An Architecture for Access Network Management with Policies (AN-PBM)

Olivier Corre[1,2], Idir Fodil[1,2], Vladimir Ksinant[1], and Guy Pujolle[2]

[1] 6WIND,
Immeuble Central Gare, Bat. C, 1 place Charles De Gaulle,
78180 Montigny-le-Bretonneux, France
[2] University of Paris 6, LIP6 Lab. Network and Performance,
8 rue du Capitaine Scott,
75015 Paris, France

Abstract. The actions led so far, especially by the IETF, have resulted in the definition of a network management architecture based on policies. Some information models, as well as transport and policy representation protocols, have been designed. The content of policies, a topic a bit neglected until now, has to answer ISPs and their customers' requirements for the definition of new value-added services. The proposal made by the IETF consists in configuring individually some network interfaces, rather than in globally managing the services. This approach has contributed to mark the difference between the service definition agreement and the network equipment configuration parameters. In this paper, we propose a policy-based service management architecture. This architecture eases the ISP implementation and management of the services it offers. Quality of Service is an area of experimentation for this architecture. Besides, this architecture gives ISP customers the possibility to carefully control their network quality of service.

Keywords. Architecture, Network Management, Policy, QoS, Service Provider, Customer

1 Introduction

For an ISP (or a SP - Service Provider), to manage a network consists in guaranteeing the service levels sold and rapidly solving the problems that may occur in the network. Network management is based on the following principles:

- Planning: customer-ISP service level specification,
- Checking: to ensure that the service level sold is really guaranteed,
- Detection: to notify that a service level is not suited,
- Reactivity: to adapt the network behaviour while the transport quality may affect the service level delivery.

Nowadays, the ISP network management is not much automated. Each router is configured with CLI commands and monitored in using SNMP directly on the

A. Marshall and N. Agoulmine: MMNS 2003, LNCS 2839, pp. 328–340, 2003.

machine or remotely. These tasks are most of the time repetitive, and need skilled staff able to work in an heterogeneous network. An accurate knowledge of the monitoring and configuration software is required for each equipment, and this is not an easy task taking into account the diversity of the devices. Moreover, the amount of data travelling the network makes the traffic heterogeneous and data come from applications which have different features. In addition, the amount of devices connected to the network is continuously increasing. It then becomes very difficult to manage the network efficiently. Network control requires a skilled manpower and some regular bandwidth extensions. The management cost will continue to grow in the near future, since service providers will offer more and more complex services, as those that exist in the Telecom world. For that reason, networks must be managed differently. In this paper, we will introduce an advanced management architecture for Service Providers. This architecture will then be experimented in the scope of Quality of Service. The IETF Policy-Based Management architecture, and our proposal, will be overviewed in the first part of the article. Quality of Service mechanisms will be detailed in a second section. Then, our network management approach will be described for QoS. The policies defined and their implementation in the 6WINDGate equipment will be detailed. Finally, a Voice over IP with Admission Control scenario will be depicted.

2 Policy Based Network Management

2.1 State of the Art

The opportunity to manage a network thanks to policies became a significant research topic from 1997. The first promising initiative has been submitted by Cisco and Microsoft in May 1997 with the Directory Enabled Network (DEN[DMT98]) information model, what objective was to use directories to give efficiency to network device management. A Working Group (DEN Ad Hoc Working Group) has been set up in order to empower most vendors to participate to the DEN specifications. By this way, the interoperability of distributed management tools was made easier [Kos01]. The Working Group success led to the creation of a consulting committee with more than 500 industrial partners, and the specifications of DEN were accepted by the DMTF in 1998. The integration of DEN has been based on the Common Information Model (CIM[DMT99][DMT]) already approved by the DMTF. CIM is an information model and its objective is to ease the management of users and machines in a company environment.

In 1999, the Policy Framework (PF) Working Group has been founded at the IETF in order to bind the IETF and the DMTF, to integrate the CIM and DEN models in a network environment, and to map DEN into LDAP. The PF Working Group has designed an extension of CIM, called Policy Core Information Model (PCIM[MESW01][MRR+01]), and some extensions of PCIM for QoS [SRS+01], and for network security [JRV01].

The IETF snmpconf Working Group has also purposed to facilitate configuration management in defining a Management Information Base (MIB) that

describes the network capabilities to be used for managing network devices through policies [WSH03].

Concurrently, the Resource Allocation Protocol (RAP) WG has submitted a policy-based network management architecture (PBNM) [YPG00]. In this approach, a central decision server, called Policy Decision Point (PDP), provides the underlying equipments, called Policy Enforcement Points (PEP), with configuration directives to be followed with policies. The policies are a set of conditions and actions. The evaluation of the conditions entails the execution of the actions. The policy exchange between the PDP and its PEPs may be achieved by using SNMP, Diameter, LDAP, or a proprietary communication protocol. However, the RAP Working Group has created the Common Open Policy Service (COPS[DBC+00]) protocol for that purpose.
The IETF architecture, as known as PEP/PDP architecture, has been declared Informational RFC during the 54th IETF meeting in July 2002. At the same time, the COPS transport protocol became an Informational Draft.

2.2 The Blanks in the Current IETF Architecture

The IETF architecture has been accepted by academic and industrial researchers as the basic architecture for implementing advanced network management solutions. Nevertheless, the major drawback of this architecture and the policy representation model purposals is the lack of transition models between the SP-client SLA and the network devices. For example, to set up a videoconference - contractually defined with a delay, a loss rate, a jitter and a bandwidth rate - the SP network administrator must know the scheduling and queuing algorithms (among others) to be used, in order to specify policies for well configuring routers and ensuring a good service delivery. Today's network equipment diversity makes it difficult to achieve correctly, due to the lack of equipment independent transition mechanism between the videoconference parameters and the network equipment configurations.

2.3 How to Fill the Gap?

The likely approach to fill the gap introduced in the previous section should be to dissociate the network infrastructure from the offered services. Adding a further abstraction level is necessary. This abstraction level provides the administrator with the possibility to deploy services without having to know which device parameters to configure. This abstraction level allows the service level agreement translation in an equipment-independent configuration. In the previous example, the SP administrator must only specify the QoS (rate, delay, jitter) and security parameters that are written in the agreement.
Our innovative management architecture purpose, Access Network - Policy-Based Management (AN-PBM), is based on the IETF PEP/PDP architecture.

The objective of the AN-PBM architecture is to provide ISPs and their customers with tools enabling them to control their network by managing their services rather than configuring their network devices.

2.4 AN-PBM Architecture

The AN-PBM architecture allows a service provider to manage its traded services and give its customers the possibility to personalize the services they buy. For this purpose, two policy classes have been designed in the AN-PBM architecture: **SP Policies** (SP) and **Customer Policies** (CPP).
According to the agreement binding the SP and its customer, the SP provides the customer's access router with first class policies. The SP administrator is the only person able to make a change in the policy content. Nevertheless, the customer can define his own policies on his access router in order to personalize the services he subscribed to. For instance, while establishing a VPN, the customer negotiates with the SP the security and QoS parameters for this VPN. With the AN-PBM architecture, the client can customize the VPN service and authorise and deny flows the way he wants without having to notify the SP.
However, conflicts between SP and Customer policies may occur. A solution consists in giving a higher priority to the SP policies and to add a referee control mechanism on the access router (CPE).
The AN-PBM architecture differentiates the SP and customer rights, using two main components: the Management Center and the customer access router (CPE).
Thanks to the Management Center, the Service Provider can offer services, translate these services into policies according to the customer requirements and deploy these services in the customer equipments.
The CPE receives the policies sent by the Management Center and installs them locally. The customer can then adapt his QoS access network in generating and installing Customer policies in the CPE.

3 AN-PBM for QoS

In the previous parts, DiffServ and the IETF Policy-Based Network Management architecture have been introduced. QoS appears as a main problem in network management, and its use is a necessity for ISP whishing to offer innovative services based on the differentiation between users and/or applications [Jud01]. However, the IETF PEP/PDP architecture is incomplete even through it is a worthy foundation, since ISP and customer needs have not been translated into suitable policies. That is the reason why we have decided to adapt the IETF architecture with respect to the ISPs and their customers requirements.

3.1 QoS Objectives

The goal of the AN-PBM architecture is to guarantee the quality of service for SPs and customers.

Service Providers. SPs needs are summarized as follows:

- Offer of differentiated and guaranteed services: bandwidth, delay, jitter and different service levels.
- Service management rather equipment configuration: dynamic and global view of the network, auto-adaptation to solve the problems, and fast and easy configuration of network equipment.

Customers. Customer needs are different from SP needs. Customer needs are focused on the Internet access, for what they have to prioritise critical applications and "privileged" users. Therefore, it is necessary to write dynamic policies granting different QoS levels according to applications and users.

3.2 Architecture

The AN-PBM architecture has two main components (figure 1):

- The Management Center takes on the SP sold SLA guarantee,
- The PE and the CPE, known as "PE/CPE" generic bloc. The CPE is the access router linking the customer to the SP core network. The PE binds a set of CPEs.

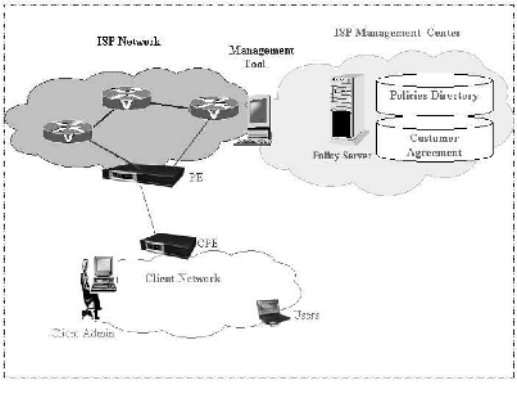

Fig. 1. AN-PBM Architecture (2)

Management Center. The Management Center is the component of the architecture related to the SP. The Management Center is responsible for the SLA negotiation, the generation of relevant policies and the application of these policies in the network devices (PE/CPE). The Management Center also allows to monitor and deploy SP services. The Management Center is a set of five modules:

- The Service Portal (SPo): the business interface between the service provider and the customers. The Service Portal provides the customers with a graphical SLA negotiation interface and a graphical service trade interface.
- The Customer Agreement Database (CAD): the database where are stored the SP-customer SLAs. The Customer Agreement Database security must be paid careful attention.
- The Policy Server (PS): the core of the Management Center. This module is the equivalent of the PDP in the IETF PEP/PDP architecture. The Policy Server is responsible for:
  - generating the set of SP policies that will be enforced in the network equipment to ensure the enforcement of the negotiated SLAs, the service levels, and to monitor the SP network.
  - enforcing the policies in equipment. If any problem occurs, the PS must take a decision to solve it.
  - monitoring the network by the way of reports periodically sent to the PS. The PS deduces a global view of the network and takes decisions when a problem occurs.
- Policy Database (PDB): the storage of the PS policies.
- Management Tool (MNT): used by the network administrator to manage the PS, the databases and the Service Portal.

PE/CPE. In the AN-PBM architecture, the PE/CPE is the equivalent of the PEP in the IETF architecture. However, the PE/CPE is more "intelligent" than a simple PEP since it gives possibility for the operator to customize policies and for the customer to insert its own policies for its own needs. The PE/CPE component plays the following roles:

- enforcement of the policies sent by the PS,
- translation of high-level policies in proprietary configurations,
- auto-adaptation according to the network state, reconfiguration or new PS policies solicitations,
- periodic delivery of monitoring information up to the PS.

Management Center $\rightleftharpoons$ PE/CPE communication. The Policy Server is the link between the Management Center and the PE/CPE. The communication between the Policy Server and the PE/CPE is achieved via 4 exchange types: provisioning (from PS to PE/CPE through a secured protocol), policy enforcement reports, monitoring information reports (periodically sent from PE/CPE to PS and stating what happens in the access network), and policy sollicitation (when an unknown behaviour occurs, the PE/CPE sends a request to the PS. The PS deals with the problem, takes the appropriate decisions and sends the relevant policies to the PE/CPE).

3.3 Policy Identification

Policies from the AN-PBM architecture are grouped in 2 families: Service Provider policies and Customer policies.

Service Provider policies. Service Provider policies constitute the set of SP requirements for guaranteeing the traded service levels. There are 3 subtypes of Service Provider policies:

- **Class Of Service policies (COS)**: COS policies point to the DiffServ class of service configuration parameters related to the SP-customer SLA. Among these parameters, the service type (EF, AF, BE), the marking (of the DSCP field of this class of service packets), the rate, the queuing algorithms (RED, TailDrop), the traffic in excess management algorithms (dropping, shaping, remarking), the queue sizes, and the allowed packet burst sizes.

- **Monitoring policies (MON)**: MON policies give a global view of the SP network and enable to make an automatic adaptation in the equipment configurations according to the network state. For instance, a SP may specify that when congestion occurs in an AF queue of one POP, the queue sizes for this POP should be increased about 20%.

- **Service policies (SRV)**: SRV policies materialize the added value a SP may offer to his customers. SRV policies allow service deployments, like a VoIP with admission control, a videoconference, or a dynamic VPN establishment. For example, for a VoIP with admission control service, the admission condition is chosen by the customer among a set of choices supplied by the provider, whereas the treatment to be done when the admission control condition is not reached is personalized by the customer.

Customer policies. Customer policies define a set of rules chosen by the customer administrator in order to carefully control the outgoing access of its network. Two subtypes of policies exist:

- **Flow policies (FLW)**: FLW policies group the classification rules for differentiating the applications and the users. For instance:
  - `if application==http then`
    `if user==CEO then marking AF1.1`
    `else marking BE`
  - web traffic is prohibited from twelve o'clock to 2pm

- **Customer Monitoring policies (CMP)**: CMP policies enable the modification of a CPE classification rule according to the network state. For example, the network administrator can specify that when congestion occurs in AF class of the customer access router, the ftp traffic has to go in the BE class.

3.4 Policy Implementation in 6WIND Equipment

The deployment and the storage of a policy differ depending on the policy family. SP policies are stored in the Management Center, performed by the PS and sent

to the PE/CPEs where they are enforced. Customer policies are stored in the CPE and translated into local classification rules.

Service Provider policies. The implementation of SP policies are detailed in this section.

– **COS policies**: the official document binding a customer and a service provider is a SLA, negotiated via the Portal Service where the offered service classes and their parameters are defined. From this SLA, the Policy Server obtains a set of COS policies that are enforced in the customer CPEs. As many COS policies are needed as there are service classes subscribed.

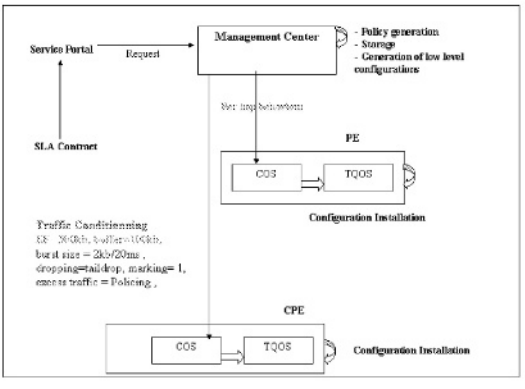

Fig. 2. COS Policies

Configurations are different between PE and CPE. A CPE is responsible for the classification and conditioning of the traffic (shaping, remarking). A CPE is then supplied with the detailed configurations of service classes, that is, with complex mechanisms like the shaping algorithm configuration parameters. A PE, connecting the customer CPE to the SP network, receives policies which contain the Per Hop Behaviour related to the customer service classes. The Policy Server generates 2 policies: one for the PE and one for the CPE. For a 6WINDGate CPE, a component called "COS" receives the policies and translates them into configuration parameters (figure 2). The Security (Setkey) and QoS (TQOS) APIs of the 6WINDGate services are then called.

– **MON policies**: When a problem occurs, the Policy Server generates some policies to modify the underlying CPE configurations. This mechanism is called network auto-adaptation. A component of the 6WINDGate, called "MON", receives these policies and translates them into low-level configurations (figure 3).

– **SRV policies**: SP value-added services representation is done thanks to these policies. In order to make the services independent of the customers, a service is a generic program written in Java. This program is stored in the Management Center, and may be completed for being in concordance with customer choices. The Java program is downloaded in the customer CPE. Each 6WINDGate owns a subscribed services database and an Execution Environment where the service program is performed when the use if the service by the customer is detected.

Customer policies. Thanks to the embedded configuration interface on the CPE, the customer network administrator is able to specify FLW and CMP policies at any time. These policies are not sent to the Policy Server since the Policy Server does not need to know the traffic travelling in the sold service classes, only in case a problem occurs when installing a policy.

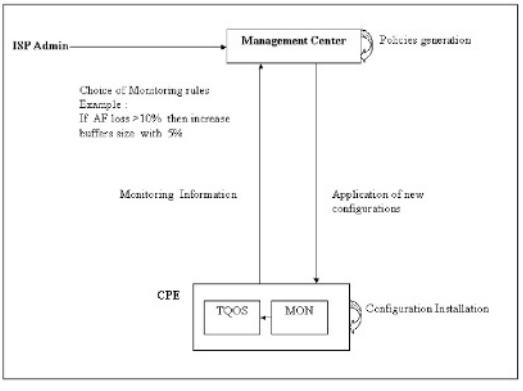

Fig. 3. MON Policies

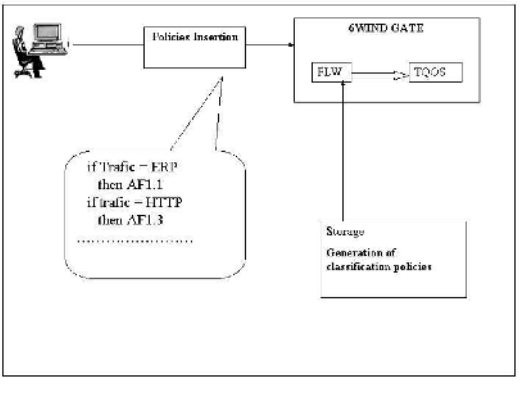

Fig. 4. FLW Policies

– **FLW policies**: the customer network administrator can make a differentiation between users and applications inside his network, in specifying the different QoS levels related to the flows. For example:

```
If User=Lambda and Traffic=beta
then mark flow with class X ..(1)
```

The administrator then insert in the rule the IP addresses and masks, as well as TCP and UDP ports used by the application. IP addresses may be specified statically or dynamically in alerting the CPE when the user connects to the network. A 6WINDGate component, called "FLW", is responsible for storing the FLW policies, generating the classification rules sent to the CPE QoS management module (figure 4).

– **CMP policies**: CMP policies allow to specify classification rules appropriate for network problems occurring during the lifetime of a service. The customer network administrator can give some privileges to critical applications and priorities to the users to provide different access qualities. A 6WINDGate component, called "CMP", is responsible for storing the CMP policies and generating the related new classification rules.

4 The VoIP with Admission Control Service

To illustrate the use of the AN-PBM architecture, we can use a service of VoIP with admission control. This service may be summarized as follows: if the access condition is true, then any new VoIP session is accepted. Else, any new session is rejected. The treatment performed when a session is accepted may be marking the relevant flow with the EF class DCSP value. The access condition is negotiated between the Service Provider and the customer when negotiating the service membership. For instance, an access condition could be that the EF class use rate must be less than 0.8, or could be that the session is accepted if it is initiated outside the working time. In the example, we consider that a new session is accepted if the number of ongoing sessions does not exceed 50. In the AN-PBM architecture, the deployment of such a service consists in the enforcement of a Service Policy (SRV) in the customer access router:

```
(VoIP Service)
If (AC Condition) then accept session
                  else reject session
```

Nevertheless, a customer may wish to control more carefully the service. Indeed, the CEO of the company will see his (her) VoIP session rejected if more than 50 employees are phoning. Such a scenario is unacceptable and compels the Service Provider to allow the company to define one or more further access conditions. The customer administrator can personalized the service in defining some Company Monitoring Policies (CMP).

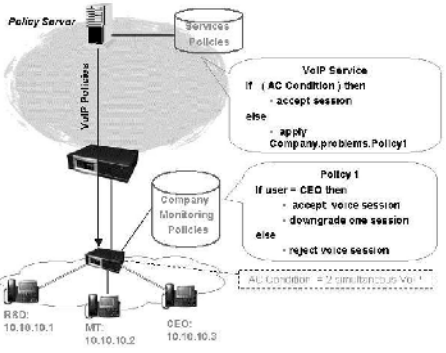

Fig. 5. Service Provisionning

```
(Company Monitoring Policy 1)
If user = CEO then accept session, downgrade one session
              else reject session
```

The Service Policy (SRV) deployed by the Service Provider becomes therefore:

```
(VoIP Service)
If (AC Condition ) then accept session
                   else company policy (Company Monitoring Policy 1)
```

Through this mechanism, the customer subscribes to a service on which he keeps a control level sufficient for solving his internal requirements. The Service Policy defined previously is sent by the Policy Server to the CPE (figure 5). This policy is then transformed into the CPE in a small program for generating suitable classification rules in the 6WINDGate Execution Environment.
Thus, any classification rule is added in the CPE classifier, but after a VoIP flow is detected, a Flow Policy (FLW) is automatically generated and the related

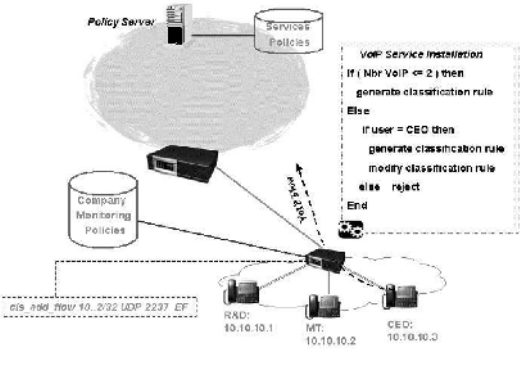

Fig. 6. Service Installation

classification rule is dynamically added in the CPE classifier (figure 6).
The service deployment is dynamic. However, it is necessary to bring a tool or a module in the AN-PBM architecture to be able to recognize the nature of the flow travelling through the customer CPE.
The AN-PBM is the warranty of easy service deployments and a good work of these services. Moreover, any information that the customer owns(like IP addresses of machines or staff first names) remains confidential. These data are only used while the classification rules are written and stored in a database of local variables. This database enables for instance the SP to provide a customer person - the CEO for example - with an appropriate service. For that, a variable called CEO in the provisioned Service Policy is used, and the exact value of this variable - the CEO computer IP address - is stored in the CPE database of local variables. The IP address is then used when writing the CPE classification rule. The AN-PBM architecture comes up to the Service Provider and customer expectations and ensures a high security level.

5 Conclusions

In this paper, the Access Network - Policy-Based Networking architecture, based on the IETF PEP/PDP architecture, has been overviewed. The lack of transition mechanisms in the IETF architecture, from the provider-customer signed agreement to the network level equipment configurations, led us to propose this architecture. The AN-PBM architecture allows Service Providers to offer value-added services and customers that buy these services to personalize them and gain control over their access network QoS. The Service Provider and customer administration areas are separated, that is why the AN-PBM architecture keeps a high security level. The AN-PBM architecture is under implementation and the testbed scenario is the VoIP with admission control application. This scenario brings up a use of policies from the Service Provider to deploy the service, and from the client to customize the service. A study is already led in order to extend the AN-PBM architecture to the mobility and security problems.

References

[DBC+00] David Durham, Jim Boyle, Ron Cohen, Shai Herzog, Raju Rajan, and Arun Sastry. The COPS Protocol. RFC 2748, January 2000.

[DMT] DMTF. *CIM Standard Schema*. http://www.dmtf.org/standards/standard_cim.php.

[DMT98] DMTF. *DEN initiative webpage*, 1998. http://www.dmtf.org/standards/standard_den.php.

[DMT99] DMTF. *Common Information Model (CIM), Specification, Version 2.2*, June 1999. www.dmtf.org/spec/cim_spec_v22.

[JRV01] J Jason, L Rafalow, and E Vyncke. Internet Draft: IPsec Configuration Policy Model. draft-ietf-policy-pcim-ext-08.txt, November 2001.

[Jud01] Michael Jude. Policy-Based Management: beyond the hype. *Business Communication Review*, pages 51–56, March 2001.

[Kos01] David Kosiur. *Understanding Policy-Based Networking*. Wiley Computer Publishing, 2001.

[MESW01] Bob Moore, Ed Ellesson, John Strassner, and Andrea Westerinen. Policy Core Information Model – Version 1 Specification. RFC 3060, February 2001.

[MRR+01] B Moore, L Rafalow, Y Ramberg, Y Snir, A Westerinen, R Chadha, M Brunner, R Cohen, and J Strassner. Internet Draft: Policy Core Information Model Extensions. draft-ietf-policy-pcim-ext-08.txt, November 2001.

[SRS+01] Y Snir, Y Ramberg, J Strassner, R Cohen, and B Moore. Internet Draft: Policy QoS Information Model. draft-ietf-policy-qos-info-model-04.txt, November 2001.

[WSH03] S Waldbusser, J Saperia, and T Hongal. Internet Draft: Policy Based Management MIB. draft-ietf-snmpconf-pm-13.txt, March 2003.

[YPG00] Raj Yavatkar, Dimitrios Pendarakis, and Roch Guerin. A Framework for Policy-Based Admission Control. RFC 2753, Informational, January 2000.