Abstract

Network Address translators impact several application protocols in the internet; this document discusses how the MGCP protocol could work through NATs. Only the signaling protocol message traversal is discussed in this version of the document. The VoIP streams NAT traversal are already documented and researched within the MIDCOM WG.

Table of Contents

Status of this Memo................................................1
Abstract...........................................................1
1 Overview......................................................................2
2 Conventions used in this document.............................2
3 MGCP NAT complications........................................2

4 NAT package description.........................................4
5 NAT traversal fragmentation considerations...................6
6 Applicability statement.............................................7
7 IANA consideration.................................................7
8 Security Considerations............................................7
9 Changes since draft-aoun-mgcp-nat-package-00.txt............7
10 References..........................................................7
11 Acknowledgments..................................................8
12 Author's Addresses...............................................8
13 Intellectual Property Statement.................................8
14 Full Copyright Statement........................................8
1 Overview

Network Address translators ([NAT]) impact several application protocols in the Internet. [NAT-COMP] provides a good reference on the impact of NATs on certain protocols. This document defines how the MGCP [MGCP] protocol could work in networks where NATs are deployed, whether a single one of them or several in a chain.

Typical examples of NAT deployments include (but are not restricted to):
- Deployment of a NAT in the customer premise network
- Deployment of a NAT in the ISP
- Deployment of NATs in both the customer premise network and the ISP (i.e. there is a chain of NATs that is traversed).

Only the signaling protocol interface is discussed in this version of the draft (i.e. the MGCP message traversal through NATs). The MGCP controlled, VoIP streams NAT traversal is already documented and researched within the MIDCOM IETF WG [MDCMFW]. The next version of the draft will provide an overview of the VoIP media traversal solutions discussed in the MIDCOM WG [MDCMFW].

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 MGCP NAT complications

When Media Gateways (MGW) controlled with the MGCP protocol are deployed behind NATs, the Media Gateway Controller (MGC) should be allowed to control the MGW transparently (or almost transparently).

When the MGW establishes MGCP communication with its MGC, the NAT creates a bind which includes the private IP address and port of the MGCP client on the MGW and the public IP address and port allocated by the NAT (case a). In some NAT implementations the binding could also include the IP address of the MGC (case b) or both the IP address and port of the MGC (case c).

A NAT package for MGCP NAT traversal    February 2003

NATs behaving as in:
- case a) are known as full cone NATs
- case b) are known as restricted cone NATs
- case c) are known as restricted port cone NATs

These NATs belong to the traditional NAT family [TNAT] and are documented in [STUN]. The created NAT bind will have an associated watch dog inactivity timer. In the event that no packets are sent from the MGW to the MGC through the bind over the established duration, the bind will be removed by the NAT.

When the bind is removed by the NAT, the MGC will no longer be able to contact the MGW.

3.1 Proposed keep alive mechanism

There are 2 possible ways to reuse existing MGCP messages as keep alives:

a) Use the audit message (AUUEP, AUDit EndPoint) sent by the MGC to which the MGW will reply, thus the response to the AUUEP will serve as the keep alive.
b) Use an event notification message, where the event is persistent.

The event in this case being that the MGW watch dog inactivity timer has timed out.

Method a) meets the requirement by sending a response to the audit request but requires the MGC host to have an inactivity timer (which is already required but with a bigger auditing period) as well as processing the audit message, and processing the audit response message. Moreover, this method doesn’t allow the MGC to reach its controlled MGW after fail-over.

Method b) requires the MGW to notify the MGC each time the inactivity watch dog timer times out. This method allows the MGC to communicate with the MGW when the MGC recovers from a failure and keeps the bind active by generating a message from the MGW to the MGC.

3.2 Method of operation of the proposed keep alive mechanism

This draft provides a solution to the NAT expiration problem by defining a timer and a persistent package/event.

The MGW must define a “keep alive” timer. The duration of the “keep alive” timer is determined by the NAT bind’s watch dog inactivity timer. The MGW must enable the “keep alive” timer after successful registration (i.e. when an RSIP message has been acknowledged by the MGC). The MGW must reset the “keep alive” timer each time the MGW sends an MGCP message. The MGW must disable the “keep alive” timer if it becomes Disconnected.

Expiry of the “keep alive” timer must cause the MGW to generate a MGCP Notification of the persistent event defined below.

If the MGW doesn’t receive a response to the Notify message after several retransmissions, the standard MGCP algorithm applies (i.e. transition into the disconnected state).

When retransmitting the Notify message (due to lack of acknowledgment) the retransmission timer should not be exponentially backed off but instead the retransmission timer should reuse the inactivity watch dog timer (else the NAT bind could expire as the exponentially backed off retransmission timer could be bigger than the NAT bind timer).

The keep alive expiry persistent event abides by the persistent event rules as defined in [MGCP].

4 NAT package description

Package Name : NAT Package
PackageID : NAT
Version : 1

This package is a new MGCP package. In its first version, only one event is defined (keep alive).

Events MUST always be prefixed with the "NAT" package name.

4.1 Properties
4.2 Events

Keep Alive

EventID : NAT/ka
Event Type : Persistent

This event must be reported by the MGW when its keep alive timer expires. The timer is reset each time the MGW sends any MGCP message (including MGW responses to commands from the call agent, such as "200 xxx OK" acknowledgements).

On timer expiry, the event must be reported from a virtual endpoint on the gateway named 'nat-timeout'.

4.3 Signals

None

4.4 Statistics

None

4.5 Procedures

The keep alive timeout is a gateway specific event, rather than a call processing event that could occur on a normal endpoint. Therefore, since the "all of" wildcard convention cannot be used with the MGCP Notify (NTFY) message, a virtual endpoint is used to report the event.

The virtual endpoint, named 'nat-timeout', does not need to be under the supervision of a NotificationRequest in order to report the event. As per the persistent event definition, a RequestID of 0 must be used to report the event if the endpoint is not under the supervision of a NotificationRequest.

Note that the sending of the keep alive event itself constitutes an outgoing MGCP message and hence the keep alive timer must be reset when this NTFY is sent.

If no response is received from the MGC, the normal retransmission algorithm for the message should be applied (bearing in mind that each of the retransmissions will also reset the keep alive timer).

If the MGC replies to the MGWÆs notify message (notifying the inactivity timer expiration) with a negative acknowledgment (i.e. error code 522, unknown event), the negative acknowledgment should be ignored and the keep alive operations continue as defined above.

Gateways that implement this package MUST provide control of operation through a provisioning system. This should include the ability to enable or disable the keep alive timer completely, and allow configuration of the timer duration in seconds.

4.6 Use Cases: Example Message Flow
The keep alive timer must be reset each time the MGW sends any MGCP message. For example:

```
200 123 OK   (keep alive timer reset)
```

If the timer expires (no MGCP message is sent by the MGW for the duration of the keep alive timer), the MGW reports the keep alive event:

```
----->
NTFY 456 nat-timeout@mgw.nortel.com MGCP 1.0
X: 0
O: NAT/ka
```

The call agent acknowledges:

```
<------
200 456 OK
```

### 5 NAT traversal fragmentation considerations

NATs have known issues with fragmentation ([NAT-COMP]):

- In case the fragments get to the NAT, the NAT may not be able to correlate the received fragment with an existing bind; only the initial fragment including the transport headers will be forwarded and the rest of fragments will be dropped.

  - Certain NATs (not all low end NATs support this behavior) install a state, containing the IP packet ID and the source address and destination pair of the packet, when the packet has the more-fragments bit enabled (i.e. packet has been fragmented). This is used to correlate fragments received with the same specified packet ID and same source and destination address pair. Even with that there might be some issues in case the initial fragment doesn’t arrive in sequence and all other fragments that arrived first will be dropped.

- When 2 clients (in our case MGWs) behind the same NAT are trying to reach the same remote end (i.e. the MGC in this case), they might use the same packet ID. If this happens when fragments reach the MGC, the MGC could get confused during reassembly of the packets as there are no ways to identify to which remote end does the fragment belong.

3 ways to engineer your network to avoid NAT fragmentation problems, listed by order of priority:

- Fragment at the data link layer if applicable (case of PPP)

- In case the MTU could be extended, extend the MTU to the data link MTU size, after analyzing the related jitter impacts.

- Minimize the size of the MGCP datagram, below the MTU, either by using fragmentation at the MGCP level (which is not yet defined) or by avoiding the aggregation of MGCP commands in single transaction messages (this needs to be configured locally when the MGW is known...
6 Applicability statement

The mechanism discussed in this draft, to maintain MGWs behind NATs reachable by their MGC, is applicable ONLY when the MGCP messages are sent and received on the same address and port.

7 IANA consideration

As the NAT package does not exist, the MGCP NAT package will follow the IANA MGCP package reservation process as defined in [MGCP]. The authors of the draft will request from IANA a specific MGCP NAT package identifier.

8 Security Considerations

Security considerations in [MGCP] apply to the introduced keep alive mechanism in this document.

9 Changes since draft-aoun-mgcp-nat-package-01.txt

Minor editing updates.

10 References

[MGCP] F. Andreasen et all, Media Gateway Control Protocol (MGCP) version 1.0, RFC 3435, January 2003

[MDCMFW] P. Srisuresh et all, Middlebox communication architecture and framework, RFC 3303, August 2002


[STUN] Rosenberg, J. et all, STUN - Simple Traversal of UDP Through NATs, draft-ietf-midcom-stun-05.txt, work in progress

[TNAT] Srisuresh, P and Egevang, K., Traditional IP Network Address Translator, RFC 3022, January 2001

Aoun, Wakley, Sassenberg Informational - Expires August 2003    7
A NAT package for MGCP NAT traversal    February 2003

11 Acknowledgments

The authors would like to thank Flemming Andreasen, Kevin Boyle, Bill Foster, Louis Levay, Tony Macdonald, Julian Mitchell, Craig Telke, Richard Willis and Dan Wing for their useful comments and suggestions related to this draft.

12 Author's Addresses

Cedric Aoun
Nortel Networks
France
Email: cedric.aoun@nortelnetworks.com

Martin Wakley
13 Intellectual Property Statement
The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to 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; neither does it represent that it has made any effort to identify any such rights. Information on the IETF’s procedures with respect to rights in standards-track and standards-related documentation can be found in RFC 2026. Copies of claims of rights made available for publication 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 implementors or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

14 Full Copyright Statement

Copyright (C) The Internet Society (2000). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English. The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns. This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.