A new policy-aware terminal

Hakima CHAOUCHI

*University of Paris 6, LIP6 Lab. Network & Performance
8 rue du Capitaine Scott
75015, Paris*

Abstract: Policy-based Management has been largely studied during the last years. The Internet Engineering Task force (IETF) has more recently introduced the Policy Based Networking as a mean for managing the IP networks according to the new constraints defined in the network such as the guarantee of the Quality of service (QoS). The network managed based on policies, is modelled as a state machine which moves from a state to another according to the enforced policy. The IETF policy based networking is defined to be applied to the network nodes. However, some recent works suggests extending the policy based networking to the end user terminals. In this paper, we present an analysis of such an extension and we propose some possible solutions to support new policy-aware terminals and a corresponding end-to-end QoS extended provisioning and outsourcing frameworks.

Key words: Policy-based management, Policy-based networking, Common Open Policy Service (COPS), outsourcing, provisioning.

1. INTRODUCTION

Network management area intends to configure network elements in order to achieve a network behaviour which is specified by a network manager. One of the key motivations of the policy-based management is flexibility and graceful evolution of the management system so that it can adapt for changing requirements over a long period of time [1]. Policy-based networking has been introduced by the IETF to facilitate the network management relatively to the new constraints such as a Quality of Service

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: [10.1007/978-0-387-35620-4_43](https://doi.org/10.1007/978-0-387-35620-4_43)

D. Gaïti et al. (eds.), *Network Control and Engineering for QoS, Security and Mobility*
© IFIP International Federation for Information Processing 2003

(QoS) guarantee. Different elements need to be introduced in the network in order to achieve this policy-based management.

In this paper, we are interested in a new vision of the policy-based networking where the end user terminal is also an element of this policy-based networking. We present an analysis of the key aspects of such an extension and propose a new architecture called policy-aware terminal.

The rest of this paper presents a survey on policy-based concept introducing the view of both the research and the IETF community. After a review of the pros and cons of extending the policy-based networking to the end user terminal is given. Then, we will come out with a proposal of a new policy-aware terminal and we finally conclude this work.

2. SURVEY ON A POLICY BASED CONCEPT

Telecommunication networks are managed according to the hierarchically distributed Telecommunications Management Network (TMN) model. Initial and subsequent reconfiguration of network elements occurs through element managers which are orchestrated by a logically centralised but physically distributed, network manager [1]. The latter has an upper view of the network-wide policy and implements it through automated logic. This is achieved by supervising the network elements and reconfiguring them in order to introduce new services. This management logic can be altered to a limited extent by modifying managed objects that are modelling its operation [1].

All configuration changes occur through an appropriate manager, which holds the physical and logical network topology and partitioning. Requests coming from service, performance, fault and other managers are carefully validated in order to maintain network consistency and integrity. Despite this validation, it is possible that different managers have conflicting configuration requirements which may lead to an inconsistent network state. Such conflicts can be avoided by careful modelling, design and testing of the management system, but then conflicts may still occur at run-time when the system is nearly-jammed by real world conditions not previously anticipated [2].

Policy-based technology may be applied to both enterprise and telecommunication networks. The view taken by the IETF seems to be compatible with the centralised model used in managing enterprise networks, though policy work in the research community has previously defined distributed models.

In the next section we present the two main views of the policy-based concept which are the research community policy based management and the IETF policy based networking views.

2.1 Policy Based management in the research community

Many efforts have been carried out in the area of policies for the management of distributed systems.

From a distributed system management point of view, policies are specified as objects which define relationship between subjects (managers) and targets (managed objects) [2]. Policy objects have attributes specifying the action to be performed and constraints limiting the applicability of the policy.

[2] proposes a generic management architecture for distributed management systems. It introduces the concept of domain which is a set of managed objects for which a policy applies.

The research effort focuses mainly on the policy classification, policy refinement process and policy specification languages.

Policies have been classified according to their actions. There are:

- Authorization policies which specify what a subject is authorized to do with respect to the managed objects; these are mainly access control policies.
- Obligation policies which specify what operations the subject must perform on a set of target objects.
- Refrain policies which define the actions that subjects must not perform on target objects.
- Finally, delegation policies which specify the actions subjects are allowed to delegate to others.

Policy refinement is the process of translating policies from a high level to low level policies to build a policy hierarchy. Many policy hierarchies have been defined by different authors. For example, [3] defines four levels of hierarchies which are:

- Corporate or high level policies,
- Task oriented policies,
- Functional policies,
- and low-level policies.

Policy languages are another research area [4]. A declarative, object oriented language are currently used for specifying policies for the

management of distributed systems including constructs for specifying the basic types of policies.

2.2 Policy Based networking in the IETF community

Enterprise networks are typically managed with Simple Network Management Protocol (SNMP), using a relatively simple management architecture consisting of a single centralised “network management centre (NMC)”. The latter supervises network elements located typically in a cluster of local / metropolitan area networks. In this architecture, the elements are typically configured one-by-one, in an isolated fashion, through the supervision of a human network manager and according to an overall network operation policy [1]. This means that configuration is not that frequent and will be made manually.

In an evolution of this scheme, configuration parameters for every device are stored in a repository which is contacted by the devices upon cold or warm starts so that a device picks up necessary parameters and configures itself; this makes the system more scalable. While this simple, centralised architecture with emphasis in monitoring rather than control, works adequately for best effort IP networks, it cannot meet the needs of emerging multi-service networks with QoS guarantees. The latter require frequent and automated configuration changes according to a network-wide view. For this purpose, a new network management has been introduced by the IETF based on policy management.

Policy based management is being adopted widely for different domains such as Quality of service (QoS), security, and Virtual Private Networks (VPNs) [5]. Also, the interface to the network device (the protocol) and the information models required for specifying policies are standardized in both the Internet Engineering Task Force (IETF) and the Distributed Management Task Force (DMTF) [6].

Policies encode the high-level goals and requirements of management. Typical usage of policies includes [7]:

- device configuration: queuing mechanisms, drop strategies, access filter lists, etc
- traffic classification/marketing (e.g. DiffServ marking)
- resource reservation and admission control based on user identity, application type, etc (e.g. With RSVP: ReSerVation Protocol)
- Service Level Agreement (SLA) between two adjacent domains.

There are two working groups in the IETF which consider the policy management, or the policy based networking. They are the Resource Allocation Protocol (RAP) and the Policy Framework (Policy) working groups.

2.1.1 RAP WG

The initial purpose of the Resource Allocation Protocol (RAP) WG is to establish a scalable policy control model for RSVP and to specify a protocol to be used among RSVP network nodes and policy servers. RAP WG describes a framework for policy-based admission control specifying the two main architectural elements illustrated on figure 1 which are the Policy Enforcement Point (PEP) and the Policy Decision Point (PDP). The PEP represents the component that runs on the policy-aware network node and it is the point where the policy decisions are effectively enforced. The PDP is the point where the policy decisions are made. RAP WG introduces a policy transport protocol called COPS (Common Open Policy Service).

Two interaction modes are specified for the PEP and the PDP interaction using COPS [5]; the outsourcing and the provisioning modes. In the outsourcing mode, when a PEP receives a message that requires a policy decision, it creates a request that includes information which describes the admission control request. Then the PEP may consult the local configuration database to identify which policy elements can be evaluated locally, passes the request to the Local Policy Decision Point (LPDP) and acquires the results. The PEP then passes all the policy elements and the partial result to the PDP which combines its result with the partial results from the LPDP and returns the final policy decision to the PEP. In the provisioning mode, the PDP provisions the configurations to the PEPs and when the PEP receives a request it processes it without interacting with the PDP since policies has already been enforced.

Figure 1. RAP WG policy based networking framework.

2.1.2 Policy Framework WG

The policy WG has provided several drafts describing a general framework for representing managing, sharing and reusing policies in a vendor independent, interoperable and scalable manner as well as defining an extensible information model for representing policies (PCIM: Policy

Common Information Model) [6] and an extension to this model to address the need for QoS management (QPIM: QoS Policy Information Model) [8].

The framework defined by the policy WG defines a policy as an aggregation of policy rules. Each policy rule includes a set of conditions and a corresponding set of actions that are intended to be device and vendor independent. Policy rules are of the form: if <condition> then <action>. The condition expression may be compound expression and it may be related to entities such as host, applications, protocols, users, etc. The <action> expression may be a set of actions that specify services to grant or deny or other parameters to be input to the provision of one or more services. The major functional elements introduced by this WG are illustrated on Figure 2, they are :

- The policy management tool to enable an entity to define, update and optionally monitor the deployment of policy rules.
- A policy repository to store and retrieve policy rules.
- A policy consumer or Policy Decision Point (PDP) which is a convenient grouping of functions, responsible for acquiring deploying and optionally translating policy rules into a form usable for policy targets.
- A policy target or Policy Enforcement Point (PEP) is an element whose behaviour is spelled out by policy rules, carrying out the action indicating by policy rule.

Figure 2. Policy WG framework.

3. EXTENDING THE POLICY BASED-NETWORKING TO THE USER TERMINAL: PROS AND CONS

3.1 Pros

The policy based networking assumes that the policy components are networks nodes in order to ensure their total control by the network provider.

Some research works introduces the extension of the policy based networking to the end user terminal for dynamic QoS negotiation [9] and for user mobility management [10]. These works introduces the direct interaction between the terminal as a policy enforcement point and the policy server in the network.

In such architecture the terminal achieves a part of the work done by the network elements in the classical policy based networking architecture. This is interesting since the terminal has important processing resources which can be used to make some processing on behalf of the network nodes.

In addition, the terminal becomes aware of the network resources by limiting the traffic generated by the terminal before going into the network.

[9] proposes a framework based on COPS (COPS-SLS) to negotiate the Service Level Specification (SLS). It assumes that the policy enforcement point may be an ISP, a corporation router or an end user terminal. The latter assumes that the terminal is a policy-aware component which interacts with the policy server in the network to negotiate the QoS parameters as illustrated on figure 3.

Figure 3. Terminal PEP in the COPS-SLS framework

[10] proposes a framework based on COPS (COPS-MU: Mobile User) and Mobile IP in order to manage the terminal and the user mobility. For this purpose a policy enforcement point is also introduced in the terminal as illustrated on figure 4.

Figure 4. Terminal PEP in COPS-MU framework.

3.2 Cons

The previous works [9,10] focus on the transport protocol achieving the direct interaction between the terminal and the policy server. However, two aspects are important to be considered in order to extend a policy based networking to the end user terminal: The **performance** aspect and the **security** aspect.

The performance problem depends on whether the end user network is a wireless or wired environment. In fact, the PEP in the terminal interacts with the PDP introducing overload information which is important to consider in a wireless environment more than in a fixed environment since the radio resource is scarcer than the wired resource.

From security point of view, defining a PEP as a component of a terminal assumes that such a PEP is a part of a network provider environment implemented in the end user terminal. The big issue is to deny access to the user to this PEP environment to make a personal configuration of his terminal. Thus, the terminal PEP needs to be highly secured to ensure that it achieves the decisions coming from the policy server of the network and not from the end user.

Another problem related to the security issues introduced by the terminal PEP environment is how to recognize at the access network, from which end user terminal packets are coming.

3.3 A new architecture of a policy-aware terminal

In order to make the terminal policy-aware by securing its environment we suggest two possible solutions:

The first one is to have an isolated box to enforce policies with no access by the user. Such a solution is interesting in a wired environment. This allows reusing the current terminals with a global policy based environment as illustrated on figure 5.

Figure 5 Black box terminal PEP.

The second solution suggests a new architecture in the terminal. In order to ensure the security of this environment in the terminal, we suggest integrating new components in the terminal network adapter, based on a smart card technology to secure this environment. Since the smart card technology is evolving to have more processing resources, we propose to have the terminal PEP and the corresponding components in a smart card as illustrated on figure 6. Such a terminal architecture makes the terminal policy-aware and secure. It will integrate this environment with the terminal network adapter and ensure that the packets going in the network behave according to the network policies enforced by the terminal PEP.

Figure 6 Smart card technology based terminal PEP.

From performance point of view we need a filter in the terminal to allow only the network provider authorized traffic to go into the network. Such a filter needs to classify the packets and recognise to which application the packet belong to. Such a classification is based on the filter configuration which is enforced by the terminal PEP according to the policy decisions of the network PDP, it allows or rejects packets before going on the network. Such a terminal architecture is very interesting in a wireless environment since it limits the traffic going into the wireless network, saving the radio resource as illustrated on figure 7.

Figure 7. Policy-aware terminal architecture.

The previous terminal-aware architecture needs a signing mechanism in order to uniquely identify the packets according to the user contract.

One possible scenario to use the proposed policy-aware terminal is to extend the policy based networking in a provisioning DiffServ network to the end user terminal to ensure an end-to-end QoS. It means that the terminal architecture is similar to a DiffServ edge router [11] with a terminal PEP to configure the DiffServ components in the terminal according to the policy decisions of the network PDP. Such DiffServ terminal is illustrated on Figure 8 with a terminal policy enforcement point.

Figure 8. Terminal PEP applied to a DiffServ Terminal.

The policy-aware terminal may be used either in the provisioning COPS-PR framework [12] or in the outsourcing COPS-RSVP framework [13] to achieve an end-to-end QoS, as illustrated on figure 9.

Figure 9. Terminal aware-policy based end-to-end QoS.

In the extended provisioning framework, the end user terminal requests its configuration to the network PDP as soon as it is on. The PDP sends the corresponding configuration of the policy-aware terminal, according to the user (Service Level Agreement) SLA.

In the extended outsourcing model, the policy-aware terminal requests network resources according to the IntServ framework and sends the packets as soon as the network PDP accepts the user request.

4. CONCLUSION

In this paper, we have presented an analysis of extending the policy-based management to the user terminal. For this purpose, the policy-based concept viewed by the research community and the IETF community has also been studied. The latter introduced the policy based networking by defining new elements in the network.

Extending the policy based networking to the terminals has pros and cons. The main advantages of such extension is making the terminal more aware about the network resources and exploiting the terminal resources by achieving some treatments in the end user terminal rather than in the network elements. Based on such a policy-aware terminal it is possible to achieve an end-to-end QoS by extending the provisioning or the outsourcing model to the end user terminal.

However, such an extension introduces mainly two problems which are performance and security ones. Performance problems are related to the overload introduced by the terminal policy enforcement point interaction with the policy server.

This problem is more important in a wireless environment since a radio is a scarce resource. The second one is related to secure the environment introduced by making the terminal policy-aware.

Two possible solutions have been introduced in this paper to support the policy-aware terminal concept. The first one builds a terminal PEP environment as a black box which is accessible only by the network policy server able to set up specific policy based configuration. This solution is interesting in order to reuse the existing terminal with no terminal PEP.

The second one is based on the smart card technology to protect the terminal policy enforcement point environment introduced in the terminal. This solution is interesting in both fixed and mobile environments.

Future work intends to implement a terminal PEP prototype in order to examine the applicability of the policy based networking extended to the end user terminal and use a smart card technology to secure the new terminal architecture.

5. REFERENCES

- [1] P.Flegkas et al, "On Policy extensible Hierarchical network management in QoS-Enabled IP networks" Proc IEEE Wksp. Policies Dist.Sys.Net, Bristol, UK, January 2001, P 230-46
- [2] M.Sloman "Policy driven management for Distributed systems", Journal and system management, Plenum Press. Vol.2.No. 4, 1994
- [3] René Wies "Policies in network and system management –formal definition and architecture-", Journal of network and system management, Plenum publishing corp, vol.2, No 1, P 63-83, March 94
- [4] Stone, G. N., B. Lundy and G. G. Xie "Network Policy Languages: A Survey and a New Approach" IEEE Network, vol. 15(1), pp. 10-21, January 2001.
- [5] Dinesh C.Verma "Simplifying Network administration using policy-based management", IEEE Network March/April 2002. Vol. 16 No.2
- [6] B. Moore "PCIM: Policy Core Information model" IETF RFC 3060.
- [7] Appan Ponnapan et al "A policy based QoS management system for the Intserv/diffser based Internet", Policy 2002 proceedings (to appear).
- [8] Y. Snir et al "Policy QoS Information Model :QPIM", IETF Draft, standard track November 2001.
- [9] M. Nguyen et al "COPS usage for SLS negotiation: COPS-SLS", Internet draft, February 2002.
- [10] H.Chaouchi et al "A new policy based management of mobile IP users », Networking 2002 proceedings
- [11] J. Antonio et al "Quality of Service and Mobility for the Wireless Internet", Proc. First ACM Wireless Mobile Internet Workshop, Rome, Italy, 2001.
- [12] K. Chan et al "COPS Usage for Policy Provisioning (COPS-PR)", IETF RFC 3084.
- [13] S . Herzog et al "COPS usage for RSVP", IETF RFC 2749.

POLICY AND VPN