                   Media Gateway Control Protocol (MGCP)
                      Lockstep State Reporting Mechanism

Status of This Memo

Copyright Notice

IESG Note

   This document is being published for the information of the
   community. It describes a non-IETF protocol that is currently being
   deployed in a number of products. Implementers should be aware of
   RFC 3015, which was developed in the IETF Megaco Working Group and
   the ITU-T SG16, and which is considered the standards-based
   (including reviewed security considerations) way to meet the needs
   that MGCP was designed to address by the IETF and the ITU-T.

Abstract

   A Media Gateway Control Protocol (MGCP) endpoint that has encountered
   an adverse failure condition (such as being involved in a transient
   call when a Call Agent failover occurred) could be left in a lockstep
   state whereby events are quarantined but not notified. The MGCP
   package described in this document provides a mechanism for reporting
   these situations so that the new Call Agent can take the necessary
   fault recovery procedures.

1. Introduction

   In the Media Gateway Control Protocol (MGCP) [2], when an endpoint
   operating in "step" mode generates a Notify, it will enter the
   notification state, where it waits for a response to the Notify.
   Furthermore, the endpoint must wait for a new NotificationRequest
   before it can resume event processing. As long as the endpoint is
   waiting for this NotificationRequest, we say that it is in the
   lockstep state.

An endpoint that is in the lockstep state cannot perform any event
processing and therefore also cannot generate a new Notify.
Endpoints should only be in the lockstep state for a very short time.
However, in adverse conditions, an endpoint could potentially end in
the lockstep state without the Call Agent realizing it. Clearly,
this could have very negative consequences in terms of the service
provided.

The Lockstep package defined in this document defines extensions to
the EndpointConfiguration and RestartInProgress commands that allow a
Call Agent to request an endpoint to inform it when the endpoint is
in the lockstep state for a specified period of time.

1.1. 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 BCP 14, RFC 2119 [1].

2. Lockstep Package

Package Name: LCK
Version: 0

Package Description: The purpose of this package is to provide a
mechanism for reporting a condition in which an endpoint has been in
the "lockstep state" for a specified period of time.

There are two aspects of this package:

   * The ability for a Call Agent to request endpoints to report if
      they are in lockstep state for a specified period of time.
      This is done with the EndpointConfiguration command, as
      described in section 2.1.

   * The reporting mechanism itself, which is done with a new
      "lockstep" RestartMethod for the RSIP command as described in
      section 2.2.

2.1. Request to Report Lockstep State

The new "LCK/LST" EndpointConfiguration parameter is used by the Call
Agent to request the reporting of "lockstep" state. It uses the
following ABNF:

    "LCK/LST:" 0*WSP LSTIME

    LSTIME = 1*(4DIGIT)

where LSTIME is expressed in seconds, with a value ranging from 0 to
9999. A value greater than 2*T-HIST (refer to [2]) is RECOMMENDED.

LSTIME is the amount of time the endpoint is in the lockstep state
before reporting. The timer starts when the endpoint enters the
lockstep state and is canceled if the endpoint leaves the lockstep
state before the timeout occurs. The value provided remains in
effect until explicitly changed (or a restart occurs). If the
endpoint is already in the lockstep state when a non-zero timer value
is provided, the lockstep timer is simply started with the value
provided; any existing lockstep timer is cancelled. The value zero
is used to turn off reporting.

This parameter can be audited by using the AuditEndpoint command.
The value returned is the last configured value, or the value zero
when no value was configured.

2.2. Lockstep Restart Method

A new "lockstep" restart method is defined in the "LCK" package. A
RestartInProgress (RSIP) will be sent with this RestartMethod if the
endpoint has been configured with a non-zero value for LSTIME and
that timer has expired. Note that once the lockstep timer has been
set, it can fire only once per Notify command; however it is possible
to set the timer more than once while an endpoint is in lockstep
state (and hence rearm it for that particular Notify). The syntax of
the restart method is as per [2]:

    "RM" ":" 0*(WSP) "LCK/lockstep"

RestartDelay (see [2]) is not used with the "lockstep" RestartMethod.
Also, the "lockstep" RestartMethod does not define a service-state,
and thus it will never be returned when auditing the RestartMethod.

3. IANA Considerations

The MGCP package title "Lockstep" with the name "LCK" and version
number zero has been registered with IANA as indicated in Appendix
C.1 in [2].

4. Security Considerations

Section 5 of the base MGCP specification [2] discusses security
requirements for the base MGCP protocol that apply equally to the
package defined in this document. Use of a security Protocol such as
IPsec (RFC 2401, RFC 2406) that provides per message authentication
and integrity services is required to ensure that requests and
responses are obtained from authenticated sources and that messages

have not been modified. Without these services, gateways and Call
Agents are open to attacks.

5. Normative References

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

[2]   Andreasen, F. and B. Foster, "Media Gateway Control Protocol
      (MGCP) Version 1.0", RFC 3435, January 2003.

Authors' Addresses

Bill Foster

Phone: +1 250 758 9418
EMail: bfoster@cisco.com

Flemming Andreasen
Cisco Systems
499 Thornall Street, 8th Floor
Edison, NJ 08837

EMail: fandreas@cisco.com

Intellectual Property

   The IETF takes no position regarding the validity or scope of any
   Intellectual Property Rights 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; nor does it represent that it has
   made any independent effort to identify any such rights. Information
   on the ISOC's procedures with respect to rights in ISOC 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.