

Groupe de travail Réseau
Request for Comments : 3991
Catégorie : Informationnel

B. Foster
F. Andreasen
Cisco Systems
Février 2005

Paquetage Redirect et Reset du protocole de commande de passerelle de support (MGCP)

Statut du présent mémo

Le présent mémo fournit des informations destinées à la communauté Internet. Il ne spécifie aucune sorte de norme Internet. La distribution du présent mémo n'est soumise à aucune restriction.

Déclaration de copyright

Copyright (C) The Internet Society (2005).

Note de l'IESG

Le présent document est publié pour l'information de la communauté Internet. Il décrit un protocole non-IETF qui est en cours de développement dans un certain nombre de produits. Les développeurs doivent avoir connaissance de la RFC 3015, qui a été développée par le Groupe de travail Megaco de l'IETF et la Commission 16 de l'UIT-T, et qui est considéré par l'IETF et l'UIT-T comme la façon normalisée (y compris les considérations révisées sur la sécurité) de satisfaire les besoins que MGCP était destiné à prendre en compte.

Résumé

La spécification de base du protocole de commande de passerelle de support (MGCP, *Media Gateway Control Protocol*) (RFC 3435) permet que les points d'extrémité soient redirigés un par un. Le présent document fournit des extensions sous la forme d'un nouveau paquetage MGCP qui procure des mécanismes pour rediriger et rétablir un groupe de points d'extrémité. Il inclut aussi la capacité de rediriger plus efficacement les points d'extrémité en permettant de spécifier une liste d'Agents d'appel dans l'ordre de préférence.

Table des Matières

1.	Introduction	3
1.1.	Conventions utilisées dans le présent document	3
2.	Paquetages Redirect et Reset.....	3
2.1.	Paramètre d'extension NotifiedEntityList.....	4
2.2.	Spécificateur de point d'extrémité	5
2.2.1.	Paramètres d'extension EndpointList et EndpointMap.....	5
2.2.2.	Application aux points d'extrémité hors service.....	6
2.3.	Redirect	7
2.4.	Paramètre d'extension Reset	8
2.5.	Codes de retour.....	8
3.	Considérations sur l'IANA.....	9
4.	Considérations de sécurité.....	9
5.	Références normatives	9

1. Introduction

La spécification de base du protocole de commande de passerelle de support (MGCP, *Media Gateway Control Protocol*) [2] permet à un Agent d'appel de spécifier un nouveau paramètre `NotifiedEntity` afin de rediriger un ou plusieurs points d'extrémité sur un nouvel Agent d'appel. Cela doit être fait dans une `NotificationRequest` ou une commande de traitement de connexion. Cependant, comme ces commandes affectent l'état du point d'extrémité ou de la connexion, une telle requête ne peut pas normalement être envoyée à un groupe de points d'extrémité avec une seule commande. Cela signifie que si un nouvel Agent d'appel prend la place d'un autre défaillant, le nouvel Agent d'appel doit rediriger les points d'extrémité un par un. Si il y a un grand nombre de points d'extrémité (par exemple, dans une grande passerelle interurbaine), cela peut prendre un temps considérable.

Le présent document définit un nouveau paquetage de redirection et de rétablissement pour MGCP qui permet à l'Agent d'appel de rediriger un groupe de points d'extrémité sans affecter l'état des points d'extrémité ou de la connexion.

Est aussi inclus un nouveau paramètre `NotifiedEntityList`, qui est similaire au paramètre `NotifiedEntity` mais permet de fournir des noms de domaine multiples. Cela permet à l'Agent d'appel de diriger plus efficacement les points d'extrémité sur une liste ordonnée par préférence des Agents d'appel de remplacement.

Une troisième capacité contenue dans ce paquetage est la faculté de rétablir et réinitialiser efficacement un ou plusieurs groupes de points d'extrémité. Cette capacité est utile dans les situations de défaillance d'Agent d'appel.

1.1. Conventions utilisées dans le présent document

Dans le présent document, les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" doivent être interprétés comme décrit par la [RFC2119].

2. Paquetages Redirect et Reset

Nom du paquetage : RED Version: 0

Ce paquetage fait ce qui suit :

- * Définit un nouveau paramètre d'extension `NotifiedEntityList`. Cela fonctionne de la même façon que le paramètre `NotifiedEntity` dans [2] mais permet de spécifier plus d'un nom de domaine.
- * Permet à un Agent d'appel de passer une nouvelle `NotifiedEntity` ou `NotifiedEntityList` à une collection de points d'extrémité spécifiés par un caractère générique "all of". Ceci

est utile si un nouvel Agent d'appel prend la place du précédent et veut rediriger le ou les points d'extrémité pour qu'ils lui envoient les messages à partir de ce moment.

- * Permet à un Agent d'appel de demander à un ou plusieurs groupes de points d'extrémité d'effectuer un rétablissement, ce qui peut être utile à la suite de certains types de défaillance.

2.1. Paramètre d'extension *NotifiedEntityList*

Le paramètre *NotifiedEntityList* est codé "NL" et il est suivi par deux points et une liste séparée par une virgule de valeurs de *NotifiedEntity* comme défini dans la spécification MGCP [2], comme suit :

RED/NL: ca1@myca.whatever.net, ca2@mybackupca.whatever.net

Le *NotifiedEntityList* fonctionne d'une façon similaire au paramètre *NotifiedEntity*, sauf qu'il permet de faire la liste de plusieurs noms de domaine. Le paramètre *NotifiedEntityList* spécifie donc une nouvelle "notified entity" pour le point d'extrémité.

Le paramètre *NotifiedEntityList* est facultatif dans toute commande ou réponse où le paramètre *NotifiedEntity* est autorisé. A la suite d'un redémarrage, le paramètre *NotifiedEntityList* est initialement vide, à moins qu'il ne soit provisionné par ailleurs. Dans les commandes ultérieures, il conserve sa valeur en cours jusqu'à ce qu'il soit explicitement changé. Si un paramètre *NotifiedEntity* et un paramètre *NotifiedEntityList* non vide ont tous deux été établis (pas nécessairement au même moment), la valeur du paramètre *NotifiedEntity* sera considérée comme étant implicitement ajoutée au début du paramètre *NotifiedEntityList*. Le paramètre *NotifiedEntity* définit donc toujours le premier nom de domaine à contacter à moins qu'il ait été explicitement réglé à vide. Dans ce cas, le *NotifiedEntityList* définit la "entité notifiée". Si la *NotifiedEntityList* est aussi vide, le traitement normal MGCP des "entité notifiée" vides s'applique alors. Nous nous référerons à la liste des noms de domaine qui résulte des règles ci-dessus comme à la "liste des entités notifiées".

Lorsque le paramètre "notified entity list" (*liste d'entités notifiées*) n'est pas vide, la transmission est d'abord tentée avec le premier nom de domaine de la liste, suivant les procédures de retransmission normales de MGCP décrites dans [2]. Chacune des adresses IP pour ce nom de domaine DOIT d'abord être essayée comme spécifié dans [2], et si cela ne réussit pas, chacune des adresses IP pour le second nom de domaine DOIT alors être tentée, etc., suivant les procédures de retransmission normales de MGCP, avec "N" (le nombre de retransmissions) mis à zéro pour chaque nom de domaine (voir le paragraphe 4.3 dans [2]). Chaque fois qu'est initialisée la retransmission à un nouveau nom de domaine, la valeur du temporisateur de retransmission par défaut (RTO), etc., DEVRAIT être utilisée. L'estimateur (T-DELAY) et les mesures (AAD et ADEV) utilisés pour la transmission du nom de domaine précédent sont considérés comme obsolètes. Noter, cependant, que les considérations de durée de vie maximale de transaction s'appliquent comme d'habitude, donc, la retransmission à toute adresse IP pour tout nom de domaine NE DOIT PAS survenir plus de T-Max secondes après l'envoi initial de la commande, sans considération de l'endroit où elle a été envoyée. L'interrogation DNS Max1 PEUT être effectuée pour chacun des noms de domaine, ou elle PEUT être simplement effectuée pour le premier nom de domaine. L'interrogation DNS Max2 NE DOIT PAS cependant être effectuée pour un autre nom de domaine que le dernier.

Noter aussi que seule la dernière adresse IP pour le dernier nom de domaine peut atteindre Max2 retransmissions; et donc, la retransmission à toute adresse IP autre que la dernière adresse IP du dernier nom de domaine de la liste DOIT se terminer après Max1 retransmissions.

La valeur en cours du paramètre NotifiedEntityList peut être vérifiée via AuditEndpoint ; la valeur du paramètre NotifiedEntity n'y sera pas incluse et doit être vérifiée séparément. La prise en charge de NotifiedEntityList dans AuditConnection est admissible, mais n'est ni exigée ni recommandée.

2.2. Spécificateur de point d'extrémité

2.2.1. Paramètres d'extension EndpointList et EndpointMap

Un simple caractère générique "all-of", comme défini en [2], peut n'être pas suffisant pour spécifier de façon appropriée les points d'extrémité intéressants. Un exemple de cela est le cas où un Agent d'appel se trouve défaillant, d'où il résulte une discordance d'état pour les points d'extrémité impliqués avec des appels en transit. Pour effectuer la re-synchronisation, l'Agent d'appel peut utiliser le paramètre d'extension reset, décrit au paragraphe 2.4 du présent document, pour s'assurer que les points d'extrémité inactifs sont bien inactifs.

Cependant, ces points d'extrémité peuvent être distribués de façon aléatoire parmi les points d'extrémité disponibles dans une grande passerelle interurbaine.

Pour satisfaire à cette exigence, le paquetage RED introduit quelques nouveaux paramètres qui peuvent être utilisés pour spécifier les points d'extrémité intéressants pour la commande EndpointConfiguration. Ce sont les paramètres d'extension EndpointList et EndpointMap. Ces paramètres ne DOIVENT être utilisés que lorsqu'un point d'extrémité virtuel correspondant à la passerelle est spécifié comme LocalEndpointName, tel que :

EPCF 1200 MG@gw1.whatever.net MGCP 1.0

où "MG" est le nom de point d'extrémité virtuel associé à la passerelle.

Le paramètre EndPointList est une liste de noms de points d'extrémité qui peut inclure une ou plusieurs lignes dans le format suivant :

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

RangedLocalName est un LocalEndpointName qui peut inclure la notation de caractère générique de gamme décrit dans l'Appendice E (section E.5) de [2] aussi bien que le caractère générique "all", mais les deux formes NE DOIVENT PAS être mélangées dans une seule commande :

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

Exemple :

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

Inclure un paramètre EndpointMap avec le format suivant peut spécifier les points d'extrémité :

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

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

"T" indique que la commande devrait être appliquée au point d'extrémité correspondant, et "F" indique qu'elle ne le devrait pas. Ce paramètre peut être utilisé en conjonction avec le paramètre d'extension reset décrit au paragraphe 2.4 du présent document pour forcer des points d'extrémité distribués de façon arbitraire à passer à l'état inactif.

Si le paramètre EndpointMap est utilisé, il DOIT être immédiatement précédé (c'est-à-dire, sur la ligne précédente) par un paramètre EndPointList pour spécifier les points d'extrémité auquel EndpointMap se réfère (EndPointList NE DOIT PAS contenir le caractère générique "all"). Plusieurs lignes de paramètres EndPointList et EndpointMap peuvent être fournies. L'extension d'un paramètre EndpointMAP au-delà des points d'extrémité spécifiés dans le paramètre EndPointList précédent est considéré comme une erreur. Dans ce cas, le code de retour 800 DOIT être utilisé (voir au paragraphe 2.5).

Les paramètres EndPointList et EndpointMap ne DOIVENT être utilisés qu'avec la commande EndpointConfiguration. Le paramètre EndPointList PEUT être fourni sans le paramètre EndpointMap. Cependant, comme indiqué plus haut, un paramètre EndpointMap DOIT être immédiatement précédé par un paramètre EndPointList. Aucun de ces paramètres ne peut être audité.

Pour un exemple d'utilisation du paramètre EndpointMap, voir au paragraphe 2.4.

2.2.2. Application aux points d'extrémité hors service

Noter que la commande EndpointConfiguration n'est normalement valide que pour les points d'extrémité en service. Si une demande de EndpointConfiguration est envoyée à un LocalEndpointName [2] avec un caractère générique et qu'un des points d'extrémité spécifié est hors service, la commande va échouer avec le code de retour 501 (point d'extrémité pas prêt).

Cependant, tant que la passerelle est en service et capable de répondre aux commandes MGCP, elle peut appliquer la commande de configuration de point d'extrémité aux points spécifiés par les paramètres EndPointList et/ou EndpointMap (indépendamment du fait que ces points d'extrémité sont ou non en service). Bien sûr, les informations de configuration de point d'extrémité ne seront pas conservées après le redémarrage de la passerelle (car l'Agent d'appel aurait à réappliquer la configuration de point d'extrémité après réception d'un RSIP avec la méthode de redémarrage "restart"). Par exemple, si une nouvelle "entité notifiée" était fournie, cela n'aurait aucun effet dans la mesure où la valeur approvisionnée serait utilisée au redémarrage.

Les paramètres EndpointList et/ou EndpointMap ne DOIVENT être utilisés qu'avec un nom de point d'extrémité virtuel correspondant à la passerelle (comme indiqué ci-dessus). Si il sont utilisés avec tout autre nom de point d'extrémité (avec ou sans caractères génériques), le code d'erreur 801 (paragraphe 2.5) DOIT être retourné.

2.3. Redirect

Un nouveau paramètre d'extension à utiliser avec la commande EndpointConfiguration est défini. Une nouvelle valeur NotifiedEntity peut être incluse avec un paramètre "RED/N" comme suit :

```
EPCF 1200 *@gw1.whatever.net MGCP 1.0  
RED/N: ca1@ca1234.whatever.net
```

Cela change la "entité notifiée" pour le ou les points d'extrémité et la met à la valeur spécifiée. Si la convention de caractère générique "all of" est utilisée, la valeur de NotifiedEntity remplace toutes les "entités notifiées" pour ces points d'extrémité. Si NotifiedEntity est omis dans une commande EndpointConfiguration ultérieure, la "entité notifiée" reste inchangée.

Si la "entité notifiée" est un nom de domaine qui se résout en des adresses IP multiples, une des adresses résolues DOIT être choisie. Si une de ces adresses IP est l'adresse IP de l'Agent d'appel qui envoie la demande, cette adresse IP DEVRAIT être choisie en premier.

Le paramètre NotifiedEntityList peut aussi être spécifié dans une commande de configuration de point d'extrémité, telle que ce qui suit :

```
EPCF 1200 *@gw1.whatever.net MGCP 1.0  
RED/NL: ca1@myca.whatever.net, ca2@mybackupca.whatever.net
```

Noter que cette commande ne réussira que si tous les points d'extrémité sur la passerelle sont en service.

Comme indiqué au paragraphe 2.2, on peut aussi appliquer cela au point d'extrémité virtuel de passerelle :

```
EPCF 1200 MG@gw1.whatever.net MGCP 1.0  
RED/EL: *  
RED/NL: ca1@myca.whatever.net, ca2@mybackupca.whatever.net
```

Noter que le résultat de cette commande n'est pas affecté par l'état de service des points d'extrémité sur la passerelle.

Comme indiqué au paragraphe 2.1, le paramètre NotifiedEntityList ("RED/NL") peut être utilisé avec toute commande pour laquelle un paramètre NotifiedEntity est autorisé. Cependant, le paramètre "RED/N" ne DEVRAIT être utilisé qu'avec la commande de configuration de point d'extrémité.

Le paramètre "RED/N" n'a pas de valeur par défaut, et le comportement d'audit pour la vérification de "NotifiedEntity" est inchangé par rapport à celui spécifié en [2], indépendamment de la façon dont la "NotifiedEntity" a été réglée (c'est-à-dire qu'il n'y a pas d'audit spécifique associé au paramètre "RED/N", et donc le paramètre "RED/N" ne peut pas être vérifié).

2.4. Paramètre d'extension Reset

Un autre paramètre EndpointConfiguration ("RED/R") permet à l'Agent d'appel de rétablir un ou plusieurs points d'extrémité. La syntaxe ABNF pour la ligne de paramètres est la suivante :

```
"RED/R:" 0*WSP "reset"
```

Cela a pour effet de rétablir et de réinitialiser les points d'extrémité spécifiés (c'est-à-dire que toute connexions sur le point d'extrémité sera supprimée, et le point d'extrémité sera remis à son état par défaut sans aucun signaux actifs).

Exemple :

```
EPCF 1200 mg@gw1.whatever.net MGCP 1.0
RED/EL: ds/e1-3/[1-30]
RED/MP: TTTTTTTFFFTTTTTTTTFFFFTFFFTTTTFF
RED/EL: ds/e1-5/[1-30]
RED/MP: TFFFFTFFFFTTFTTFFFFTFFFFTTTTTT
RED/R: reset
```

Dans ce cas, les points d'extrémité particuliers spécifiés par "T" par le paramètre EndpointMap dans les couples E1 ds/e1-3 et ds/e1-5 sont rétablis.

Le paramètre "RED/R" NE DOIT PAS être utilisé avec toute autre commande que la commande de configuration de point d'extrémité. Il n'y a pas de valeur par défaut pour le paramètre, et donc il n'est pas affecté par son omission. Il n'y a pas de comportement spécifique d'audit associé à ce paramètre, c'est-à-dire qu'il ne peut pas être vérifié.

2.5. Codes de retour

Les codes de retour spécifiques du paquetage suivants sont définis pour le paquetage "RED" :

Code	Texte	Explication
800	EndpointMap hors de la gamme	Les paramètres EndpointMap sont en-dehors de la gamme spécifiée par le paramètre EndpointList, ou le paramètre EndpointList n'était pas inclus lorsqu'un paramètre EndpointMap l'était.
801	Utilisation incorrecte des paramètres	Utilisation incorrecte des paramètres, tels que le paramètre EndpointList, utilisé alors que le nom de point d'extrémité n'était pas le nom de point d'extrémité virtuel correspondant à la passerelle.

3. Considérations sur l'IANA

Le paquetage MGCP intitulé "Redirect and Reset" avec le nom "RED" et le numéro de version 0 a été enregistré auprès de l'IANA, comme indiqué dans l'Appendice C.1 de [2].

4. Considérations de sécurité

La Section 5 de la spécification de base de MGCP [2] expose les exigences de sécurité pour le protocole de base et elle s'applique également au paquetage défini dans le présent document. L'utilisation d'un protocole de sécurité fournissant des services d'authentification et d'intégrité message par message, tel que IPsec (RFC 2401 [3], RFC 2406 [4]), est exigé afin de garantir que demandes et réponses sont obtenues auprès de sources authentifiées et que les messages n'ont pas été modifiés. Sans ces services, les passerelles et Agents d'appel sont désarmés contre les attaques.

Par exemple, un agresseur peut se déguiser en Agent d'appel et lancer une attaque de déni de service en remettant à zéro des points d'extrémité qui sont engagés dans des communications valides. Une autre attaque utilisant le paquetage décrit dans le présent document pourrait amener à rediriger les points d'extrémité sur l'agresseur de sorte qu'il agisse comme l'Agent d'appel pour ces points d'extrémité.

5. Références normatives

[1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels" (*Mots clé utilisés dans les RFC pour indiquer les niveaux d'exigence*), BCP 14, RFC 2119, mars 1997.

[2] Andreasen, F. et B. Foster, "Media Gateway Control Protocol (MGCP) Version 1.0" (*Protocole de commande de passerelle de support (MGCP)*), RFC 3435, janvier 2003.

[3] Kent, S. et R. Atkinson, "Security Architecture for the Internet Protocol" (*Architecture de sécurité pour l'protocole Internet*), RFC 2401, novembre 1998.

[4] Kent, S. et R. Atkinson, "IP Encapsulating Security Payload (ESP)" (*Incorporation d'une charge utile de sécurité dans IP*), RFC 2406, novembre 1998.

Adresse des auteurs

Flemming Andreasen	Bill Foster
Cisco Systems	Cisco Systems
499 Thornall Street, 8th Floor	
Edison, NJ 08837	
email : fandreas@cisco.com	email : bfoster@cisco.com

Déclaration de copyright

Copyright (C) The Internet Society (2005).

Le présent document est soumis aux droits, licences et restrictions contenus dans le BCP 78, et à www.rfc-editor.org, et sauf pour ce qui est mentionné ci-après, les auteurs conservent tous leurs droits.

Le présent document et les informations y contenues sont fournies sur une base "EN L'ÉTAT" et LE CONTRIBUTEUR, L'ORGANISATION QU'IL OU ELLE REPRÉSENTE OU QUI LE/LA FINANCE (S'IL EN EST), LA INTERNET SOCIETY ET LA INTERNET ENGINEERING TASK FORCE DÉCLINENT TOUTES GARANTIES, EXPRIMÉES OU IMPLICITES, Y COMPRIS MAIS NON LIMITÉES À TOUTE GARANTIE QUE L'UTILISATION DES INFORMATIONS CI-ENCLOSES NE VIOLENT AUCUN DROIT OU AUCUNE GARANTIE IMPLICITE DE COMMERCIALISATION OU D'APTITUDE À UN OBJET PARTICULIER.

Propriété intellectuelle

L'IETF ne prend pas position sur la validité et la portée de tout droit de propriété intellectuelle ou autres droits qui pourrait être revendiqués au titre de la mise en œuvre ou l'utilisation de la technologie décrite dans le présent document ou sur la mesure dans laquelle toute licence sur de tels droits pourrait être ou n'être pas disponible ; pas plus qu'elle ne prétend avoir accompli aucun effort pour identifier de tels droits. Les informations sur les procédures de l'ISOC au sujet des droits dans les documents de l'ISOC figurent dans les BCP 78 et BCP 79.

Des copies des dépôts d'IPR faites au secrétariat de l'IETF et toutes assurances de disponibilité de licences, ou le résultat de tentatives faites pour obtenir une licence ou permission générale d'utilisation de tels droits de propriété par ceux qui mettent en œuvre ou utilisent la présente spécification peuvent être obtenues sur répertoire en ligne des IPR de l'IETF à <http://www.ietf.org/ipr>.

L'IETF invite toute partie intéressée à porter son attention sur tous copyrights, licences ou applications de licence, ou autres droits de propriété qui pourraient couvrir les technologies qui peuvent être nécessaires pour mettre en œuvre la présente norme. Prière d'adresser les informations à l'IETF à ietf-ipr@ietf.org.

Remerciement

Le financement de la fonction d'édition des RFC est actuellement fourni par Internet Society.