UDC 621.396.65:621.397.2

Unified IP Service Control Architecture Based on Mobile Communication Scheme

●Mitsuaki Kakemizu ●Masaaki Wakamoto ●Akira Orita

(Manuscript received December 1, 2000)

The Internet is rapidly evolving. However, the present Internet is not intelligent. Although it has begun to provide many users with multiple services such as VPN and QoS, it cannot provide users with customized IP services. In this paper, we propose a unified IP service control architecture that makes the Internet practically intelligent and provides both fixed and mobile users with customized IP services. The basic idea of our proposed architecture is based on the mobile communication scheme. That is, the IP service control mechanism is embedded in the location registration and resolution procedures, which are indispensable for mobile communication. To implement this idea, we enhanced the mobility management mechanism, taking into account the following two points: 1) a fixed user is regarded as a mobile user whose mobility is zero so that not only mobile users but also fixed users can enjoy IP services and 2) user service customization is supported by cooperation with policy-based network management systems. The proposed architecture was successfully applied to the mobile IP which is being studied at the IETF as a key technology for the forthcoming mobile Internet.

1. Introduction

The Internet is rapidly evolving all over the world, and many technologies, for example, the tera-bit router and WDM are increasing its throughput. The Internet has also begun to provide many users with multiple services such as VPN and QoS. However, because the present Internet is not intelligent, it cannot provide customized IP services that meet the special requirements of individual users. Methods of interworking[1] between the Internet and PSTN using the intelligent network (IN) are actively being studied. The IN enables the PSTN to provide supplementary services such as free-phone by analyzing the signaling messages. The IN therefore can make the PSTN intelligent, but it cannot make the Internet broadly intelligent. This is because the Internet is a connectionless network and fundamentally does not have signaling messages for connection establishment except for resource reservation protocol (RSVP) messages. Active networks[2] therefore are being studied to make the Internet more intelligent. However, we must address many unresolved issues such as security before we can put them to practical use. This is because in an active network, programs and data are embedded in the packets by users and are executed in network elements such as routers. In this paper, we propose a unified IP service control architecture that makes the Internet practically intelligent through cooperation with policy-based network management systems and provides not only fixed users but also mobile users with customized IP services.

2. Requirements for IP service control

To flexibly adapt to the evolving Internet, the IP service control architecture must satisfy the following requirements:

1) Support of customized IP services on a user-by-user basis

Requirements for IP services differ among users. Also, the users' communication environments, for example, the type of terminal being used and the connecting network, are also different. To enable users to enjoy their own IP services anywhere, anytime, an IP service control architecture should provide customized IP services on a user-by-user basis regardless of the users' communication environment, for example, regardless of whether a user is using a mobile or fixed environment.

2) Harmonization of various user service requirements

Even through the users' Internet service requirements are constantly changing, the Internet is expected to provide the required services. This requires an IP service control architecture that allows each user to customize his or her services at any time without degrading the services of other users.

3) Independence of link layer and physical layer technology

The evolving Internet always needs more packet forwarding capability. Many technologies, for example, the tera-bit router, WDM, and MPLS are being introduced to increase the throughput of the Internet in the link or physical layer of the OSI reference model. The IP service control architecture should be independent of these technologies so as to be applicable to any type of IP network.

4) Smooth migration

When introducing this architecture to the Internet, modification to the basic IP packet forwarding function at the network layer should be minimized so that the architecture can be quickly put into wide use.

3. Proposed architecture

3.1 Basic concepts

We propose a unified IP service control architecture to satisfy the requirements mentioned in the previous chapter. **Figure 1** shows a conceptual network model of our proposed architecture. The basic concepts of our architecture are as follows:

1) Unified service control mechanism

A common IP service control mechanism is essential to providing the same IP services for both fixed and mobile users. We regarded fixed users as mobile users with zero mobility and then unified our architecture based on the mobile

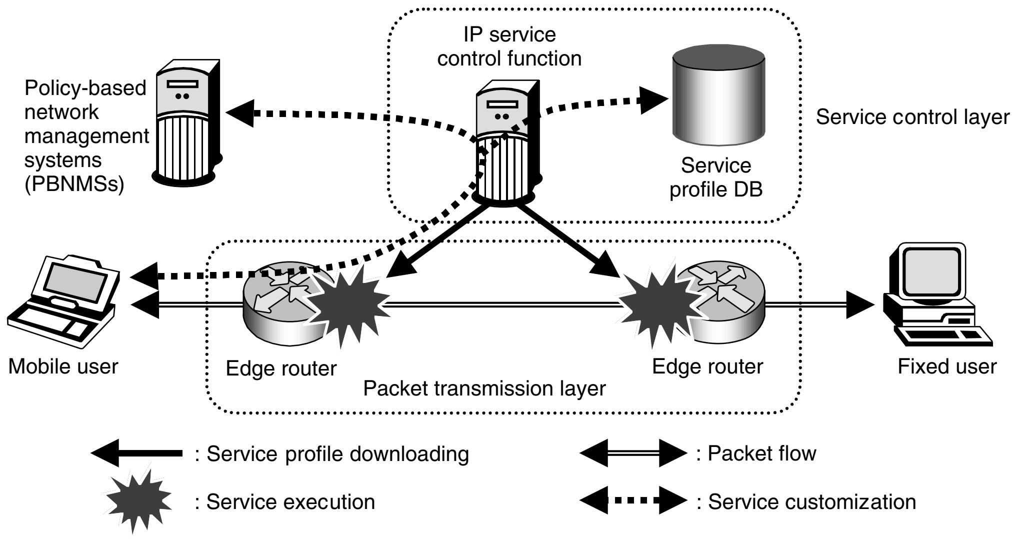

Figure 1
Conceptual network model.

communication scheme.

2) Separation of the service control layer from the packet transmission layer

The architecture separates the service control layer from the IP packet transmission layer. The service control layer manages each service profile for each fixed or mobile user in a service profile database (DB). A service profile consists of a set of procedures and data to control customized IP services for a fixed or mobile user. The service control layer downloads each service profile copy to the IP packet transmission layer. The IP packet transmission layer can execute the customized IP services for each user by referring to the cached copy on a packet-by-packet basis, without needing to know the details of the user's service contract. As a result, this separation allows Internet service providers to deploy this architecture in their IP networks with minimum modification. That is, this separation makes it easy to add a service profile copy management function to an IP network.

3) Enhanced location registration procedure

Policy-based networking (PBN) can be regarded as an approach for introducing network intelligence to IP networks. However, if the policy server manages each service profile as policy data, the policy server has to download a copy of the service profiles for each mobile user to all edge routers. This is because the policy server cannot learn the location of each mobile user. This implies that the IP service control mechanism based on PBN is not suitable for large-scale IP networks. Our proposed architecture is based on the mobile communication scheme and enhances the location registration procedure. That is, when replying to each location registration request from mobile users, the IP service control function only downloads a service profile copy to the edge router that is accommodating the mobile user. This enhanced location registration procedure makes the proposed architecture scalable because only those routers that need a copy of a service profile actually cache one. In the case of a fixed user, the IP service control function caches a copy of the user's service profile in the router that accommodates the user when the user subscribes to the service.

4) Cooperation with policy-based network management systems

Policy-based network management systems (PBNMSs) supervise and control a network based on the network operator's policy for maintaining the overall performance of the network. The proposed architecture cooperates with PBNMSs to comply with frequent user-demands for customization of services without degrading services provided to other users.

3.2 Mobile IP-based architecture

Mobile IP, which is being studied by the Internet Engineering Task Force (IETF), is considered a promising mobility mechanism for the forthcoming mobile Internet. Therefore, as shown in **Figure 2**, we have applied our proposed architecture to the mobile IP. The IETF is also studying how to make the mobile IP cooperate with the authentication, authorization, and accounting (AAA) functions to put the mobile IP protocol to practical use.[3] The IETF is studying how to use Diameter[4] for this cooperation, which is an AAA policy protocol and an extension of RADIUS.[5] In this extended mobile IP, each mobile user's terminal is called a mobile node (MN) and receives IP packets from a corresponding node (CN), which is a fixed or mobile terminal, via a home agent (HA) of the MN. An HA manages the location of each MN. The HA is statically or dynamically selected by an AAA server during the location registration phase. To apply our architecture to such an enhanced mobile IP, in our design, an AAA server supports the IP service control function and downloads each service profile for an MN to the corresponding HA. Thus, the IP services for the incoming packets to the MN are executed in the HA based on the cached service profile. Moreover, the service profile is also downloaded to the foreign agent (FA) that accommodates the MN. This

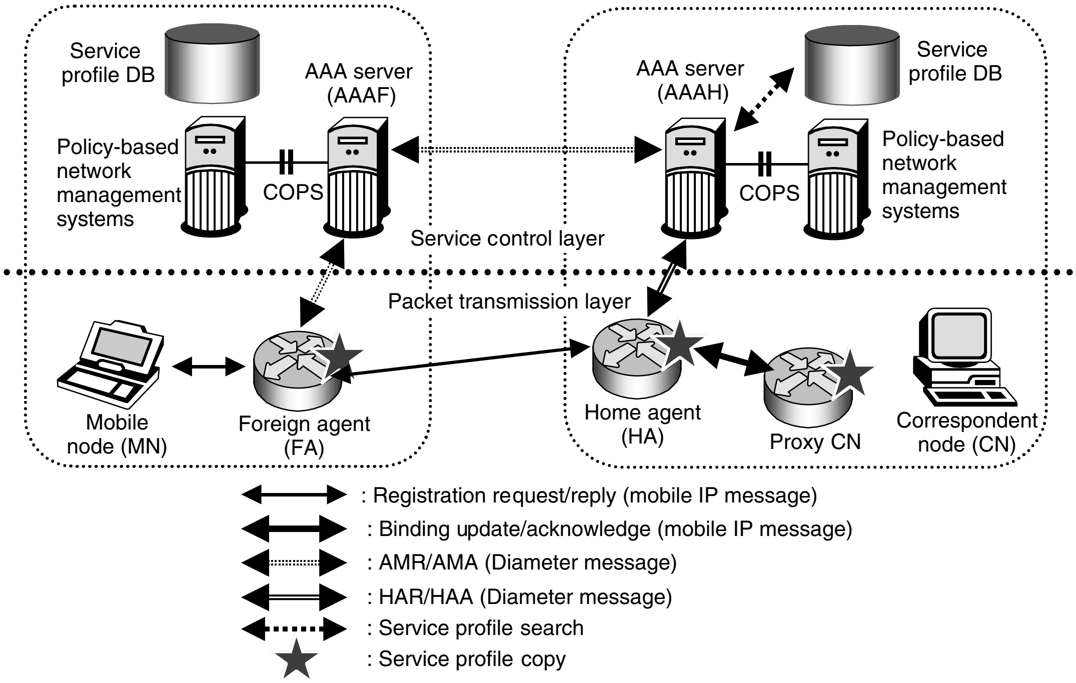

Figure 2
Proposed architecture.

enables the IP services for the outgoing packets from the MN to be executed in the FA. The main features of the proposed architecture are as follows:

1) Enhanced location registration procedure by Diameter extension

An AA-Mobile-Node-Request (AMR) Diameter message packing a mobile IP registration request message is used to register the location of an MN and to authenticate/authorize the MN. An AMR message also includes a network access identifier[6] (NAI) used to authenticate/authorize the MN. In the proposed architecture, the HA and FA can only cache a copy of a service profile for each MN when registering the location of the MN by Diameter extension messages, as described below.

An AAA Home (AAAH), which is an AAA server administered by an ISP to which an MN subscribes, searches the service profile DB containing the MN's service profile from the NAI as a function of authentication/authorization. The AAA server then downloads a copy of the service profile to an HA and FA by sending them in Diameter messages. These Diameter messages are a Home-Agent-MIP-Request (HAR) Diameter message sent to the HA and an AA-Mobile-Node-Answer (AMA) Diameter message sent to the FA via an AAA Foreign (AAAF), which is any other AAA server that is not administered by the ISP to which the MN subscribes.

2) Cooperation with policy-based network management systems (PBNMSs) via COPS

An AAAH notifies the PBNMSs about each user customization demand via the common open policy service (COPS).[7] The PBNMSs then send the AAAH an acknowledgement of the demand after confirming that none of the services provided to other users will be degraded. The AAAH then updates the service profile in the service profile DB and downloads another copy of the modified service profile to the HA and FA. This customization mechanism enables users to customize their services without degrading the services of other users.

3) Introduction of proxy CN

In the IETF, a route optimization method[8] is being studied in which a CN receiving a binding update (BU) mobile IP message from an HA

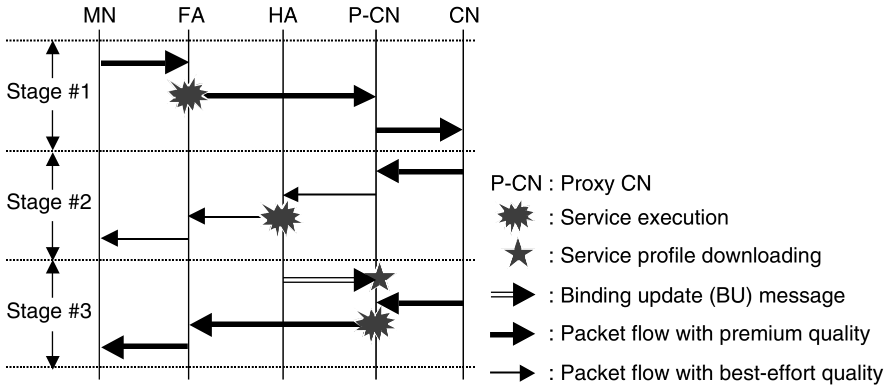

Figure 3
Sequence chart for service execution.

sends encapsulated data packets directly to an FA without going the roundabout way through the HA. In the proposed architecture, a BU message also includes a copy of a service profile for an MN. This optimization method forces a CN to include various functions such as IP-in-IP encapsulation and the management of service profile copies in addition to the FAs' care-of-addresses. We introduce the proxy CN concept to exclude these functions from a CN. A proxy CN is substantially a router accommodating a CN. It has these functions as a proxy of the CN and executes the functions by capturing a BU message sent to the CN.

If src ip ==#MN, dst_ip==*
Then QoS=Expedited service
Else QoS=Best_effort service

(a) Copy cached in FA.

If src ip==*, dst_ip==#MN
Then QoS=Expedited service
Else QoS=Best_effort service

(b) Copy cached in HA and proxy CN.

Legend
src_ip: source IP address.
dst_ip: destination IP address.
* : don't care.

Figure 4
Example service profile copies for an MN.

3.3 Service control example

This section describes an example of executing a customized IP service by using a differentiated services[9] capability to provide an expedited forwarding service and best-effort service. **Figure 3** shows a sequence chart for service execution between an MN and a CN. Assume that the HA and FA for the MN have already cached the copies shown in **Figure 4 (a)** and **(b)**, respectively, after receiving them from the same AAAH server. In stage #1, the FA assigns the packet flow from the MN expedited service class by referring to the service profile copy shown in Figure 4 (a). The MN can therefore send the CN packet flow with expedited service quality. In stage #2, although the HA assigns the packet flow to the MN expedited service class, the MN cannot receive the packet flow with expedited service quality from the CN, because the packet flow between the proxy CN and the HA is limited at this time to the best-effort quality. However in stage #3, the proxy CN caches the service profile copy shown in Figure 4 (b) after it captures the BU message with the copy sent to the CN. As a result, the MN can receive the packet flow with expedited service quality from the CN.

4. Conclusions

In this paper, we proposed a unified IP service control architecture that provides network intelligence to IP networks. We have applied our architecture to the mobile IP in cooperation with authentication, authorization, and accounting servers. The proposed architecture is characterized as follows:

- It enables effective service profile caching in only the essential routers by enhancing the location registration procedure.
- It enables user service customization through cooperation with policy-based network management systems.
- It enables network functions to be excluded from correspondent nodes by introducing a proxy CN.

The proposed architecture can therefore make the Internet practically intelligent and provide both fixed and mobile users with customized IP services on a user-by-user basis.

References

1) F. Cuervo, N. Greene, C. Huitema, and A. Rayhan: Megaco Protocol 0.8. RFC2885, August 2000.
2) D. Tennenhouse, J. Smith, W. Sincoskie, D. Wetherall, and G. Minden: A Survey of Active Network Research. IEEE Communications Magazine, January 1997.
3) P. Calhoun and C. Perkins: Diameter Mobile IPv4 Extensions: draft-ietf-aaa-diameter-mobileip-04.txt, Work in Progress, May 2001.
4) P. Calhoun, H. Akhtar, J. Arkko, E. Guttman, A. Rubens, and G. Zorn: Diameter Base Protocol. draft-ietf-aaa-diameter-04.txt, Work in Progress, May 2001.
5) C. Rigney S. Willens, A. Rubens, and W. Simpson: Remote Authentication Dial In User Service (RADIUS). RFC2865, June 2000.
6) P. Calhoun and C. Perkins: Mobile IP Network Access Identifier Extension for IPv4. RFC2794, March 2000.
7) J. Boyle, R. Cohen, D. Durham, S. Herzog, R. Rajan, and A. Sastry: The COPS (Common Open Policy Service) Protocol. RFC2748, January 2000.
8) C. Perkins and D. Johnson: Route Optimization in Mobile IP. draft-ietf-mobileip-optim-10.txt, Work in Progress, November 2000.
9) S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, and W. Weiss: An Architecture for Differentiated Services. RFC2475, December 1998.

Mitsuaki Kakemizu received the B.S. degree in Electrical Engineering from Osaka City University, Osaka, Japan in 1984. He joined Fujitsu Laboratories Ltd., Kawasaki, Japan in 1984 and has been engaged in research on intelligent networks, public/private internetworking architectures, and IP-over-ATM technology. He is a member of the Institute of Electronics, Information and Communication Engineers (IEICE) of Japan.

Masaaki Wakamoto received the B.E. and M.E. degrees in Information Engineering from Yokohama National University, Japan in 1980 and 1982, respectively. He joined Fujitsu Laboratories Ltd., Kawasaki, Japan in 1982, where he has been engaged in research on a CAD system for switching software, an expert system for communications networks, and intelligent network architectures. He is now responsible for research on IP service control systems.

Akira Orita received the M.S. degree in Electrical Engineering from the University of Tokyo, Tokyo, Japan in 1982. He joined Fujitsu Ltd., Kawasaki, Japan in 1982, where he has been engaged in the development of software for switching systems.