SIP-based VoIP-over-MPLS Architecture Design and System Development for Interactive and Secure Multimedia Services

Chih-Wei Hsu, Wen-Hsing Shen, Huan Chen, Ting-Chao Hou

Department of Electrical Engineering & Center for Telecommunication Research, National Chung Cheng University
Email: m9121, m92143@cn.ee.ccu.edu.tw; huan, tch@ee.ccu.edu.tw

Abstract

With the success of Internet and the advances of network technologies, the number of multimedia users increases dramatically in recent years. The next generation communication networks shall provide interactive and secure multimedia services to the public. Among multimedia services, VoIP is one of the most popular applications due to its low cost compared to conventional voice services via the Public Switched Telephone Network (PSTN). However, inherited from its interactive and real-time nature, it is very sensitive to network congestions and it requires more stringent quality of service (QoS). To carry good quality of voice over an IP network, it needs both a good signaling protocol as well as high speed backbone to forward IP packets efficiently. The emerge of the Session Initiation Protocol (SIP) and the Multi-Protocol Label Switching technology (MPLS) provide a good QoS solution to the VoIP applications. The former provides an easy and flexible signaling strategy for the IP environment, while the later provides QoS guarantees with the use of the traffic engineering. In this paper, we propose a novel architecture to integrate these two technologies, which is suitable for VoIP applications with secure and QoS guarantees. This VoIP-over-MPLS architecture employs the SIP protocol for signaling to set up call connection and uses the MPLS core network to forward packets efficiently. Especially, we put emphasis on the necessary components to provide interactive and secure services. This architecture comprises three major parts: Edge devices, access network, and the MPLS core network. The necessary elements and requirements are described in this paper, which is followed by the modified SIP registration and signaling process to provide the secure and traffic engineering functionalities.

Keywords: SIP, VoIP and MPLS

1. Introduction

With the success of Internet and advances of broadband access technologies, the number of multimedia users is increasing rapidly in recent years. To take the advantages of the resource on the Internet, users access broadband networks through various technologies such as xDSL, Cable Modem, Fiber-to-the-Home (FTTH), and Digital Wavelength Division Multiplexing (DWDM). However, the hybrid high-speed networks incur several security and QoS concerns that can cause the network to collapse. Such weaknesses accelerate the propagation of virus and attack storm. How to design a secure and QoS-aware high-speed network to satisfy the security and QoS requirements of users is a great challenge.

A prominent technology known as the *Differentiated Service Model over Multi-protocol Label Switch* (Diff-Serv/MPLS) [1] can enhance QoS provisioning ability for the conventional IP-based networks. This DiffServ based MPLS network is a suitable platform to run VoIP application since it can support differentiated traffic classes and provide preferential treatments to users. In addition, such networks also make it possible to provide many salient functions such as QoS provisioning, Fast Forwarding, Traffic Engineering (TE) and Virtual Private Network (VPN) applications [2]–[5]. The DiffServ-based MPLS technology is scalable and practical, and it has been deployed in most advanced routers.

Among all services run over the broadband access networks, the VoIP is one of the most popular multimedia applications [6] due to its low cost compared to the conventional voice service via Public Switched Telephone Networks (PSTN). Inherited from its interactive and real-time nature, the VoIP application is very sensitive to network congestions and it requires more stringent QoS criteria than those for other non-interactive multimedia and data traffic. For VoIP applications, some security and QoS requirements shall be maintained to make them attractive to users [7].

In this paper, we adopt the most popular application protocol *"SIP"* for the peer-to-peer multimedia services in our project, and we then propose a SIP-based VoIP-over-MPLS architecture for the interactive and secure

This research is sponsored in part by NSC Taiwan under the grant Number NSC-93-2219-E-194-005 and NSC-93-2219-E-194-008, and in part by ITRI CCL Taiwan under the grant number T1-94025-6.

multimedia services in this paper. We employ the SIP protocol for service signaling to set up call connections and use the MPLS core network to forward packets efficiently. This architecture comprises three major parts: Edge devices, access network, and the MPLS core network. The necessary elements and requirements are described in this paper, which is followed by the modified SIP registration and signaling process to provide the secure and traffic engineering functionalities.

The remaining part of this paper is organized as follows. In section 2, the background for the MPLS-TE and SIP are briefly reviewed. In section 3, the SIP-based VoIP-over-MPLS architecture is presented, which is followed by the SIP signaling and message flow in section 4. Finally, section 5 concludes this paper.

2. Background

A. Traffic Engineering in MPLS

Multi-Protocol Label Switching (MPLS) [2] is a technology that integrates the label-swapping paradigm with the network-layer routing among the Label Switch Routers (LSRs). One of the most important mechanisms to ensure the QoS is MPLS-TE. MPLS-TE facilitates the efficient and reliable network operations while optimizes network resource utilization and traffic performance simultaneously [8].

The goal of MPLS-TE is to compute a path from one given node to another such that the path does not violate any constraints (bandwidth/administrative requirements) and is optimal with respect to required QoS metrics. Once the path is determined, TE is responsible for establishing and maintaining the forwarding state along this path. The conventional OSPF routing protocol have been extended, to support the traffic engineering in MPLS, which is known as OSPF Traffic Engineering (OSPF-TE) [9]. OSPF-TE provides more information such as network topology, constraints, and administrative attributes pertaining to links to MPLS network. Specifically, OSPF-TE generates the opaque LSAs, which carry traffic engineering parameters. These parameters have additional link attributes that can be used to build an extended link state database, known as the traffic engineering database (TED). TED is used by the Constraint-based Shortest-Path First (CSPF) algorithm to compute a path that satisfies all constraints (bandwidth and administrative requirements) and is shortest for TE LSP to take.

According to the service level agreement (SLAs) contracted between network providers and VoIP service provides, the QoS-based LSPs have to be established in advance as one-way virtual trunks for a group of VoIP subscribers. These virtual trunks can be established based on the approaches of topology driven or configuration driven. The data-driven service policy is not recommended since the LSPs could incur a longer call setup delay and cause higher system complexity.

In our system design, when a new VoIP call arrives, the VoIP traffic of control messages and media data will be aggregated into a virtual trunk by the ingress edge router according to the location of this callee. In addition to MPLS routines, the security and QoS control functions have to be design into the edge routers or the cooperative agents of the edge routers in our project.

B. Session Initiation Protocol (SIP)

SIP is an application-layer control protocol that can establish, modify, and terminate multimedia sessions [10]. SIP supports five facets of establishing and terminating multimedia communications: user location, user availability, user capabilities, session setup, and session management. SIP is rather a component that can be used with other IETF protocol to build a complete multimedia architecture. These architectures will include protocols such as Real-time Transport Protocol (RTP), the Real-time Streaming Protocol (RTSP), the Media Gateway Control Protocol (MEGACO), and Session Description Protocol (SDP). SIP is based on an HTTP-like request/response transaction model. Each transaction consists of a request that invokes a particular function on the server and at least one response.

SIP cannot provide any kind of network resource reservation and enhanced security capabilities. How to provide a secure and QoS-based MPLS network to SIP users are the significant studies of this paper. Based on the conventional MPLS network, we propose a SIP-based VoIP-over-MPLS architecture and design new components. All of them are introduced in the following sections.

3. SIP-based VoIP-over-MPLS Architecture

Fig. 1 shows the reference Architecture for SIP over MPLS. This Architecture is divided into three parts: Edge Device, Access Network and MPLS Core Network.

A. Edge Devices

Edge devises are defined as the application

terminals that either provide multimedia services or request them. Without loss of generality here we assume that the user agent client (UAC) plays the role the caller who initiates a session, and the user agent server (UAS) is the callee who will respond to the caller and setup connection with it. The detail functions for the above elements are described as below:

- Caller (UAC): The UAC (User Agent Client) start a SIP call-setup session, the Access Network will provide call control functions and signaling functions [11].
- Callee (UAS): The UAS (User Agent Server) can receive a SIP request and give appropriate response back to UAC.

B. Access Network

The access network comprises three major modules: OAM module, Security module and SIP Signaling module. Here the OAM module is responsible the operation, administration and monitoring the session status. Security module is responsible for intrusion detection and reporting tasks and the SIP Signaling module is responsible for the session connection. The detail functions for the above elements are described as below:

(1) OAM Module: The OAM module is responsible the operation, administration and monitoring the session status.

- Call Control Agent: The Call Control Agent (CCA) coordinate the network transport resource and transport content, it is responsible for coordinating the resource between CAP and users. When the users need the network resource, CCA will decide how to satisfy the user's request, transform the requests to the QoS parameters and ask the NRB for network resource. Thus, CCA can configure the classification rules in the Ingress LSR.
- Network Resource Broker: The Network Resource Broker (NRB) is responsible for the network management. Based on the topology information of the MPLS network, it has the capability of resource management and call admission control. The management software of NRB is SNMP that monitor the states of LSRs and LSPs. We illustrate the interaction with MPLS network components (CCA and NRB) and message flows in Fig. 2.

(2) Security Module: The security module is responsible for the intrusion detection and attacking reporting.

- Content Awareness Processor: The Content Awareness Processor (CAP) investigates practical solutions to the issues of content-aware and network security for SIP-enable MPLS networks. It introduces many advanced functions such as Content Aware Classification, Intrusion Defense and Computing Resources Detection on VoIP network. When detecting suspicious packet, CAP will drop the intrusion packet send by malice user. Further more, by catch the bandwidth from SIP packet requested by caller and callee, CAP can communicate with NRB and then allocate the required bandwidth in real-time. Two Intel IXP 425 [12] are used to perform the function of Content Awareness Processor.

(3) SIP Signaling Module: The SIP Signaling module is responsible for the session connection.

- SIP Proxies: The SIP proxies are elements that route SIP requests to UAS and SIP responses to UAC. Proxy servers can be classified according to the amount of state information that they store during a session. A proxy can operate in either a stateful or stateless mode for each new request. Here, we setup a stateful proxy [10].
- SIP Server: The functions of SIP server comprise the registrar and SIP proxy. Registrar offers a discovery capability, while the SIP proxy resolves the content of SIP message.

C. MPLS Core Network

MPLS core network consists of ingress label switched router (Ingress LSR), core label switched routers (core LSRs) and egress label switched router (Egress LSR). MPLS core network provides a vehicle for packet forwarding. The detail functions for the above elements are described as below.

- Ingress LSR: The Ingress LSR in its role in handling traffic as it enters an MPLS Network. Ingress LSR will be aware and classify the SIP control message, and will be capable of forwarding the SIP control message to CAP. One Intel IXP 2400 [13] is used to perform the function of Ingress LSR.
- Core LSR: The Core LSR will be aware of MPLS application-layer control protocol, will operate one or more L3 routing protocols, and will be capable of forwarding the SIP control message to CAP. A Core LSR may optionally be also capable of forwarding native L3 packets. Two Intel IXP 1200 [14] are used to perform the function of Core LSR.
- Egress LSR: The Egress LSR in its role in

handling traffic as it leaves an MPLS Network, and will be capable of forwarding the SIP control message to CAP. One Intel IXP 2400 [13] is used to perform the function of Egress LSR.

4. Proposed SIP Registration and Signaling Processes

Following the same convention and notation in SIP (RFC 2543, 3261 [10], [15]), we proposed two modified message sequence for registration and signaling process to support the required QoS and security functions. Finally, the interactions between the components in the access network are illustration in the flow diagram.

A. Registration Process

Register process is completed through the use of two SIP methods, REGISTRATION and OK. REGISTRATION offers a discovery capability, while OK responds the registration results. If a client UAC wants to initiate a session with another party (UAC or UAS), the SIP server known as the registrar must be aware of these hosts before the session can be setup. Therefore, it requires for each host to register with the registrar whenever it joins a new network domain. Another SIP server, known as location server, provides these address bindings for each registered host. These address bindings map an incoming SIP URI via the SIP server [10], [15].

We describe the registration message flow as below. As illustrated in Fig. 3 (a), if a caller (UAC) wants to initiate a session with another party, a callee (UAC or UAS) it registers itself with the registrar first. The caller gets the SIP server address by consulting its local SIP proxy, and this local SIP proxy will keep the REGISTER message in order to report the connection status to security unit CAP and OAM units such as CCA, NRB and SIP servers. These RESGISTRATION message are collected by SIP proxies and relayed to CAP to be analyzed for security problem. If they are considered to be safe, these messages will be forwarded to the OAM units (CCA and NRB) for administration controlling and operation monitoring. Next they are forwarded to SIP server for session control and service locating, which are done by referencing a SIP session database in the SIP server. Finally, SIP server will send back to caller an OK message to acknowledge that the registration is successful.

B. Signaling Process

The signaling process is an application level three-way handshaking. The SIP methods used in the signaling process consist three signaling sequences: Invite sequence, OK sequence and Ack sequence. Here we focus ourselves on the interaction between access network elements in the access network. We illustrate the signaling process in Fig. 3 (b) and describe this three-way handshaking process as follows.

(1) INVITE Sequence: As depicted in Fig. 3 (b), when a caller wants to initiate one session with the callee over the SIP-based MPLS network, the caller will send an INITVE request to the local SIP proxy to get the SIP server address. Each local SIP proxy keeps session state information since it is running in a stateful mode by default in our architecture. The local SIP proxy of the caller sends an INVITE request to CAP1 and CAP1 checks whether the INVITE request is a malicious message with security concern. If this request message is considered safe, CAP1 records this request and forwards this request to the CCA and NRB module. After this INVITE request arrives CCA and NRB, the QoS parameters of the session are recorded for the purpose of admission control, load balancing calculating and operation monitoring tasks. The INVITE request finally arrives the SIP server, who will search the callee URI in session database. After leaving the SIP server, the INVITE message is intercepted by the CAP2 for security check when it leaves the MPLS core network. The INVITE message then arrives the SIP local proxy located in the callee side and finally, it arrives the callee.

(2) OK and ACK Sequence: After the INVITE message arrive the callee, the callee will respond with a 200 OK message to the caller. As illustrated in the lower part of the Fig. 3 (b), the OK message will traverse each access network component by the following order: callee, SIP proxy (callee side), CAP2, NRB, SIP server/CCA, CAP1, SIP proxy (caller side), caller. Note that the order is not the exactly identical to the incoming path as INVITE request. We design this way to overcome the generic problem that NRB knows the location of SIP server, but not vice versa. When the OK message traces back to NRB, NRB will know all session information that can start to build the session. After the OK message arrive the caller with acknowledge session information, the caller will sends an ACK message to guarantee that the session cannot be timeout.

5. Conclusion

In this paper, we proposed a novel architecture to integrate two advanced

technologies: SIP and MPLS to provide good quality to users. The proposed architecture is suitable for VoIP applications. Especially, it also provides a solution to security and traffic engineering issues. This VoIP-over-MPLS architecture employs the SIP protocol for signaling to set up call connection and uses the MPLS core network to forward packet efficiently. Traffic engineering in MPLS can contribute to congestion avoiding, load balancing and fast rerouting capabilities. With the implementation of traffic engineering, VoIP packets can be forwarded fast and efficiently. Especially, we put emphasis on the necessary components to provide such interactive and secure services. The three major parts in this architecture are described in detail, which includes the edge devices, access network, and MPLS core network. The necessary elements and requirements for these major parts are also described in details in this paper as well. The modified SIP registration and signaling process are proposed to give a global view of how this architecture functions well in achieving the security purpose and maintaining the QoS for the VoIP applications.

References

[1] F. L. Faucheur, B. D. L. Wu, S. Davari, P. Vaananen, R. Krishnan, P. Cheval, and J. Heinanen, "Multi-Protocol Label Switching (MPLS) Support of Differentiated Services," RFC 3270, May 2002.

[2] E. Rosen, A. Viswanathan, and R. Callon, "Multiprotocol Label Switching Architecture," RFC 3031, Jan. 2001.

[3] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, and W. Weiss, "An Architecture for Differentiated Services," RFC 2475, Dec. 1998.

[4] K. Muthukrishnan and A. Malis, "A Core MPLS IP VPN Architecture," RFC 2917, Sept. 2000.

[5] F. L. Faucheur and W. Lai, "Requirements for Support of Differentiated Services-aware MPLS Traffic Engineering," RFC 3564, July 2003.

[6] B. Goode, "Voice over Internet protocol (VoIP)," Proceedings of the IEEE, vol. 90, pp. 1495–1517, Sept. 2002.

[7] V. Fineberg, "A practical architecture for implementing end-to-end QoS in an IP network," IEEE Communications Magazine, vol. 40, pp. 122–130, Jan. 2002.

[8] D. Awduche, J. Malcolm, J. Agogbua, M. O'Dell, and J. McManus, "Requirements for Traffic Engineering Over MPLS," RFC 2702, June 1999.

[9] D. Katz, D. Yeung, and K. Kompella, "Traffic Engineering Extensions to OSPF Version 2," draft-ietf-ccamp-ospf-gmpls-extensions-09.txt, Dec. 2002.

[10] J. R. et al, "SIP: Session Initiation Protocol," RFC 3261, June 2002.

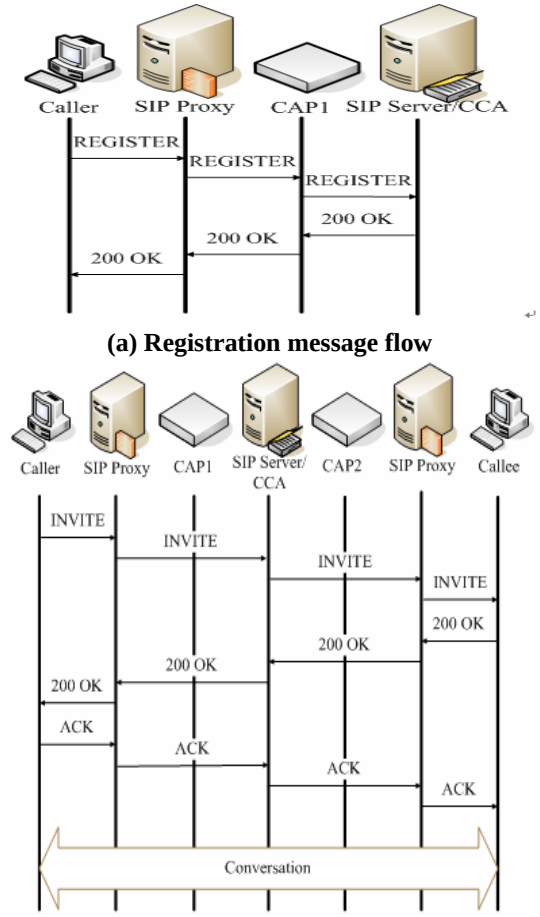
[11] C. G. G. C. Zhang, "TE-SIP server Design for a SIP-over-MPLS based network," ICCT (International Conference Communication Technology), Apr. 2003.

[12] Intel Corportation, "IXP 425 Software Development Kit, v4.0," http://developer.intel.com/design/network/products/n pfamily, Sept. 2004.

[13] Intel Corportation, "IXP 2400 Software Development Kit, v4.1," http://developer.intel.com/design/network/products/n pfamily, Apr. 2003.

[14] Intel Corportation, "IXP 1200 Software Development Kit, v2.0," http://developer.intel.com/design/network/products/n pfamily, Mar. 2001.

[15] M. H. et al, "SIP: Session Initiation Protocol," RFC 2543, Mar. 1999.



(a) Registration message flow

(b) Signaling message flow

Fig.3. Proposed SIP registration and signaling message flow

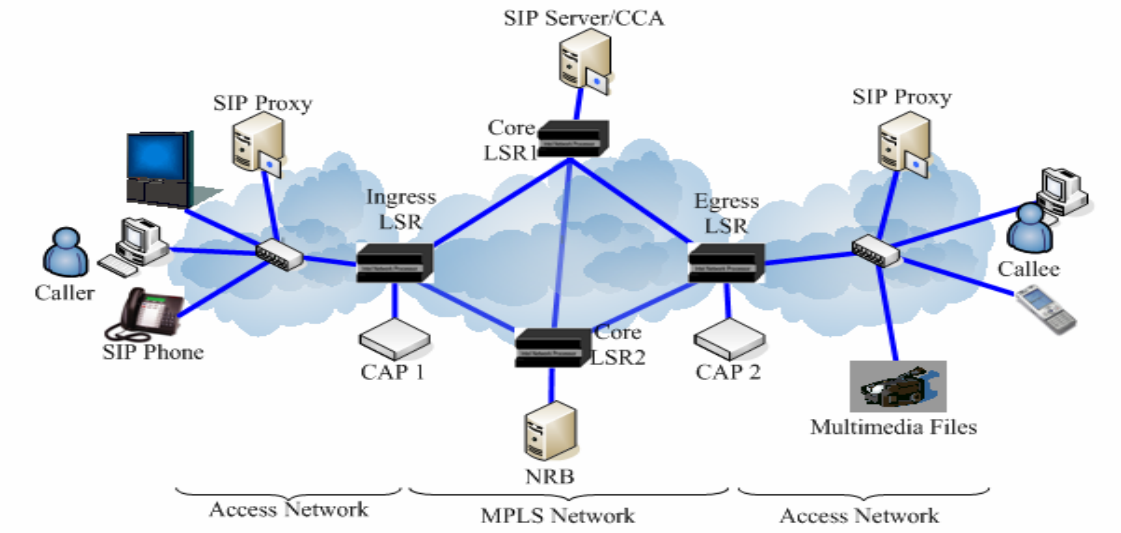


Fig.1. Proposed VoIP-over-MPLS SIP Architecture

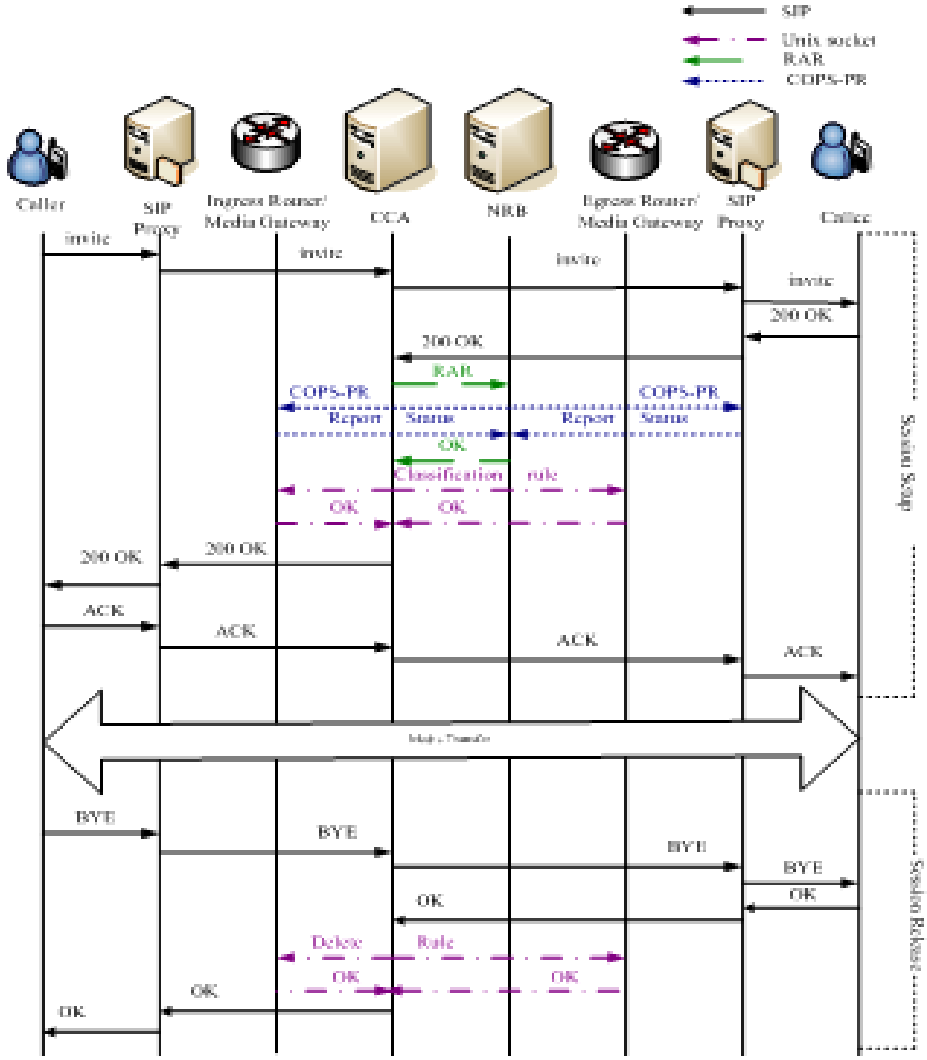


Fig.2.Interaction with MPLS network components and message flows