

Network Working Group
Request for Comments: 3991
Category: Informational

B. Foster
F. Andreasen
Cisco Systems
February 2005

Media Gateway Control Protocol (MGCP) Redirect and Reset Package

Status of This Memo

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2005).

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

The base Media Gateway Control Protocol (MGCP) specification (RFC 3435) allows endpoints to be redirected one endpoint at a time. This document provides extensions in the form of a new MGCP package that provides mechanisms for redirecting and resetting a group of endpoints. It also includes the ability to more accurately redirect endpoints by allowing a list of Call Agents to be specified in a preferred order.

Table of Contents

1.	Introduction.....	2
1.1.	Conventions Used in This Document.....	3
2.	Redirect and Reset Package.....	3
2.1.	NotifiedEntityList Extension Parameter.....	3
2.2.	Endpoint Specifier.....	4
2.2.1.	EndpointList and EndpointMap Extension Parameters.....	4
2.2.2.	Application to Out-of-Service Endpoints.....	6
2.3.	Redirect.....	6
2.4.	Reset Extension Parameter.....	7
2.5.	Return Codes.....	8
3.	IANA Considerations.....	9
4.	Security Considerations.....	9
5.	Normative References.....	9
	Authors' Addresses.....	10
	Full Copyright Statement.....	11

1. Introduction

The base Media Gateway Control Protocol (MGCP) specification [2] allows a Call Agent to specify a new NotifiedEntity parameter in order to redirect one or more endpoints to a new Call Agent. This must be done in a NotificationRequest or a connection handling command. However, because these commands affect endpoint or connection state, such a request cannot typically be sent to a group of endpoints with a single command. This means that if a new Call Agent takes over for a failed one, the new Call Agent must redirect endpoints one at a time. If there is a large number of endpoints (e.g., within a large trunking gateway), this could take considerable time.

This document defines a new redirect and reset package for MGCP that allows the Call Agent to redirect a group of endpoints without affecting endpoint or connection state.

Also included is a new NotifiedEntityList parameter, which is similar to the NotifiedEntity parameter but allows for multiple domain names to be provided. This allows the Call Agent to more accurately direct endpoints to a preferred ordered list of alternate Call Agents.

A third capability contained in this package is the ability to reset and re-initialize one or more groups of endpoints efficiently. This capability is useful in Call Agent failover situations.

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. Redirect and Reset Package

Package Name: RED

Version: 0

This package does the following:

- * Defines a new NotifiedEntityList extension parameter. This works the same as the NotifiedEntity parameter in [2] but allows more than one domain name to be specified.
- * Allows a Call Agent to pass a new NotifiedEntity or NotifiedEntityList to a collection of endpoints specified by an "all of" wildcard. This is useful if a new Call Agent takes over from a previous one and wants to redirect endpoint(s) to send messages to it from now on.
- * Allows a Call Agent to request one or more groups of endpoints to do a reset, which can be useful following certain types of failures.

2.1. NotifiedEntityList Extension Parameter

The NotifiedEntityList parameter is encoded as "NL" and is followed by a colon and a comma-separated list of NotifiedEntity values as defined in the MGCP specification [2], as follows:

```
RED/NL: cal@myca.whatever.net, ca2@mybackupca.whatever.net
```

The NotifiedEntityList works in a way similar to the NotifiedEntity parameter, except that it allows multiple domain names to be listed. The NotifiedEntityList thus specifies a new "notified entity" for the endpoint.

The NotifiedEntityList parameter is optional in any command or response where the NotifiedEntity parameter is allowed. Following a restart, the NotifiedEntityList is initially empty, unless provisioned otherwise. In subsequent commands, it retains its current value until explicitly changed. If both a NotifiedEntity parameter and a non-empty NotifiedEntityList parameter have been set (not necessarily at the same time), the NotifiedEntity parameter value will be viewed as being implicitly added to the beginning of

the `NotifiedEntityList` parameter. The `NotifiedEntity` parameter thus always defines the first domain name to contact unless it has explicitly been set to empty. In that case, the `NotifiedEntityList` defines the "notified entity". If the `NotifiedEntityList` is also empty, then the normal MGCP handling of an empty "notified entity" applies. We will refer to the list of domain names that result from the above rules as the "notified entity list".

When the "notified entity list" is non-empty, transmission is first attempted with the first domain name in the list, as in the normal MGCP retransmission procedures described in [2]. Each of the IP addresses for this domain name MUST first be tried as specified in [2], and if this is unsuccessful, each of the IP-addresses for the second domain name MUST then be attempted, etc., following the normal MGCP retransmission procedures, with "N" (the number of retransmissions) set to zero for each domain name (see Section 4.3 in [2]). Whenever retransmission to a new domain name is initiated, the default retransmission timer value (RTO), etc., SHOULD be used. The estimator (T-DELAY) and measurements (AAD and ADEV) used for the transmission to the previous domain name are considered obsolete. Note, however, that the maximum transaction lifetime considerations apply as usual; therefore, retransmission to any of the IP addresses for any of the domain names MUST NOT occur more than T-Max seconds after the command is initially sent, irrespective of where it was sent. The Max1 DNS query MAY be performed for each of the domain names, or it MAY simply be performed for the first domain name. The Max2 DNS query however MUST NOT be performed for any but the last domain name. Also note that only the last IP-address for the last domain name can reach Max2 retransmissions; therefore, retransmission to all IP addresses other than the last IP address of the last domain name in the list MUST end after Max1 retransmissions.

The current value of the `NotifiedEntityList` parameter can be audited via `AuditEndpoint`; the value of the `NotifiedEntity` parameter will not be included here and must be audited separately. Support for the `NotifiedEntityList` in `AuditConnection` is permissible, but it is neither required nor recommended.

2.2. Endpoint Specifier

2.2.1. EndpointList and EndpointMap Extension Parameters

A simple "all-of" wildcard, as defined in [2], may not be sufficient to accurately specify endpoints of interest. An example of this is a case where a Call Agent fails over, resulting in a state mismatch for endpoints involved with transient calls. To re-synchronize, the Call Agent can use the reset extension parameter described in section 2.4 of this document, to ensure that idle endpoints are in fact idle.

However, these endpoints may be randomly distributed across the available endpoints in a large trunk gateway.

To satisfy this requirement, the RED package introduces some new parameters that may be used to specify the endpoints of interest for the EndpointConfiguration Command. These are the EndpointList and the EndpointMap extension parameters. These parameters MUST only be used when a virtual endpoint corresponding to the gateway is specified as the LocalEndpointName, such as:

```
EPCF 1200 MG@gw1.whatever.net MGCP 1.0
```

where "MG" is the virtual endpoint name associated with the gateway.

The EndPointList parameters is a list of endpoint names that can include one or more lines in the following format:

```
"RED/EL:" 0*WSP RangedLocalName 0*("," 0*WSP RangedLocalName)
```

RangedLocalName is a LocalEndpointName that may include the range wildcard notation described in Appendix E (section E.5) of [2] as well as an "all" wildcard, but the two forms MUST NOT be mixed in a single command:

```
RangeWildcard = "*" / "[" NumericalRange *("," NumericalRange)"]"
NumericalRange = 1*(DIGIT) [ "-" 1*(DIGIT) ]
```

Example:

```
RED/EL: ds/ds1-1/[1-24], ds/ds1-2/[1-24], ds/ds1-3/[1-24]
```

Including an EndpointMap parameter with the following format can further specify the endpoints:

```
"RED/MP:" 0*WSP TrueOrFalse 0*(TrueOrFalse)
```

```
TrueOrFalse = "T" / "F"
```

"T" indicates that the command should be applied to the corresponding endpoint, and "F" indicates that it should not. This parameter can be used in conjunction with the reset extension parameter described in section 2.4 of this document to force arbitrarily distributed endpoints into an idle state.

If the EndpointMap parameter is used, it MUST be immediately preceded (i.e., on the previous line) by an EndPointList parameter to specify the endpoints the EndpointMap is referring to (the EndPointList MUST NOT contain the "all" wildcard). Several EndpointList and

EndpointMap parameter lines can be provided. It is considered an error if an EndpointMap parameter extends beyond the endpoints specified in the preceding EndPointList parameter. In that case, return code 800 MUST be used (see section 2.5).

The EndpointList and EndpointMap parameters MUST only be used with the EndpointConfiguration command. The EndpointList parameter MAY be provided without an EndpointMap parameter. However, as indicated earlier, an EndpointMap parameter MUST be immediately preceded by an EndpointList parameter. Neither of these parameters is auditable.

For an example of EndpointMap parameter usage, see Section 2.4.

2.2.2. Application to Out-of-Service Endpoints

Note that the EndpointConfiguration command is normally only valid for in-service endpoints. If an EndpointConfiguration request is sent to a wildcarded LocalEndpointName [2] and any of the endpoints specified are out-of-service, the command will fail with return code 501 (endpoint not ready).

However, as long as the gateway is in service and able to respond to MGCP commands, it can apply the endpoint configuration command to endpoints specified by the EndpointList and/or EndpointMap parameters (regardless of whether those endpoints are in-service). Of course, the endpoint configuration information will not be maintained over gateway restarts (as the Call Agent would have to reapply the endpoint configuration after it receives an RSIP with the restart method "restart"). For example, if a new "notified entity" was provided, it would have no effect since the provisioned value would be used upon restart.

EndpointList and/or EndpointMap parameters MUST only be used with a virtual endpoint name corresponding to the gateway (as indicated above). If it is used with any other endpoint name (whether wildcarded or not), then error code 801 (section 2.5) MUST be returned.

2.3. Redirect

A new extension parameter for use with the EndpointConfiguration command is defined. A new NotifiedEntity value can be included with a "RED/N" parameter as follows:

```
EPCF 1200 *@gw1.whatever.net MGCP 1.0
RED/N: cal@cal234.whatever.net
```

This changes the "notified entity" for the endpoint(s) to the value specified. If the "all of" wildcard convention is used, the NotifiedEntity value replaces all of the existing "notified entities" for those endpoints. If NotifiedEntity is omitted in a subsequent EndpointConfiguration command, the "notified entity" remains unchanged.

If the "notified entity" is a domain name that resolves to multiple IP addresses, one of the resolved addresses MUST be selected. If one of those IP addresses is the IP address of the Call Agent sending the request, that IP address SHOULD be selected first.

The NotifiedEntityList parameter can also be specified in an endpoint configuration command, such as follows:

```
EPCF 1200 *@gw1.whatever.net MGCP 1.0
RED/NL: cal@myca.whatever.net, ca2@mybackupca.whatever.net
```

Note that this command will only succeed if all the endpoints on the gateway are in-service.

As indicated in section 2.2, it can also apply this to the gateway virtual endpoint:

```
EPCF 1200 MG@gw1.whatever.net MGCP 1.0
RED/EL: *
RED/NL: cal@myca.whatever.net, ca2@mybackupca.whatever.net
```

Note that the outcome of this command is not affected by the service state of the endpoints on the gateway.

As indicated in section 2.1, the NotifiedEntityList ("RED/NL") parameter may be used with any command for which a NotifiedEntity parameter is allowed. However, the "RED/N" parameter SHOULD only be used with the endpoint configuration command.

The "RED/N" parameter does not have a default value, and the auditing behavior for auditing the "NotifiedEntity" is unchanged from that specified in [2], regardless of how the "NotifiedEntity" was set (i.e., there is no specific audit associated with the "RED/N" parameter, and therefore the "RED/N" parameter cannot be audited).

2.4. Reset Extension Parameter

Another EndpointConfiguration parameter ("RED/R") allows the Call Agent to reset one or more endpoints. The ABNF syntax for the parameter line is as follows:

3. IANA Considerations

The MGCP package title "Redirect and Reset" with the name "RED" and version number 0 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 protocol that apply equally to the package defined in this document. Use of a security protocol that provides per message authentication and integrity services, such as IPsec (RFC 2401 [3], RFC 2406 [4]), is required in order 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.

For example, an attacker could masquerade as a Call Agent and initiate a denial of service attack by resetting endpoints that were involved in valid calls. Another attack using the package described in this document could involve redirecting endpoints to the attacker so that it acts as the Call Agent for those endpoints.

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.
- [3] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.
- [4] Kent, S. and R. Atkinson, "IP Encapsulating Security Payload (ESP)", RFC 2406, November 1998.

Authors' Addresses

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

EMail: fandreas@cisco.com

Bill Foster
Cisco Systems

EMail: bfoster@cisco.com

Full Copyright Statement

Copyright (C) The Internet Society (2005).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and at www.rfc-editor.org, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM 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.

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.

Acknowledgement

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

