BELL LABS
TECHNICAL
JOURNAL

9

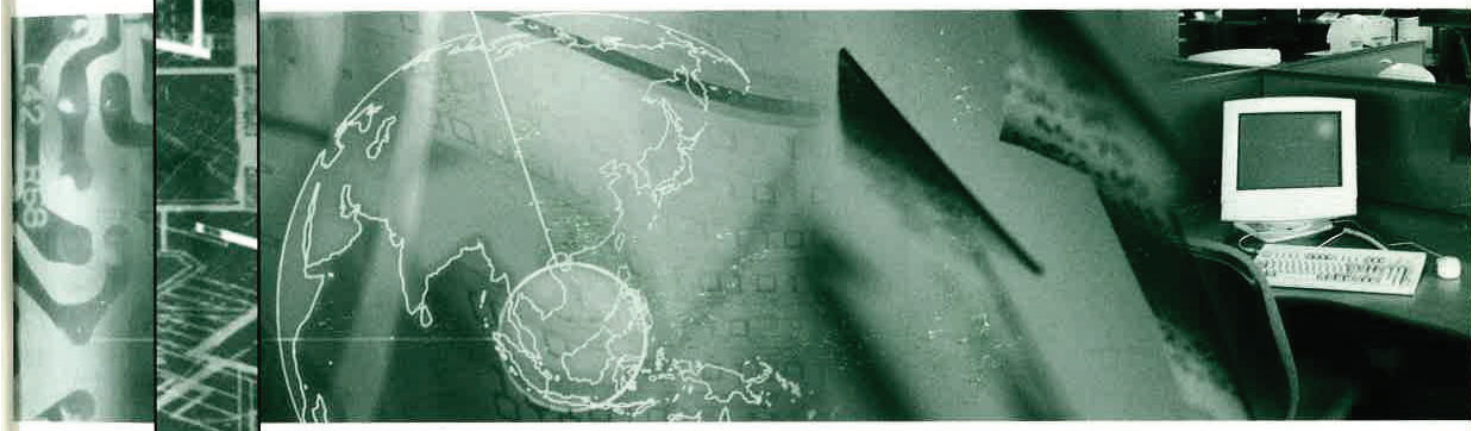
2004-05

INCOMPLETE

TK 5101
.A1 B12
Set 1

Lucent Technologies
Bell Labs Innovations

Bell Labs Technical Journal



General Papers

Volume 9, Number 1
2004

WILEY
Publishers Since 1807

The *Bell Labs Technical Journal* (Print ISSN: 1089-7089; Online ISSN: 1538-7305 at Wiley InterScience, *www.interscience.wiley.com*) is published quarterly, four issues per year, by Wiley Subscription Services, Inc., a Wiley Company, 111 River Street, Hoboken, NJ 07030-5774.

Subscription price (Volume 9, 2004): Print only: $240.00 in U.S.; $280.00 in Canada and Mexico; and $314.00 outside North America. Electronic only: $240.00 world wide. A combination price of $264.00 in U.S.; $304.00 in Canada and Mexico; and $338.00 outside North America. Personal rate: $110.00 in the U.S.; $134.00 in Canada, Mexico, and outside North America. All subscriptions containing a print element, shipped outside the U.S., will be sent by air. Payments must be made in U.S. dollars drawn on a U.S. bank. Claims for undelivered copies will be accepted only after the following issue has been received. Please enclose a copy of the mailing label. Missing copies will be supplied when losses have been sustained in transit and where reserve stock permits. Please allow four weeks for processing a change of address. Address subscription inquiries to Subscription Manager, Jossey-Bass, a Wiley Company, 989 Market Street, San Francisco, CA 94103-1741; Tel: 888-378-2537, 415-433-1740 (International); E-mail: jbsubs@jbp.com.

Postmaster: Send address changes to *Bell Labs Technical Journal*, Subscription Distribution U.S., c/o John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030-5774. Application to mail at the periodical rate is pending at Hoboken, NJ, and additional mailing offices.

Advertising Sales: Inquiries concerning advertising should be forwarded to Advertising Sales, c/o John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030-5774; Tel: 201-748-8832. Advertising Sales, European Contact: Jackie Sibley, c/o John Wiley & Sons, Ltd., The Atrium, Southern Gate, Chichester, West Sussex, UK, P019 8SQ; Tel: 44(0) 1243 770 351; Fax: 44(0) 1243 770 432; E-mail: adsales@wiley.co.uk.

Reprints: Reprint sales and inquiries should be directed to the Customer Service Dept., Attn: Gale Krouser, c/o John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030-5774; Tel: 201-748-8789; E-mail: gkrouser@wiley.com.

Manuscripts: The *Bell Labs Technical Journal* welcomes submissions by members of the Lucent Technologies technical community. The *Journal* issues calls for papers on selected theme issues through company communication vehicles. Persons with inquiries about submissions may contact the editor at: Frances A. Grimes, Editor-in-Chief, *Bell Labs Technical Journal*, Lucent Technologies, Room 2F-233, 600-700 Mountain Avenue, Murray Hill, NJ 07974; Tel: 908-582-8299; Fax: 908-582-1337; E-mail: fagrimes@lucent.com.

Other Correspondence should be addressed to *Bell Labs Technical Journal*, Publisher, Professional/Trade Group, c/o John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030-5774.

Bell Labs
Technical Journal
Volume 9, Number 1

Lucent Technologies
Bell Labs Innovations

◆ General Papers

Guest Editor: Kristin F. Kocan

May 2004

(continued)

♦ Policy-Based Network Management

Abdur Rahim Choudhary

Depending on the context, a policy can be a paper document, a table for selecting options, a sequence of logical assertions to automate operational decisions, or a tool to articulate business goals and service priorities and facilitate decisions in enforcing business rules and service priorities. In this paper, we will analyze these aspects of policies and show how they relate to each other. We will also analyze industry practices, examine applicable standards, and explore some advantages that a policy-based system can offer in such areas as network management, quality of service (QoS), and network security. © 2004 Lucent Technologies Inc.

Introduction

In its formulation, a policy-based approach [18] uses three basic constructs: policy events, policy actions, and policy rules.

Policy events represent the system states that are of interest in the context of the business objectives and their operational realization. Examples of a policy event include the occurrence of congestion in a router, the failure of a network node, the repeated failed attempts at logging on to a system, the occurrence of an emergency, the arrival of a call from a hot number, and the detection of a denial of service (DoS) attack.

Policy actions are the responses that an organization wishes to enforce in case one or more of the specified policy events actually take place. Examples of a policy action include rerouting traffic, switching on a backup system, suspending a user account, denying service to all calls except those related to an emergency operation, monitoring a call from and/or to a hot number, and disconnecting service to those clients suspected of causing a DoS attack.

Policy rules can be simply explained as the mechanisms to bind the policy events with the policy actions. However, this process can be fairly complicated, except for cases that represent simple operations. For example, a simple rule may detect that a router is experiencing congestion, but it may take a complex ensemble of rules to detect that a DoS has occurred. The rules to invoke a policy action may be similarly complicated. Even in a simple case when a router experiences congestion, the policy action may depend on a set of defined congestion alert levels and the policy rules may become somewhat complex for situations that fall in the middle of the defined alert levels. Further complications arise for the policy rules when the consequences of a false-positive or false-negative detection are considerable, or the consequences of an overreaction or underreaction to a policy event are crucial. For a detailed discussion of such factors, their impact on the policies, and an approach toward mitigation, see [8].

A policy-based approach to management can also allow the separation of the rules that govern the behavior of a system from the functionality provided by the system. Hence, policy-based management can make it possible to adapt the behavior of a system without the need to recode its functionality. Further, changes can be applied by changing policies without

Bell Labs Technical Journal 9(1), 19–29 (2004) © 2004 Lucent Technologies Inc. Published by Wiley Periodicals, Inc. Published online in Wiley InterScience (www.interscience.wiley.com). • DOI: 10.1002/bltj.20002

stopping the system or having to restart it. This aspect of policy-based management permits the system to adapt to the evolutionary changes in the system and to new application requirements [1].

In this paper, we first present a reference architecture for policy-based management that will also form the basis for further discussion. Next, we discuss the policy-based approaches to network management, quality of service (QoS), and network security. This discussion is in terms of industry practices, applicable standards, and ongoing research. We then describe the potential advantages that the policy-based approach can offer and, finally, we present conclusions.

Reference Architecture for Policy-Based Management

In this section, we present an architecture that supports the functionality and behavior described above for a policy-based approach to management.

Policy Reference Architecture

A simple but powerful architecture for the purpose of policy based systems was formulated [31] in the context of policy-based admission control management to enable QoS. The essence of this architecture is shown in **Figure 1**.

Policies are formulated by a human and introduced in to the policy-based system via the policy management module shown in Figure 1. The policy decision point (PDP) is the module where the policy expertise resides. The PDP uses a policy repository that contains the parameters and data structures that the PDP needs to evaluate the policy rules to make policy-based management decisions. The policy repository is often implemented as a directory that can communicate using lightweight directory access protocol (LDAP).

Each managed object supports a policy agent known as a policy enforcement point (PEP). A PEP is

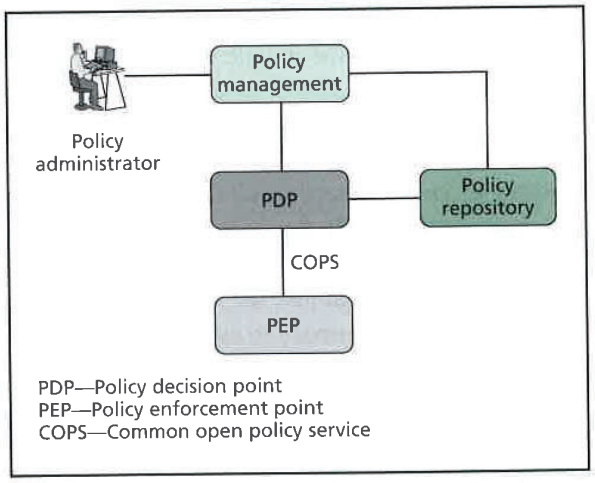


Figure 1.
Policy reference architecture.

Panel 1. Abbreviations, Acronyms, and Terms

ACL—access control list
CIDF—common intrusion detection framework
CLI—command line interface
COPS—common open policy service
DARPA—Defense Advanced Research Projects Agency
DiffServ—differentiated services
DoS—denial of service
FTP—file transfer protocol
IDWG—Intrusion Detection Exchange Format Working Group
IDXP—intrusion detection exchange protocol
IETF—Internet Engineering Task Force
IPSP—Internet protocol security policy
ITU-T—International Telecommunication Union, Telecommunication Standardization Sector
LDAP—lightweight directory access protocol
MIB—management information base
MSL—multiple security level
PCIM—Policy Core Information Model
PCIMe—PCIM extensions
PDP—policy decision point
PEP—policy enforcement point
PHB—per-hop behavior
PIB—policy information base
QoS—quality of service
QPIM—QoS Policy Information Model
RFC—request for comments
RSVP—resource reservation protocol
SNMP—simple network management protocol
VoIP—voice over Internet protocol
XML—Extensible Markup Language

designed and implemented for each managed object that the policy-based system is supposed to manage. An example of a managed object is a softswitch or one of its subsystems such as call control, call detail records, and low-level communications. The managed object does not have to be a physical entity such as a switch or a router. Software systems, subsystems, applications, and other entities can also be managed by the policy-based management system using appropriate PEPs. The PEP is a mechanism to abstract the managed object's operations and management characteristics using a general and preferably standard data model. The PEP communicates with the PDP using a standard protocol called common open policy service (COPS) [11].

An Example: Policy Management in the Lucent Softswitch

A somewhat modified version of this architecture was implemented as the policy-based management component of the Lucent Softswitch [21]. The architecture brings forth the generic components discussed above, as well as some details that are inevitable in the context of an implementation. **Figure 2** shows this policy-based management in the Lucent Softswitch. It also shows all the generic components of policy-based management, viz., the PDP, PEP, policy management, and policy repository (shown in this figure as policy information base [PIB]), as well as some additional details. In addition to the COPS interface, the figure also shows support

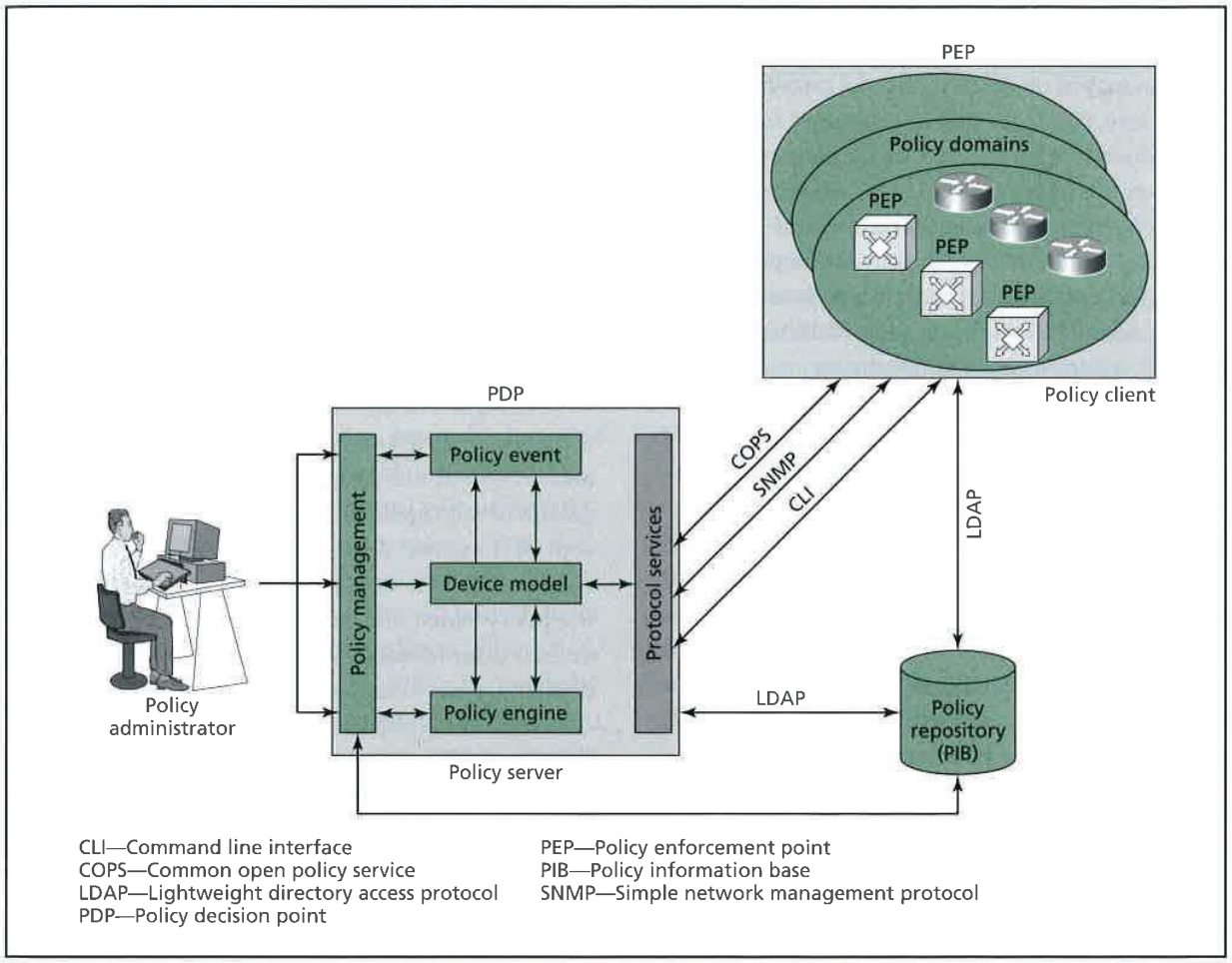


Figure 2.
Policy management in the Lucent Softswitch.

for simple network management protocol (SNMP). It is intended for cases where an SNMP agent is available for the managed object, and some PEPs are so designed that they can also serve as an SNMP agent. Other interfaces, such as a command line interface (CLI) or the file transfer protocol (FTP), are also often supported. The interface communicates the policy information, the policy decisions, and data sensed from the managed object.

The COPS protocol has been extended [6] to add mechanisms and conventions to facilitate policy provisioning.

The PDP makes decisions based on the policies it retrieves from a policy repository and perhaps other locations such as authentication servers. We also show some of the internal structure of this PDP. It contains the policy events that can be used to trigger information flow to and from the PEP, an abstracted model of the managed object in terms of a standardized data model (see [24, 25]) that can be used to formulate policy directives for the PEP, and a policy engine that evaluates the policy rules to make decisions. The policy management module can be implemented as part of the PDP, and a policy administration point is used as a management client with a graphical user interface. Further, the communication with the PEP uses a protocol service module to use the appropriate protocol when multiple protocols are supported.

To make policy decisions, the PDP performs the following functions: retrieving policy, interpreting policy, detecting policy conflicts, receiving interface messages, receiving policy decision requests from PEPs, receiving policy events (conditions) from PEPs, determining which policy is relevant, applying the policy, returning the results of policy application (possibly with other policy elements such as error information), sending policy elements to the PEP based on policy updates or requests from external entities, and receiving policy provisioning messages.

Figure 2 shows only one PDP. However, that is only for simplicity of representation. In reality, an organization can have multiple PDPs. These can often be organized hierarchically so that policy decisions can be defined and implemented at various levels of increasing abstraction starting from an organization's business goals to the configuration settings for an endpoint for the purpose of delivering a service. As an example, one could have a PDP for each domain shown in Figure 2. A PDP would serve its PEPs within the domain that it manages and, at the same time, the PDP could itself act as a managed object for the purpose of the PDP at a higher echelon within the hierarchy of PDPs.

The PEP enforces the PDP decisions and communicates the local events to the PDP. The PEP applies actions according to PDP decisions based on relevant policies and current network conditions. These conditions may be static, such as source and destination addresses or ports, and/or dynamic, such as current bandwidth availability or date and time.

Hierarchical Policy Organizations

The above description of the architecture does not indicate how the managed objects can be organized, how the policies can be mapped onto the managed objects, and how a combination of policies can be used to manage an object. These issues are addressed in the ITU-T recommendation "Management Domain and Management Policy Management Function" [17]. It provides a model for the behavior of the policy without defining the nature of any interactions that result in the use of the management domain and policy function.

For logistic or other management reasons, there is a requirement to modularize management activities and groups of managed objects. The need to define groups of managed objects is associated with the concept of domains. A domain-managed object allows the specification of a set of objects of interest from the policy-based management point of view. A policy defines a set of management activities that apply to domains, encapsulating any rules and rule combination semantics used to construct that policy.

For management domains, there is the requirement that it be possible to determine which management policies apply to the domain. For this purpose, we introduce the concept of a jurisdiction, which is a managed object that represents the relationship between a policy and a domain to which the policy is applied. The relationship defined by a jurisdiction indicates to which managed objects, identified by the

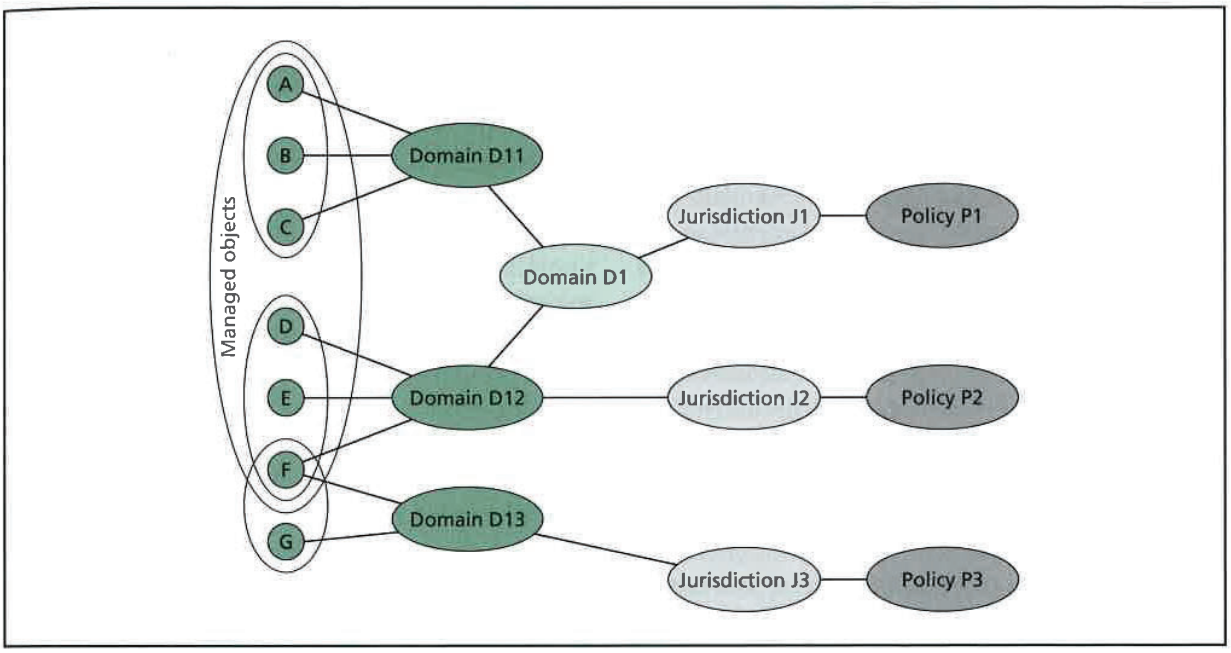


Figure 3.
Domain hierarchy and application of policies to managed objects.

domain, the policy applies. Determining which policies apply to the membership of a domain requires retrieving the attribute that names its policy from all jurisdictions that directly or indirectly reference the domain in question.

Figure 3 shows how the application of policies to the management objects takes place via the jurisdictions applied to a hierarchy of domains.

Jurisdiction J1 associates policy P1 with domain D1. This means that policy P1 applies to objects A, B, C, D, E, F, the members specified directly or indirectly by D1.

Jurisdiction J2 associates policy P2 with domain D12. This means that policy P2 applies to objects D, E, and F, the members specified directly or indirectly by D12. Thus, both policies, P1 and P2, are applicable to objects D, E, and F. Therefore, a change to domain D12, e.g., changing the membership of the domain, can affect the applicability of both policy P1 and P2. Jurisdiction J3 associates policy P3 with domain D13. Objects F and G are subject to policy P3. Object F is also subject to policy P1 and to P2.

To summarize, Figure 3 illustrates the hierarchical domains for administrative convenience, e.g., the domains D11 and D12 may be administered separately. It also illustrates the reuse of a domain for multiple jurisdictions, e.g., the domain D12 is used for both jurisdiction J1 and jurisdiction J2. Finally, Figure 3 demonstrates the application of multiple policies to a single object, e.g., object F is subject to policies P1, P2, and P3.

The Parlay Group [26] has defined standard APIs [13] to enable handling the domains, the managed objects within the domains, and the jurisdiction relationship that shows which policies apply to which managed objects. In particular, the jurisdiction relationship is realized by explicitly "associating" a set of policies with a domain or with a sub-entity referred to as a "group" in the Parlay API.

Policy-Based Network and Services Management

Network management is one of the first areas to which the policy-based approach has been applied. The policy-based implementations within the industry are mostly the cases of simple policies. These include the cases of simple events, rules, and actions such as a tabular description of decisions that allow or

drop the traffic that corresponds to certain ports, certain addresses, or certain protocols. Many policy-based management schemes that currently exist in the market for the firewalls and routers can fall under such a simple table-based approach. This is because the current state of network management is essentially the management of individual network elements, so the simple cases of policy-based network management merely seek to configure the individual devices. However, the real value of the policy-based approach to network management is to achieve business objectives by managing services that require the network as a whole to have a desired overall behavior. In this sense, managing the services such as QoS or security is a different challenge from conventional network management [2].

One of the first industry products in which the policy-based management approach and a standard architecture were implemented was the policy-based IP network monitoring system from Lucent Technologies [23]. The product is also called NetMon. It is included as the management module within the Lucent Softswitch. The architecture shown in Figure 2 describes this product. Such products are a good starting point for a more general policy management solution, deploying policies that are dynamic and enable real-time network management decisions for network reconfiguration.

The policy information base (PIB) shown in Figure 2 is a repository for the policy data. It is not much different from a management information base (MIB) that is used for network management using SNMP management framework [5]. Both PIBs and MIBs make it possible for vendors to add proprietary information. A proliferation of PIBs, just like a proliferation of MIBs, is likely to complicate the management function for large heterogeneous networks—e.g., the scripts in a network management system can breakdown, not only when a similar product by a different vendor is used, but also when a different version of the same product is introduced, and this can cause problems with scalability, flexibility, and evolvability.

In an attempt to mitigate this situation, the Policy Framework Working Group of the Internet Engineering Task Force (IETF) has defined a Policy Core Information Model (PCIM) [24] and extensions to it (PCIMe) [25]. A framework PIB has also been defined [27] as a common component of all PIBs. As many policy-based management systems of today use a directory for policy repository, the IETF has invested some effort in mapping the information model to LDAP schemas [30]. However, these efforts seem to address the traditional network management problem in terms of the management of the individual network elements, while the more sophisticated policy-based approach for service management continues to pose a challenge.

Policy-Based QoS

Initiatives such as voice over Internet protocol (VoIP) have helped highlight the importance of the QoS [14]. To apply the policy framework to the QoS domain, the Policy Framework Working Group has extended the PCIM for the QoS domain (QPIM) [28]. A Lucent product called RealNet Rules [29] is a good example of industry implementation.

The IETF has devised two schemes for QoS in the IP networks, the differentiated services (DiffServ) approach [3] and the integrated services approach with resource reservation protocol (RSVP) [4]. Both approaches readily benefit from a policy-based management.

The DiffServ approach works via the use of the DiffServ byte in the IP header. Six most significant bits of this byte are used for marking the traffic with DiffServ code points that correspond to a per-hop behavior (PHB). The two least significant bits are used for explicit congestion notification. The marking of the DiffServ bits for a desired PHB needs "classification" policies; the treatment of the packets with a particular PHB needs policies to allocate resources for this segment of the traffic; handling and shaping of traffic needs policies for those packets that exceed the envelope of a service-level agreement profile; and such DiffServ functions as traffic conditioning (e.g., via remarking the DiffServ byte) also need policies. A PIB has been defined [7] to facilitate the implementation of DiffServ policies.

The RSVP explicitly includes policy data objects in its messages. Policy data may include user authentication and user authorization credentials, billing

information, and service privileges. These require policies for security, billing, service accessibility, and access criteria. The RSVP messages also contain the flow descriptor data, with the flow-spec data and the filter-spec data. The flow-spec data describe the QoS needed for the reservation, and the filter-spec data describe the data flow that must receive the specified QoS. Clearly, policies are needed for provisioning the requested QoS and for treating the specified data flows according to the given QoS description. A set of extensions to RSVP has been specified [15] to facilitate policy-based controls.

Policy-Based Security

The approach at the IETF defines a policy framework as is documented in [25, 30], and other related documents, and further applications of the policy framework are envisioned to be done under the appropriate working groups in the appropriate areas. The application to IP security is the charter of the IP Security Policy (IPSP) Working Group [20] established for the purpose within the security area of the IETF. The group has formulated the requirements, an information model, and a PIB for IP security policies. These documents are still Internet drafts at the time of this writing.

The architecture shown in Figure 1 is a general architecture for policy-based management and, in particular, it is valid for policy-based security management. The communication of the security information between the PEP and the PDP may be able to use an evolving standard at the Intrusion Detection Exchange Format Working Group (IDWG) [19] of the IETF. The purpose of the IDWG is to define data formats and exchange procedures for sharing information of interest to intrusion detection and response systems and to the management systems that may need to interact with them. The working group has produced the requirements, the intrusion detection exchange protocol (IDXP), and a data model using Extensible Markup Language (XML). These results are documented as Internet drafts, though they are sufficiently stable, waiting to be issued as RFCs after review and approval. This work was originated at the Defense Advanced Research Projects Agency (DARPA) under the project Common Intrusion Detection Framework (CIDF) [10].

Multiple security level (MSL) is one area that has challenged the industry and the research community. For the present purpose, it means that an organization may have multiple levels of classification of security, depending upon the nature of the assets that need to be protected and the type of users who need to access those assets in multiple capacities. There are multiple levels of protection that are used to secure those assets, each level of protection potentially using different security technologies and procedures. There are strict rules for the information flows between these classified levels and for providing the users authorization to access the classified assets. These rules must be strictly observed because the cost of violation of these rules can be significant for national security and for critical infrastructure protection programs [9].

The MSL problem can be a good challenge for the policy-based management approach. Of course, the policies will have to do a lot better than the table-based representation that is currently dominant in the industry and also better than the directory-based schemas that seem to be the current emphasis for the standards activity in the IETF. Below, we use the MSL problem to explain the larger potential of policy-based management as well to as draw attention to some practical issues [8]:

- The PEPs shown in Figure 1 are the architectural elements that have two important functions. The first is to execute actions on the network element according to the directives received from the PDP. These actions form part of the policy actions. The second is to gather information on the events that occur in the network element. These events form part of the policy events. The richness of a policy framework is determined by the set of these events and actions, and it must suffice for the MSL requirements.
- The PDP is the heart of the policy decisions. It performs the desired analysis on the policy events that are obtained from the various PEPs, not only from the PEPs in the domain managed by the PDP but also from the PEPs in other domains via their PDPs. This analysis must be made

as extensive and as sophisticated as required by the MSL.

- The PDP examines the policy events that it receives from the PEPs to carry out logic to decide whether or not certain policy conditions have arisen. The logic within the policy rules must expand well beyond the *if-then* type of simple logic that is afforded by the table-based policies. This logic must now be expressed using full-fledged programs to evaluate the complicated MSL rules. Further, certain rules may not be expressible in terms of statistical and correlative metrics and simple logic. In such cases, artificial intelligence techniques such as intelligent agents, pattern matching, and fuzzy logic may be needed. These techniques are also very relevant in mitigating the problem of false positive and false negative detections, as well as the problem of overreaction and underreaction in responding to the detected conditions.
- Policy decisions may be dependent on the context in which the policy events are observed, and the security metrics [8] are computed. Hence, a formalism is needed to specify context. A prioritization scheme based on this context is also needed. An obvious example of the need for such a prioritization scheme is provided by the situation in which a human is in the loop for making policy decisions or for executing policy actions. Thus, high priority can be assigned to the most serious violations of the policy and the most urgent policy actions. In [8], an architectural solution that embodies the context and a context-based service priority is provided.
- The standards activities need to keep pace with the above requirements and the industry needs to remain sufficiently motivated to implement them.

To summarize, the policy events are collected from the network elements; these events are analyzed into management metrics; the events and the metrics are used to model the behavior of interest, e.g., the occurrence of congestion; the policies are defined using the events, metrics, and behavior models; the policy-based management system is used to predict or at least to detect the policy violations and to respond to them using the policy actions that are performed on the network elements.

Promise of Policy-Based Management

As explained earlier, the true promise of the policy-based approach to management lies in its value as a decision support tool and in its ability to support decision-making in real time, as well as to respond to the changes in the context of the operations. The work in the industry and at the standards forums has not yet realized that potential [12].

Current State

The industry has largely addressed the case of simple policies, such as those that can be addressed via a tabular description of ACLs. These cases may be described as a table-based or an ACL-based approach to management, with simple *if-then* type policy rules and a limited set of policy conditions and policy actions. The policy conditions and policy actions are few and only the vendor can introduce new ones. Further, the rules in these simple cases are not procedures, so only the very simplest policies can be expressed.

The IETF seems to have accepted LDAP directories as the policy repository mechanism, as can be seen from the emphasis it places on defining LDAP schemas. Directories are not like databases and lack many desirable features such as the referential integrity, the atomicity of transactions, notification service, real-time dynamic changes to the directory content, and fast retrieval for real-time policy decisions, to name a few.

The conventional operations, administration, maintenance, and provisioning systems are slow response systems with infrequent updates to their information bases, and a significant part of configuration changes and provisioning is done manually. The directory-enabled network allowed a logically central information base so that the network nodes could pull their configuration data from it. This allowed a central administration approach so that changing the configuration data in the central repository could change the configuration of the network elements. Currently, the industry and the IETF tend to view

policy-based management as a progression in the same direction.

Challenge of Service Management

The departure comes when one performs service management [22] versus network element management. Some services, such as virtual private networks, can still be handled under the traditional paradigm described above because rapid changes and dynamic responses in real time are not needed. In services such as QoS, the parameters such as delay, jitter, and loss need to be kept within prescribed bonds irrespective of the unpredictable changes in traffic patterns. The QoS and security services are examples of services that require the network as a whole to exhibit a desired aggregate behavior.

One challenge is in the description of the policies themselves. Policies must be unambiguous, verifiable, resolving to a single decision, and consistent across domain boundaries. One approach [16] is to specify global policy rules and decompose them into local policy rules using clear methodologies that incorporate constraints of interacting and collaborating network elements.

Another challenge is to make policy decisions dynamically respond to context information (i.e., the dynamic part of the business environment), as well as to changes in the context information due to ongoing operations [8].

Security service can be challenging, as described above, for the MSL service. However, not all security requirements pose the same challenge. Thus, the authentication, authorization, privacy, integrity, and non-repudiation requirements do not generally require very complicated policies nor do the policies change dynamically in real time. However, the requirement of intrusion management, in general, can pose serious challenges. Intrusion management service (not just an intrusion detection system) is one area where policy-based management is needed. A policy-based management system can accommodate complex and context-based analysis of the observed events using sophisticated and intelligent algorithms to predict and detect the intrusions, and offer reliable and possibly automated responses to them.

Conclusions

Most policy-based management systems available in the market today are more accurately described as table-based systems. Much work is ongoing at the IETF for policy-based management of networks, QoS, and security, though it tends to view the policy-based management as an extension of the directory-enabled networks with LDAP schemas. It focuses more on the network elements rather than the aggregate behavior of the network as a whole within the context of delivering a service. However, the policy-based approach to management has great potential not only in managing simple services such as the network element configuration and virtual private networks, but also in managing complex services such as a multi-level security service and an intrusion management service. Much research is still needed to realize its full potential.

Acknowledgments

I am thankful to my colleagues for many illuminating discussions.

References

[1] A. K. Bandara, E. C. Lupu, and A. Russo, "Using Event Calculus to Formalize Policy Specification and Analysis," IEEE 4th Internat. Workshop on Policies for Distributed Systems and Networks (Policy 2003), (Lake Como, Ital., 2003), pp. 26, <http://csdl.computer.org/comp/proceedings/policy/2003/1839/00/18390026abs.htm>.

[2] R. T. Banke, T. K. Lybarger, and M. L. Patton, "Service Assurance for Converged Networks," Bell Labs Tech. J., 7:1 (2002), 99–114.

[3] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, and W. Weiss, "An Architecture for Differentiated Services," IETF RFC 2475, Dec. 1998, <http://www.ietf.cnri.reston.va.us/rfc/rfc2475.txt?number=2475>.

[4] R. Braden, L. Zhang, S. Berson, S. Herzog, and S. Jamin, "Resource ReSerVation Protocol (RSVP)," V1, IETF RFC 2205, Sept. 1997, <http://www.ietf.cnri.reston.va.us/rfc/rfc2205.txt?number=2205>.

[5] J. Case, R. Mundy, D. Partain, and B. Stewart, "Introduction to Version 3 of the Internet Standard Network Management Framework," IETF RFC 2570, Apr. 1999, <http://www.ietf.cnri.reston.va.us/rfc/rfc2570.txt?number=2570>.

[6] K. Chan, J. Seligson, D. Durham, S. Gai, K. McCloghrie, S. Herzog, F. Reichmeyer, R. Yavatkar, and A. Smith, COPS Usage for Policy Provisioning (COPS-PR), IETF RFC 3084, Mar. 2001, <http://www.ietf.cnri.reston.va.us/rfc/rfc3084.txt?number=3084>.

[7] K. Chan, R. Sahita, S. Hahn, and K. McCloghrie, "Differentiated Services Quality of Service Policy Information Base," IETF RFC 3317, Mar. 2003, <http://www.ietf.cnri.reston.va.us/rfc/rfc3317.txt?number=3317>.

[8] A. R. Choudhary, "Service Intelligence Through Agile Information Controls," Bell Labs Tech. J., 8:4 (2003), 61–70.

[9] W. J. Clinton, Report of the President of the United States on the Status of Federal Critical Infrastructure Protection Activities, Jan. 2001.

[10] Common Intrusion Detection Framework, Sept. 1999, <http://www.isi.edu/gost/cidf/>.

[11] D. Durham, J. Boyle, R. Cohen, S. Herzog, R. Rajan, and A. Sastry, "The COPS (Common Open Policy Service) Protocol," IETF RFC 2748, Jan. 2000, <http://www.ietf.cnri.reston.va.us/rfc/rfc2748.txt?number=2748>.

[12] M. Eder, H. Chaskar, and S. Nag, "Considerations from the Service Management Research Group (SMRG) on Quality of Service (QoS) in the IP Network," IETF RFC 3387, Sept. 2002, <http://www.ietf.cnri.reston.va.us/rfc/rfc3387.txt?number=3387>.

[13] European Telecommunications Standards Institute, "Open Service Access (OSA); Application Programming Interface (API); Part 13: Policy Management SCF," ETSI ES 202 916-13 v1.1.1 (2003-01), <http://portal.etsi.org/Portal_Common/home.asp>.

[14] S. Garg and M. Kappes, "Can I Add a VoIP Call?," IEEE Internat. Conf. on Commun., (Anchorage, AK, 2003), <http://ieeexplore.ieee.org/xpl/RecentCon.jsp?puNumber=8564>.

[15] S. Herzog, "RSVP Extensions for Policy Control," IETF RFC 2750, Jan. 2000, <http://www.ietf.cnri.reston.va.us/rfc/rfc2750.txt?number=2750>.

[16] R. Hull, B. Kumar, and D. Lieuwen, "Towards Federated Policy Management," IEEE 4th Internat. Workshop on Policies for Distributed Systems and Networks (Policy 2003), (Lake Como, Ital., 2003), pp. 183, <http://csdl.computer.org/comp/proceedings/policy/2003/1839/00/18390183abs.htm>.

[17] International Telecommunications Union, Telecommunications, Information Technology—Open Systems Interconnection—Systems Management: Management Domain and Management Policy Management Function, ITU-T Rec. X.749, Aug. 1997, <http://www.itu.int/ITU-T/publications/index.html>.

[18] Internet Engineering Task Force, Policy Framework (policy), Dec. 2002, <http://www.ietf.org/html.charters/policy-charter.html>.

[19] Internet Engineering Task Force, Intrusion Detection Exchange Format (idwg), Oct. 2003, <http://www.ietf.org/html.charters/idwg-charter.html>.

[20] Internet Engineering Task Force, IP Security Policy (ipsp), Oct. 2003, <http://www.ietf.org/html.charters/ipsp-charter.html>.

[21] R. A. Lakshmi-Ratan, "The Lucent Technologies Softswitch—Realizing the Promise of Convergence," Bell Labs Tech. J., 4:2 (1999), 174–195.

[22] L. Lymberopoulos, E. Lupu, and M. Sloman, "An Adaptive Policy Based Framework for Network Services Management," Proc. IEEE 3rd Internat. Workshop on Policies for Distributed Systems and Networks (Policy 2002), (Monterey, CA, 2002), pp. 147–158, <http://www.doc.ic.ac.uk/~mss/Papers/Policy2002.pdf>.

[23] D. Mitra, K. E. Sahin, R. Sethi, and A. Silberschatz, "New Directions in Services Management," Bell Labs Tech. J., 5:1 (2000), 17–34.

[24] B. Moore, E. Ellesson, J. Strassner, and A. Westerinen, Policy Core Information Model—Version 1 Specification, IETF RFC 3060, Feb. 2001, <http://www.ietf.cnri.reston.va.us/rfc/rfc3060.txt?number=3060>.

[25] B. Moore, Policy Core Information Model (PCIM) Extensions, IETF RFC 3460, Jan. 2003, <http://www.ietf.cnri.reston.va.us/rfc/rfc3460.txt?number=3460>.

[26] Parlay Group, <http://www.parlay.org/specs/index.asp>.

[27] R. Sahita, S. Hahn, K. Chan, and K. McCloghrie, "Framework Policy Information Base," IETF RFC 3318, Mar. 2003, <http://www.ietf.cnri.reston.va.us/rfc/rfc3318.txt?number=3318>.
[28] Y. Snir, Y. Ramberg, J. Strassner, R. Cohen, and B. Moore, "Policy QoS Information Model," IETF Internet Draft, May 2003, <draft-ietf-policy-qos-info-model-05.txt>.
[29] M. L. Stevens and W. J. Weiss, "Policy-Based Management for IP Networks," Bell Labs Tech. J., 4:4 (1999), 75–94.
[30] J. Strassner, B. Moore, R. Moats, and E. Ellesson, "Policy Core LDAP Schema," IETF Internet Draft, Oct. 2002, <draft-ietf-policy-core-schema-16.txt>.
[31] R. Yavatkar, D. Pendarakis, and R. Guerin, "A Framework for Policy-based Admission Control," IETF RFC 2753, Jan 2000, <http://www.ietf.cnri.reston.va.us/rfc/rfc2753.txt?number=2753>.

(Manuscript approved January 2004)

ABDUR RAHIM CHOUDHARY was formerly a member of technical staff in the Government Communications Laboratory of the Advanced Technologies Program at Bell Labs in Whippany, New Jersey. He was involved in researching the specification of the business and operational context such that the context can change dynamically and can help prioritize the business and operational activities. He holds a Ph.D. in physics from Queen Mary College at the University of London in the United Kingdom. Dr. Choudhary's research interests include end-to-end network security and information assurance, quality of service, voice over Internet protocol (VoIP), and reusable cross-product reference architectures. ◆