Policy-based Network Management

Won-Ki Hong
DP&NM Lab.
Dept. of Computer Science and Engineering
POSTECH, Pohang Korea
Tel: +82-562-279-2244
Email: jwkhong@postech.ac.kr
http://dpnm.postech.ac.kr/
Contents

- Introduction
  - Network Management: What? and why?
  - Policy, Policy-based Network Management (PBNM)
- IETF/DMTF Approach
- PBNM Products
- Summary
- References
What is network management?

- Monitoring: collect data, events, etc.
- Interpret & make decisions
- Perform management control actions
- Managers & Agents

Management Control Loop
Why is network management needed?

- Fault Management
- Configuration Management
- Accounting Management
- Performance Management
- Security Management
- Service Management
- Network Planning & Migration
Policy

• Rule governing choices in behavior of the system
• Derived from enterprise goals and service level agreement (SLA)
• Need to specify and modify policies without coding into automated agents
• Policies are persistent, but can be dynamically modified

⇒ Change system behavior without modifying implementation
Why policy?

- facilitates the dynamic change of behavior of a distributed management system
- permits the reuse of policies in different environments
Policies in Organizations

• Most organizations have and use policies for computing and networking

• However, most organizations have the policies written in the form of paper

• Policy-based network management (PBNM) is an approach to specify and store policies *electronically*

• PBNM is needed to manage networks and systems simply and effectively
Policy-based Network Management (PBNM)

• Performs network management based on policies

• Enables a manager to specify what he wants to do, the end result, without having to know how to accomplish it for the specific devices

• Policies typically relate to QoS or Security
  – Quality of Service: bandwidth, latency, priority, DiffServ
  – Security: authentication, authorization, access control, audit

• Directory is typically used for storing policies
IETF/DMTF Approach

• Directory-Enabled Networking
• Directory-Enabled Networks (DEN)
• Policy Framework
• Policy Architecture
• Possible Implementation Protocols
  – Common Open Policy Service (COPS)
  – Lightweight Directory Access Protocol (LDAP)
• Policy Standards
Directory-Enabled Networking

• Confusion exists between the term “directory-enabled networking” and “directory-enabled networks (DEN)”

• **Directory-enabled networking** is a design philosophy that enables applications to use directories to store information related to the network
  – e.g., user profiles, network element and service configuration information

• **DEN** is a specification that defines an information model and schema that serve as the foundation for policy-based network management

  ⇒ **IETF/DMTF Policy Work**
Directory-Enabled Networks (DEN)

- sponsored by IETF/DMTF
- Acts as a repository for information about users and computing resources, network devices, services and applications
- Developed as an extension to Common Information Model (CIM)
  - DEN information model adds network devices & services to the CIM information model

⇒ An information model that defines management abstraction of
  - user profiles, policies
  - devices, protocols, and services
DEN (2)

- Implementation in directory services that support LDAP as the access control
- Helps to deploy QoS
  - Can be deployed from central console that creates policies in a directory
  - Can automatically distribute configurations to network devices, operation systems, and applications

⇒ Allows for PBNM using directories as the underlying repository of policy information
What is a Directory?

• Directory is a special-purpose database
  – far more reads than writes
  – Changeable: can alter the rules about what goes into directory
  – Discoverable: don’t need to know all the rules ahead of time
  – Accessible via standard protocols (e.g., LDAP)

• Directories
  – protect the date they store
  – are not all in one place
  – can store multiple copies of data
  – eliminate confusion about names
LDAP

- Lightweight Directory Access Protocol (LDAP)
- Standard protocol defined by IETF
- A client-server protocol specifically designed for accessing directories over a network.
- Defines standard communications methods for storing and accessing information in directories
- A “light” version of X.500
LDAP (2)

- LDAP defines four basic models that describe its operation
  - Information model (directory schemas): entries containing attributes
  - Naming model: hierarchical naming structure
  - Functional model: interrogation, update, authentication operations
  - Security model: simple client authentication

- LDAP provides the following operations
  - Interrogation operations: search, compare
  - Update operations: add, delete, modify, modify DN (rename)
  - Authentication and control operations: bind, unbind, abandon
Policy Framework

- Based on object-oriented Common Information Model (CIM) with mapping onto LDAP schema
- Policy of the form:
  - If a set of conditions is satisfied, then perform a set of actions
- Specifies components of policy as objects
- Uses directory for storing policies
Example Policies

• Provide high QoS to nightly backup on server at IP address 141.223.2.15 from 2-4 a.m. on weeknights and Saturdays

If ( ((srcIPaddress == 141.223.2.15) ||
(destIPaddress == 141.223.2.15)) &&
(timeOfDay = 0200-0400) &&
(dayOfWeek = _MTWRFS) )
then priority == HIGH endif
Policy Schema

Policy Group

0..n

- Contained policy groups

Policy Rule

0..n

- Contained policy rules

Policy Condition

0..n

- Contained policy conditions

Policy validity

0..n

- Period condition

Policy Action

0..n

- Contained policy actions

Range of Time

- Time Masks
  - Month of year
  - Day of Month
  - Day of Week
  - Time of day
Schema Concepts

- Policy group is a set of related policy rules
- Each policy rule component (condition, action) is stored as an LDAP object
- Can reuse (share) policy component objects between multiple rules to avoid re-specifying multiple rules can use the same period condition object
IETF Policy Architecture

- **Policy Server**
  - **Policy Management Application**
  - **Policy Consumer (PDP)**
  - **Policy Target (PEP)**

**Policy Repository** (e.g., Directory, DB)
- User interface
- Conflict detection
- Notification generation
- Management information repository
- Policy Decision Point
- Policy translation

- Policy Protocol (e.g., COPS ..)
- Policy Enforcement Point
- Network element interface

Repository Access Protocol (e.g., LDAP)
- Status & Config. Info.
- Notification

**NETSEC-KR 2000 Policy-based NM Tutorial**
Policy Management Application

- Policy Editing
- Policy Presentation
- Rule Translation
- Rule Validation
- Global Conflict Resolution
Policy Repository

- Storage
- Search
- Retrieval
Policy Consumer

• Receives policy and translates it into format applicable to target
• Knows about target capabilities
• Policy Decision Point (PDP)
  – makes policy decisions based on policy conditions
  – configures target to enforce policy such as access list, priority queue relating to packet address
• Executes policy rule translation & policy transformation
• Each target is controlled by one consumer
• Consumer may control multiple targets
Policy Target

• Policy Enforcement Point (PEP)
• A specific functional feature (interface) of a device such as priority queuing, committed access rate for a router
  – e.g., a router with 2 interfaces and 4 manageable features for each interface will have 8 targets
• A sophisticated device may include both PDP and PEPs ⇒ optionally, executes policy rule validation
Policy-based Management Scenario

- Administrator makes a new policy or retrieves existing policy from directory service using LDAP and views or edits policy
- Administrator associates the policy with policy targets
- Policy and association with targets is stored in the repository via LDAP
- The associated consumer for each target is notified that a new policy is available
- The consumer obtains the policy from the repository via LDAP e.g., using query to find the policy
- The consumer processes the policy and configures the targets using target-specific mechanism
- For each target which received policy data, the consumer provides status information back to the policy management application
Example: PEP – PDP Interaction

1. Event (e.g., RSVP Request)
2. REQ: Request (Source addr, etc)
3. DEC: Decision (resources)
4. Reserve resources
5. RSVP Request

- Can also pre-configure devices with policy data, so they do not have to query PDP on every event provisioning.
Example: Layer 3 Packet Filtering

- Policy: Only engineers are allowed HTTP access; only engineers who are managers are allowed HTTP access during business hours.

1. HTTP request, 1:30 p.m.
2. COPS client request (IP source Address, HTTP)
3. Obtain user profile for user with this IP address
4. Time query
5. COPS policy decision: DENY request
6. Router installs packet filter denying access
Why is this approach needed?

• Cannot provision such a packet filter statically
  – Access permissions depend on user identity
  – Router only has access to user’s IP address, which may be dynamically assigned via DHCP

• Greatly simplified administration via decoupling of separate concerns
  – HR maintains employee rank information in the directory (i.e. whether an employee is an engineer, a manager, etc.)
  – DHCP process maintains user-to-IP address mapping in directory
  – Policy Server fetches all required data to arrive at a decision
Example: Dynamic SLA Enforcement

• Service scenario:
  – Customer is an enterprise with two geographically distributed sites
  – Service provider provides IP VPN service between these two sites
  – SLA provides the following guarantees:
    ▪ “Gold traffic” (identified via IP precedence marking at ingress customer routers) is guaranteed a pre-defined bandwidth
    ▪ Best effort delivery for all other traffic

• Traffic congestion occurs in network core
  – Detected by network monitoring system
  – Congestion threatens violation of above SLA

• Dynamic remedial action is initiated by Policy Server
  – Network elements are dynamically reconfigured to ensure that SLA is not violated
SLAs and Policies: Example

(1) Network Congestion detected; potential for SLA violation

(2) Policy server is informed about threatened SLA violation

(3) Policy server retrieves applicable policy rule from directory

(4) Policy Server computes device-specific configuration for two customer routers based on policy rule

(5) Policy Server pushes new configuration info (to enforce SLA) to routers
Possible Implementation Protocols

Policy Server

Policy Management Application
Status & Config. Info.
HTTP, COPS, SNMP
Notification
HTTP, COPS, SNMP

Policy Consumer (PDP)

Policy Target (PEP)
HTTP, COPS, SNMP

Policy Repository (e.g. Directory, DB)
LDAP, HTTP, COPS, SNMP
LDAP, HTTP, COPS, SNMP
LDAP, HTTP, COPS, SNMP

HTTP, COPS, SNMP
COPS

- Common Open Policy Service (COPS)
- Defined by IETF
- Common protocol between elements and policy server
- Client-server protocol for PEP to send status updates, requests to remote PDP to get back policy decisions
  - The PEP is a COPS client
  - The PDP is a COPS server
- Provide mechanisms to push/pull policies
  - PEPs query PDP for policy information whenever needed
  - PDP can push policy information asynchronously to PEP
COPS Usage

- Policy Provisioning
- QoS Provisioning
- RSVP admission control
- VPN connectivity
- Policy-based Routing
- etc.
COPS Messages

• Operations
  – Request(REQ): PEP → PDP
  – Decision(DEC): PDP → PEP
  – Report State(RPT): PEP → PDP
  – Delete Request State(DRS): PEP → PDP
  – Synchronize State Req(SSQ): PDP → PEP
  – Client-Open(OPN): PEP → PDP
  – Client-Accept(CAT): PDP → PEP
  – Client-Close(CC): PEP ← → PDP
  – Keep-Alive(KA): PEP ← → PDP
  – Synchronize Complete(SSC): PEP → PDP
IETF Policy Internet Draft (1)

• A working effort linked to the DMTF to standardize *semantics* and *syntax* for policy data in the form of a model extension to the CIM and an LDAP schema

• Became available at the end of 1999

• The IETF working group is targeting mid-2000 for a standard schema
  – Policy Framework LDAP Core Schema
  – Policy Core Information Model - Version 1 Specification
  – Requirements for a Policy Management System
  – Policy Framework
IETF Policy Internet Draft (2)

• QoS
  – QoS Policy Schema
  – Policy Framework QoS Information Model
  – Information Model for Describing Network Device QoS Mechanisms

• Security
  – Security Policy Specification Language
  – IPsec Configuration Policy Model
  – for Firewall & VPN
Problems with the IETF Approach

• Association of policy with consumer (subject) and target is not clearly specified
• No event triggering of policies
• No language for specifying policies
• Instance-based reuse rather than specification based reuse
• Very QoS management oriented, although meant to be applicable to other applications
• Conflicts detection and resolution identified but not defined

⇒ IETF/DMTF are currently working towards resolving these problems
PBNM Products

- HP PolicyXpert
- Extreme Extremeware Enterprise Policy Manager
- Cisco Ciscoassure Policy Networking
- Cabletron Smart Networking Services
Products (1) – HP PolicyXpert

- Policy-based network management tool
  - End-to-end QoS
  - Services, traffic shapers, switches, and routers

- Can configure multiple heterogeneous devices
  - Variety of device types and vendors via Agents
  - Simultaneous deployment to multiple devices

- PolicyXpert agents translate policy information into device-specific configuration details for network devices and network servers
  - e.g., Cisco routers, HP ProCurve switches, Packeteer PacketShapers, Nortel routers, NT servers
Policy types in PolicyXpert

- Prioritized class of service (COS)
  - Eight levels of priority
- Committed bandwidth
  - Aggregate committed information rate and burst rate
- Per-flow assured bandwidth
  - Per-flow information rate and burst priority
- RSVP disallow
  - Disallow RSVP signalled flows
- RSVP maximum bandwidth
  - Allocate maximum kbps to reserve for signalled flows
- RSVP priority
  - Eight levels of priority for competing RSVP flows
PolicyXpert Architecture

- Console creates, assigns, and deploys policies
- Primary server stores and distributes policies & maintains status information
- Secondary server (PDP) provides intra-domain scalability
- Configuration proxy provisions network elements
- COPS is used to communicate policies, requests, decisions between PDP and PEPs
PolicyXpert User Interface

- Policy
- Rule
- Action
- Condition
- Resource
Product (2) – Extreme

• Extremeware Enterprise Manager
• Policy configuration for QoS and Security for users, customers, and applications
• Layer-independent policy enforcement
• Web-based policy console tool
• Dynamic Link Context System supports the tracking of user to IP address mappings ⇒ enables dynamic user based QoS and Security policies
• Multi-vendor policy configuration for Extreme, Cisco and Lucent network devices
Extremeware Enterprise Manager

Policy System

Create: Network QoS Policy

Name: Databases

Description: Medium Priority for DB group

Properties:
- Servers: Database server
- Clients: Admin Group
- Application: SQL
- Treatment: Medium
Products (3) – CiscoAssure

• Cisco QoS Policy Manager: enables mapping policies onto QoS enforcement mechanisms – admission control, congestion management, traffic shaping, etc.

• Cisco Secure Manager: provides a centralized, coordinated mechanism for Cisco PIX Firewall policy management

• Cisco User Registration Tool: identifies users within the network and creates “user registration policy bindings” and provides policies based on users.
Products (3) – Cisco Secure Manager

Policy Assignment

[Diagram showing policy assignment with various network components and policies such as Trusted Networks, Internet, Corporate Web Server, DMZ Network, Cisco Security Manager, and ADMIN-NT.]
Products (4) – Cabletron

- SmartNetworking Policy Manager
- Offers Policy-based Security and QoS solutions
- LDAP/DEN support
- Can use Directory from Netscape, Novell, Microsoft
- Multi-vendor support
- Defines access control policy & bandwidth policy
- Binds policies to devices & applications
- Schedules policies
Cabletron Policy Manager UI
Comparison of Products (1)

HP/Intel Policyxpert
Ship date: April 1999

- Policy-enabled device
- Master copy of policy
- Cached local copy of policy
Comparison of Products (2)

Extreme Extremeware Enterprise
Policy Manager

Ship date: August 1999
Comparison of Products (3)
Comparison of Products (4)

Cabletron Smart Networking Services
Ship date: May 1999

- Redundant policy server
- Standalone policy server
- Directory (Netscape, Novell)
- DHCP server
- GUI Net management console
- 100/1,000-Mbit/s Ethernet
- 10/100/1,000-Mbit/s Ethernet
- Backbone switch or Cisco router
- Layer 3 departmental or workgroup switch
- To other departmental/workgroup switches
Summary

- PBNM provides a basis for dealing with automated, dynamic & reusable management
- PBNM has been mainly applied to QoS and Security management
- IETF/DMTF is working on standardization
- More work on the following topics are needed:
  - policy analysis (interpret)
  - conflict detection & resolution
  - policy enforcement
Future Directions

• Support QoS for mobile users based on PBNM
PBM of Networks & Systems

• Policy agents: licensed to manage
References (1)

- **Standards related to PBNM**
  - IETF Policy Framework Working Group
    http://WWW.ietf.org/html.charters/policy-charter.html
  - DMTF Information Service Level Agreement (SLA) Working Group
    http://www.dmtf.org/info/sla.html
  - Common Open Policy Service (COPS) – RFC 2748
  - Directory Enabled Networks (DEN), http://www.murchiso.com/den
References (2)

- **Policy-based Network Management**
  - Policy Work
    - http://www-dse.doc.ic.ac.uk/policies
    - http://www-dse.doc.ic.ac.uk/~mss/MSSPubs.html
References (3)

- **DP&NM Lab, POSTECH**
  - http://dpnm.postech.ac.kr/policy

- **Products of PBNM Systems**
  - HP OpenView PolicyXpert
    http://www.openview.hp.com/products/policy
  - Cisco CiscoAssure Policy Networking
  - Intel Policy-based Network Management (PBNM)
    http://www.intel.ie/ial/pbnm/index.htm
  - Extreme Extremeware Enterprise Policy Manager
  - Cabletron Smart Networking Service
    http://www.cabletron.com/smartnetworking/policy
Q & A