Session PEERing for Multimedia
INTerconnect
Internet-Draft
Expires: March 8, 2007

M. Haberler
IPA
M. Hammer
Cisco
O. Lendl
enum.at

September 4, 2006

A Federation based VoIP Peering Architecture
draft-lendl-speermint-federations-03

Status of this Memo

Copyright Notice

Abstract

This document defines the federation concept and proposes a peering and routing architecture for SIP-based applications. Federations can be used to establish selective peerings e.g. in the Voice over IP and Instant Messaging space. Service providers may announce federation membership as domain attributes. This document contains the policy-

type definition for federations within the Domain Policy DDDS Application.

Table of Contents

1. Terminology

This document uses the terminology as defined in draft-ietf-speermint-terminology-00 [1].

The acronym VSP will stand for "VoIP Service Provider".

Our definition of VSP encompasses commercial service providers as well as enterprises and end user operating their own SIP [4] proxy.

2. Introduction

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [3].

The domain policy DDDS application [2] defines a generic method how a domain owner may announce the conditions to accept incoming communications. This documents defines the policy-type for publishing federation membership.

This document focuses on the use of federations for SIP peering. The same mechanism may be applied to other application protocols as well. The difference is in the protocol field of the service parameter in the NAPTR records.

3. Federations

The proposed method is based upon the concept of a "Federation". A federation is defined as follows:

A Federation is a group of VoIP service providers which
* agree to accept calls from each other via SIP,
* agree on a set of administrative rules for these calls

(settlement, abuse-handling, ...), and
* agree on rules for the technical details of the interconnection.

The actual rules are private to the federation and need not be published. Federation members are expected to know and abide by these rules.

Federations are identified by URIs. It is RECOMMENDED that federations use URLs as identifiers which point to documents describing the federation.

For the purposes of the domain policy DDDS application, federation identifiers are opaque strings. The only operations performed on these identifiers are string comparisons. If the identifier is in the form of an URL, the document referred to by that URL is never evaluated during the basic peer discovery process.

The federation named "urn:ietf:rfc:3261" stands for the public Internet. A SIP service provider who announces his membership in "urn:ietf:rfc:3261" will accept calls as defined in the generic SIP RFC [4].

Any VSP can be a member in multiple federations.

Federations as defined by this document may map to industry alliances or other incorporated entities. This does not need to be a 1:1 relationship, though: Any alliance can sponsor multiple federations and there is no requirement that a federation needs a corporate backer.

Examples:

- A group of VoIP service providers forms an association and agrees to accept calls from each other via the public Internet provided the TLS transport is used for SIP signalling and members present a valid X.509 cert signed by the association's certificate authority.

- A group of VoIP service providers build a Layer 3 network for VoIP peering ("walled garden", e.g. similar to the 3GPP GRX network).

They agree to accept calls from all participants in that network and settle through a clearinghouse.

- A group of VoIP service providers agree to accept calls originating from from each other. They use firewall rules to block calls from all other networks.

- Peering fabric based on SIP: A SIP hub acts as a forwarding proxy between participants. Intra-federation calls are to be routed through the SIP hub.

- Peer to Peer SIP clouds: P2P SIP proposes an alternative resolution method based on distributed hash tables (DHT). The set participants in each such DHT can be seen as a federation whose technical rules stipulate the URI resolution via the DHT ring.

4. Federation based Routing

This section outlines how the federations concept relates to the Speermint routing architecture.

4.1. Assumptions

Many VSPs will prefer not to run open SIP proxies and accept calls from the public Internet.

Some VSPs will establish private peerings between each other.

Groups of VSPs will enter into mutual peering agreements. In other cases, third parties might build such peering fabrics as a service.

Both private peerings and such peering fabrics are federations as defined by this document.

VSPs might choose to join several federations if it suits their business strategy. This set of federations defines the range of destination VSPs reachable with a direct SIP connection.

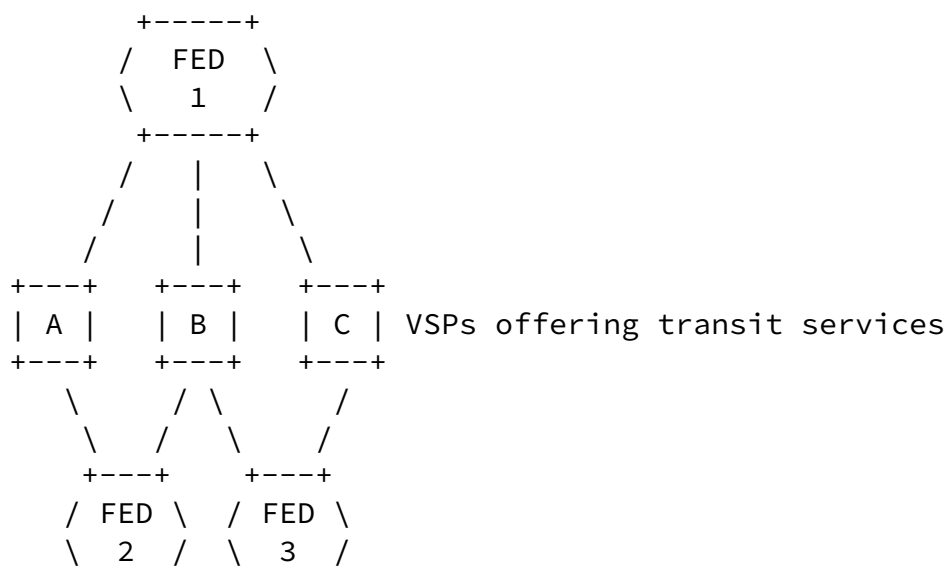
VSPs which are members of multiple federations may choose to provide transit services to other VSPs. Such VSPs act as bridges between

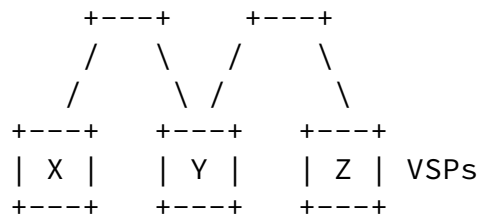
federations.

On the other hand, the VSPs who decline to join many federations might choose to buy transit from VSPs which offer such services.

4.2. Call Flows

To visualize the possible call flows we use the following set of VSPs and federations:





X, Y, and Z are terminating VSPs which serve as SIP providers for end-customers. A, B, and C are VSPs offering transit into a federation to members of other federations.

4.2.1. Direct Intra-federation calls

Calls from customers of X to customers of Y can be passed directly according to rules of federation 2. Transit is not required.

Details how X passes traffic to Y are internal to federation 2 - it could be end-to-end or, for example, through a SIP hub.

4.2.2. Single-transit Inter-federation calls

Calls from X to Z need to traverse a third VSP as X and Z do not share a common federation. B shares federations with X and Z, thus it can bridge calls between X and Z. VSP X thus may elect to enlist the help of B to complete calls to Z.

On a high level this call is the combination of two intra-federation call legs - one within FED2 from X to B, and one within FED3 from B to Z. If FED2 and FED3 share the same Layer 3 network, then the RTP stream may well be end to end (X to Z directly). If not (e.g. FED3 employs a private network), then B needs to provide media relay service as well.

4.2.3. Multiple-Transit calls

If B is not available, calls from X to Z need to traverse via FED2 to A, then via FED1 to C, and finally via FED3 to Z. Now there are three segments in the call.

4.3. Procedures

The basic call flow is as follows (this is an extension to draft-mahy-speermint-direct-peering):

1. If number-based dialing is used, then the initiating VSP converts the dial-string to a fully qualified E.164 number and retrieves a SIP URI through User ENUM and/or Infrastructure ENUM.

2. The initiating VSP performs the Domain Policy DDDS Application [2] and thus retrieves the set of federation of the target VSP. If source and destination VSP share a federation then the call is established according to its rules. The destination VSP can use non-terminal NAPTRs in his policy announcements to indicate that he has contracted another VSP to provide transit services towards him. In that case, the originating VSP repeats this step in the algorithm in order to find shared federations with the transit providing VSP.

3. If either no Domain Policy records were found, or the target announces its membership in the predefined "urn:ietf:rfc:3261" federation, then the standard SIP procedures (RFC 3261 [4] and RFC 3263 [5]) can be used to complete the call. The former case is the fallback scenario if the target VSP has not adopted the Domain Policy framework.

4. If no common federation is found, the initiating VSP may choose to enlist the help of a transit VSP on his side. The call to the transit VSP follows normal federation rules. See the next section for details how a suitable transit VSP is selected.

5. For number-based dialing: if no path can be found through either a common federation or any transit VSP, then the originating VSP may fall back to PSTN delivery. Thus, the PSTN may be viewed as just another "default" federation where all VSPs using E.164 numbers and having PSTN connectivity are members.

4.4. Routing Architecture

For the direct intra-federation call, it is sufficient to match the federation memberships of the initiating and destination VSP. This matching can be achieved through the domain policy DDDS application.

While direct matching of federations enables direct peering, it does

not solve the universal reachability problem.

In the general case, a routing algorithm is needed: Once the source VSP does not share a common federation with the destination VSP the source VSP needs select a transit VSPs. This transit VSP in turn needs to make a routing decision.

The "next hop" selection is akin to other routing problems, thus similar approaches can be used. In some way, topology information beyond the next hop needs to be communicated between VSPs. Other than in IP (layer 3) routing, announcements need not exclusively be learned from adjacent nodes and can be published through other means since IP connectivity can be assumed.

Non-terminal NAPTRs in the Domain Policy DDDS can be used by the destination VSP to publish a list of VSPs which provides transit services towards that network. If one assumes that a multi-tier hierarchy of VSPs will emerge (similar to the current PSTN or Internet one), then such referrals point up the hierarchy on the destination side. If the source VSP is a major carrier then climbing up the hierarchy ladder on the destination side will likely lead to a known peer.

If the call originates within a small VSP then he might not find a common federation with one of the major VSPs the destination (directly or indirectly) refers to. He will need to hand the call to some larger VSP which he pays to connect him to the major transit networks.

This document does not propose a routing protocol for that. The following options are intended to stimulate discussions in the SPEERMINT working-group.

4.4.1. Static configuration

For small VSPs this can be simple choice: everything that cannot be handed off to the destination network directly is relayed to a default transit provider.

4.4.2. Forward Search

Another option is to follow the referrals up the hierarchy on the source side, too. Any VSP can do this offline to learn the set of VSPs and thus the range of federations that are reachable via the VSPs it has contracted to provide transit service.

Walking the domain policy referrals generates a tree of VSPs which

are all willing to pass calls from/to the root of the tree. Building these trees both for the source and the destination VSP and then checking for shared VSPs (or federations) between these two trees will find a valid path if the top-tier VSPs peer amongst each other.

4.4.3. Route Announcements

SIP messages between federation members could be used to distribute reachability information. To use the above example:

If X buys transit from B then X might subscribe to a "topology" event package with B. Using NOTIFIES, B may announce to X its reachable federations.

The same mechanisms can be used amongst transit VSPs (e.g. in federation 1) to exchange reachability information. VSP A could learn through a NOTIFY from C that C is a member of FED3.

5. Policy-Type template

Policy Type: "fed"

URI Scheme(s): Any URI is allowed.

Functional Specification: The URI acts purely as an identifier of a federation. If both the sender and the destination are members of the same federation then they can communicate using this federation's rules.

Security considerations: Federations must guard themselves against non-members announcing membership in the DNS.

Intended usage: COMMON

Author: Otmar Lendl

6. Examples

The first two examples show the NAPTR records for some the VSPs from the diagram from section 4.2. The VSPs shall use domains like vsp-X.example.com and federations use identifiers like "http://fed-1.example.org/".

- VSP X is only reachable through FED2, thus:

```
$ORIGIN vsp-X.example.com
@ IN NAPTR 10 50   "U"  "D2P+SIP:fed" (
           "!^.*$!http://fed-2.example.org/!" . )
```

- VSP C is a member of both FED1 and FED3, thus:

```
$ORIGIN vsp-C.example.com
@ IN NAPTR 10 10   "U" "D2P+SIP:fed" (
           "!^.*$!http://fed-1.example.org/!" . )
@ IN NAPTR 20 10   "U" "D2P+SIP:fed" (
           "!^.*$!http://fed-3.example.org/!" . )
```

  The lower order value indicates that C prefers to receive calls via FED1. B, who is also a member of FED1 and FED3, can choose to honor that preference and use FED1 when contacting C.

- A set of VSPs found a Joint Venture to tightly couple their VoIP networks. Their internal systems bridge the respective walled garden L3/L5 network of each participating VSPs while maintaining guaranteed levels of QoS, security and service assurance. The JV defines the federation "http://jv.example.com/internal" as set of VSPs connected to this internal interconnection system.

```
$ORIGIN A.example.com
@ IN NAPTR 10 10   "U" "D2P+SIP:fed" (
           "!^.*$!http://jv.example.com/internal!" . )

$ORIGIN B.example.com
@ IN NAPTR 10 10   "U" "D2P+SIP:fed" (
           "!^.*$!http://jv.example.com/internal!" . )
```

  These entries provide the intra-JV routing information. If the JV wants to open up its networks to calls from the public Internet in a controlled fashion then they have various options: The first is to define a second federation (e.g.

"http://jv.example.com/inbound") whose rules define the requirements placed on inbound calls. The peering elements of any VSPs which can support these rules can thus be configured to use these peering rules to connect to the JV. The DNS looks now like this:


```
$ORIGIN A.example.com
@ IN NAPTR 10 10   "U" "D2P+SIP:fed" (
           "!^.*$!http://jv.example.com/internal!" . )
  IN NAPTR 30 10   "U" "D2P+SIP:fed" (
           "!^.*$!http://jv.example.com/inbound!" . )

$ORIGIN B.example.com
@ IN NAPTR 10 10   "U" "D2P+SIP:fed" (
           "!^.*$!http://jv.example.com/internal!" . )
  IN NAPTR 30 10   "U" "D2P+SIP:fed" (
           "!^.*$!http://jv.example.com/inbound!" . )
```

In the words of [2] this is a policy notification.

Another option is to direct incoming calls from the Internet to just one of the JV partners, e.g. A:

```
$ORIGIN A.example.com
@ IN NAPTR 10 10   "U" "D2P+SIP:fed" (
           "!^.*$!http://jv.example.com/internal!" . )
  IN NAPTR 20 10   "U" "D2P+SIP:fed" (
           "!^.*$!http://jv.example.com/inbound!" . )

$ORIGIN B.example.com
@ IN NAPTR 10 10   "U" "D2P+SIP:fed" (
           "!^.*$!http://jv.example.com/internal!" . )
  IN NAPTR 20 10   "U" "D2P+SIP"  "" A.example.com
```

Instead of using an opaque federation identifier to publish the JV's requirements for incoming calls, A could also use the policy-type "std" as defined in [6] to explicitely spell out the

requirements:

```
$ORIGIN A.example.com
@ IN NAPTR 10 10   "U" "D2P+SIP:fed" (
           "!^.*$!http://jv.example.com/internal!" . )
  IN NAPTR 20 10   "U" "D2P+SIP:std" (
           "!^.*$!^.*$!urn:ietf:id:ietf-sip-privacy-02!" . )
  IN NAPTR 20 11   "U" "D2P+SIP:std" (
           "!^.*$!^.*$!urn:ietf:rfc:3325!" . )
  IN NAPTR 20 12   "U" "D2P+SIP:std" (
           "!^.*$!^.*$!urn:ietf:rfc:3326!" . )

$ORIGIN B.example.com
@ IN NAPTR 10 10   "U" "D2P+SIP:fed" (
           "!^.*$!http://jv.example.com/internal!" . )
  IN NAPTR 20 10   "U" "D2P+SIP"  "" A.example.com
```


B still refers to A as the ingress point into the JV.

7. Security Considerations

The publishing of the access policy via the DNS RR described in this draft will reduce the amount of unwanted communication attempts, as all well-meaning clients will follow them, but these records cannot substitute measures to actually enforce the published policy.

8. IANA Considerations

This document registers the policy-type "fed" for the domain policy DDDS application.

9. Acknowledgements

The authors would like to thank Alexander Mayrhofer, Henry Sinnreich, Eli Katz, Reinaldo Penno, Patrick Melampy, Daryl Malas, Sohel Khan, and Richard Stastny for their contributions.

10. References

10.1. Normative References

[1] Meyer, D., "SPEERMINT Terminology", draft-ietf-speermint-terminology-04 (work in progress), August 2006.

[2] Lendl, O., "The Domain Policy DDDS Application", draft-lendl-domain-policy-ddds-00 (work in progress), February 2006.

10.2. Informative References

[3] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

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

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

[6] Lendl, O., "Publishing Policies using the Domain Policy DDDS Application", draft-lendl-speermint-technical-policy-00 (work in progress), August 2006.

Authors' Addresses

Michael Haberler
Internet Foundation Austria
Waehringerstrasse 3/19
Wien A-1090
Austria

Phone: +43 664 4213465
Email: mah@inode.at
URI: http://www.nic.at/ipa/

Mike Hammer
Cisco Systems
13615 Dulles Technology Drive
Herndon VA 20171
USA

Phone: +1-703-484-3069
Email: mhammer@cisco.com

Otmar Lendl
enum.at GmbH
Karlsplatz 1/9
Wien A-1010
Austria

Phone: +43 1 5056416 33
Email: otmar.lendl@enum.at
URI: http://www.enum.at/

Intellectual Property Statement

pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has 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.