MULTI-DOMAIN POLICY ARCHITECTURE FOR IP MULTIMEDIA SUBSYSTEM IN UMTS

Wei Zhuang, Yung Sze Gan, Qing Gao,
Kok Jeng Loh and Kee Chaing Chua
Siemens ICM Mobile Core R&D, Siemens Pte. Ltd., Singapore

Abstract The UMTS IMS network offers IP based multimedia applications with end-to-end QoS guarantee by using policy-based control principles. To support end-to-end QoS, the UMTS IMS network should be scalable, reliable and flexible in policy deployment and enforcement, characteristics that are not found in a single-domain policy architecture. We propose that a hierarchical architecture be applied to a single-operator multi-domain environment, while multi-operator networks are peered at their hierarchical roots. This multi-operator multi-domain policy architecture potentially minimizes the session setup delay and policy exchange load while maximizing network scalability.

Keywords: UMTS, IMS, QoS, multi-domain policy, peering, hierarchical

1. Introduction

The 3rd Generation Partnership Project (3GPP) is in the process of standardizing the Universal Mobile Telecommunication System (UMTS) as the next generation high-speed mobile system that provides both circuit switched and packet switched services. Since 3GPP UMTS Release 5, the IP Multimedia Subsystem (IMS) ([1],[2]) has been added as a part of the UMTS to provide IP based multimedia services. With IMS, the operators can offer Session Initiation Protocol (SIP) [3] based IP multimedia services such as video and audio conferencing that require end-to-end QoS guarantees.

The 3GPP has decided to use the policy-based QoS control architecture [4] as illustrated in Figure 1 to satisfy the end-to-end QoS requirements of a UMTS IMS network. In this architecture, the Policy Control Function (PCF) [4], which is a logical component of the Proxy Call State Control Function (P-CSCF), plays the role of a Policy Decision Point ([5], [6]) that translates the business rules specified by the network operator into the corresponding network resource management configura-

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

D. Gaïti et al. (eds.), *Network Control and Engineering for QoS, Security and Mobility*

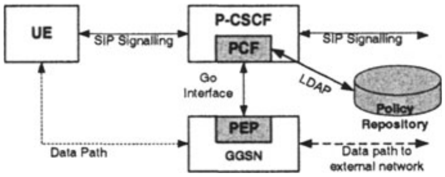


Figure 1. Policy architecture of the UMTS

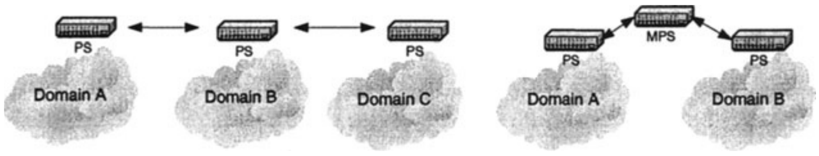
tions. Being in the data path and controlling the connections to external networks, the Gateway GPRS Support Node (GGSN) installs these configurations through its embedded Policy Enforcement Point (PEP) to enforce the resource allocations determined by the business rules. In this way, the operator can easily control the QoS of multimedia services by providing suitable business rules. To facilitate the transport of policy information between the PCF and PEP, the Go interface employs the Common Open Policy Service-Provisioning (COPS-PR) [7] protocol.

When considering end-to-end communications, it is likely that several administrative domains are traversed. For example, the calling and called parties may reside in networks of different operators with separate policy domains. In order to provide service consistent to that requested by the users, policy enforcement in the domains along the data path must not impact the service contracted to the users. In a multi-domain, multi-operator environment, a simplistic single policy server per domain architecture is not scalable and does not offer flexibility in providing policy consistency. An architecture that takes into consideration the issues of a multi-domain environment must be devised to make the deployment of policy-based QoS control viable for UMTS IMS networks.

We propose a QoS policy architecture for a multi-domain, multi-operator environment in this paper, which is organised as follows. In Section 2, we describe the two general approaches of policy architecture in a multi-domain environment, namely the peering and hierarchical architectures. We suggest that the QoS policy framework be structured in multiple levels in Section 3. It is our opinion that this approach fits the multi-domain, multi-operator environment better. Hence, we propose a hybrid architecture that realizes the framework in Section 4. Section 5 concludes the paper and describes some of the outstanding issues in our proposed architecture that need further study.

2. Multi-domain QoS Policy Architecture

In order to support end-to-end QoS, the IMS network should be scalable, reliable and flexible in policy deployment and enforcement, characteristics not available in a single domain architecture. For example, it



(a) Peering architecture (b) Hierarchical architecture

Figure 2. Two basic types of policy control architecture

is impossible to manage all GGSNs under a single policy domain if the network of one operator grows larger and covers a wider area. Operators may want to manage their networks as several interconnected domains with different policies. In short, a multi-domain architecture is more scalable, reliable and efficient for distributed control. There are two types of multi-domain policy control architectures, (a) peering (Figure 2(a)) and (b) hierarchical (Figure 2(b)) [8].

For the peering multi-domain architecture, all policy servers work as peers. There is no master policy server. Each policy server has a set of policies that is applicable only to its own policy domain. The peering policy servers need to exchange inter-domain policies. One particular instantiation of the peering architecture is the bandwidth broker architecture ([9], [10]).

In hierarchical multi-domain architecture, policy domains are grouped hierarchically. The policy servers are divided into master policy servers and local policy servers. A Master policy server handles inter-domain policy exchange.

Comparing the peering architecture with the hierarchical architecture, the peering architecture is more scalable since the policy servers only need to interact with their neighbors. To establish an end-to-end QoS relationship, the originating domain policy server depends solely on interactions with its connecting domain policy server to ensure that all other domains on the path to the terminating domain can support the required QoS requirements. The connecting domain policy server in turn depends solely on its next connecting domain policy server to provide the same assurance. Thus, an end-to-end QoS relationship is established by chaining bilateral inter-domain policy agreements on the path of a session. As a result, the session setup time is long if there are many domains in the path of a session.

In the hierarchical multi-domain architecture, an end-to-end QoS relationship is established by interactions of multiple domain policy servers through their common master policy server (MPS). This MPS is con-

Architecture	Scalability	Flexibility	Policy exchange load	Inter-Domain administrator	Response delay
Peering	High	High	High	Not Required	Slow
Hierarchical	Low	Low	Low	Required	Fast

Table 1. Comparison between two types of architecture

nected to the policy servers that control all domains on the end-to-end path. And the MPS must exchange policies with each connected network individually to ensure all domains on the path of a session can support the QoS requirements. Thus, end-to-end QoS relationship is established only after the MPS has set up a multilateral inter-domain policy agreement among all policy servers on the path of a session. As a result, the MPS has a higher load if many operators' networks are interconnected.

In both policy architectures, the operator has some flexibility in deciding on their network connectivity with other networks. In the peering architecture, the operator decides on its peering partners by connecting its policy server to the desired peering policy servers. In the hierarchical architecture, the operator decides on its peering partners by connecting its policy server to the MPS that is connected to the desired policy servers.

The peering and hierarchical policy architectures offer both advantages and disadvantages. As seen in Table 1, the peering architecture offers high scalability and flexibility without placing the peering parties under the authority of a common policy administrator. These are desirable advantages in a multi-operator environment. In contrast, session setup delay and policy exchange load are potentially lower in the hierarchical architecture where a policy administrator controls the entire network. To utilise the advantages offered by the peering and hierarchical architecture in a multi-operator multi-domain environment, we suggest a hybrid policy architecture, where the hierarchical architecture is employed within the multi-domain network of an operator and the peering architecture connects multiple operators.

3. End-to-End QoS Policy Framework

An end-to-end QoS policy that supports a UMTS IMS service may span multiple domains that are managed by different network operators. Before a multi-domain QoS policy architecture can be designed, it is necessary to define a framework that describes how end-to-end QoS policies can be structured across a multi-operator, multi-domain network.

The end-to-end QoS policy framework that we have employed to design our proposed multi-domain QoS policy architecture is illustrated in

Figure 3. In this framework, there are three levels of QoS policies that must be provided to support a QoS service. At the highest level is the service level, where the network operators who support the same service must agree on its QoS requirements. By necessity, the service level spans the domains of all participating network operators and it defines the characteristics of the end-to-end QoS services that can be provided to their customers. The service QoS requirements are described in the form of Service Level Specifications (SLS) that the operators make with one another. A typical SLS would describe a QoS service like premium data service by specifying its guaranteed bit-rates, tolerable loss rate, permissible network delay and delay jitter. By agreeing on a mutual SLS, peering operators are committed to configure their networks in such a way that the specified QoS is provided.

Once the operator obtains a SLS, it will be able to translate this into policies that manage QoS resources in its network to satisfy the specifications in the SLS. The network resource management policies describe the QoS requirements of the contracted service with reference to its peering arrangement with neighboring operators' networks. These network level policies may be constrained by administrative requirements like provision of government mandated emergency services and performance considerations of the operator's network. Thus, network resource management policies control the policing and conditioning of incoming traffic at the network edge and its route through the network so that the contracted QoS service requirements are satisfied.

Commonly, the operator will divide its network into multiple interconnected domains that implement different sets of network resource management policies to create a minimal two-level policy hierarchy. The upper level network resource management policies enforce the QoS requirements described in the SLS, subject to the operator's network-wide administrative requirements. The lower level network resource management policies customize the upper level network resource management policies to the topology and administrative requirements of the individual domain within the network. Additional levels may be added to the policy hierarchy by nesting domains within existing domains. The advantage of adopting a policy hierarchy within an operator's network is to limit the impact of topology or administrative changes on the network resource management policies implemented in the network. As an example, an operator defines a policy hierarchy that groups the routers into distinct domains in its network. Any policy change due to a router failure is restricted to the portion of the network governed by its policy domain. Without the use of the policy hierarchy, the policy change caused by the single router failure will affect the entire network.

The network resource management policies are not targeted at the network devices in the network. They only describe how the traffic utilizing a QoS service should be treated as it transits the network. They do not describe how the QoS mechanisms in the routers and switches in the network should be configured to provide the required QoS resources. Thus, the network level policies must be translated into device level policies that configure the QoS mechanisms in the routers and switches in accordance with the resource management requirements. These policies are highly specific to the types of QoS methodology, e.g., the Integrated Services (IntServ) and Differentiated Services (DiffServ) mechanisms, employed in the network devices. The policies applicable to IntServ routers are on a per-flow basis while flows are aggregated before the policies are applied to them in DiffServ routers. In addition, different vendors may implement the QoS mechanisms in the same QoS methodology differently. As an example, either a Weighted Fair Queuing (WFQ) scheduler or a Weighted Round Robin (WRR) scheduler could service a DiffServ flow aggregate to satisfy its delay requirement. Therefore, device level policies must be translated into actual QoS mechanism parameters before they can be installed in the network devices.

Looking at the end-to-end QoS policy framework, two distinct forms of QoS policy interactions can be discerned. SLSs must be negotiated among the network operators who contract services from one another. Within an operator's network, the SLSs are translated into network level and device level policies that are implemented in the network. In our proposed multi-domain QoS policy architecture, the QoS policy interactions are similarly divided into two forms. Across operators' networks, a peering architecture is adopted since the operators have management authority only over their own networks. Within an operator's network, a hierarchical architecture is adopted to mirror the policy hierarchy in which the network is structured.

4. Proposed Multi-domain QoS Policy Architecture in UMTS IMS

The proposed multi-domain QoS policy architecture designed with reference to the end-to-end QoS policy framework is shown in Figure 4. A 2-level hierarchy is shown for illustrative purpose only. The depth of the hierarchy depends on the relationship among the policies that are to be applied to the network. Complex policy relationship is usually represented as multi-level policy hierarchy. There is only one Master PCF (MPCF) in an operator's network that is peered with MPCFs of adjacent networks through an Inter-domain Policy Agent (IPA). The

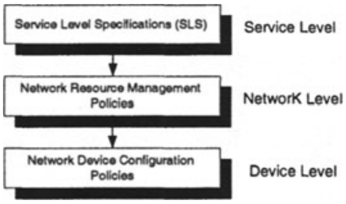

Service Level Specifications (SLS)
Service Level
Network Resource Management Policies
NetworK Level
Network Device Configuration Policies
Device Level

Figure 3. End-to-end QoS policy framework

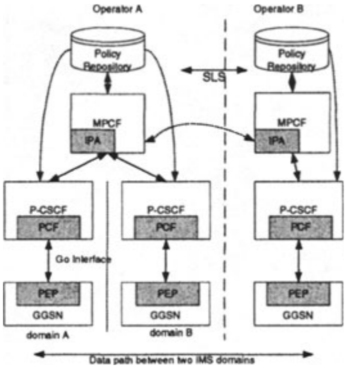


Figure 4. Proposed multi-domain QoS policy architecture in UMTS IMS

IPAs facilitate SLS negotiation between two interconnected operators' networks. After an IPA exchanges updated SLS information successfully with its peering IPAs, the MPCF will translate the new SLS into network level policies applicable to its network before updating its policy repository. When the PCF is performing local domain policy control for an IP multimedia session, the PCF just retrieves and enforces the relevant network level policies from the policy repository. Thus, the MPCF is able to retrieve policies from the policy repository and modify the policies in the repository. However, PCFs have only read access rights to the policy repository.

4.1. Multi-operator inter-network policy architecture

The network level policies to be employed by interconnecting UMTS IMS networks are determined by the SLSs that are agreed between the peering network operators. In these SLSs, there are static service requirements and dynamic service requirements. The static service requirements can be directly translated into enforceable network level policies to be retrieved by the PCFs in the individual network. But the dynamic service requirements are dependent on the state of the UMTS IMS network like its resource utilization, and can only be translated into enforceable network level policies after negotiation with the connecting networks. The purpose of SLS negotiation is to enable interconnected networks' IPAs to agree on the specific service requirements that must be supported under the prevailing network states. Once the SLS negotiation is successfully completed, the participating IPAs can translate the agreed service requirements into enforceable policies in their respec-

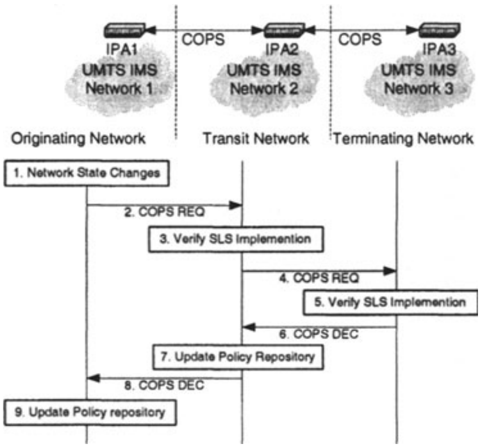


Figure 5. Communications between IPAs of peering UMTS IMS networks

tive networks. Note that this runtime negotiation may not be initiated on a per-session basis. Instead, the SLS negotiation is usually initiated when the IPA detects that the state of its network has changed and the existing policies are no longer enforceable.

IPAs participating in the SLS negotiation must be connected so that SLS information can be exchanged. We propose to use the COPS protocol as the communication protocol between the peering IPAs (IPA1, IPA2 and IPA3). The operator of a UMTS IMS network will configure its IPA with the locations of its peering counterparts. The COPS protocol can be suitably extended with new messages to carry SLS information, as is attempted in the COPS-SLS [11] protocol.

The SLS negotiation process between IPAs is depicted in Figure 5:

1 The MPCF detects a change in the network state of UMTS IMS network 1 that invalidates the current network level policies implementing the dynamic QoS service requirements in the SLS. The MPCF updates the SLS dynamic QoS parameters based on the new network state before translating it into network level policies.

2 Before the policy repository is updated with the new policies, IPA1 encapsulates the updated SLS parameters in a COPS request message and sends it to IPA2 of the connecting UMTS IMS network 2.

3 Once IPA2 receives the SLS information in the COPS request message from its peer IPA1, its MPCF will check whether its current network level policies can implement the updated SLS parameters requested by UMTS IMS network 1. If the current network level

policies can implement the SLS parameters, IPA2 just returns a positive COPS decision message to IPA1. The SLS negotiation terminates at this point because it is assumed UMTS IMS network 2 is guaranteeing that UMTS IMS network 3 can support the new QoS service requirements. If the updated SLS parameters cannot be supported, the MPCF of UMTS IMS network 2 will translate the updated SLS into network level policies for verification purposes. If the translation cannot be made, IPA2 will return a negative COPS decision message to IPA1. Otherwise, IPA2 will have to change its network level policies to meet the new QoS service requirements and consult UMTS IMS network 3 about its ability to meet the new QoS service requirements.

4 Before the new network level policies can be written into the policy repository, IPA2 must check with IPA3 whether UMTS IMS network 3 can support the new QoS service requirements by forwarding the COPS request message.

5 IPA3 repeats the SLS implementation verification procedure in step 3.

6 IPA3 returns either a positive COPS decision message if the updated SLS parameters can be implemented by current or new network level policies, or returns a negative COPS decision message if otherwise.

7-9 The reception of a COPS decision message from IPA3 will trigger IPA2 to send a matching COPS decision message to IPA1. Thus, IPA1 gets a positive COPS decision message if IPA3 accepts the updated SLS parameters. Once the IPAs receive a positive COPS decision message, they will write the new network level policies translated from the updated SLS into their policy repositories. If the IPAs receive a negative COPS decision message, the updated SLS cannot be supported and no update is made to their policy repositories. In that case, the MPCF of UMTS IMS network 1 can modify the SLS dynamic QoS parameters and repeat the SLS negotiation process. The operator of the originating UMTS IMS network 1 determines the number of SLS negotiation rounds before giving up.

4.2. Single operator inter-domain policy architecture

For the multi-domain environment in a single operator's network, the hierarchical policy architecture will be used. The MPCF connects to the

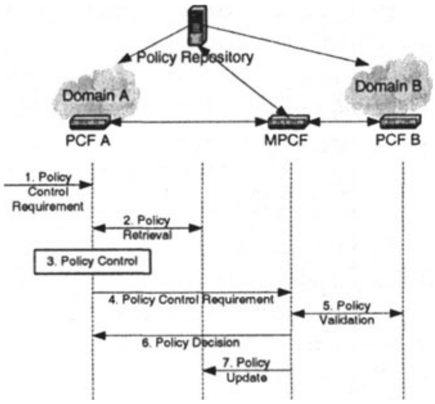


Figure 6. **Procedure for inter-domain policy control in a UMTS IMS network**

PCF of every policy domain in the UMTS IMS network. The MPCF translates the network-wide policies into domain specific network level policies on behalf of the PCFs and stores them in the policy repository. The PCFs just retrieve these network level policies from the repository, translate them into device level policies and install these policies in the network devices under their control. The network level policies are also retrieved by the PCFs so that IP multimedia sessions can be policed and conditioned on setup. The communication protocol between the MPCF and PCFs is based on the COPS protocol.

The policy control process activated during an IP multimedia session set-up is illustrated in Figure 6 and described below:

1 During the session set-up period, the P-CSCF of domain A will pass the QoS parameters in the SDP description obtained through SIP signaling to PCF A.

2 PCF A will retrieve relevant network level policies from the policy repository

3 PCF A checks that the requested QoS parameters are permitted by the network level policies. If the QoS parameters are permitted, the PCF generates an authorization token and returns it to the P-CSCF. If the QoS parameters are explicitly forbidden by the policies, the PCF notifies the P-CSCF that policy control has failed.

4 If the retrieved network level policies are contradictory to the authorization of the requested QoS parameters, PCF A will ask the MPCF to resolve the policy conflict. The PCF encapsulates the

requested QoS parameters in a COPS request message and sends it to the MPCF.

5 The MPCF resolves the policy conflict by creating new network level policies based on the network-wide policies. Before the new policies are supplied to PCF A, the MPCF must validate them with PCF B since domain B is on the data path of the session and thus must be capable of implementing the requested QoS parameters as well.

6-7 Once the policy validation with PCF B succeeds, the MPCF sends the new network level policies back to PCF A. At the same time, the MPCF writes the new policies into the policy repository for future retrieval by PCFs.

As stated earlier, the multi-domain architecture in the UMTS IMS network needs not be restricted to the minimal two-level hierarchy described in the policy control process. The network operator may decide to provide intermediate levels of policy conflict resolution for more granular control over its network.

5. Conclusion

After comparing the peering multi-domain policy architecture with the hierarchical multi-domain policy architecture, we propose that the hierarchical architecture be applied in a multi-domain environment of a single operator UMTS IMS network, while the peering architecture be employed in a multi-operator UMTS IMS network. This multi-domain QoS policy architecture can minimize the session set-up delay and policy exchange load while maximizing network scalability. Finally, the SLS negotiation and policy conflict resolution mechanisms are described to support our multi-domain QoS policy architecture.

Several problems, which are the foci of our future work, are foreseen in the proposed multi-domain QoS policy architecture. These are:

- To facilitate successful negotiation between IPAs, the parameters of SLS must be standardized to provide the basis of negotiation. This requires analysis of the format of QoS requirements that may be specified in SLS so that the definition of the QoS resource elements carried in the COPS messages can be determined.

- The security of the communications channel between the connecting policy entities is important. This is especially true for the peering architecture adopted to interconnect different operators' networks. The operators are highly sensitive to the risk of policy leakage through snooping, unauthorized tampering of COPS messages en route between IPAs and interactions with unauthenticated policy entities. Although the COPS protocol has the ability to secure messages by encapsulating integrity objects, additional mechanisms may have to be deployed to address other security risks.

- Policy negotiation in a peering architecture is a slow process, especially if the chain of participating networks is long. Network design in this case will play an important role in minimizing the delay.
- The depth of the hierarchical architecture affects the policy provisioning time in an operator's network. The deeper the policy hierarchy, the longer will the PCFs at the lowest level have to wait for a decision from the MPCF. Proper policy hierarchy design will help to reduce the number of policy levels.

References

[1] 3GPP TS 22.228, "IP Multimedia Subsystem, Stage 1", Dec. 2001

[2] 3GPP TS 23.228, "IP Multimedia Subsystem, Stage 2", Jan. 2002

[3] M. Handley, H. Schulzrinne, E. Schooler, J. Rosenberg, "SIP: Session Initiation Protocol", work in progress, IETF, Feb. 2002

[4] 3GPP TS 29.207, "Policy Control Over Go Interface (Rel 5)", Apr. 2002

[5] R. Yavatkar, D. Pendarakis and R. Guerin, "A Framework for Policy-based Admission Control", RFC 2753, IETF, Jan. 2000

[6] R. Rajan, D. Verma, et al., "A Policy Framework for Integrated and Differentiated Services in the Internet", IEEE Network Magazine, vol. 13, no. 5, pp. 36-41, Sept./Oct. 1999

[7] K. Chan, D. Durham, S. Gai, S. Herzog, K. McCloghrie, F. Reichmeyer, J. Seligson, A. Smith and R. Yavatkar, "COPS Usage for Policy Provisioning", RFC 3084, IETF, Mar. 2001

[8] T. Ebata, M. Takihiro, S. Miyake, et al., "Interdomain QoS Provisioning and Accounting", INET 2000, Yokohama, Japan, July 2000

[9] K. Nichols, V. Jacobson, L. Zhang, "A Two-bit Differentiated Services Architecture for the Internet", RFC 2638, IETF, July 1999

[10] B. Teitelbaum, P. Chimento, "QBone Bandwidth Broker Architecture", work in progress, http://qbone.internet2.edu/bb/bboutline2.html

[11] T. M. T. Nguyen et al., "COPS Usage for SLS Negotiation (COPS-SLS)", work in progress, IETF, Feb. 2002