MIDCOM Working Group
Internet Draft
Category: Informational
Expires on July
2001
February 2002

C.Aoun
S. Sen
Nortel Networks

Identifying intra-realm calls and Avoiding media tromboning

<draft-aoun-midcom-intrarealmcalls-00.txt>

Status of this Memo

Abstract

This draft suggests several ways to identify calls initiated between users within the same addressing realm. By having this capability, media flows are kept within the same realm, thus avoiding usage of certain network intermediaries and reducing bandwidth requirements on certain access links.

Table of Contents

1 Introduction

This draft suggests several ways way to identify if a call is being initiated between users within the same realm. If this capability is implemented, media flows are kept within the same addressing realm whenever possible, thus avoiding usage of certain network intermediaries and reducing bandwidth requirements on external links into the realm.

Within the MIDCOM and pre-MIDCOM frameworks a solution must be found to avoid calls established within the same realm using unnecessary resources on the Middleboxes and on other devices such as Media Proxies that could the pre-MIDCOM framework.

Within the MIDCOM framework, if there is no means to identify which calls are intra-realm calls, all media flows will be routed to the Middlebox applying the NAT function on the media flows and will need to be looped back into the same realm at the Middlebox. Whether this loop back behavior works correctly may depend on the Middlebox implementation.

Within the pre-Midcom framework, if intra-realm calls are not identified when reflector methods such as STUN ([STUN]) are used, the Middlebox will need to loop back the flows. As discussed above this requires a specific behavior of the Middlebox.
When Middleboxes have symmetric NAT implementations, Media Proxies located outside the realm are used during the call and the media flows will need to traverse the Middleboxes and the external links to the realm. This is a serious waste of bandwidth on the Middleboxes' external links which are often one of the major bottlenecks in a network.

A generic model must be found by handling the source of the problem, which is identifying intra-realm calls and then providing appropriate address and port pairs to both parties in call that avoid the media flows leaving the realm.

Several potential methods will be discussed in this draft. By issuing this draft, the authors would like to start discussions on solving this problem. The authors recognize that there might be other alternatives to solve the problem.

Before proposing solutions to the problem, deployment scenarios need to be considered.

Section 4 discusses network deployment cases.
Section 5 discusses potential solutions to the problem.

2 Conventions used in this document

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 RFC-2119.

3 Terminology Used

MB: Middle Box - ref to the terminology used in [FRMWRK]

4 Deployment scenarios

```
                                          ++++++++++++++++++++++++++
+++++++++++++++++++   ++++++++++++++++    +         y.com          +
+finance.us.x.com +   +              +    ++++++         +++++++++++
+           +++++ +   +              +----++MB6+         +   tg1   +
+ fg1       +MB2+ +--/+              +    ++++++         + is.y.com+
+           +++++ + / +The Internet  +    +              +++++++++++
+           +++++ +/  +              +    +++++++++++++++          +
+           +MB1+ +   +              +    +finance.y.com+          +
+ fg        +++++ +   +              +    +    fg       +          +
+++++++++++++++++++   +              +    +             +          +
       |              ++++++++++++++++    ++++++++++++++++++++++++++
       |             /        |      |
       |            /         |      |
       | ++++++++++++++++++   |      |
       | +       +MB3+    +   |      |
       | +       +++++    +   |      |
       | +eng.europe.x.com+   |      |
       | +       tg1      +   |      |
       | ++++++++++++++++++   |      |
       |     |                |      |
     +++++++++++++       +++++++++++++++++++++++++++++++++++++++++
     + x.com     +       + +MB4+  +MB5+                          +
     + Intranet  +       + +++++  +++++                          +
     +           +-------+ Europe.x.com    +++++++++++++++++++++++
     +++++++++++++       +                 + finance.Europe.x.com+
                         +++++++++++++++++++                     +
                         +eng.Europe.x.com++        fg           +
                         +                ++++++++++++++++++++++++
```

```
+ tg2       tg3  +                      +
+++++++++++++++++++++++++++++++++++++++++
```

This section covers different network types, multi-homed networks spanning several sites (with different registered address blocks) as well as standard networks having one interconnect.

One assumption in this document is that inside a corporate network, all private addresses are unique within the corporate's address realm.

When corporations merge together, NAT will need to be used between the private network segments during network migration.

4.1 Call scenarios

Since the document tries to provide solutions that will avoid intra-realm calls going through the various MBs. These call scenarios need to be used to check if the solution allows the required functionality.

There are several intra-realm call types:

a1) Intra-name domain calls on same site or
a2) between different sites:
    tg1.eng.europe.x.com calls tg2.eng.europe.x.com
    or
    tg2.eng.europe.x.com calls tg3.eng.europe.x.com

b1) Inter-name domain calls within same site (same public address block)or
b2) different sites(different public address blocks):
    tg2.eng.europe.x.com calls fg.finance.europe.x.com
    or
    tg1.eng.europe.x.com calls calls fg.finance.europe.x.com

Solutions need to be found to avoid the media streams from all these call types going through MBs.

Registered address allocation might be important for the problem's solution; the following two cases are considered:

Corporate networks could have a single main registered address block provided by a regional (RIPE, ARIN, APNIC, etc) Internet registry, which could be split across several sites. Alternatively several non-contiguous registered blocks could be provided by one or several Internet regional registries.

4.2 Application requirements

Certain applications may involve an entity handling the application session control and another entity handling media processing (i.e. a decoupled approach), other applications may involve a single entity to host both roles (i.e. a coupled approach).

In case the used solution to identify intra-realm calls uses the address or the Fully Qualified Domain Name (FQDN) of the application session control flow host, it may not solve the problem for applications using the decoupled approach mentioned above.

5 Potential solutions to the problem

5.1 Use domain name comparisons

Several applications' signaling protocols (H323, SIP, MEGACO or MGCP) use FQDNs in their messages to identify the originator of the signaling message.

When the "signaling proxy" (could be a SIP Proxy, an H323 GK in routed mode or an MGC) receives the signaling messages from both ends it will compare the domain names from the two messages. The comparison will be done by comparing all characters following the first "." in the FQDN.

The same could be done for peered relations between application clients (i.e. the signaling does not go through an intermediary).

When tg1.eng.europe.x.com calls tg2.eng.europe.x.com, the result of the comparison will show that both parties are in the same realm.

However when call types b1) or b2) are established, the comparison will erroneously indicate that the parties to the call are not in the same realm.

Accordingly this solution is not applicable to all network deployments.

A further problem is that the protocols mentioned above do not always use FQDNs to identify the application end points, which would further limit this approach.

5.2 Use realm identifiers

A realm identifier could be used within the application signaling messages to link the address provided with a certain realm.

Since users will be calling people from several different networks, the realm identifier is required to be globally unique.

This might require that a single organization which would manage the realm identifiers within the Internet, in the same way that ICANN/IANA does for the root name servers.

This is a serious operational burden.

There are some possible alternative ways to provide a unique realm identifier without the previous burden such as :

a) Registered network addresses as realm ID.

If a corporate has several non-contiguous address blocks, the signaling proxy or the peer (if the signaling is not proxied) will need to compare the network address prefix to all the others used by the same company. If the network address does not match any of the prefixes in the list of its company network addresses, the remote end is assumed to be in another addressing realm.

b)In case a corporation (or customer) has a globally unique AS number with a random customer number as a realm ID else the customer's ISP AS number with a 32 bit customer identifier unique within the customers of the ISP as the realm ID. Some corporation have their own globally unique AS number, their realm ID will be their AS number added to a random (or null) customer ID

If the customer network spans across several sites, the customer network could be connected to several ISPs depending on the site location.
In this case we consider that the customer or corporation will choose one of its ISPs' AS number along with one of the assigned customer Ids to the corporation, as the realm ID.

In both a) and b), it will be necessary to inform the customers' application clients of the realm ID. We can assume that there are some out of band mechanisms (configuration or otherwise) to achieve this.

The authors acknowledges that there might be better approaches to define a unique realm ID in the Internet without having the operational burden raised above.

In addition, in order for this scheme to work, it requires that the calling party sends both private and public addresses, because the calling party is not aware of the called party's realm so a single address/port pair won't help.

It is obvious that the realm ID approach requires extension to the application signaling protocols, specifically for the media's session description information carried as part of the protocols, namely:

- -H.245 for H.323
- -SDP for SIP, Megaco and MGCP
- -And other description means for other protocols

5.3 Offer/Answer both private and public addresses

Discovering intra-realm calls can be looked upon as a way to discover the ideal media session for the call. Using the SDP Offer/Answer model [OA], the initial Offer from the caller can advertise two media sessions one with private IP address/port (called private media session) and the other with public IP address/port (called public media session). The Answer similarly contains two corresponding media session descriptions accepting the

Offer. With this transaction, both the caller and the callee knows about the media session representations of each other. In the next step, the caller sends a simple probe message to the private media session of the callee and starts a Timer. If the callee receives a probe message, then it acknowledges it with a response to the private media session address of the caller. This peer-to-peer probe protocol is TBD, but it can be a derivate of any echo-server protocol.

If the callee receives a probe message, then it must send an updated Offer to the caller accepting the private media session and rejecting the public media session. If the callee end-point decides to send media after responding to the initial Offer (but before receiving any probe message), it must always use the public IP address/port. Once it has received a probe message and has not yet started sending media, it should do so only after sending out the updated Offer.

If the caller has sent out a probe message toward the callee, it should not start sending media before the Timer expires or it receives an updated Offer from the callee. In case the Timer expires, it must send media to the public IP address/port only.

There is a possible scenario where the callee located in a different address realm is using a private address that is being used in the realm of the caller. Then the probe packet of the caller, intended to be sent to the private address of the callee, will reach an unintended destination in his own realm. But it would be extremely difficult for this endpoint to hijack the session with a made-up Offer, as it had not received the initial Offer.

Other security implications of this scheme is for further study.

6 Conclusion

The authors believe that there is some potential in the methods discussed in 5.2 and 5.3 as solutions to identify intra-realm calls.

The authors invite the IETF community to start tackling the problem and build a standard way to solve the issue.

7 References

[FRMWRK] Srisuresh, Kuthan, Rosenberg, Molitor, Rayhan, "MIDCOM Architecture & Framework", Internet draft, draft-ietf-midcom-framework-06.txt

[STUN] Rosenberg,Weinberger,Huitema,Mahy,

"STUN - Simple Traversal of UDP Through NATs",
Internet draft, draft-rosenberg-midcom-stun-00.txt

[OA]   Rosenberg, Schulzrinne,
"An Offer/Answer Model with SDP",
Internet draft, draft-ietf-mmusic-sdp-offer-answer-01.txt

8 Acknowledgments

The authors would like to thank the following people for their useful comments and suggestions related to this draft: Francois Audet, Patrick Bradd, Elwyn Davies, Julian Mitchell and Moses Sun.

9 Authors' Address

Cedric Aoun
Nortel Networks
33 Quai Paul Doumer
92415 Courbevoie Cedex
FRANCE

Email: cedric.aoun@nortelnetworks.com

Sanjoy Sen
Nortel Networks
2735-C Glenville Drive
Richardson, Texas
USA
Email: sanjoy@nortelnetworks.com

10 Intellectual Property Statement

11 **Full Copyright Statement**