Network Working Group Y. Lee
Internet-Draft Comcast Cable
Expires: March 27, 2007 September 2006

Session Peering Use Case for Cable
draft-lee-speermint-use-case-cable-01.txt

Status of this Memo

Copyright Notice

Abstract

This document describes a typical use case of session peering in cable industry. Caller Alice makes a VoIP call to Callee Bob. Alice and Bob are served by two different cable operators, mso-o and mso-t. mso-o and mso-t have bi-lateral peering agreement to peer at SIP layer. This document focuses on the SIP layer interactions and discuss some common practices for Layer 5 Peering in cable industry.

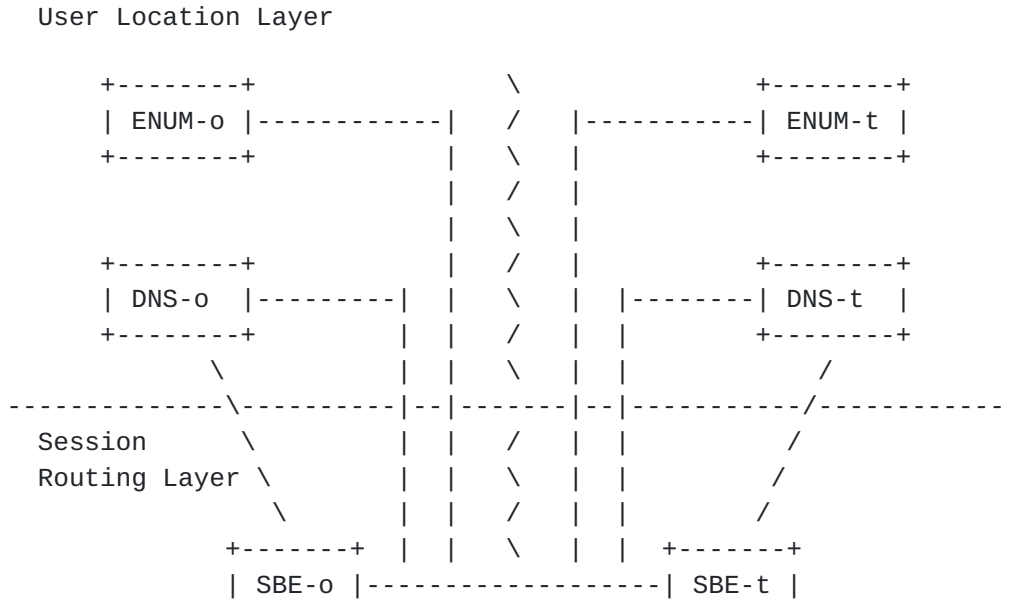
Table of Contents

1. Introduction

The purpose of this document is to outline the current best practice use case for establishing interconnection of MSO/Cable service Providers for delivery of SIP call termination over those interconnections. These interconnections are to establish real-time sessions between SIP servers at layer 5 network. While voice calls are the primary motivation for this today, other forms of real-time communications are and will continue to evolve as natural additions to such real-time sessions. This document depicts the network setup and the steps involved in the call flow from a caller in originating MSO network to a callee in another terminating MSO network, by using Call Routing data (CRD) [ID.speermint-terminology] obtained though ENUM services. The scenario is shown in the figure below; Alice calls Bob where Alice and Bob are served by two different cable operators, MSO-o and MSO-t, respectively. Both MSOs connect to an ENUM [ID.speermint-terminology] server that provides ENUM service. Both MSOs have full Layer 3 connectivity. We make no assumption whether they directly peer to each other or through any Layer 3 transit network. This document describes the Layer 5 Peering interactions when Alice calls Bob.

2. Terminology

Figure 1 shows the logical entities involved in peering.



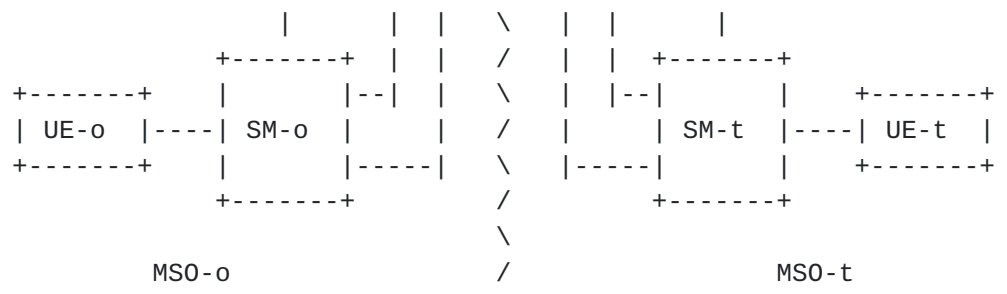


Figure 1

ENUM Server: An ENUM server stores the ENUM information and provides an interface for ENUM query for peering cable operators. The input to server is an E.164 number and the output is the NAPTR record. The ENUM client resolves the NAPTR record to formulate a sip URI associated to the input E.164 number. This ENUM server can be the Public ENUM server that hosts namespace "e164.arpa" [ID.speermint-terminology] or Infrastructure ENUM server that hosts namespace "(i)e164.arpa" [ID.enum-infrastructure].

Using Public or Infrastructure ENUM is a business decision. Some cable operators MAY deploy Infrastructure ENUM for peering in the initial stage and migrate to Public ENUM when they see the need. In this document, the only technical requirement for the ENUM server is that it can return the associated NAPTR that can be resolved to a sip URI of the users for peering.

Originating ENUM (ENUM-o): The ENUM server in the originating network.

Terminating ENUM (ENUM-t): The ENUM server in the terminating network.

In Figure 1, although we did not show any connection between ENUM-o and ENUM-t, these two entities has a trusted relationship and MUST provide a mechanism to synchronize the ENUM data. The synchronization mechanism can be a simple manual flat file transfer via sftp. Or, it can be more sophisticated and automated mechanism [ID.enum-validation-epp]. In this context, we assume that any ADD/DELETE/MODIFY of the any ENUM record in one ENUM database that affects the peering relationship MUST synchronize to the peer ENUM server.

DNS [RFC1034]: DNS resolves the domain part of the sip URI to an IP address so that SM or SBE can route the Request and Response to the target.

Originating DNS (DNS-o): The DNS server in the originating network.

Terminating DNS (DNS-t): The DNS server in the terminating network.

Similar to ENUM servers, we did not show the connection between DNS-o and DNS-t. We assume that any ADD/DELETE/MODIFY of any DNS resource record in one DNS server that affects the peer to locate the target Signaling Path Border Element(SBE) MUST synchronize to the peer DNS server.

Session Manager (SM): A SM is the entity responsible for sending and receiving the SIP messages from or to Signaling Path Border Element (SBE). It is also responsible for locating the user home proxy. SM is logical, it MAY contain one functional entity or multiple functional entities. For example, SM can be the P-CSCF, I-CSCF and S-CSCF defined in IMS [23.228]. SM can also be the Call Manager Server (CMS) defined in PacketCable (PC) 1.5 [PC1.5].

Originating SM (SM-o): The SM originates the call. In this content, it is Alice's SM.

Terminating SM (SM-t): The SM terminates the call. In this content, it is Bob's SM.

Signaling Path Border Element (SBE): A SBE [ID.speermint-terminology] is the entity that peers to the external. In this context, it is the border element that speaks SIP inside and outside the MSO network. It also enforces peering policies.

To protect the communication channel between the two SBEs, SBE MUST support TLS [RFC2246]. If the channel is secured by other security mechanisms such as IPSec [RFC4301], or if the two SBEs peer directly via dedicated private circuit, the MSOs MAY decide NOT to use TLS because it is protected at the lower layer.

Optionally, SBE MAY provide additional functions such as Topology Hiding Interworking Gateway function (THIG), Network Address Translation (NAT) function, and SIP header normalization.

Originating SBE (SBE-o): The SBE connects the SM-o and the remote SBE.

Terminating SBE (SBE-t): The SBE connects the SM-t and the remote SBE.

User Endpoint (UE): User Endpoint is the client that makes or receives calls. UE can be sip based or non-sip based. For non-sip based UE, SM acts as a signaling gateway and translates the non-sip signaling to sip signaling before sending to SBE.

Originating UE (UE-o): Alice's UE.

Terminating UE (UE-t): Bob's UE.

3. User Setup

Alice signs up a VoIP service with MSO-o. MSO-o assigns her a globally unique E.164 number +1-215-111-2222. Also, MSO-o assigns her an ENUM entry where +1-215-111-2222 maps to NAPTR record that formulates sip URI <sip:alice@mso-o.com>. For Public ENUM, the E.164 number is in namespace e164.arpa. If MSO-o supports only Infrastructure ENUM for peering, the E.164 number is in namespace ie164.arpa.

Bob signs up with MSO-t and his globally unique E.164 number is +1-212-333-4444. MSO-t assigns him an ENUM entry where +1-212-333-4444 maps to a NAPTR record that formulates sip URI <sip:bob@mso-t.com>. For Public ENUM, the E.164 number is in namespace e164.arpa. If MSO-t supports only Infrastructure ENUM for peering, the E.164 number is in namespace ie164.arpa.

4. Network Setup

In Figure 1, we divide the diagram into 2 layers: (1) User Location Layer and (2) Session Routing Layer. User Location Layer is responsible for locating the network serving the terminating UE. It includes ENUM server and DNS server. Each of them provides different services.

ENUM server accepts an E.164 number as input and returns a NAPTR record to the ENUM client as output. ENUM client parses the regular expression and formulates the sip URI associated to the input E.164 number. DNS server accepts a FQDN as input and returns either a SRV record [RFC2782] or an A Resource Record as output. In the diagram, SM has the interface to interact with both ENUM and DNS servers. SBE has the interface to interact with DNS server only.

The actual SIP routing happens in the Session Routing Layer. It includes UE-o, SM-o, SBE-o, UE-t, SM-t and SBE-t. UE-o and UE-t are sip clients which can make VoIP call.

SM-o and SM-t are the home SIP proxies to UE-o and UE-t. SM-o and SM-t are enable to perform normal SIP routing operations defined in [RFC3261]. In addition, it has an interface to access user profile

data associated to the registered user for authentication and authorization. They also have ENUM and DNS clients built-in. They can

issue ENUM query and formulate URI from the NAPTR records. SM makes routing decision based on the user profile information and the request URI.

SBE-o and SBE-t are the peering proxies where the actual peering happens. SBE-o connects the SM-o to the remote SBE-t. SBE-o is the last point in MSO-o's domain. SBE-o is responsible for establishing the peering relation to SBE-t. MSO-o and MSO-t SHOULD have signed bi-lateral agreement. All the necessary peering policies and security measurements such as THIG function and NAT function SHOULD be performed in SBE. In the diagram, SIP messages flow between:

(UE-o)<->(SM-o)<->(SBE-o)<->(SBE-t)<->(SM-t)<->(UE-t)

We do not show the media in the diagram. Media can flow from UE-o to UE-t directly or through some media proxy/gateway for NAT or media transcoding.

5. Call Setup

Alice is a user served by MSO-o. She has a sip phone registered to SM-o. She has an E.164 number +1-215-111-2222 and a public sip URI <sip:alice@mso-o.com>. She picks up the phone and calls Bob. She enters Bob's TN number +1-212-333-4444 into her key pad. Alice UE-o initiates an INVITE with Bob's global unique tel URI [RFC3966] which is <tel:+1-212-333-4444> in the request URI.

SM-o receiving the SIP INVITE SHOULD process it according to the following logic:

1. Perform an ENUM query on the called party in the SIP request URI.

2. If the ENUM server fails to return the response, SM-o forwards the call to PSTN.

3. ENUM server returns a NAPTR record. SM-o parses the regular expression and formulates the sip URI of Bob which is <sip:bob@mso-t.com>.

4. SM-o finds out that it does not own "mso-t.com". SM-o has local policies to send the request to SBE-o.

5. SM-o sends a DNS query to locate SBE-o s IP address.

6. DNS returns SBE-o s IP address to SM-o. SM-o sends the SIP INVITE to SBE-o. SM-o MAY choose to record-route to stay on the signaling path.

7. SBE-o receives the SIP INVITE. It examines the request URI and sends a query to DNS server to get the IP address of Bob s domain "mos-t.com".

8. SBE-o performs all the necessary operations such as sip header normalization and THIG function and sends the INVITE to SBE-t. Optionally, SBE-o MAY act as a SIP Back-to-Back User Agent (B2BUA). This is necessary when SBE-o provides NAT function or IP version translation function. Section 7.2 and 7.3 describes the steps.

9. SBE-t receives the INVITE. It examines the request URI to verify the domain is one of its serving domains. If it is, SBE-t will forward the INVITE to SM-t that has access to Bob's user data to locate Bob s home proxy. If not, SBE-t generates the proper SIP error response and forwards it to SBE-o.

Based on the user profile information, SM-t MAY re-write the request URI to something more location specific. For example, SM-t knows that Bob's home proxy is the San Jose proxy, so it re-writes the request URI to <sip:bob@sanjose-proxy.mso-t.com> to the INVITE and deliver the message to the San Jose proxy directly. This location service is internal to the domain. MSO-t MAY use internal DNS or some other proprietary methods to retrieve the location information. MSO-t chooses the method best fit to the internal architecture.

If SM-t fails to locate the user, SM-t will generate the proper sip error response to SBE-t at which will propagate the error response to SBE-o. Upon receiving the error response, based on the MSO-o s routing algorithm, SM-o MAY forward the call to PSTN to complete the call.

10. SM-t receives the SIP INVITE. SM-t contains the registration information of Bob s UE-t. This is the home proxy which hosts the contact information of Bob s UE-t. SM-t forwards the SIP INVITE request to UE-t.

11. Bob's UE-t receives the SIP INVITE request. Bob accepts the call. UE-t sends the 200OK and Alice acknowledges it.

12. Alice and Bob starts 2-way conversation.

Figure 2 illustrates the message interactions:

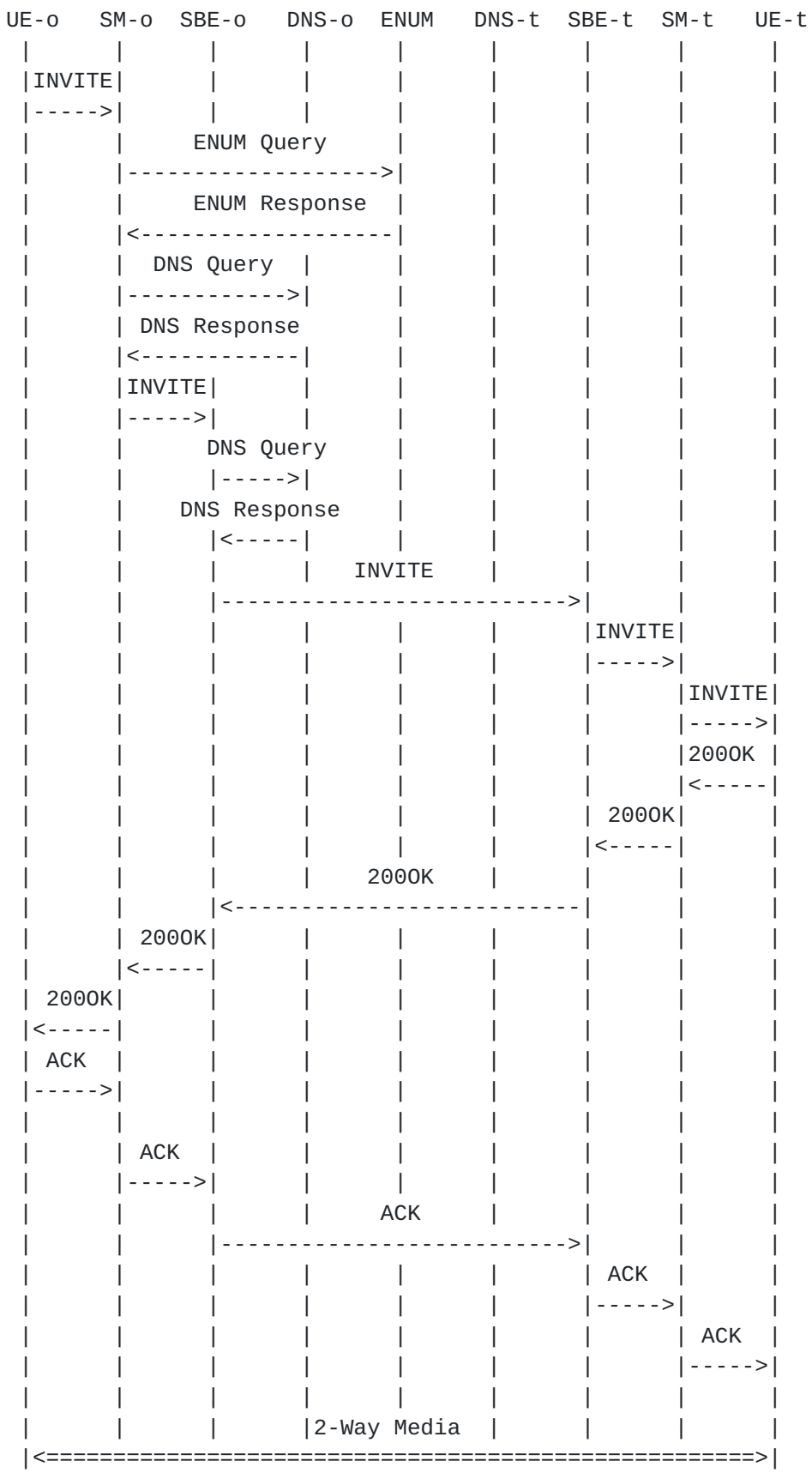

UE-o
SM-o
SBE-o
DNS-o
ENUM
DNS-t
SBE-t
SM-t
UE-t
INVITE
ENUM Query
ENUM Response
DNS Query
DNS Response
INVITE
DNS Query
DNS Response
INVITE
INVITE
200OK
200OK
200OK
ACK
ACK
ACK
2-Way Media

Figure 2

6. User Location Layer

In the call flow shown in Figure 2, when SBE-o receives the SIP INVITE request from SM-o, SBE-o queries DNS to resolve the IP address of the domain "mso-t.com". SBE-o MAY choose not to query DNS server to resolve "mso-t.com". By examining the domain part of Bob's sip URI, SM-o knows that "mso-t.com" is one of its trusted peer. In many cases, SBE-o's configuration will have static configuration pointing to a static IP address associated to SBE-t. There is number of reasons to have this setup. Most common reason is security such that SBE-o only peers to the pre-configured IP address. In this setup, SBE-o MAY skip querying DNS to resolve the domain name of the remote target. That said, it does not stop SBE-o to use DNS to resolve the domain name.

Only SM has an interface to ENUM server to resolve the E.164 number to sip URI. When SM-o queries the ENUM server and realizes that Bob resides in a different domain, SM-o will re-write the request URI from Bob's sip URI before sending the request to SBE-o.

When SBE-o sends a query to the DNS for "mso-t.com", it MAY return an A-record or a SRV record of SBE-t. Hence, SBE-o MUST prepare to accept a SRV record and try to reach the available SBE-t in the returned list. Once SBE-o selects a SBE-t, it SHOULD stick with the same SBE-t for the duration of the call. This is important because peering policies MAY vary from session to session. So, SBE-t will contain the peering state of that particular session.

7. Session Routing Layer

Session Routing Function performs generic SIP routing function. With regard to session peering in cable environment, there are few specific functions that cable operators MAY consider to support.

7.1 Number Probability

[RFC3482] describes the overview of E.164 telephone number portability (NP) which allows telephony subscribes to carry their

numbers to any service provider. Since NP impacts the call routing decision algorithm, additional NP-related information is required to

carry in the request URI for making routing decision. [ID.iptel-tel-np] defines the necessary NP-related information in the tel URI.

For VoIP peering, when SM-o receives a call setup request from UE-o and decides to route the call to PSTN due to routing policies, SM-o requires the NP information in order to route the call if the target number is ported. Consider the User Setup stated in Section 3 with the following modification:

> Bob s geographical telephone number is "+1-212-333-4444" and is ported to "+1-212-999-0000".

Assume that this information has been provisioned in the ENUM-o. When SM-o queries ENUM-o for +1-212-333-444, ENUM-o will return both Bob s sip URI and tel URI with the NP information:

- sip:bob@mso-t.com
- tel:+1-212-333-4444;npdi;rn=+1-212-999-0000

Based on SM-o routing decision algorithm, if MSO-o decides to complete the call via PSTN, SM-o will have the necessary NP information in Bob s tel URI.

7.2 Topology Hiding Interworking Gateway Function

In the case SBE-o performs THIG. PP-o SHOULD remove the proxies written in Via and Record-Route headers and replace itself to the Via and Record-Route headers. When SBE-o sends a message to SBE-t, it will look the same as SBE-o is the only proxy in MSO-o. Similarly, when SBE-t sends a message to SBE-o, the message will look the same as SBE-t is the only proxy in MSO-t. Alternately, SBE-o MAY act as B2BUA such that it is the UAC to the peer.

7.3 Network Address Translation Function

In Figure 2, we assume that the UE-o and UE-t use public routable IP addresses so that they can establish direct peer-to-peer 2-way conversation. However, some cable operators use [RFC1918] addresses for their UEs. Since those addresses are not routable outside its domain, UE-o and UE-t require some way to perform NAT function. NAT is problematic in SIP. Detailed description can be found in [RFC3489]. The NAT function can happen in two places, it can happen in either the edge layer or the network layer. Either way, the network MUST pass the NAT information to the session layer. This requires some form of communications between the session layer and

network layer. There are several protocols [RFC3489, ID.behave-turn, ID.mmusic-ice] being worked out in IETF.

If UE is aware of NAT, it will be responsible for putting the public transport address in the SIP/SDP. UE MAY use ICE [ID.mmusic-ice] to discover the best possible way such as STUN [RFC3489] or TURN [ID.behave-turn] to overcome NAT. However, this requires both UEs to support ICE. ICE runs a STUN server per transport address, this adds significant load to UE. In today cable environment, the most common UE is the Embedded Media Termination Adaptor (eMTA), they have limited memory and processing power, so they MAY require hardware upgrade to support ICE.

If UE is unaware of any NAT, it will simply put its [RFC1918] address in the SIP/SDP and sends the SIP message to SM. It relies on the network to perform the NAT function. Consider a UE-o wants to make a call to UE-t, UE-o uses [RFC1918] address. In this setup, the originating MSO-o is responsible for NAT function. The NAT function MAY happen in the access network or at the network border. Regardless where it happens, MSO-o MUST replace the [RFC1918] address in the session layer before sending the SIP message to MSO-t. MSO-t also needs to relay the media packets before sending the traffic to UE-t. Since it is not well defined how to pass the NAT information between network layer and session layer, most cable operators chooses SBE to perform the NAT function. Figure 3 shows the network setup.

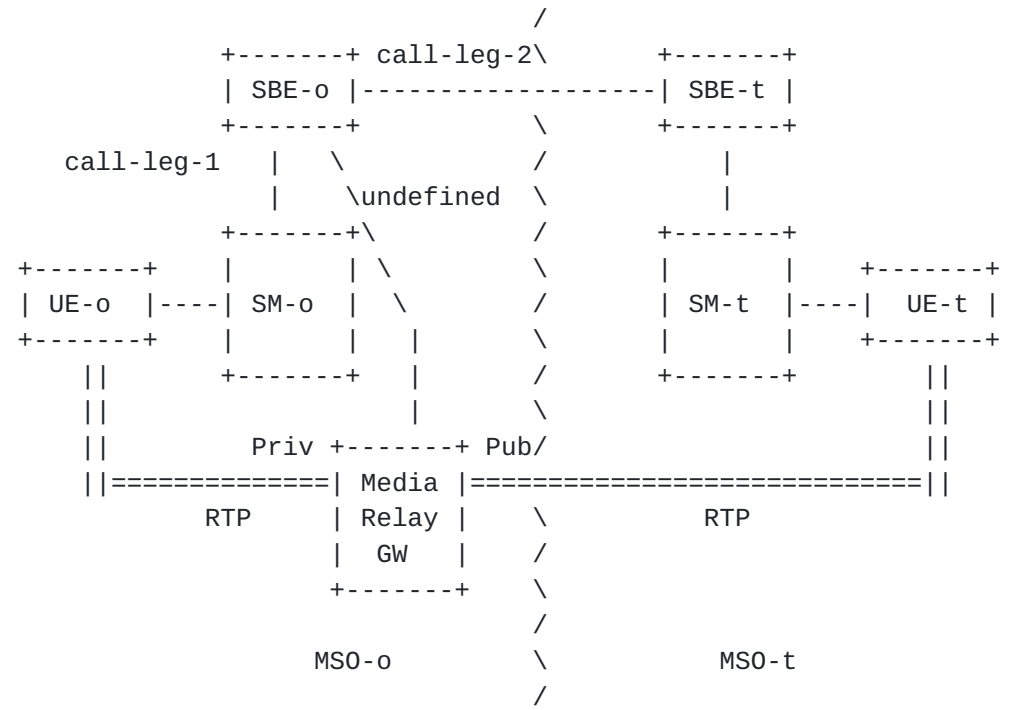


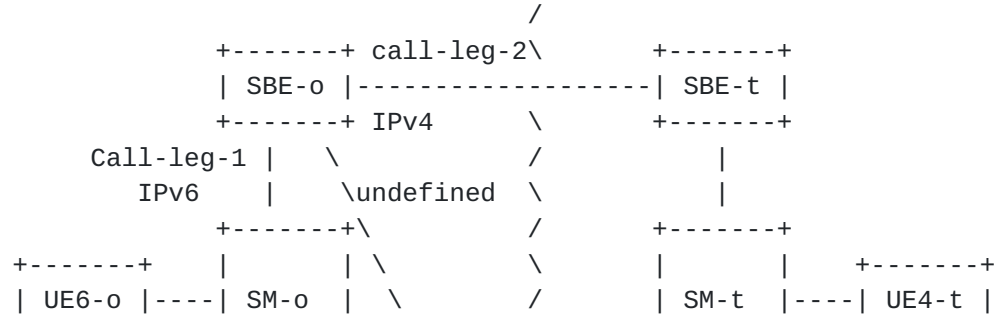
Figure 3

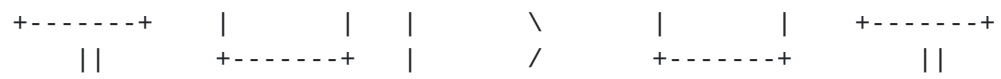
In this setup, SBE-o acts as a B2BUA. When SBE-o receives the SIP INVITE request, it terminates the INVITE (Call-Leg-1) and creates a new INVITE (Call-Leg-2) to relay the header information to MSO-t. SBE-o creates the Private-to-Public address binding between the internal and external networks and perform any necessary address translation in the SIP header. The address translation of signaling happens in SBE-o, the address translation of media MAY happen in a different physical entity. To allow this, SBE-o and the Media Relay Gateway require to exchange Private-to-Public address binding information. UE-o sees SBE-o the UAS and forwards all the SIP messages to SBE-o. UE-t sees SBE-o the UAC and forwards all the SIP messages to SBE-o. Media passes through the Media Relay Gateway in MSO-o for NAT binding for the media stream.

7.4 IPv4/IPv6 Interworking Function

Some cable operators are actively working on IPv6 [RFC1883]. This allows an IPv6 device to register to SM. Many UEs in the market support IPv4/IPv6 dual stacks. During provisioning, the cable operator MAY offer IPv4, IPv6 or both addresses to it. For the discussion here, we restrict that a UE can choose to register with either an IPv4 or an IPv6 address [RFC3483]. In other words, a UE can only register to SM with one IP address, either an IPv4 or an IPv6 address. During IPv4/IPv6 transition [RFC2893], the cable operator which runs IPv4/IPv6 dual stacks (MSO6) will probably peer with many IPv4 only peers. When setting up sessions with them, MSO6 MUST perform all the necessary translations inside the MSO6 s network. IPv4 peer cable operator (MSO4) does not understand IPv6 address. From the MSO4 point of view, it sees MSO6 an IPv4 network.

Consider an example, an IPv6 device (UE6-o) wants to make a call to an IPv4 device (UE4-t). UE6-o registers to a cable operator which runs dual stacks (MSO6-o). UE4t registers to an IPv4 cable operator (MSO4-t). Figure 4 shows the network setup.





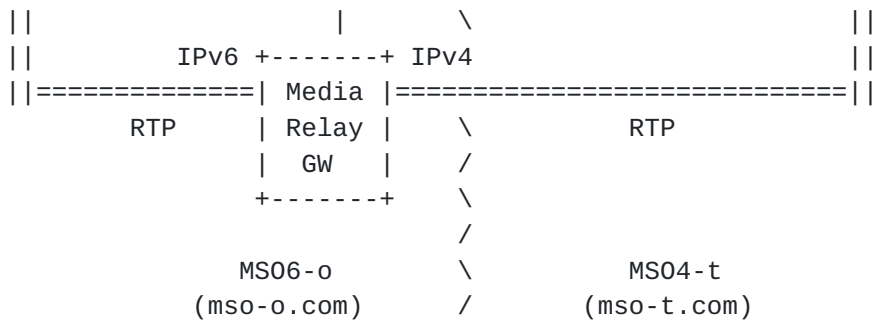


Figure 4

To form a session between UE6o and UE4t, MSO6-o MUST translate UE6-o s IPv6 address to an IPv4 address. This translation is similar to NAT function discussed in Section 7.2. SBE-o performs any necessary IPv6-to-IPv4 address translation. When SBE-o receives the INVITE from SM-o, it sends a DNS query for domain "mso-t.com". Since MSO4-t supports only IPv4, the DNS will return an IPv4 address to SBE-o. Upon receiving the response, SBE-o realizes that it needs to perform IPv4/IPv6 interworking function. SBE-o allocates IPv4 addresses and ports from its IPv4 address pool and creates the IPv6-to-IPv4 address binding. It also instructs the Media Relay Gateway to do the same for media relay.

8. Future Works

This document illustrates a simple use case for session peering in cable industry. We describe the major entities that participate the peering. We also outline the high-level interactions between these entities. From the interactions, we see some areas for future work.

- Peering Policy

- User Location Service

- Peering Security

- Peering QoS

- Peering Accounting and Billing

8.1 Peering Policy

Currently most of the peering policies are local to the domain and statically configured. There MAY be needs for the two trusted peers

to exchange peering policies. These need further investigation in the working group.

8.2 Peering Location Function

ENUM and DNS provide a way to locate the peering point of a peer domain. Once the request enters the home domain, SM uses [RFC3263] to locate the next-hop proxy of the target. There MAY be needs to provide more sophisticated information than what ENUM and DNS provide today. This is future item for the working group.

8.3 Peering Security

There are existing security mechanisms today to ensure peer authentication. Most current peering deployments use TLS or other similar mechanism to ensure security channel. SBE MUST support TLS for transport. When two MSOs peer via an untrusted connection, SBE MUST use TLS. For the TLS, client certification MUST be supported. SIP-level domain validation for certification SHOULD be used for untrusted connection if the two SBEs peer directly together at Layer-5.

This MAY not scale well when an operator tries to peer with few hundred peers. This happens for cable operators provide peering service to large numbers of enterprise customers. Peering security is a working item for the working group.

8.4 Peering QoS

Even thought we do not discuss media QoS in the use case, media QoS most impacts the user experience. For some critical services, guaranteed media QoS is a MUST. SIP has defined a framework for pre-condition in SIP [RFC3312, RFC4012]. This framework is for the UA to request end-to-end QoS for media. But, it is unclear how to propagate the session information to the lower network layer when a QoS media session is needed. This requires collaborate effort between working groups to identify the requirements.

8.5 Peering Accounting and Billing

In today PSTN peering model, two cable operators compare the outbound minutes for accounting. For Internet peering, they compare the total bandwidth of outbound traffic for accounting. For session peering, it is unclear what is the right model for accounting and billing.

Session peering is similar to Internet service, the PSTN peering accounting model MAY not fit very well. Today, most cable operators do not charge users for per minute usage for Internet. Instead, they charge them for bandwidth usage. For the Internet peering accounting model, since signaling and media can possibly travel in two different paths, signaling itself does not necessary convey the accurate bandwidth usage to the cable operators.

9. Security Considerations

Security is a major area for session peering. We MUST prevent unauthenticated peer from making calls to the network and protect the network from DoS attack at session layer. A lot of security work has been done on other working groups to ensure channel security and user authentication. We SHOULD evaluate them and develop some recommendations to the working group.

10. IANA Considerations

This document has no IANA considerations.

11. Acknowledgements

Special thanks go to Gaurav Khandpur, Tom Creighton, Jason Livingood and Jean-François for their valuable input to this documents

12. References

12.1 Normative References

[ID.behave-turn] Rosenberg, J., Mahy, R. and Huitema, C., "Obtaining Relay Addresses from Simple Traversal of UDP Through NAT (STUN)", I-D draft-ietf-behave-turn-01, February 2006.

[ID.enum-validation-epp] Hoeneisen, B., "ENUM Validation Information Mapping for the Extensible Provisioning Protocol", I-D draft-ietf-enum-validation-epp-03.txt, February 2006.

[ID.enum-infrastructure] Livingood, J., Pfautz, P. and Stastny, R., "The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation

Discovery System (DDDS) Application for Infrastructure ENUM", I-D draft-ietf-enum-infrastructure-00, February 2006.

[ID.iptel-tel-np] Yu, J. "Number Portability Parameters for the "tel URI", I-D draft-ietf-iptel-np-11, August 2006.

[ID.mmusic-ice] Rosenberg, J., "Interactive Connectivity Establishment (ICE): A Methodology for Network Address Translator (NAT) Traversal for Offer/Answer Protocols", I-D draft-ietf-mmusic-ice-10, August 2006.

[ID.speermint-terminology] Meyer, D., "SPEERMINT Terminology ", I-D draft-ietf-speermint-terminology-06.txt, September 2006.

[RFC1034] Mockapetris, P., "Domain Names Concepts and Facilities", RFC 1034, November 1987.

[RFC1883] Deering, S. and Hinden, R., "Internet Protocol, Version 6 (IPv6) Specification", RFC 1883, December 1995.

[RFC1918] Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G. J. and Lear E., "Address Allocation for Private Internets", RFC 1918, February 1996.

[RFC2782] Gulbrandsen, A., Vixie, P. and Esibov, L., "A DNS RR for Specifying the location of services (DNS SRV)", RFC 2782, February 2000.

[RFC2893] Gilligan, R., "Transition Mechanisms for IPv6 Hosts and Routers", RFC 2893, August 2000.

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., COarks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.

[RFC3263] Rosenberg, J. and H. Schulzrinne, "Session Initiation Protocol (SIP): Locating SIP Servers", RFC 3263, June 2002.

[RFC3312] Camarillo, G., Marshall, W. and Rosenberg., J., "Integration of Resource Management and Session Initiation Protocol (SIP)", RFC 3312, October 2002.

[RFC3403] Mealling, M., "Dynamic Delegation Discovery System (DDDS) Part Three: The Domain Name System (DNS) Database", RFC 3403, October 2002.

[RFC3482] Foster, M., McGarry, T. and Yu, J., "Number Portability in the Global Switched Telephone Network (GSTN): An Overview", RFC 3482, February 2003.

[RFC3483] Draves, R., "Default Address Selection for Internet Protocol version 6 (IPv6) , RFC 3483, February 2003.

[RFC3489] Rosenberg, J., Weinberger, J., Huitema, C. and Mahy, R., "STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)", RFC 3489, March 2003.

[RFC3966] Schulzrinne, H., "The tel URI for Telephone Numbers", RFC 3966, December 2004.

[RFC4032] Camarillo, G. and Kyzivat, P., "Update to the Session Initiation Protocol (SIP) Preconditions Framework", RFC 4032, March 2005.

12.2
Informative References

[23.228] 3GPP TS 23.228 V7.6.0, "IP Multimedia Subsystem (IMS); Stage 2 (Release 7)", March, 2006.

[PC1.5] CableLabs, "PacketCable 1.5 Architecture Framework Technical Report" PKT-TR-ARCH1.5-V01-050128, January, 2005.

[RFC2246] Dierks, T. and Allen, C., "The TLS Protocol Version 1.0", RFC 2246, January 1999.

[RFC4301] Kent, S. and Seo, K. "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

Authors Addresses

Yiu L. Lee
Comcast Cable Communications
1500 Market Street,
Philadelphia, PA 19102
US

Phone: +1-215-320-5894
Email: yiu_lee@cable.comcast.com

Intellectual Property and Copyright Statements

Intellectual Property Statement

made any independent effort to identify any such rights. Information

on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.