Chapter 1

Introduction

Nowadays telecommunications networks are based on different technologies in order to convey data, telephony, videoconferences and other services. These networks usually have extremely expensive complex management systems and that is the reason why new heterogeneous network management system models are studied.

Throughout history we can find different proposals to simplify all system management tasks. As examples, we can mention the network management systems using the Simple Network Management Protocol (SNMP), the users and groups management in local area network devices by means of the Network Information Service (NIS) or the conversion of names into IP addresses in networks using the Domain Name Service (DNS). All these solutions show us just a partial solution to a partial problem too. However, the network management as an integral system unit is a more complex task that must solve different aspects such as a long-term scheduling and the day-to-day provision of resources.

One of today's biggest challenges is to improve the automated management tasks and expand their application area always considering integrity, security and reliability in the system. This Thesis proposes a global solution to automate the management tasks using a schedule based on service and network policies, which becomes a low-level configuration that all the network devices must have to guarantee the level of quality previously established. The designed platform allows a flexible and scalable management concerning all Quality of Service parameters within heterogeneous network domains.

The structure of the Thesis is the following: This chapter consists of a general introduction of the Thesis and the exposition of the main concepts related to policy-based management. Chapter 2 details the IETF and the OMG (object management group) Policy system architectures. Chapter 3 is a proposal of a policy-based management architecture giving exhaustive details about the classes of service created for our system; in the same way it also exposes all parameters coming from the Service Level Agreements (SLA) between the Internet Service Provider and the user. As a consequence, a mapping of Quality of Service (QoS) parameters has been established towards the configurable parameters in the proposed classes of service. This chapter also explains the different policy levels that we use and their translation into low-level policies that can be implemented in the different network devices.

Chapter 4 presents the design of the policy repository for our system and the LDAP mapping of the Policy Core Information Model (PCIM) to an LDAP schema. Next chapter is an algorithm to evaluate and to select policies. This algorithm is applied as an example to the routing management but it can be extended to the other functional areas of the management system. Chapter 6 details the conflict resolution problem between policies. Finally the conclusions are presented. The Appendix II explains the implementation of the system.

1.1 Distributed Hierarchical Management

Distributed systems play a more and more important role everyday within the network communications. The way in which some aspects of these systems are managed, such as the Quality of Service, routing, etc. represents an interesting field of action.

In the last decade, the classic paradigm centralised on the aspect "manager-agent" was the dominating network management architecture, for example, the SNMP (Simple Network Management Protocol).

These architectures have a network management centre which acts as a monitor of the managed devices, provides the current state of the network, alerts the human manager in case of a wrong running but the human managers is still in charge of changing the network operation to solve all possible problems.

The OSI model owns 5 functional areas: fault management, configuration management, accounting management, performance management and security management. The following figure shows the relation between the manageable objects and the manager.

Figure 1. Manageable objects and the manager

The SNMP owns three main components: an agent allocated on a network manageable device that stores management data and responds to all the petitions about those data; a manager allocated on the network management station and asks agents questions by means of SNMP commands and a Management Information Base (MIB). The agent stays as simple as possible while the management load lies on the manager.

On the other hand, the TMN model owns three functional areas: the functional architecture that defines the functional blocks through which the TMN is built; the physic architecture that describes the interfaces and the way in which the functional blocks are implemented in physic equipments and an information architecture that follows the OSI management model principles (CMIS and CMIP) and the directory ones (X.500). Following figure shows the TMN levels.

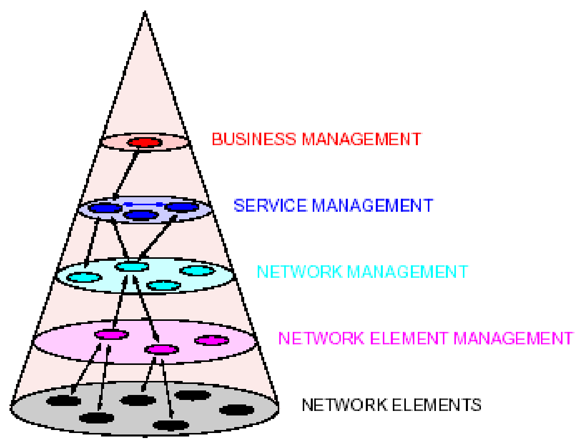

Figure 2. TMN Levels

Previously mentioned architectures do not have conflicts, except from those ones caused by the human managers configuration. These architectures are emphatically centralised on observing more than on controlling, works in an adequate way for best effort networks, but it doesn't reach all the requirements of the emerging multi-service networks with quality guarantee, that is to say, it is necessary to use new management paradigms that keep simplicity on the management platforms of the last decade and, at the same time, help the competitive nature to appear in the current network services demanding economic management operations.

In this way, hierarchical and distributed management paradigms emerge, as for example, the distributed object computation, the network management based on webs, the network management based on java, the code mobility, the intelligent agents, the active networks, the management based on policies, etc

As we can see, there are different methods to solve specific high scale distributed system management problems. In this Thesis the system management problem will be analysed as whole taking into account the priority of achieving an auto-regulated and auto-ruled network management. That is the reason why we chose one of the newest management techniques that bases all the management tasks on policies.

The use of LDAP directories based on the X.500 scheme to store the IETF policy models makes the management integration easier among networks based on the IETF with networks based on ITU rules, as for example, GSM, UMTS, ISDN, etc. They provide a great synergy. This means that a Policy-Based Management System (PBMS) carries out functions equivalent to a TMN in order to manage communication networks.

The following part of the Thesis presents an explanation of the main concepts for the policy-based management systems.

1.2 Policy-based Management Systems (PBMS)

The policy- based management systems are one of the latest achievements in the field of network and distributed system management. It provides a specific way to assign network resources, the Quality of Service and security, considering a previously defined set of policies. These systems provide a big easy way of scaling and they easily adapt to the changeable network conditions and to the different QoS requirements in the multimedia applications, in the virtual systems and in the complex applications processing that takes place at real time.

Policy concept has several meanings: it can be considered as “the set of rules that determines the network management distributed system behaviour”[Sloman94] or as “an aim, process or action method to guide or determine present and future decisions” [Wright99]; in [Blight00] policies are defined as “a set of rules to administrate, manage and control the access to the different resources in the network”.

PBMS are in charge of the specification process, evaluation and distribution of the necessary policies to manage heterogeneous networks that offer different kind of applications with QoS guarantees. Both the network and the policy devices own the characteristic of independence, which makes it possible to configure automatically all nodes in the network, without taking into account if they are coming from different Internet providers or are equipped with different capabilities. The network administrator does not need to worry about the implementation details that the individual nodes own.

The following figure represents the heterogeneity of the networks that can be controlled by means of PBMS.

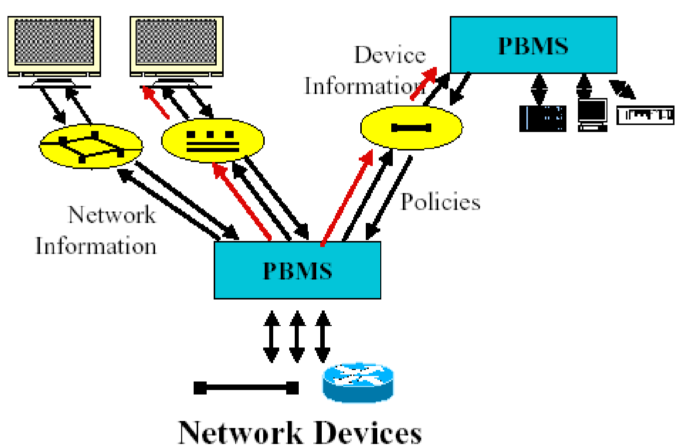

Figure 3. PBMS with heterogeneous components

Systems based on policies are very efficient in high-scale networks where there are a great number of devices that present constant changes. In order to achieve that, it is only necessary to modify or eliminate the corresponding policies or to add new policies capable of reaching the new requirements without having to execute any change neither in the applications nor in the software or hardware platforms. In this way, the policy-based systems have an optimal development under changeable conditions in the network and an easy adaptation before new services.

The fact of keeping the integrity of the system and the fact of avoiding conflicts among policies are two important factors that make very difficult the running of the policy-based systems. It is essential to consider that the bigger the control about the system in the policies is, the more efficient the selection algorithm and the high-level policy translation into low-level policies are.

The policy-based management is in the state-of-the-art. There are some researches related to the policy specification and to their implementation in specific application areas [Lobo99], [Gary01], [Georgalas99], etc. In [Zhi01] and [Ribeiro99] there is interesting research about security policies. Other interesting works [Munareto02] propose policy-based systems to support mobility. In [Bhatia00] a model that lets the policy specification, distribution and evaluation has been developed.

In the Computation Department of the Imperial College of Science, Technology and Medicine in London they are working on several policy management areas. One of the most remarkable works is the development of the Policy Framework PONDER, which includes management domains, a policy language, a role-based management and security policies [Damianou01].

Fujitsu Laboratories are studying issues about Quality of Service in management IP, taking into account the scaling process in the networks management as the main challenge in the operation of big-scale networks based on policies.[Hamada00]

Brunner [Brunner 01] proposes en efficient integration of a policy plane into different management functions and within routing schemes such as MPLS. In [Prieto01] they introduce the Service Level Specifications mapping problem towards differentiated IP services by means of PBMS.

However all of these interesting researches the policy-based management is a quite recent issue that still have a lot of open problems. This Thesis tries to solve some of them, as for example, the control of the policies over the system from the point of view of an integral unity, the translation of high-level policies into low-level policies, the policy selection process, conflict resolution between policies, etc.

1.3Contributions of this Thesis

This Thesis proposes a policy-based architecture management for big-scale networks that guarantee a Quality of Service level to their users. The management platform shown here is based on the architecture of the IETF working groups, on the information models proposed by the DMTF and the OMG and on several researches carried out by companies and universities related to the network management.

The main contributions of the system are the design of a policy framework that controls all functional areas of heterogeneous domains via policies. This framework has different components, for example a policy selector (see chapter 5) that decides which policy or set of policies must be applied in the network, another important component is a conflict resolution process to solve the problem when two or more policies can be applied in the network elements, solving network inconsistencies, etc. (see chapter 6). Another contribution to PBMS is a proposed mapping from the Service Level Specification parameters (SLS) towards configurable policy rules in the network devices.

References

[Bhatia00] Bhatia R., Lobo J., Kohli M. Policy evaluation for network management. IEEE Infocom 2000

[Blight00] Blight D., Hamada T., *Policy-Based Networking Architecture for QoS Interworking in IP Management*. Lecture Notes in Computer Science Vol 1960. Springer. DSOM 2000

[Damianou01] Damianou N, et.al. "The Ponder Policy Specification Language" Computer Science vol.1995 IEEE Policy 2001. Springer Bristol, U.K. 2001

[Gary01] Gary N. Stone, Bert Lundy Geoffrey G. Xie. *Network Policy Languages: A Survey and a New Approach.* IEEE Network. January/February 2001

[Georgalas99] Georgalas N. *Policy-driven Customisation of Personalised Services.* Proceedings of Policy Workshop 1999, HP-Laboratories, Bristol, U.K. 15-17 Nov 1999

[Hamada00] T. Hamada, P. Czezowski, T. Chujo. *Policy-based Management for Enterprise and Carrier IP Networking*. FUJITSU Sci. Technology .Journal vol 36-2 December 2000. pp 128-139.

[Lobo99] Lobo J., Bathia R., Naqvi S. *A policy description Language*. Proceedings of AAAI Press. Orlando. U.S. 1999 pp.291298.

[Munaretto02] M. Anelise, N. Agoulmine, M. Fonseca, *Policy-based Management of Ad-hoc Enterprise Networks,* HP Openview University Association 9th Annual Workshop, HP-OVUA, June 2002

[Prieto01] A. Prieto, M. Brunner, "SLS to DiffServ Configuration Mapping", IFIP/IEEE International Workshop on Distributed Systems: Operations and Management (DSOM´01), Nancy, France, 2001.

[Ribeiro99] C.Ribeiro, P.Guedes. SPL: An access control language for security policies with complex constraints. Technical Report RT/0001/99, INESC. Enero 1999

[Sloman94] M. Sloman, *Policy Driven Management For Distributed Systems*, Plenum Press Journal of Network and Systems Management, vol 2, Nº 4, Dec. 1994. pp. 333-360

[Wright99] M. Wright *Using Policies for Effective Network Management* International Journal of network Management Nº 9, 1999. pp. 118-125

[Zhi01] Zhi Fu, Feliz Wu. *Automatic Generation of IPSec/VPN Security Policies in an Intra-domain Environment*. 12th International Workshop on Distributed Systems: Operations and Management DSOM'2001 Nancy France, October 15-17, 2001. O.Festor and A. Pras (Eds.)