UDC 621.395.74:681.32

Policy-based Management for Enterprise and Carrier IP Networking

●Takeo Hamada ●Peter Czezowski ●Takafumi Chujo

(Manuscript received September 15, 2000)

Policy-Based Management (PBM) will play a key role as a management technology for end-to-end IP-nized integration of enterprise networks and telecommunication networks. In this paper, we examine PBM and its requirements for managing the new telecommunication network service environment, and propose a scalable new PBM architecture based on relevant research at Fujitsu Laboratories of America. A new development in PBM, called active policy, is illustrated. We expect that the active policy will bring new insights on the integration of PBM and intelligent agent systems, benefiting service management and customer care in the new network service environment.

1. Introduction

The Internet has given rise to explosive growth of communication demand. The Internet traffic doubling period of 90 days, also known as Gilder's law,[1)] is a clear indication of its huge impact on our society for years to come. In last 5 years, a new generation of equipment vendors and carriers has emerged, responding to insatiable bandwidth demand of the Internet users. The Internet has brought a new paradigm of communication and networked services, and it has also brought a set of new IP-based technologies, new technical standards, and new business styles.

Telecommunication is, in contrast to the Internet, a much more mature technology. Since Graham Bell's invention in 1876, the basic service paradigm of PSTN (Public Switch Telephone Network) has changed little: a network optimized for human voice communication. Over the long years, the telecommunication has served as one of the most important pieces of social infrastructure, responding to the high demand on its reliability and universal availability.

The two network paradigms are based on different views of network design and its operation, resulting in different approaches toward network management. Predictable dominance of the Internet in the data traffic and network service spheres, however, has put the two paradigms in a collision course, and it seems clear that a new network management paradigm must be born out of this cultural collision. We at Fujitsu Laboratories of America have been engaged in research to bring forth the vision of the new network management paradigm into reality. In particular, we believe that Policy-Based Management (PBM) is at the center of this new paradigm.

2. Network management for the new network service paradigm

Encounter between the two paradigms has been one of the driving forces behind several important technical developments in late 1990s; Voice over IP, and NGN (Next Generation Network), to name a few. The same is true for network management, whose aim is to achieve high reliability and accountability of network operations and services through the use of NMS (Network

Management System). In the early stages of the Internet, there was fairly clear separation between the Internet and the telecommunication, both in terms of technologies and management responsibilities. The majority of traffic was still voice, and the telecommunication network provided WAN infrastructure, upon which the Internet was built as an overlay.

With the growth of the Internet, the volume of data traffic surpassed that of voice traffic, and it has become common to build an all IP-based backbone network, which is overlaid directly on SONET or WDM (Wavelength Division Multiplexing). The Internet is quickly becoming an essential public network infrastructure, replacing some of the roles of the telecommunication network. In other words, these two networking paradigms – Internet and telecommunication network – will merge into a new telecommunication infrastructure.

Moridera et al.[2] suggests that the future telecommunication service environment will look like a virtual network server, which consists of a set of application specific servers running on IP-based application protocols interconnected by a high-speed all optical network. The virtual server provides access to actual servers and service/network management support (**Figure 1**). In this new paradigm, network/service management itself is a service, provided by a set of specialized servers. Though it resembles the Internet, this new telecommunication must provide the good characteristics as found in today's telecommunication network, i.e. high reliability and universal availability.

Network management is one of the key technologies needed to fulfill the above requirements. In other words, a new paradigm for network management is also needed, in order to address the requirements arising both from the Internet side and the telecommunication side of the new telecommunication infrastructure. In particular, the new network management paradigm will incorporate the Internet management framework consisting of related IETF (Internet Engineering Task Force) standards, along with the telecommunication management framework, notably TMN (Telecommunication Management Network) standards from ITU-T. The challenge of the new paradigm is to cast the two existing management frameworks into a new, unified framework, capable of end-to-end management of both data and multimedia traffic.

3. Policy-Based Management

Policy-Based Management (PBM) has attracted significant attention both from the industry and the academic research community in recent years, as it has been recognized that PBM can effectively provide a good means to solve the puzzle of integrated IP/telecom management. Early works on PBM include Sloman[3] and others in early 1990s. Inspired by DEN (Directory Enabled Network)[4] initiative by Cisco and Microsoft, works on PBM followed in IETF Policy WG and DMTF, forming a strong technical trend in the IP networking community. Although the center of PBM activities is in IP networking, PBM can be applied to wide range of control and management issues both in IP networks and telecommunica-

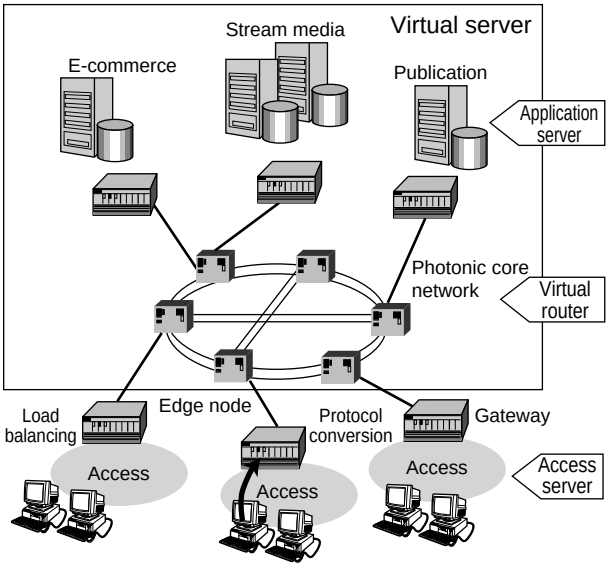

Figure 1
New network service environment.

tion networks.

Figure 2 illustrates the IETF standard PBM architecture.[5] The figure illustrates realization of the standard architecture in typical IP management environment as offered by Fujitsu SystemWalker. The architecture is designed in such a way that high-level management knowledge is captured by policy rules, which are stored in a policy repository, known also as directory server. In general, the policy rules have the following form.

IF *policy_activation_codition* THEN *policy_action*

The policy activation condition describes the condition when the following policy action is to be activated. For example, monitoring events, which report network state, node state, or traffic type at ingress router, can trigger a policy action resulting in provisioning of the network resources. Once these policies are defined and deployed at the policy-server (PDP, Policy-Decision Point), they are further translated and downloaded to corresponding network devices (PEP, Policy-Enforcement Point) to put the policies in effect. This interaction between PDP and PEP works in the opposite direction also. For example, a piece of policy is uploaded from PEP to PDP, so that the PEP requests a policy decision made by the PDP. In IETF, protocols for the standard reference model have been standardized: LDAP (Light-weight Directory Access Protocol) for the communication between the policy-repository (LDAP server) and PDP, and COPS (Common Open Policy Service) for the communication between PDP and PEP.

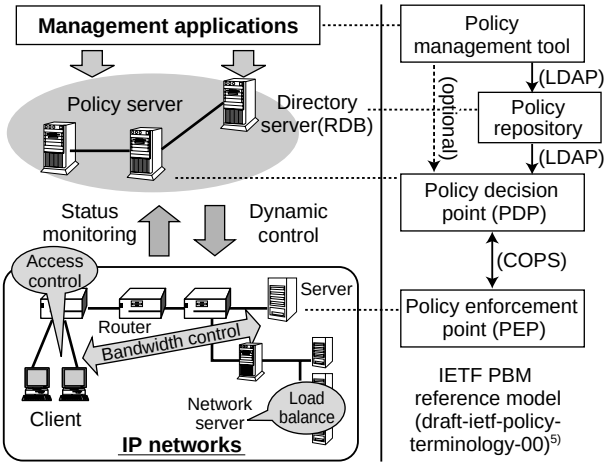

Figure 2
Policy-based management architecture.

A major motivation for developing IETF standard PBM has been to give remedy to SNMP (Simple Network Management Protocol)-based management framework, whose usage has been limited primarily to monitoring. In a historical perspective, this is a result of rapid deployment and technical maturity of IP network, to which IP management technology needed time to catch up. We think the following technical characteristics of PBM are particularly noteworthy from the standpoint of the integrated IP/telecom network management.

Built-in network intelligence: through its information model and policy rules, PBM provides richer context for more intelligent operation and management for increasingly complex IP network than what is available in IP networks today. In a crude sense, each policy rule can be seen as a fragment of a distributed intelligent information system, of which expert knowledge is solely focused on IP network operation and management.

The above feature has been emphasized as one of the advantages of PBM, in particular in the original DEN proposal. From our point of view of the integrated IP/telecom network management, we believe that the following three features will be important for the future development of PBM.

Integration of control and management: the same information model, called PIB (Policy-Information Base), enables more effective integration of network control and management. Although current PIBs available in IETF standards are mostly device-specific, control architecture specific models, the semantics implied by the PIB can be made into a set of information model for integrated control and

management of network and service management, when the model is extended as it is exemplified in DMTF CIM (Common Information Model).

For example, network control addresses issues such as MPLS (MultiProtocol Label Switching) signaling, connection admission, and congestion control at nodes, which all involve real-time processing at network elements. Network management, on the other hand, addresses issues such as monitoring and accounting of established MPLS connections, whose focus has been more on maintaining functions of network resources once communication path is established by network control. PBM connects these two phases of network operation in a unique manner, in such a way that policies, which are installed by network management using PDP-PEP model, dictate the behavior of network control. For example, a congestion control policy describes how a node handles packets when congestion occurs. In other words, through policies, network management can directly or indirectly affect the way network control is done in the network.

PBM is also called PBN (Policy-Based Networking) when its network control aspects are more emphasized. PBN allows the network operator to work on IP network operation issues at a higher, service-focused level, rather than at a device-specific level, leaving details on the control parameters to the relevant policy-rules.[note 1)]

Management function layers: the same mechanism can be utilized to provide management function layers as they are defined in TMN (Telecommunication Management Network) model. The TMN functional layers provide levels of abstraction for network operation and management, from network devices up to network services.

Protocol-independent information model: Although PIB is not protocol independent in most of its current usage and its syntax closely follows SMI, which was originally developed for SMNP MIB, the information model represented by the PIB can be made protocol independent, when its usage is extended. For example, IETF standard protocol for policy service, i.e. COPS, does not enforce any structural constraints on its contents, allowing the PIB fragment to be carried from a policy server to a network device, and to be interpreted free of SNMP or other protocols with structural constraints. In other words, the information model and policy expressions can be made independent of protocols by which they are carried.

Figure 3 illustrates the two network management paradigms, namely the Internet and the TMN-based telecommunication, are illustrated. The Internet is primarily date centric, and is characterized by simple and easy provisioning, while it offers less or no service management in comparison with telecommunication networks. Telecommunication networks are characterized by high reliability and clear layering in the management architecture, while offering more comprehensive service management scheme, which includes more complete coverage of FCAPS (Fault, Configuration, Accounting, Performance, Security) and usage-based billing.

The two seemingly different approaches can be unified, in such a way that they are bridged

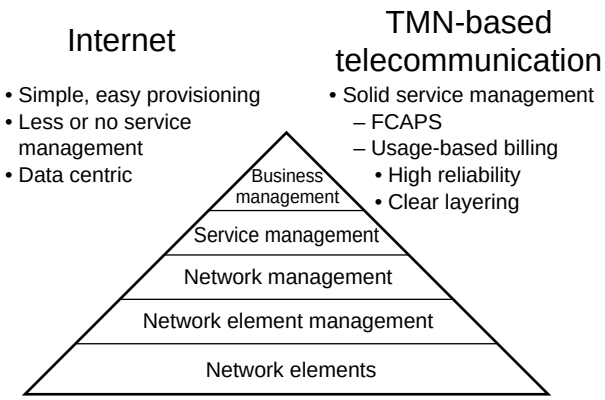

Figure 3
Internet vs.Telecom: Two NM paradigms.

note 1) In this paper, we use the term PBM consistently throughout the paper. In most cases, the two terms, PBM and PBN, can be used interchangeably.

using PBM with a set of coherent information models for the new IP-based end-to-end network infrastructure. **Figure 4** shows how this integration will be achieved. There are several sources for this new network information model. From the Internet camp, IETF PIB and DMTF CIM[6] will provide basis for the unified model. From the telecommunication camp, ITU-T TMN, TINA[note 2] RIM (Resource Information Model),[7] TMF[note 3] CaSMIM[8] shall be counted as efforts important in this process.

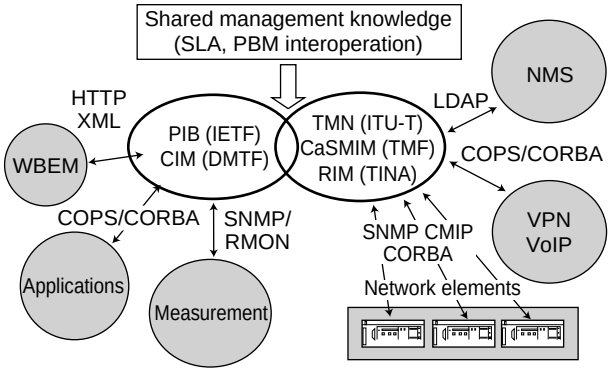

Figure 4
PBM as information centric management.

4. End-to-end IP policy management architecture

In the emerging network service paradigm, end-to-end support both for network management and service management will be very important. The end-to-end IP management should be able to provide guaranteed service, QoS (Quality of Service), QoE (Quality of Experience) for various IP-based services, across administrative domains involved with the service provisioning. The new management paradigm should bring about smoother, more flexible, and more effective integration of service offerings from players in the new network service paradigm, including network providers, service providers, ASPs (Application Service Provider), and end users.

Our group at Fujitsu participated in a joint effort to compile the vision for the new network management paradigm. During its study period, the prospective market for management products and competitor trends were studied, and compet-

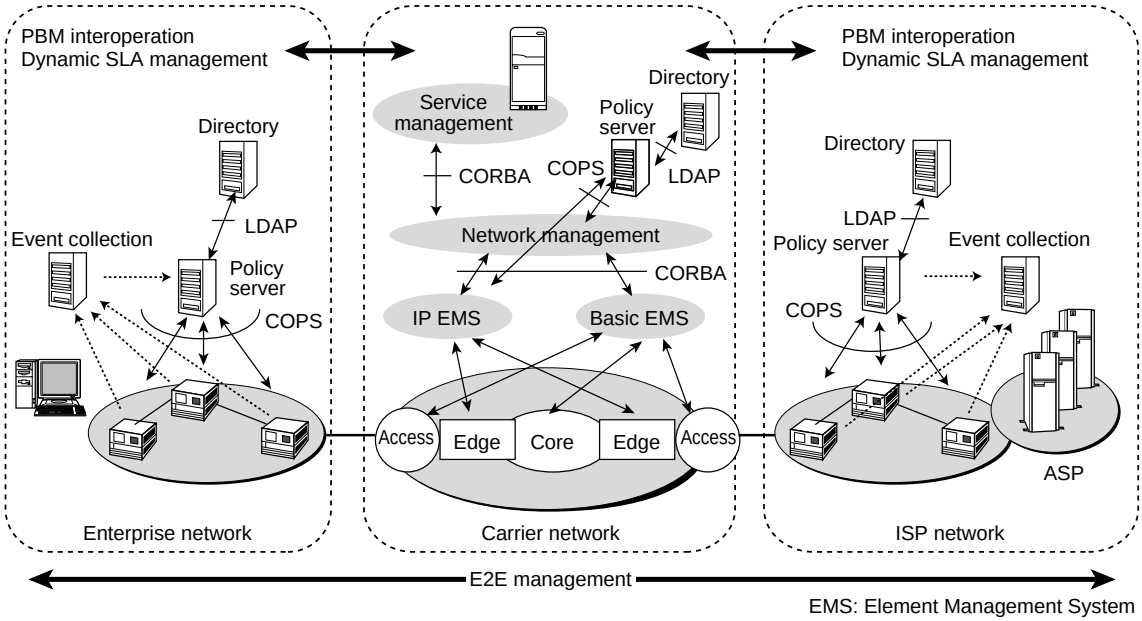

Figure 5
End-to-end IP management architecture.

note 2) TINA, Telecommunication Information Network Architecture.
http://www.tinac.com

note 3) TeleManagement Forum.
http://www.tmforum.org

itive analysis with current Fujitsu management products was performed. **Figure 5** illustrates the end-to-end IP management architecture, which is a part of the vision created by the study. The key item in the architecture is PBM. The vision entails the following three-step evolution path for the next 5 years.

1) IP-nization of telecommunication network

The next telecommunication network infrastructure will be predominantly IP-based, and IPv6 will play a primary role in the IP-nization process.[9] In particular, we believe that mobile IP and requirements of number portability will globally accelerate acceptance of IPv6. The key events will occur within 2 to 3 years. IP-based, or IP-enabled network devices will gradually replace traditional telecommunication network elements. In the process of this transition, network management systems, including EMSs (Element Management System) and NMSs (Network Management System) will be increasingly IP-enabled.

2) PBM deployment in telecommunication networks

In 3 to 4 years, the needs of integrated end-to-end IP network management will initiate wide deployment of PBM-based network management system, which will enable more sophisticated integration of enterprise network management and WAN (Wide Area Network) management. The IETF standard architecture will be the base of this development, but several technical innovations such as architecture scalability and efficient conflict detection will be needed, in response to requirements from telecommunication network management.

3) End-to-end integration of service management

In 4 to 5 years, true integration of management systems will start addressing service management and application program performance issues, making it possible to solve end-to-end QoS guarantee or QoE guarantee in a more quantifiable manner. In contrast to what is available today, all the management actions will be more tightly integrated with business workflow, enabling end-to-end flow-through operations. The business workflow typically includes provisioning, monitoring, and billing.

In Figure 5, the three-step evolution results in a PBM-based end-to-end IP management architecture. The three interworking PBM domains, an enterprise network, a carrier network, and an ISP network, communicate with each other through PBM interworking interfaces, with which dynamic SLA (Service Level Agreement) information is exchanged. The dynamic SLA is a flexible template for IP network management and service management operations, which drives respective business processes in the domains in such a way that flow-through operations throughout the three domains become possible. The seminal paper on dynamic SLA[10] gives an example that an end customer's management policy is embedded in an SLA, so that the policy is negotiated and deployed through a customer-provider negotiation process.

5. Scalable PBM architecture for enterprise/telecom integrated management

The IETF policy WG architecture provides the starting point toward the end-to-end IP management. The new service paradigm, however, imposes a new set of architectural requirements, which entails the PBM to be more scalable, more reliable, and more flexible in terms of policy deployment and enforcement. These developments are a natural consequence of IP network expansion, from enterprise networks with a dozen of host computers and routers to end-to-end integrated LAN-WAN-LAN networks with hundreds, or even thousands of hosts and routers.

We have been engaged in research to overcome the architectural limits of the standard PBM, by enhancing the original PBM architecture with a few technical improvements. We observed that

the standard PBM architecture has the following architectural limitations on scalability, due to physical architecture scalability, policy rule complexity, and management knowledge complexity. We at Fujitsu Laboratories of America have studied techniques to overcome these architectural limitations, for the scalable PBM system for integrated management of telecom and enterprise networks.

1) Physical architecture scalability

PBM is a client-server system, where clients are network devices as PEPs (Policy Enforcement Point) and servers are policy servers as PDPs (Policy Decision Point). In a generic usage example of the standard PBM architecture in enterprise networks, there is one policy server in the given management domain, and a few dozens of network devices. The architecture does not scale well for carrier scale networks with thousands of network devices. Standard techniques such as hierarchically distributed directories, policy servers with policy caching, scalable signaling path by using multicast between policy servers and network devices can improve scalability of the PBM architecture.

Figure 6 illustrates a scalable PBM architecture augmented with these enhancements. In this scalable architecture, a single directory server in the standard PBM architecture is replaced by a set of hierarchical servers, which maintains coherency, eliminating the single point of failure. The information stored in directory servers is distributed to a set of policy servers through multicast channels. The policy servers operate both as points of policy deployment as well as policy caches between directory servers and network devices, enhancing both PBM performance and fault tolerancy.

2) Policy rule complexity

Although a simple IF-THEN rule is sufficient for many situations, the complexity of policy rules can grow rapidly when the number of applications and traffic types increases.[11] For example, when PBM is used for per user flow provisioning, a policy rule typically looks like:

IF [*the user is the department VP*]
THEN [*give his traffic the highest priority*].

A first-cut formula for the number of policies in a PBM domain is given by:

# of policies (P) =
# of users (U) × # of current applications (C).

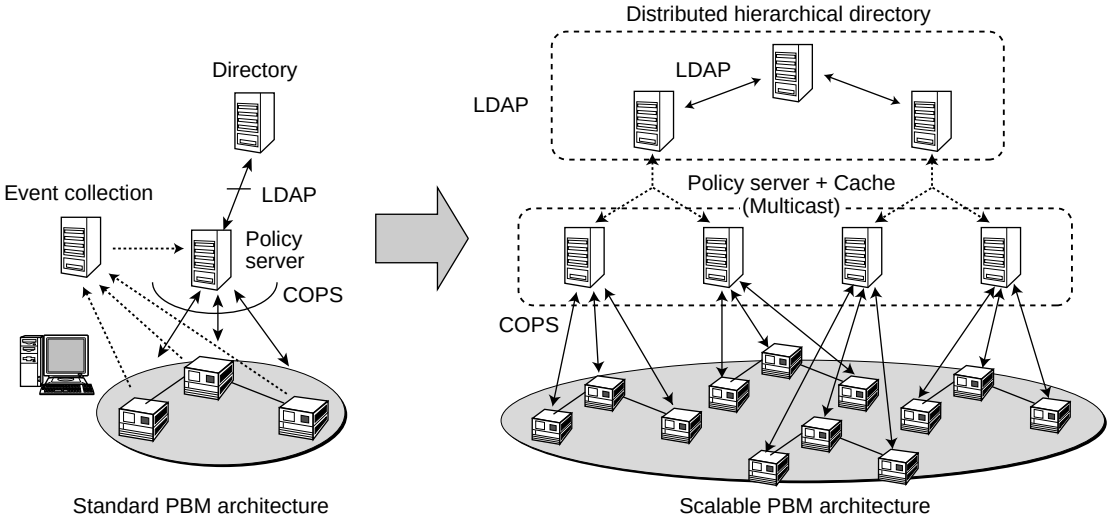

Figure 6
PBM scalability enhancements.

It is not difficult to see that the number of policies grows very rapidly, when both the number of users and the number of applications increase. To keep the complexity of the policy rules at a manageable level, policies need to be organized using grouping (aggregation) and layering (abstraction) principles. For example, by classifying users into a set of user groups, which may be mapped to distinctive DiffServ traffic classes, description of policy rules can be made simpler. Similarly, a set of applications can be grouped to give an abstract application class, of which policy rule dictates the behavior of all the applications in the class.

3) Management knowledge complexity

PIB (Policy Information Base) represents management knowledge in the network. When TMN layer principle is applied, management knowledge is organized in such a way that higher layer such as SML (Service Management Layer) represents service management aspects whereas lower layer such as NML (Network Management Layer) represents network control and management aspects. As we discussed in 2), complexity of policy system is largely dependent on the organization of management knowledge, in particular how the knowledge is represented as PIB.

Classical techniques of modeling techniques such as aggregation and abstraction are organized into principles of OOAD (Object-Oriented Analysis and Design), whose notations and language mapping conventions are being standardized as UML (Universal Modeling Language).[12] Another important principle for modeling is RM-ODP (Reference Model of Open Distributed Processing),[13] a set of ISO standards that allow description of a system from five distinctive viewpoints. Although these technologies offer generic techniques to construct models of different levels of behavior and levels of abstraction, their usage depends on the application domain. When incorporated into PIB design, their usefulness is dictated by how efficiently management knowledge is incorporated into the design.

Protocol independent modeling (PIM) has been a kind of Holy Grail of telecommunication network management.[7),8] It is rather a natural concept from service provisioning point of view, since there are often many choices of transport technologies such as ATM, SONET, IP, etc. to support the same type of connectivity service. Similarly, there are quite a few of management protocols such as SNMP, CMIP, CORBA, etc., which are dealing with essentially the same kind of management knowledge. Managing service provisioning will become simpler, if not easier, therefore, if we use protocol (technology) independent representation of management knowledge, particularly at service management layer.

The power of abstraction impacts PIB design twofold. In the basic IF-THEN syntax of policy rules, abstraction of network/service resources allows simplifying the conditional statement of the rule, making the rule itself to be more general and powerful for versatile network resource environment. For example, when the rule deals with management condition of QoS at the service level, the rule shall equally apply to various network technologies that guarantees the same QoS to end customers. In a similar manner, abstraction at network resources shall contribute to simplify the action statement of the policy rule, since minor differences in network devices are absorbed into generic network device model represented by the PIB.

Figure 7 illustrates a layered PBM architecture, which makes use of protocol independent modeling and management knowledge structure by TMN layers. As it is exemplified by DEN, combination of the two “P”s, namely policy based management and protocol independent modeling, turned out to be powerful as well as natural. With a layered PBM architecture, it becomes possible to handle service provisioning and SLA management issues in a more structured manner, handling multiple application layer protocols for optimal presentation of management operations.

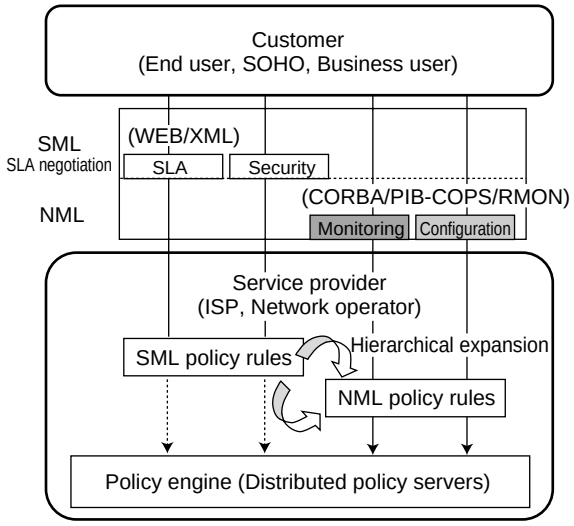

Figure 7
Multi-layered PBM.

In this architecture, service requirements of the customer drive provisioning of service and network resources in the service provider, and PBM serves as the key execution mechanism to deploy the service requirements dictated by the SLA (Service Level Agreement) between the customer and the service provider. The service terms of SLA, which are resulted from negotiation between the customer and the service provider, can include both SML (Service Management Layer) terms and NML (Network Management Layer) terms.

For example, conditions on security and billing terms are considered at SML level, whereas monitoring and QoS requirements such as bandwidth and packet loss rate are considered at NML level. SML terms had better be negotiated using application level representations such as Web and XML, whereas NML terms had better be handled using protocols such as CORBA and COPS. These SLA terms need to be translated into appropriate policy rules, so that the policy engine of service provider OSS (Operation Support System) can execute and enforce the prescribed SLA terms. Some SML policy rules such as application-specific QoS requirements need to be translated into NML policy rules first, so that the requirements are deployed in terms of network resources such as bandwidth and assignment of a proper priority class.

6. Active policy and intelligent agent

Policy-based management is likely to be the most expressive statement of the Internet impact on the telecommunication management. It is also a positive statement on the value of network intelligence, particularly in the form of management knowledge. Among the three planes of the telecommunication, namely data, control, and management, the management plane is to assume most of network intelligence so as to provide better customer care and service provisioning for end customers. Subsequently the other two planes had better be simple and fast to provide very high-speed IP connectivity. In particular, the control plane must perform a large volume of connectivity provisioning request in real-time through signaling, thus it usually can not afford much intelligence to handle complex customer data.

An intelligent agent is a piece of programming code that can move around in the network. It is expected to behave more intelligently than a piece of data, by adjusting itself to versatile network environment. Therefore, it does not necessarily contribute something drastically different from what is achieved by a current network management system (NMS). It should rather be considered a technical concept to be used complementarily in combination with NMS. It is also to be noted that intelligent agents and policy-based management have a common theme, which is representation of management knowledge through a set of agents (rules) with rudimentary intelligence.

Active policy[14] is a crossover of the two concepts, i.e. intelligent agents and policy-based management. In particular, when the policy rules are written in a protocol independent, platform independent language, the policy rule can execute on the client side as an “active” policy, when the policy is deployed. Therefore, an active policy can be seen as a special case of PBM as well as of intelligent agent. We consider the following features of active policy are most important, giving

extra advantages over regular (non-active) PBM.

Improved SLA negotiation: added intelligence permitted by active policy should allow more intelligent negotiation between the customer and the service provider, improving the SLA negotiation process. For example, this process resembles personalization at portal services, which additional intelligence at the portal server assists the customer to make better selections in presumably shorter time. In a similar token, added intelligence of active policy should help customize service requirements of the customer, assisting the customer to set up his/her own system environment.

Improved customer self-operation: once SLA is negotiated and agreed between the two parties, its execution can also be assisted by active policy. For example, an active policy can communicate with a policy server in the service provider, so that it optimizes user profile of the customer and relevant policy rules, improving customer self-operation with less or no assistance from human customer service representatives.

Better customer care management: the two features above inclusively contribute to better customer care management, as the customer should find that the network is more responding to his/her service needs and management requirements. Intimately related to this issue is monitoring of service perception of the customer, which is called QoE (Quality of Experience), an essential tool for measuring and improving customer care. As we illustrate in the following, active policy provides the potential to improve QoE.

Figure 8 illustrates our architectural view on the active policy. The active policy augments the network intelligence of network OSS (Operation Support System) by adding more intelligent behavior at service management layer (SML). Management knowledge is represented by PIB, which is constantly updated by periodic measurement and sampling from network devices. Operations at SML takes advantage of active policies to support better SLA negotiation and QoE monitoring between customer and service provider. An active policy, for example, is able to measure QoE of the end customer with regards to Web server response.

IF [*the Web server response >= 8 sec*]
THEN [*notify it to the Web server operator*].

This active policy shown above seems like a normal policy rule, but it works only when the policy rule is (actively) downloaded to client equipment, and the notification address of the Web server operator is dynamically filled when the active policy is initiated. It should be noted also that QoE of the end customer can not be measured and reported by any other way.

Figure 9 shows a physical architecture image of QoE monitoring using active policy. Access

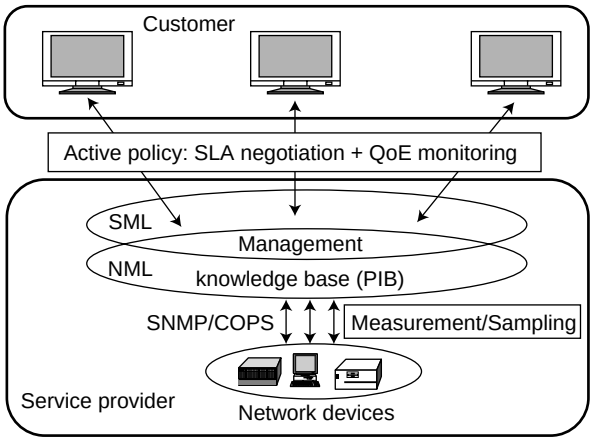

Figure 8
Active PBM architecture.

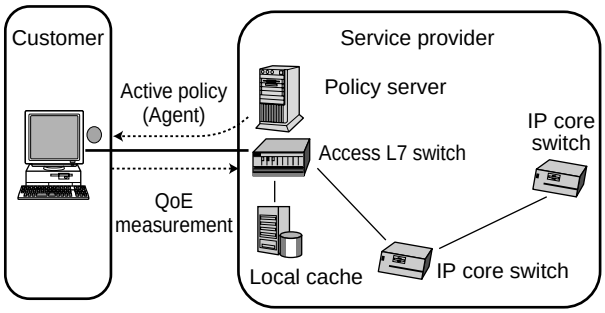

Figure 9
QoE monitoring using active policy.

L7 switch is able to either switch or to retrieve from local cache, depending on the application characteristics as Web switches in CDN (Content Delivery Networks) use them. An active policy is downloaded from a policy server on a host computer in the customer domain. Application performance is directly measured as QoE on the host computer, which is fed back to the access L7 switch to control application specific network flows.

7. Conclusion

Policy-based management is likely to serve as a key integration technology for end-to-end IP management, and also for IP-nized telecommunication network. Though the concept was originally motivated by technical developments in the enterprise network market, we have examined PBM in this paper, and have concluded that PBM is applicable, with several architectural enhancements, to the management of new telecommunication network service environment. We have also discovered that PBM, despite its historical context, has key technical concepts rooted deep both in the development of IP management and that of telecommunication management, confirming our belief in PBM that it will continue playing an important role as the key technology for managing the new service environment.

Active policy is a relatively new research area, which is to be explored in a coming few years. It is of particular interest whether and how PBM and intelligent agent systems are advanced and integrated, to offer better service management and customer care in the new service environment.

Acknowledgement

The authors like to thank Mr. Katsuyama, Mr. Chugo of Fujitsu Laboratories, Japan, and Mr. Ejiri of Fujitsu Ltd. for their expert knowledge and discussions on PBM and telecommunication management. Special thanks go to Mr. Iseda of Fujitsu Laboratories, Japan, for his comments and advices on the early drafts of this paper. The authors also thank Dr. Frank McCabe and Network Agent Research group members at Fujitsu Laboratories of America, and Dr. David Blight of Palm Computing for helpful discussions and suggestions on intelligent agent systems.

References

1) G. Gilder: *Telecosm: How Infinite Bandwidth Revolutionize Our World*, Free Press, 2000.
2) A. Moridera, K. Murano, and Y. Mochida: The Network Paradigm of the 21st Century and Its Key Technologies. *IEEE Communication Magazine*, **38**, 11, pp.94-98 (Nov. 2000).
3) M. Sloman: Policy Driven Management for Distributed Systems. *Journal Of Network and Systems Management*, **2**, 4, pp.333-360 (1994).
4) J. Strassner: *Directory Enabled Networks.* Macmillan Technical Publishing, 1999.
5) IETF draft: draft-ietf-policy-terminology-00.txt, work in progress, July 2000.
6) DMTF, CIM schema ver.2.4, Aug. 2000. *http://www.dmtf.org*
7) TINA-C: Resource Information Model ver.4.0, Aug. 2000.
8) TMF, CaSMIM (Connection and Service Management Information Modeling) team. *http://www.tmforum.org*
9) Internet 2 project home page. *http://www.internet2.org*
10) K. Fukuda et al.: Policy-based Networking Service over Heterogeneous Public IP Service (DynaServ). Proc. of ICCC'99, Tokyo, June 1999.
11) D. Blight and T. Hamada: Policy-Based Networking Architecture for QoS Interworking in IP Management. Proc. of IM'99, Boston, May 1999.
12) OMG, UML 2.0 WG draft, available form *http://www.omg.org*
13) ISO/IEC DIS 10746-1-5: Information technology – Open Distributed Processing Reference Model, 1995.
14) T. Hamada, D. Blight, and P. Czezowski:

Active Policies in Knowledge Hyperspace: Intelligent Agents and Policy-Based Networking. *KNOM-review Journal*, **2**, 2, pp.31-41 (Dec. 1999).
http://dpnm.postech.ac.kr/knom/knom-review/index.html

Takeo Hamada received B.E. and M.E. degrees in Electrical Engineering both from the University of Tokyo, Tokyo, Japan in 1984 and 1986, respectively and Ph.D. in Computer Science from UC San Diego. He joined Fujitsu Laboratories Ltd., Kawasaki, Japan in 1986. He has been with Fujitsu Labs. of America, Inc. since 1998. His current research interests include network management, service management issues in IP networks, and policy-based management. He is a member of IEICE Japan, IEEE, and ACM.

E-mail: thamada@fla.fujitsu.com

Peter J. Czezowski joined Fujitsu Labs. of America, Inc. as a Member of the Research Staff in March 1999. He holds a M.Sc. in Electrical Engineering from the University of Manitoba, Canada in 1994, where he is currently a Ph.D. candidate. His research interests include policy-based network management, agent-based computing, and the Internet. He is a member of IEEE.

E-mail: peterc@fla.fujitsu.com

Takafumi Chujo joined Fujitsu Laboratories Ltd., Kawasaki, Japan in 1978. He graduated from Kanazawa University, Kanazawa, Japan and from Nagoya University, Nagoya, Japan with B.E. and M.E. degrees in Electronics Engineering, respectively. Since he joined Fujitsu, he engaged in broad range of network systems design, including SONET/SDH, ATM link system, network management system for WDM optical cross-connect system. He is currently a senior research fellow at Fujitsu Laboratories Ltd., Japan. He has served regularly as program committee member of several international conferences on network management. His current research interests include optical networking, network management systems, telecommunication OSS, security management, and policy-based management.

E-mail: chujo@fla.fujitsu.com