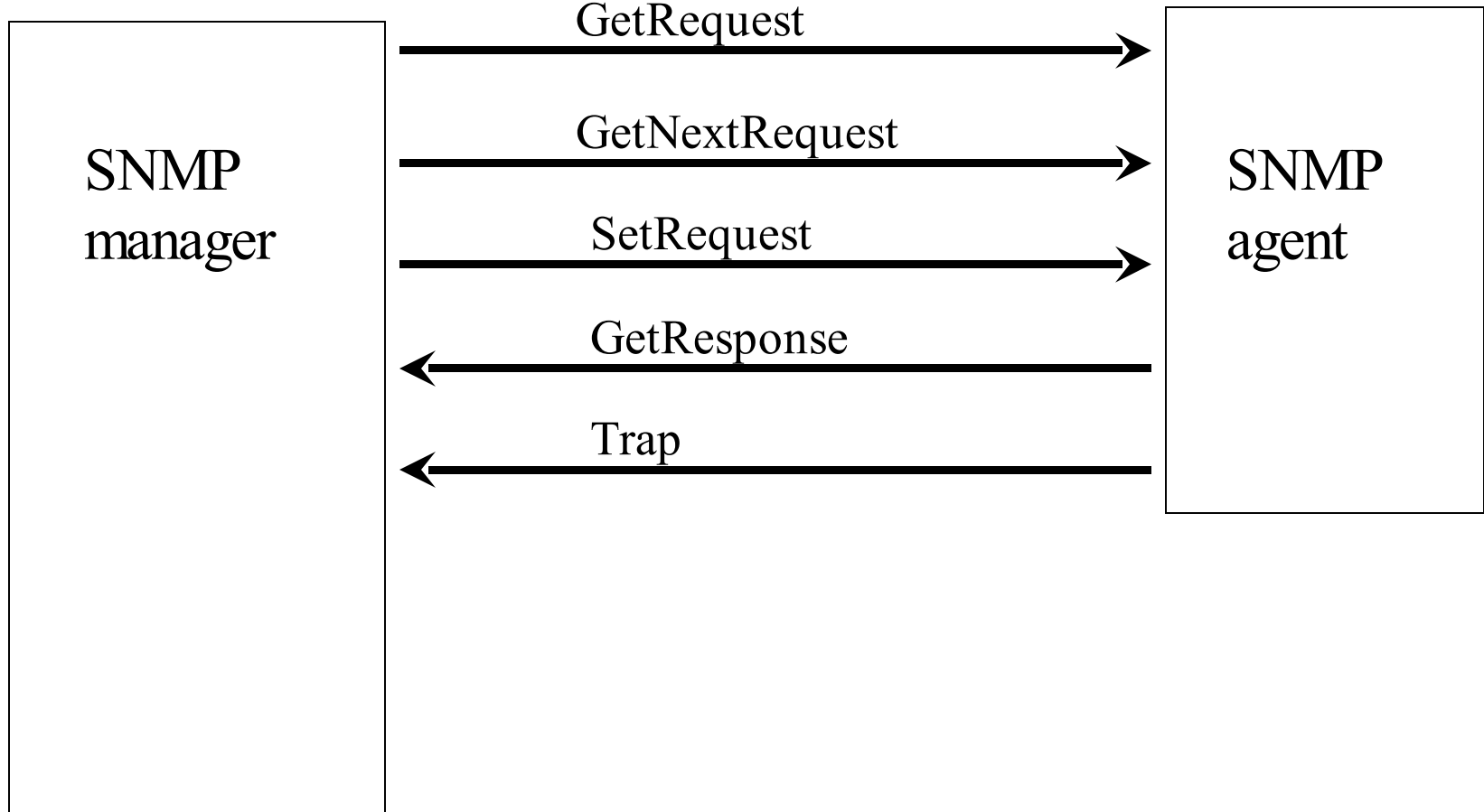
All of these should be manageable

SNMP Management Framework includes:

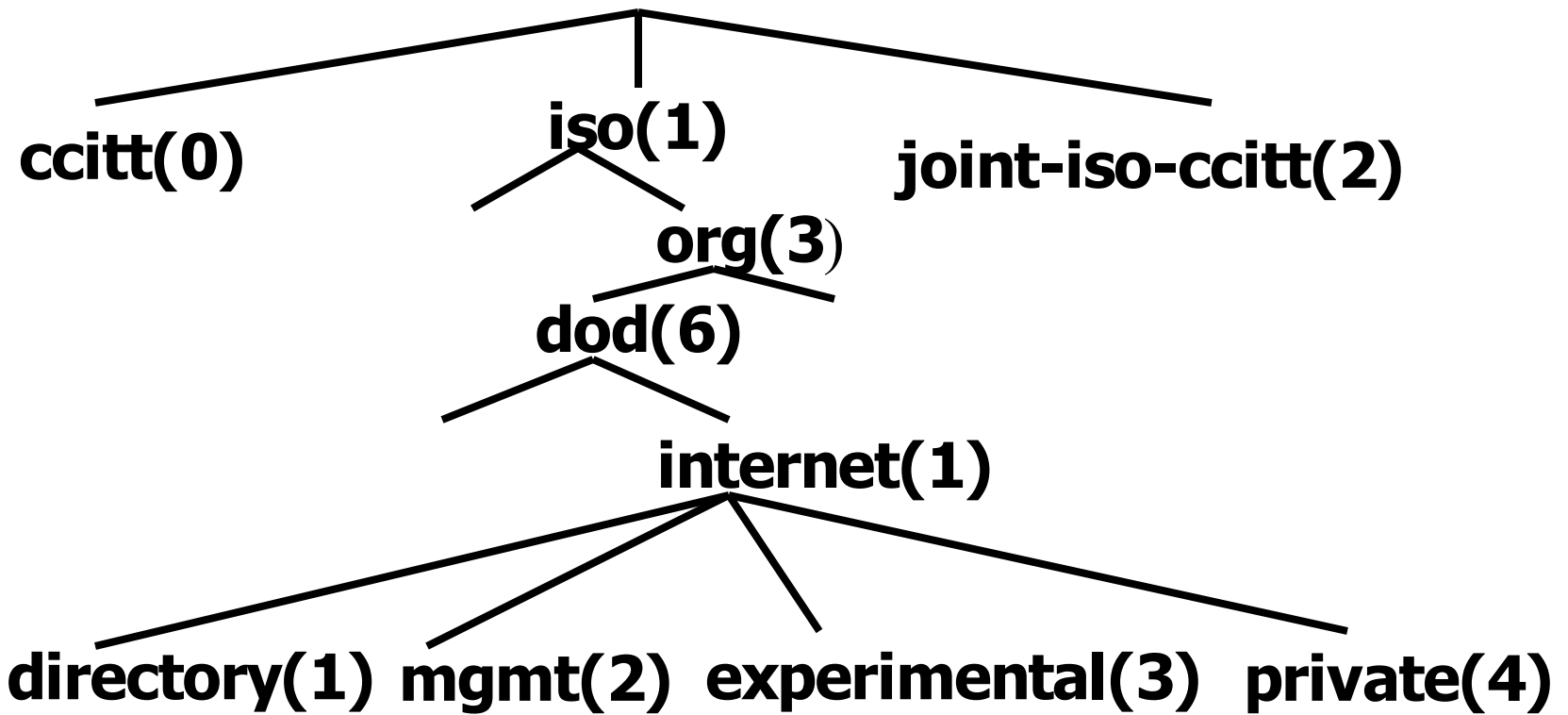
- network elements
- network management stations
- network management protocol
- network management information

SNMP PDU types

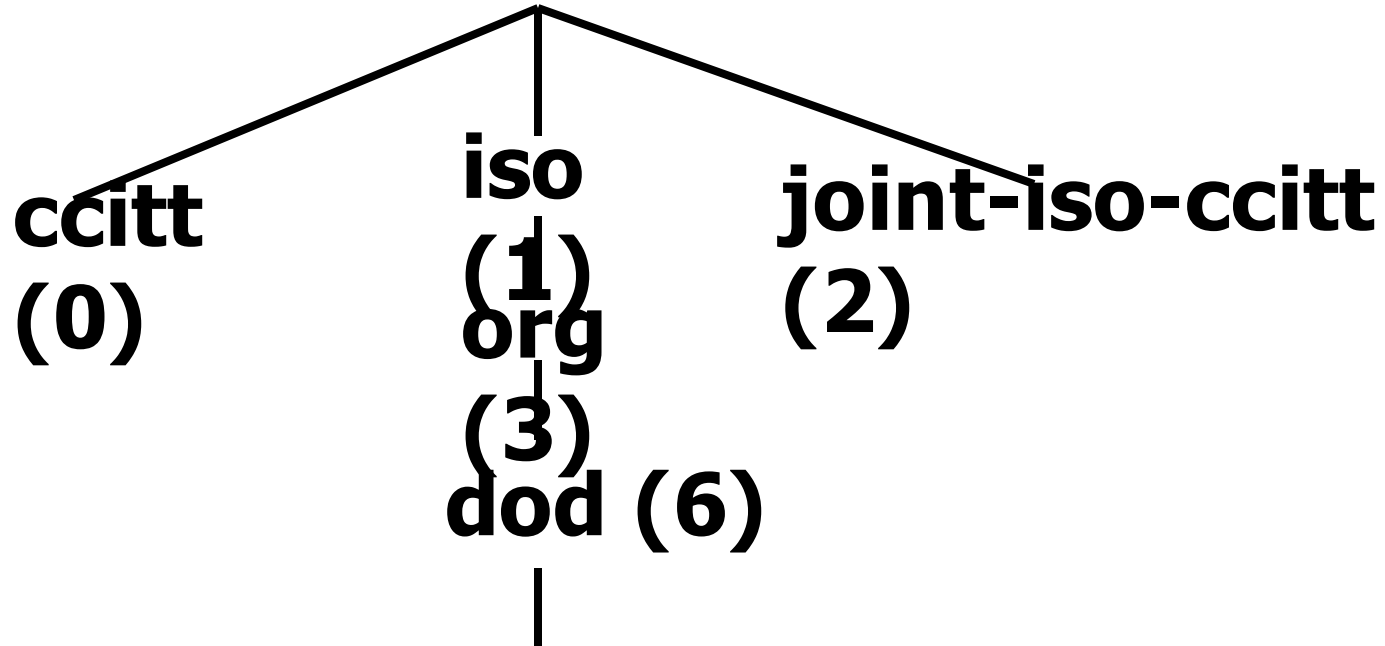
UDP connections



Object Identifier Prefix for Internet



virtual information store



Management Information Base



dod(6)

internet(1)

mgmt(2)

mib(1)

system(1)

interfaces(2)

ip(4)

icmp(5)

tcp(6)

udp(7)

snmp(12)

MIB Elements



- System
- Interfaces
- Address Translation (-)
- IP
- ICMP
- TCP
- UDP
- SNMP (+)

SysDescr	description of device
SysObjectId	numeric identity of agent software
SysUpTime	time since agent started
SysContact	name of responsible person
SysName	name of device
SysLocation	device physical location
SysServices	services provided

Example objects



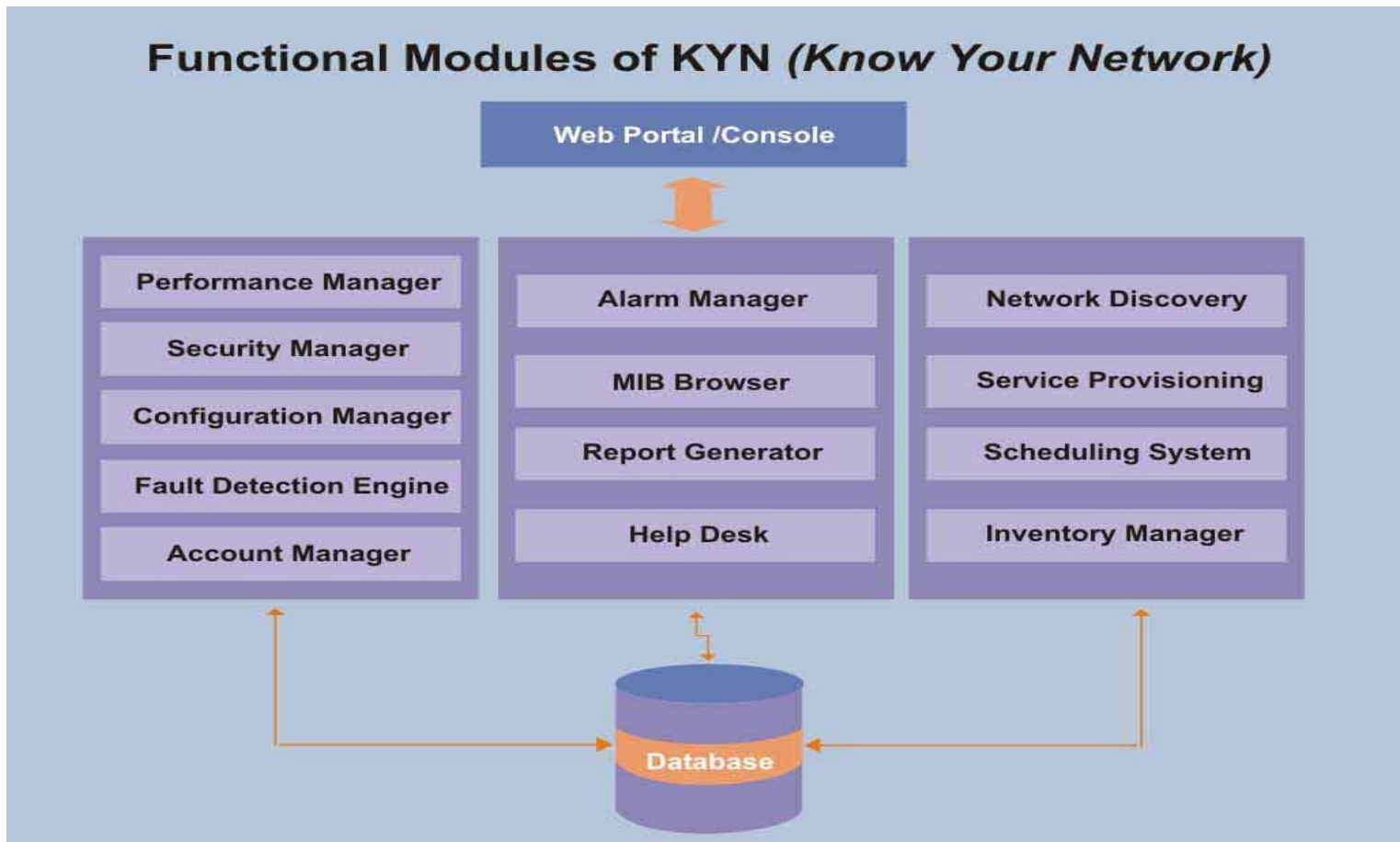
- The UDP group
 - udpTable 1.3.6.1.2.1.7.5
 - udpEntry 1.3.6.1.2.1.7.5.1
 - udpNoPorts 1.3.6.1.2.1.7.2

KYN (Know Your Network)



- KYN is a network measurement and management system for efficient monitoring and management of the network
- KYN is an open-source based integrated platform which provides a uniform visualization model of various well known public domain network tools
- KYN supports monitoring, management, fault diagnosis, traffic trend analysis etc.

KYN Architecture



KYN Status



Capabilities

- Network Discovery
- Performance statistics
- Video Conferencing statistics

Open Source tools integrated

- MRTG
- H.323Beacon
- iperf
- Weathermap
- Remote Ping
- Remote Trace Route

<http://sourceforge.net/projects/kyn/> or..

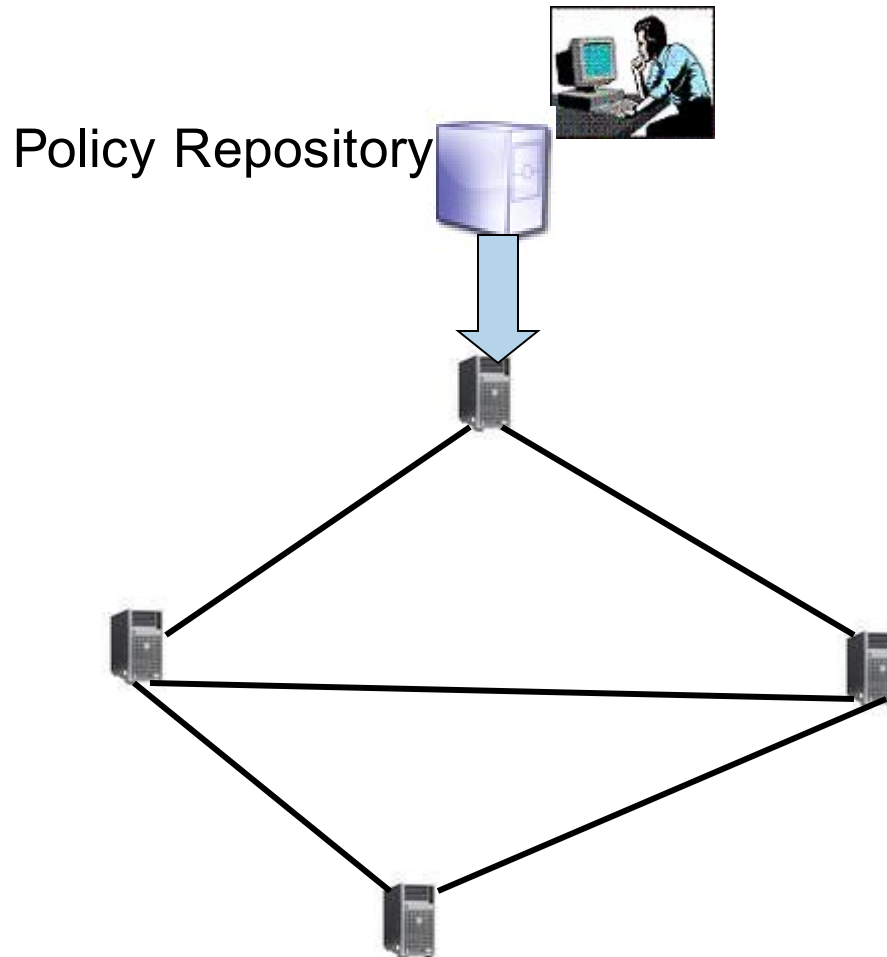
<http://ncb.ernet.in/kyn> --> C-DAC site

Development Platform



- Web-based
 - JSP, Apache Server
- Linux 2.6
- jakarta-tomcat-5.0.28
- mrtg-2.14.3
- net-snmp-5.2.1
- j2sdk 1.4.2
- postgresql-8.0.3-1
- perl-5.8.6-24
- Follow README....for installation..

Self-Managed Networks



Self-Managed network elements controlled by policies

Self-Network management need



- Not humanly solvable
- Operator error causes largest cause of service failures in some environments
- In many environments operators may not be tech savvy or even not immediately available

- Evolving self* (self-adapting, self-configuring, self-healing...) approaches for systems and networks
- Research Projects..
 - ANA [1], ACF [2], BIONETS [3], HAGGLE [4], and CASCADAS [5]
- QoS & Security perspectives

- Static to Dynamic management of network
- QoS and Security needs
- Deriving meaning from various sources inputs

- Self-Managing Networks
 - Self-deploying and Self-cleaning
 - Self-configuring and Self-adapting
 - Self-optimizing
 - Self-protecting
 - Self-monitoring
 - Self-diagnosing
 - Self-healing

Prevention is better than cure

A self-* system requires knowledge of itself and its environment, it is self-aware.

Some Real Examples



- Policy distribution systems allow auto deployment of configuration across a network
- Routing protocols auto-adapt to topology changes and failures (ex: RIP, OSPF etc.)
- TCP auto-adapts to congestion
- Automatic response to security breaches

C-DAC approach



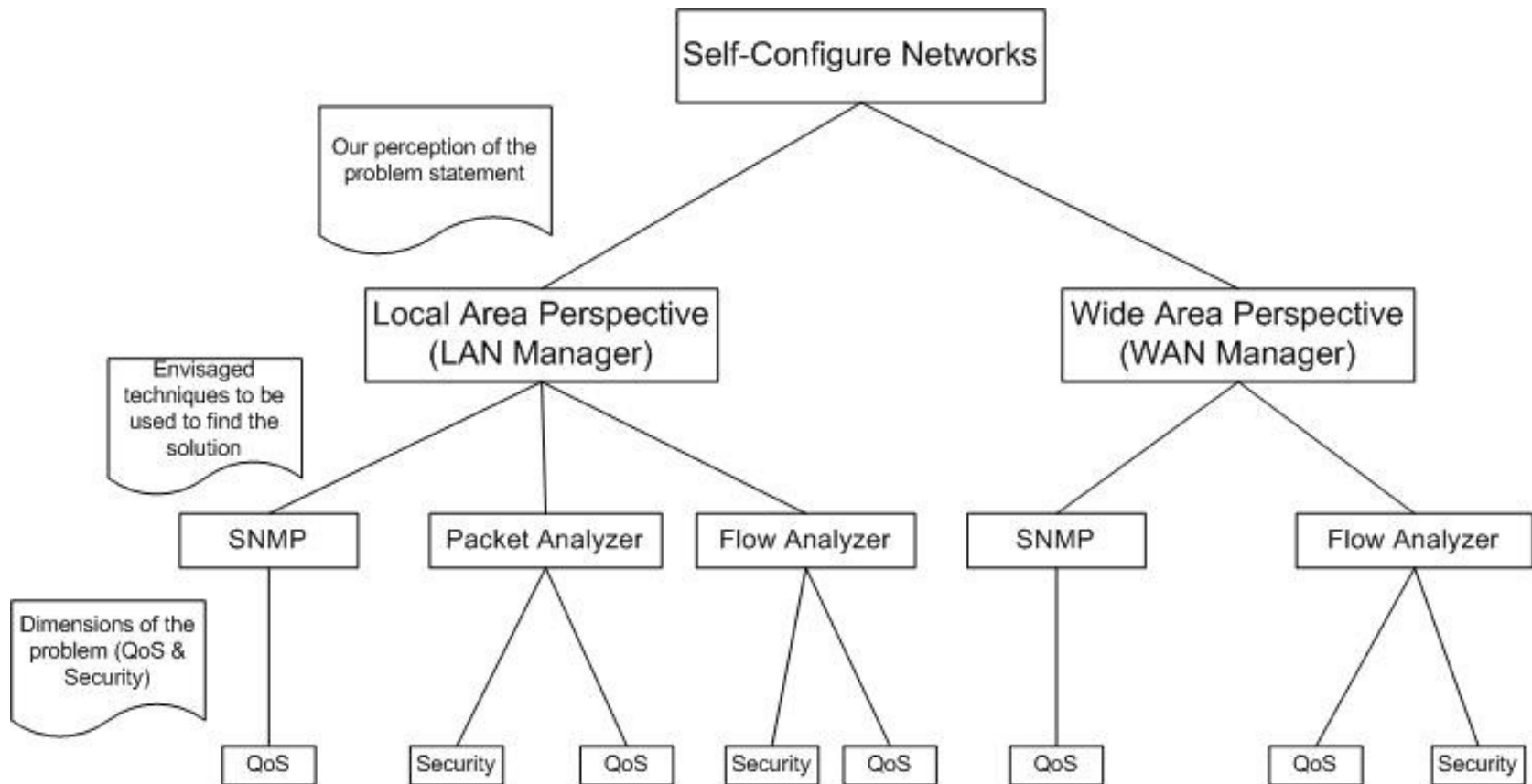
- Our approach towards self-configuration of network is to, firstly aggregate various network inputs
- Secondly carryout step by step analysis to generate interesting QoS and security events (individually based on flow and snmp)
- Thirdly, to correlate these events to decide on the reconfiguration aspects of network entities
- Our main contribution in this paper is in devising an architecture for such a self-configuring system aggregating various inputs

C-DAC's Approach toward Self- Managing Networks



- Network Classification
 - LAN
 - WAN
- Monitoring mechanisms
 - Flow Analysis
 - Packet Analysis
 - SNMP

Input Sources



Flow Analysis

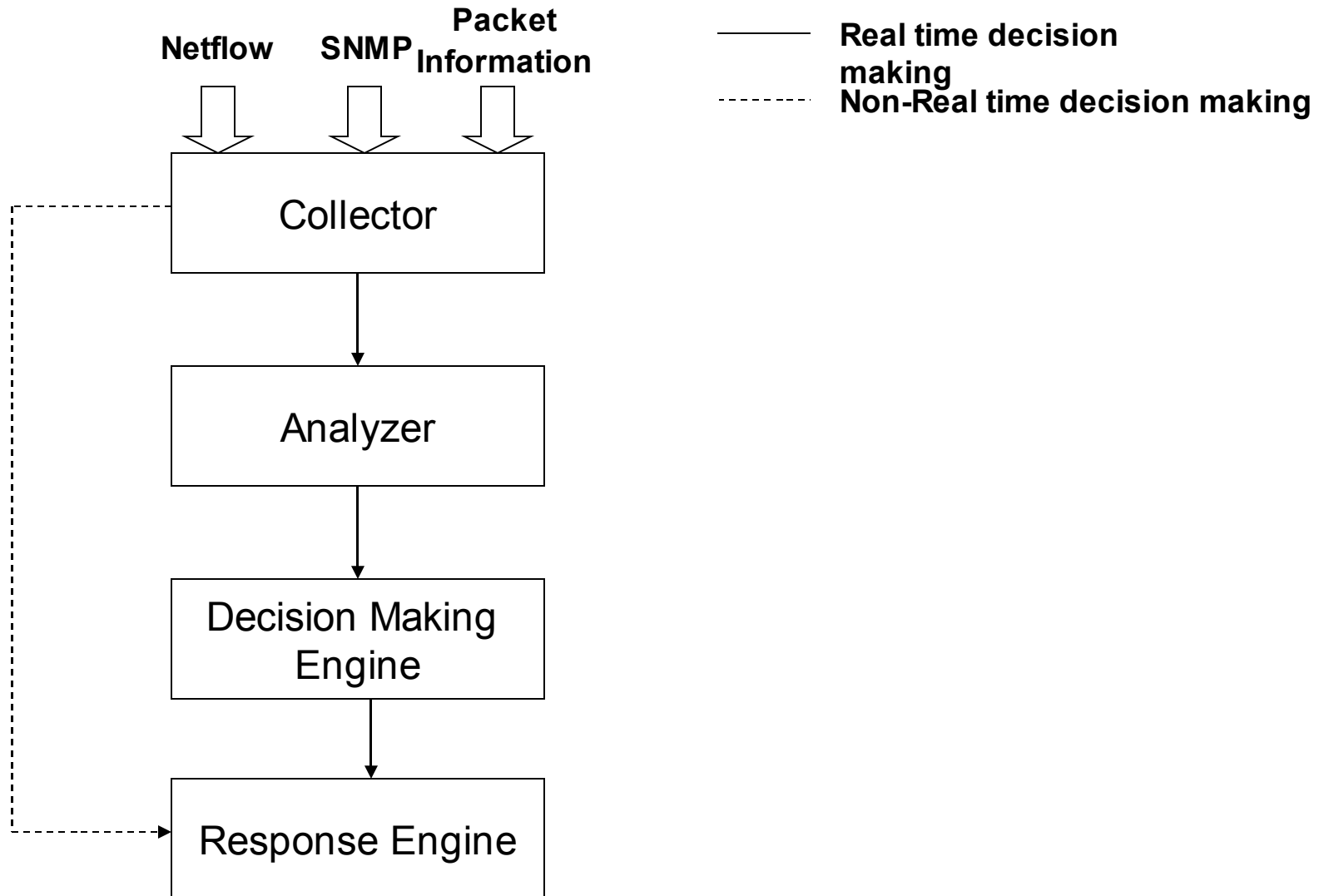


- Flow is an aggregated network traffic information available from network devices
- Different flow definitions are available like netflow from CISCO and jflow from JUNIPER
- IPFIX is an IETF standard version for exporting flow packets from flow creator to collector

- Packet analyzer is a computer software or hardware that can intercept or log traffic passing over digital network or part of network
- Packet analyzer is also known as network analyzer or sniffer
- Sniffer captures each packet, decodes and analyzes its content according to the given specification

- Used for network management with the help of SNMP agents
- Gives user the provision to poll different network elements and to get information about them from their MIB (Management Information Base)

Overview Architecture



- Decision Making Engine
 - Includes Suggestion Verifier, Impact Analyzer and Decision Maker
 - Makes decision about network reconfiguration, depending on events generated by analyzers
- Response Engine
 - Generates scripts for reconfiguration
 - Reconfiguration can be guided and unguided network configuration

- Scenario: An application server inside the network is under DoS Attack (Flooding from multiple sources)
- Input reflections
 - Flow: Deviations in number of flows for that host during a time window
 - SNMP: Deviations in traffic (interface statistics) for the interface of that entity
- Event Correlation
 - Flow and SNMP deviations confirm flooding attack
- Self-configuration
 - Disconnect the attack source (reconfiguration of firewall/packet-filter rule in gateway)

- Scenario: Providing priority for a real-time application (video conference) when the network utilization is very high
- Input reflections
 - SNMP: Provides network utilization (indicates very high)
 - Flow: Provides % of distribution based on various applications and transport protocols (TCP Vs UDP)
- Event Correlation
 - Based on Flow and SNMP inputs a correlated event is generated for providing priority for real-time application at this network state
- Self-configuration
 - Provide top-priority (EF) to all VC packets

- Profiling issues
 - SNMP, Flow and Packet profiles
 - Synchronization of various input profiles
- Network Measurement challenges
 - Interface, traffic (Accuracy, periodicity)
- Input analysis
 - Performance, Security, Fault, Configuration
- Research challenges
 - Accuracy and performance
 - Consistency in auto configurations

Call For Participation



- Opensource development
- www.ncb.ernet.in/kyn
- We will announce the to-do list for developers
- Researchers may contact us for specific problem statement

References



- [1] <http://www.ana-project.org>
- [2] <http://www.autonomic-communication-forum.org>
- [3] <http://www.bionets.eu/>
- [4] http://www.hagggleproject.org/index.php/Main_Page
- [5] <http://www.cascadas-project.org>

Acknowledgements



- Project Review and Steering Group Members
- Department of Information Technology, Ministry of Communications and Information Technology, Government of India, Delhi

Thank You