International Civil Aviation Organization and
Aeronautical Radio of Thailand Limited

Aeronautical Telecommunication Network (ATN) Seminar

Chiang Mai, Thailand, 11 -14 December 2001

Policy Based Management System

(Presented by United States)

Summary

The aim of policy-based management is to apply an integrated management system so that system management, network management and application management can cooperate. From a network operations point of view, policy-based network management is about minimizing the complexity of end-to-end management and security. Also, it is mandatory to support or address legacy systems and device limitations.

1. Introduction

Policy-based management offers a new possibility for managing networks and networks systems. Every network function or process has a role and specific rules on how to proceed. The goal is to control behavior of network elements, process applications and network resources by employing well defined rules. Moreover, critical network resources must be aligned to observe and enforce network-wide policies, to provide dynamic features for service creation and enable control from a network provider to the administrator to the end-user. The migration allows for and optimization of infrastructure costs. The concept of policy-based network management is evolving and capable products are becoming more available.

Policy-based management can offer solutions to:

Diminish increasing cost of management

Reduce complication of control

Align management information that is not shared everywhere in the system

The need for policy-base management merges from the complexity of today's networks and network systems. Policies are considered to bring routine to everyday operations. As networks grow and complexity increases quality of service and security needs increase. There is an evident need for rules to automate and govern processes and functions. Policies are also needed to define strictly regulated access to various resources. Non-standardized policies for management functions can already exist in a system but they are not created conveniently and are not collected or directed to the same database.

The infrastructure of ATN is made up of technology from a host of different States. The type of management policy desired would determine which equipment will be involved in receiving and enforcing policy information. One of the key features of policy-based server is to centralized management of network management resources and the allocation of resources which ensures that only authorized clients have appropriate access to and use of network resources.

2. Functional Overview and Policy Server Structure

The components of a policy-based management system include the policy console, policy server, policy data base and policy clients. The policy console provides administrative and operational access to the policy-based system.

The policy server embodies the decision-making functionality of policy-based management. One or more such policy servers exist in a control domain, with each server configured to support policy management for a defined group of clients. The **policy server** provides each policy client with policy information; the **policy client** in turn enforces the policies to the best of it abilities. The policy client **communication component** handles all exchanges between policy clients and policy server. The **messaging processing component** is responsible for policy protocol message decomposition and composition. The **core-processing component** embodies the logic needed to support the policy server's policy decision making. This component logs all relevant usage by policy clients. The policy **console communication component** gives support for communicating with the policy console. This allows multiple policy servers to be maintained from one policy console. It also allows multiple consoles to access the same policy server.

3. Implementation of Policy-Based System

A policy-based system can be implemented as an aspect of the management process within a State environment or managed network domain.

First, create a network baseline and track network usage against key applications, network services and unit users or usergroups. Follow this by establishing network domains, policy groups, group identities and hierarchies that map to core activities.

Next establish organizational directives and create corresponding policy rules and service level requirements over various applications supporting policy users on the priority use of critical infrastructure resources. Administer policies across the network infrastructure on a domain or inter-domain basis. Now, audit and validate network policies against service requirements, refine directives and network policies based on policy enforcement.

4. Policy Framework

Policy framework describes the architecture for policy management. It defines the policies, how policies are used and where they are stored. It also defines objects, which are managed by certain rules. The architecture can be constructed so that there is a domain (managed object) space, rule space, policy driver, and action space. The policy procedure can be the following: policy drivers monitor the network and can be triggered into action by events in the network, then the policy driver takes a managed object from the object base as a parameter, processes the rule from the rule space and executes actions in the rule. The managed object in domain space refers to a real attribute of the physical network and can be e.g. transactions between network elements and between themselves.

The structure of policy-based management architecture can contain data repository, policy server, and managed objects, which the policy server controls. The policy server detects triggered events and makes policy decisions for actions. The needed data can be stored in the repository which can be managed. The repository can be, for example, a directory server. The policy server also takes care of device discovery and device configuration. The policy server also enforces objects and devices to obey policies.

5. Policy-Based Management in Security Management

Policy-based management approach can be used also in security management. It defines authentication and verification processes, encryption procedures (key/certificate management, encryption/decryption procedures) and user profiles and roles. The policy server can be a single device, which handles every policy actions or a set of servers, which can communicate with each other to proceed policy actions. In this approach the user communicates with a policy server before it can use a resource and the policy server performs the defined actions. End-to-end security will require a tighter integration of policy across separate security realms, which are traditionally disjointed among networks, applications and servers. The management of policies is simplified because the information is centralized and policies can be made consistent.

The model requires a policy server, which performs the security policies and rules. This means that a trustworthy server node has to be defined which can be difficult. One solution is to use a fixed node, but creates in itself some new security problems. When the security server is chosen and the authentication-tree is formed, the problem becomes reality of service. A group of server nodes can decrease vulnerability and increase reliability. If the server model is required the described solution can be considered. These aspects decrease possibilities for security attacks. If the policy based model is adjusted so that policies, certificates and keys are delivered in advanced, a policy based model can be a better choice for security management.

6. Conclusion

Policy-based management is a new concept and intended for quality of service management. In general, a policy-based approach can be useful because it has well defined rules for security management and defines what functions the nodes can perform. However, there are still some issues that will not be resolved until policy-based network management matures. Industry standards in the areas of policy-based directory design, quality of service technologies and policy and directory communication protocol are still under development. Enterprise strategies are requiring timely evolution of network infrastructure and

management to support delivery and management of end-user and network services. Within this context, quality of service, security, productivity and infrastructure efficiency are critical to achieving the highest level of performance results.