Groupe de travail Réseau
Request for Comments : 3515
Catégorie : En cours de normalisation

R. Sparks, dynamicsoft
avril 2003
Traduction Claude Brière de L'Isle

Méthode Refer du protocole d'initialisation de session (SIP)

Statut de ce mémoire
Le présent document spécifie un protocole Internet en cours de normalisation pour la communauté de l'Internet, et appelle à des discussions et des suggestions pour son amélioration. Prière de se reporter à l'édition actuelle du STD 1 "Normes des protocoles officiels de l'Internet" pour connaître l'état de normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Résumé
Le présent document définit une méthode REFER. Cette extension au protocole d'initialisation de session (SIP, *Session Initiation Protocol*) demande que le receveur se REFERe à une ressource fournie dans la demande. Il donne un mécanisme qui permet à la partie qui envoie le REFER d'être notifiée du résultat de la demande référencée. Cela peut être utilisé pour activer de nombreuses applications, y compris de transfert d'appel.
En plus de la méthode REFER, le présent document définit le paquetage d'événement refer et l'en-tête de demande Refer-To.

Table des Matières

1. Présentation....2
2. Méthode REFER....2
2.1 Champ d'en-tête Refer-To....2
2.2 Prise en charge de champ d'en-tête pour la méthode REFER....3
2.3 Inclusion du corps de message....4
2.4 Comportement des agents d'utilisateur SIP....4
2.5 Comportement des registraires/serveurs de redirection SIP....6
2.6 Comportement des mandataires SIP....6
3. Détails du paquetage : événement refer....6
3.1 Nom de paquetage d'événement....6
3.2 Paramètres de paquetage d'événement....6
3.3 Corps de SUBSCRIBE....6
3.4 Durée d'abonnement....6
3.5 Corps de NOTIFY....7
3.6 Traitement par le notificateur des demandes SUBSCRIBE....7
3.7 Génération par le notificateur des demandes NOTIFY....7
3.8 Traitement par l'abonné des demandes NOTIFY....7
3.9 Traitement des demandes fourchées....7
3.10 Taux des notifications....7
3.11 Agents d'état....7
4. Exemples....7
4.1 Prototype de flux d'appel REFER....7
4.2 REFER multiples dans un dialogue....9
5. Considérations sur la sécurité....11
5.1 Construction d'un URI Refer-To....11
5.2 Considérations d'autorisation pour REFER....11
5.3 Considérations sur l'utilisation de message/sipfrag....12
6. Éléments d'historique....12
7. Considérations relatives à l'IANA....13
8. Remerciements....13
9. Références....13
10. Considérations de propriété intellectuelle....13
11. Adresse de l'auteur....14
12. Déclaration complète de droits de reproduction....14

1. Présentation

Le présent document définit la méthode REFER. Cette extension à SIP [RFC3261] demande que le receveur se REFERe à une ressource fournie dans la demande.

Cela peut être utilisé pour activer de nombreuses applications, y compris de transfert d'appel. Par exemple, si Alice est engagée dans une conversation avec Bob, et qu'elle décide que Bob a besoin de parler à Carol, Alice peut donner pour instruction à son agent d'utilisateur (UA, *user agent*) SIP d'envoyer une demande SIP REFER à l'UA de Bob pour lui donner les informations de contact SIP de Carol. En supposant que Bob en ait donné la permission, l'UA de Bob va tenter d'appeler Carol en utilisant ce contact. L'UA de Bob va alors faire rapport à l'UA d'Alice de la réussite ou de l'échec à établir le contact.

2. Méthode REFER

REFER est une méthode SIP comme définie par la [RFC3261]. La méthode REFER indique que le receveur (identifié par le Request-URI) devrait contacter un tiers en utilisant les informations de contact fournies dans la demande.

Sauf mention contraire, le protocole pour émettre et répondre à une demande REFER est identique à celui d'une demande BYE dans la [RFC3261]. Le comportement des entités SIP qui ne mettent pas en œuvre la méthode REFER (ou toute autre méthode inconnue) est explicitement définie dans la [RFC3261].

Une demande REFER établit implicitement un abonnement à l'événement refer. Les abonnements d'événements sont définis dans la [RFC3265].

Une demande REFER PEUT être placée en-dehors de la portée d'un dialogue créé avec un INVITE. REFER crée un dialogue, et PEUT être Record-Routed, et donc DOIT contenir une seule valeur de champ d'en-tête Contact. Les REFER qui surviennent à l'intérieur d'un dialogue existant DOIVENT suivre la logique Route/Record-Route de ce dialogue.

2.1 Champ d'en-tête Refer-To

Refer-To est un champ d'en-tête de demande (request-header) comme défini par la [RFC3261]. Il n'apparaît que dans une demande REFER. Il fournit un URL à référencer.

Refer-To = ("Refer-To" / "r") HCOLON (name-addr / addr-spec) * (SEMI generic-param)

Ce qui suit devrait être interprété comme si cela apparaissait dans le Tableau 2/3 de la {RFC3261].

Champ d'en-tête	où	mandataire	ACK	BYE	CAN	INV	OPT	REG
Refer-To	R	-	-	-	-	-	-	-

Le champ d'en-tête Refer-To PEUT être chiffré au titre du chiffrement de bout en bout.

Le champ d'en-tête Contact est une partie importante du mécanisme Route/Record-Route et n'est pas disponible pour indiquer la cible de la référence.

Exemples :

Refer-To: sip:alice@atlanta.example.com

Refer-To: <sip:bob@biloxi.example.net?Accept-Contact=sip:bobsdesk.
biloxi.example.net&Call-ID%3D55432%40alicepc.atlanta.example.com>

Refer-To: <sip:dave@denver.example.org?Replaces=12345%40192.168.118.3%3B
to-tag%3D12345%3Bfrom-tag%3D5FFE-3994>

Refer-To: <sip:carol@cleveland.example.org;method=SUBSCRIBE>

Refer-To: http://www.ietf.org

Les longues valeurs d'en-tête ne sautent à la ligne que pour des besoins de lisibilité.

2.2 Prise en charge de champ d'en-tête pour la méthode REFER

Le tableau suivant ajoute une colonne au tableau 2/3 de la [RFC3261], qui décrit la présence de champs d'en-tête dans une méthode REFER. Voir à la Section 20 de la [RFC3261] la clé des symboles utilisés. On devrait en déduire une ligne pour l'en-tête de demande Refer-To qui est obligatoire pour REFER. Refer-To n'est applicable à aucune autre méthode. La colonne 'mandataire' dans la [RFC3261] s'applique sans modification à la méthode REFER.

En-tête	**Où**	**REFER**
Accept	R	o
Accept	2xx	-
Accept	415	c
Accept-Encoding	R	o
Accept-Encoding	2xx	-Accept-Encoding 415 c
Accept-Language	R	o
Accept-Language	2xx	-
Accept-Language	415	c
Alert-Info		-
Allow	Rr	o
Allow	405	m
Authentication-Info	2xx	o
Authorization	R	o
Call-ID	c	m
Call-Info		-
Contact	R	m
Contact	1xx	-
Contact	2xx	m
Contact	3-6xx	o
Content-Disposition		o
Content-Encoding		o
Content-Language		o
Content-Length		o
Content-Type		*
Cseq	c	m
Date		o
Error-Info	3-6xx	o
Expires	R	o
From	c	m
In-Reply-To		-
Max-Forwards	R	m
Min-Expires		-
MIME-Version		o
Organization		o
Priority	R	-
Proxy-Authenticate	401	o
Proxy-Authenticate	407	m
Proxy-Authorization	R	o
Proxy-Require	R	o
Record-Route	R	o
Record-Route	2xx,18x	o
Reply-To		-
Require		c
Retry-After	404,413,480,486	o
Retry-After	500,503	o
Retry-After	600,603	o
Route	R	c
Server	r	o
Subject	R	-
Supported	R,2xx	o
Timestamp		o

To	c(1)	m
Unsupported	420	o
User-Agent		o
Via	c(2)	m
Warning	r	o
WWW-Authenticate	401	m
WWW-Authenticate	407	o

Tableau 1 : Prise en charge du champ d'en-tête

2.3 Inclusion du corps de message

Une méthode REFER PEUT contenir un corps. La présente spécification n'affecte pas de signification à un tel corps. Un agent receveur peut choisir de traiter le corps conformément à son type de contenu.

2.4 Comportement des agents d'utilisateur SIP

2.4.1 Formation d'une demande REFER

REFER est une demande SIP qui est construite comme défini dans la [RFC3261]. Une demande REFER DOIT contenir exactement une valeur de champ d'en-tête Refer-To.

2.4.2 Traitement d'une demande REFER

Un UA qui accepte une demande REFER bien formée DEVRAIT demander l'approbation de l'utilisateur pour continuer (cette demande pourrait être satisfaite avec une interrogation interactive ou par l'accès à une politique configurée). Si l'approbation est accordée, l'UA DOIT contacter la ressource identifiée par l'URI contenu dans le champ d'en-tête Refer-To comme exposé au paragraphe 2.4.3.

Si l'approbation recherchée ci-dessus pour une demande REFER bien formée est immédiatement refusée, l'UA PEUT décliner la requête.

Un agent qui répond à une méthode REFER DOIT retourner un 400 (Mauvaise demande) si la demande contenait zéro ou plus d'une valeurs de champ d'en-tête Refer-To.

Un agent (incluant des mandataires qui génèrent des réponses locales) PEUT retourner un 100 (Essai) ou toute réponse appropriée de classes 4xx-6xx comme prescrit par la [RFC3261].

Il faut faire attention lors de la mise en œuvre de la logique qui détermine si il faut ou non accepter la demande REFER. Un UA sans capacité d'accéder à des URI non SIP NE DEVRAIT PAS accepter de demandes REFER pour eux.

Si une réponse finale n'a pas été générée selon les règles ci-dessus, l'UA DOIT retourner un 202 Réponse acceptée avant l'expiration de la transaction REFER.

Si une demande REFER est acceptée (c'est-à-dire, si une réponse de classe 2xx est retournée) le receveur DOIT créer un abonnement et envoyer des notifications de l'état du refer comme décrit au paragraphe 2.4.4.

2.4.3 Accès à la ressource désignée par Referred-to

La ressource identifiée par l'URI Refer-To est contactée en utilisant les mécanismes normaux pour ce type d'URI. Par exemple, si l'URI est un URI SIP qui indique INVITE (en utilisant par exemple un paramètre URI method=INVITE) l'UA va produire un nouvel INVITE en utilisant toutes les règles normales d'envoi d'un INVITE définies dans la [RFC3261].

2.4.4 Utilisation des événements SIP pour rapporter les résultats de la référence

Le mécanisme NOTIFY défini dans la [RFC3265] DOIT être utilisé pour informer l'agent d'envoi du REFER de l'état de la référence. Les identifiants de dialogue (To, From, et Call-ID) de chaque NOTIFY doivent correspondre à ceux du REFER comme ils le feraient si le REFER avait été une demande SUBSCRIBE.

Chaque NOTIFY DOIT contenir un champ d'en-tête Event avec une valeur de refer et éventuellement un paramètre id (voir au paragraphe 2.4.6).

Chaque NOTIFY DOIT contenir un corps de type "message/sipfrag" [RFC3420].

La création d'un abonnement, comme défini par la [RFC3265] résulte toujours en un NOTIFY immédiat. De même que dans le cas de SUBSCRIBE décrit dans la présent document, l'agent qui a produit le REFER DOIT être prêt à recevoir un NOTIFY avant l'achèvement de la transaction REFER.

L'abonnement implicite créé par un REFER est le même que celui créé avec une demande SUBSCRIBE. L'agent qui produit le REFER peut terminer prématurément cet abonnement en se désabonnant au moyen des mécanismes décrits dans la [RFC3265]. Terminer un abonnement, soit par un désabonnement explicite, soit par un rejet de NOTIFY, n'est pas une indication que la demande référencée devrait être retirée ou abandonnée. En particulier, un agent agissant sur une demande REFER NE DEVRAIT PAS produire un CANCEL à des demandes SIP référencées parce que l'agent qui a envoyé le REFER a terminé son abonnement à l'événement refer avant l'achèvement de la demande référencée.

L'agent qui produit le REFER peut étendre son abonnement en utilisant le mécanisme de rafraîchissement d'abonnement décrit dans la [RFC3265].

REFER est le seul mécanisme qui puisse créer un abonnement à l'événement refer. Si une demande SUBSCRIBE pour l'événement refer est reçue pour un abonnement qui n'existe pas déjà, elle DOIT être rejetée avec un 403.

On remarquera qu'à la différence de SUBSCRIBE, la transaction REFER ne contient pas une durée pour l'abonnement, ni dans la demande, ni dans la réponse. La durée de vie de l'état abonné est déterminée par le progrès de la demande référencée. La durée de l'abonnement est choisie par l'agent qui accepte le REFER et est communiquée à l'agent qui envoie le REFER dans le NOTIFY initial de l'abonnement (en utilisant le paramètre d'en-tête Expiration de l'état d'abonnement). Noter que les agents qui acceptent REFER et ne souhaitent pas conserver l'état d'abonnement peuvent terminer l'abonnement avec ce NOTIFY initial.

2.4.5 Corps du NOTIFY

Chaque NOTIFY DOIT contenir un corps de type "message/sipfrag" [RFC3420]. Le corps d'un NOTIFY DOIT commencer par une ligne d'état de réponse SIP comme définie dans la [RFC3261]. La classe de réponse dans cette ligne d'état indique l'état de l'action mentionnée. Le corps PEUT contenir d'autres champs d'en-tête SIP pour fournir des informations sur le résultat de l'action référencée. Ce corps fait une déclaration complète de l'état de l'action référencée. Le paquetage d'événement refer ne prend pas en charge les deltas d'état.

Si un NOTIFY est généré lorsque un état d'abonnement est en instance, son corps ne devrait comporter qu'une ligne d'état contenant un code de réponse de 100.

Une mise en œuvre minimale, mais complète, peut répondre avec un seul NOTIFY contenant soit le corps :
SIP/2.0 100 Trying si l'abonnement est en instance,
soit le corps : SIP/2.0 200 OK si la référence a réussie,
soit le corps : SIP/2.0 503 Service indisponible si la référence a échoué,
soit le corps : SIP/2.0 603 Refus si la demande REFER a été acceptée avant que l'approbation de suivre la référence ait pu être obtenue et que l'approbation a été ensuite refusée (voir le paragraphe 2.4.7).

Une mise en œuvre PEUT inclure plus d'un message SIP dans ce corps pour convoyer plus d'informations. Les valeurs de champ d'en-tête Warning reçues dans les réponses à l'action référencée sont de bonnes candidates. En fait, si la référence était à un URI SIP, la réponse entière à l'action référencée pourrait être retournée (peut être pour aider au débogage). Cependant, faire ainsi pourrait avoir de graves répercussions sur la sécurité (voir la Section 5). Les mises en œuvre doivent considérer avec attention ce qu'elles choisissent d'inclure.

Noter que si la référence était à un URI non SIP, l'état dans tous les NOTIFY au référant doit quand même être sous la forme de lignes d'état de réponse SIP. La mise en œuvre minimale discutée ci-dessus est suffisante pour donner une indication basique de succès ou d'échec. Par exemple, si un client reçoit un REFER à un URL HTTP, et si il réussit à accéder à la ressource, son NOTIFY au référant peut contenir le corps de message/sipfrag de "SIP/2.0 200 OK". Si le notificateur souhaite retourner des informations supplémentaires spécifiques d'un protocole non SIP sur l'état de la demande, il les placer dans le corps du message sipfrag.

2.4.6 Demandes REFER multiples dans un dialogue

Un REFER crée un abonnement implicite qui partage les identifiants de dialogue dans la demande REFER. Si plus d'un REFER est produit dans le même dialogue (par exemple, une seconde tentative de transfert d'un appel) les identifiants de

dialogue ne fournissent pas assez d'informations pour associer les NOTIFY résultants avec le REFER approprié.

Donc, pour la seconde demande REFER et les suivantes qu'un UA reçoit dans un dialogue, il DOIT inclure un paramètre id [RFC3265] dans le champ d'en-tête Event de chaque NOTIFY, contenant le numéro de séquence (le numéro tiré de la valeur du champ d'en-tête CSeq) du REFER auquel ce NOTIFY est associé. Ce paramètre id PEUT être inclus dans les NOTIFY au premier REFER qu'un UA reçoit dans un dialogue. Un SUBSCRIBE envoyé pour rafraîchir ou terminer cet abonnement DOIT contenir ce paramètre id.

2.4.7 Utilisation du champ d'en-tête État d'abonnement avec l'événement référence

Chaque NOTIFY doit contenir un champ d'en-tête État d'abonnement comme défini dans la [RFC3265]. Le NOTIFY final envoyé en réponse à un REFER DOIT indiquer que l'abonnement a été "terminé" avec une raison de "noresource". (La ressource à laquelle on est abonné est l'état de la demande référencée).

Si un NOTIFY indique une raison qui montre qu'un réabonnement est approprié selon la [RFC3265], l'agent qui envoie le REFER N'EST PAS obligé de se réabonner.

Dans le cas où un REFER a été accepté avec un 202, mais où l'approbation de suivre la référence a été ensuite refusée, les éléments raison et réessayer-après du champ d'en-tête État d'abonnement peuvent être utilisés pour indiquer si et quand le REFER peut être réessayé (comme décrit pour SUBSCRIBE dans la [RFC3265]).

2.5 Comportement des registraires/serveurs de redirection SIP

Un registraire qui ignore la définition de la méthode REFER va retourner une réponse 501 comme défini dans la [RFC3261]. Un registraire qui connaît la définition de REFER DEVRAIT retourner une réponse 405.

La présente spécification ne fait peser aucune exigence sur le comportement du serveur de redirection au delà de celles spécifiées dans la [RFC3261]. Donc, il est possible que les demandes REFER soient redirigées.

2.6 Comportement des mandataires SIP

Les mandataires SIP n'exigent pas de modification pour prendre en charge la méthode REFER. Précisément, comme exigé par la [RFC3261], un mandataire devrait traiter une demande REFER de la même façon qu'il traite une demande OPTIONS.

3. Détails du paquetage : événement refer

Le présent document définit un paquetage d'événement comme défini dans la [RFC3265].

3.1 Nom de paquetage d'événement

Le nom de ce paquetage d'événement est "refer".

3.2 Paramètres de paquetage d'événement

Ce paquetage utilise le paramètre "id" défini dans la [RFC3265]. Son utilisation dans le paquetage est décrite au paragraphe 2.4.6.

3.3 Corps de SUBSCRIBE

Les corps SUBSCRIBE n'ont pas de signification particulière pour ce paquetage d'événement.

3.4 Durée d'abonnement

La durée d'un abonnement implicite créé par une demande REFER est initialement déterminée par l'agent qui accepte le REFER et elle est communiquée à l'agent souscripteur dans le paramètre Expire du champ d'en-tête État d'abonnement dans le premier NOTIFY envoyé dans l'abonnement. Les choix raisonnables pour cette durée initiale dépendent du type de demande indiqué dans l'URI Refer-To. La durée DEVRAIT être choisie plus longue que le temps qui sera donné à la demande référencée pour s'achever. Par exemple, si l'URI Refer-To est un URI INVITE SIP, l'intervalle d'abonnement

devrait être plus long que la valeur de Expire dans le INVITE. Du temps supplémentaire PEUT être inclus pour tenir compte du temps nécessaire pour autoriser l'abonnement. L'agent souscripteur PEUT étendre l'abonnement en le rafraîchissant, ou le terminer en se désabonnant. Comme décrit au paragraphe 2.4.7, l'agent qui accepte le REFER va terminer l'abonnement lorsque il fait rapport du résultat final de la référence, en indiquant cette terminaison dans le champ d'en-tête État d'abonnement.

3.5 Corps de NOTIFY

Les corps des demandes NOTIFY pour les événements refer sont exposés au paragraphe 2.4.5.

3.6 Traitement par le notificateur des demandes SUBSCRIBE

Le traitement par le notificateur des demandes SUBSCRIBE est exposé au paragraphe 2.4.4.

3.7 Génération par le notificateur des demandes NOTIFY

La génération par le notificateur des demandes NOTIFY est exposée au paragraphe 2.4.4.

3.8 Traitement par l'abonné des demandes NOTIFY

Le traitement par l'abonné des demandes NOTIFY est exposé au paragraphe 2.4.4.

3.9 Traitement des demandes fourchées

Un REFER envoyé dans le cadre d'un dialogue existant ne va pas fourcher. Un REFER envoyé hors du contexte d'un dialogue PEUT fourcher, et si il est accepté par plusieurs agents, PEUT créer plusieurs abonnements. Ces abonnements sont créés et gérés selon le "traitement des demandes fourchées" de la [RFC3265] comme si le REFER avait été un SUBSCRIBE. L'agent qui envoie le REFER gère séparément l'état associé à chaque abonnement. Il NE fusionne PAS l'état des différents abonnements. L'état est celui de la demande référencée à chacun des agents qui l'acceptent.

3.10 Taux des notifications

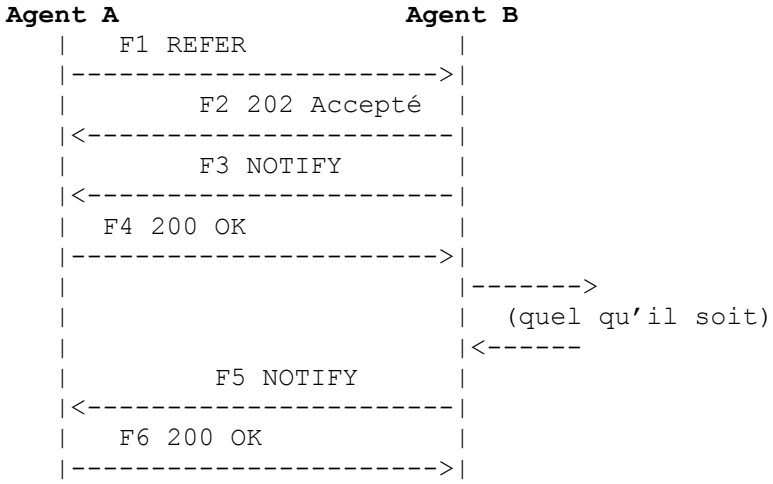
Un événement refer NOTIFY peut être généré chaque fois que devient disponible une nouvelle connaissance de l'état d'une demande référencée. Par exemple, si le REFER était un INVITE SIP, les NOTIFY peuvent être générés avec chaque réponse provisoire et pour la réponse finale à l'INVITE. Autrement, l'abonnement peut ne résulter qu'en deux demandes NOTIFY, le NOTIFY immédiat et le NOTIFY qui porte le résultat final de la référence. Les NOTIFY aux événements refer NE DEVRAIENT PAS être envoyés plus fréquemment qu'une fois par seconde.

3.11 Agents d'état

Des agents d'état séparés ne sont pas définis pour l'événement refer.

4. Exemples

4.1 Prototype de flux d'appel REFER



Voici des exemples de ce à quoi peuvent ressembler les quatre messages entre l'agent A et l'agent B si la référence que fait l'agent B (quelle qu'elle soit) réussit. Les détails de ce flux indiquent que ce REFER particulier survient en dehors d'une

session (il n'y a pas d'étiquette To dans la demande REFER). Si le REFER survient à l'intérieur d'une session, il y aurait une étiquette To non vide dans la demande.

Message un (F1)

REFER sip:b@atlanta.example.com SIP/2.0
Via: SIP/2.0/UDP agenta.atlanta.example.com;branch=z9hG4bK2293940223
To: <sip:b@atlanta.example.com>
From: <sip:a@atlanta.example.com>;tag=193402342
Call-ID: 898234234@agenta.atlanta.example.com
CSeq: 93809823 REFER
Max-Forwards: 70
Refer-To: (whatever URI)
Contact: sip:a@atlanta.example.com
Content-Length: 0

Message deux (F2)

SIP/2.0 202 Accepted
Via: SIP/2.0/UDP agenta.atlanta.example.com;branch=z9hG4bK2293940223
To: <sip:b@atlanta.example.com>;tag=4992881234
From: <sip:a@atlanta.example.com>;tag=193402342
Call-ID: 898234234@agenta.atlanta.example.com
CSeq: 93809823 REFER
Contact: sip:b@atlanta.example.com
Content-Length: 0

Message trois (F3)

NOTIFY sip:a@atlanta.example.com SIP/2.0
Via: SIP/2.0/UDP agentb.atlanta.example.com;branch=z9hG4bK9922ef992-25
To: <sip:a@atlanta.example.com>;tag=193402342
From: <sip:b@atlanta.example.com>;tag=4992881234
Call-ID: 898234234@agenta.atlanta.example.com
CSeq: 1993402 NOTIFY
Max-Forwards: 70
Event: refer
Subscription-State: active;expires=(dépend de l'URI Refer-To)
Contact: sip:b@atlanta.example.com
Content-Type: message/sipfrag;version=2.0
Content-Length: 20
SIP/2.0 100 Trying

Message quatre (F4)

SIP/2.0 200 OK
Via: SIP/2.0/UDP agentb.atlanta.example.com;branch=z9hG4bK9922ef992-25
To: <sip:a@atlanta.example.com>;tag=193402342
From: <sip:b@atlanta.example.com>;tag=4992881234
Call-ID: 898234234@agenta.atlanta.example.com
CSeq: 1993402 NOTIFY
Contact: sip:a@atlanta.example.com
Content-Length: 0

Message cinq (F5)

NOTIFY sip:a@atlanta.example.com SIP/2.0
Via: SIP/2.0/UDP agentb.atlanta.example.com;branch=z9hG4bK9323394234
To: <sip:a@atlanta.example.com>;tag=193402342
From: <sip:b@atlanta.example.com>;tag=4992881234
Call-ID: 898234234@agenta.atlanta.example.com
CSeq: 1993403 NOTIFY
Max-Forwards: 70

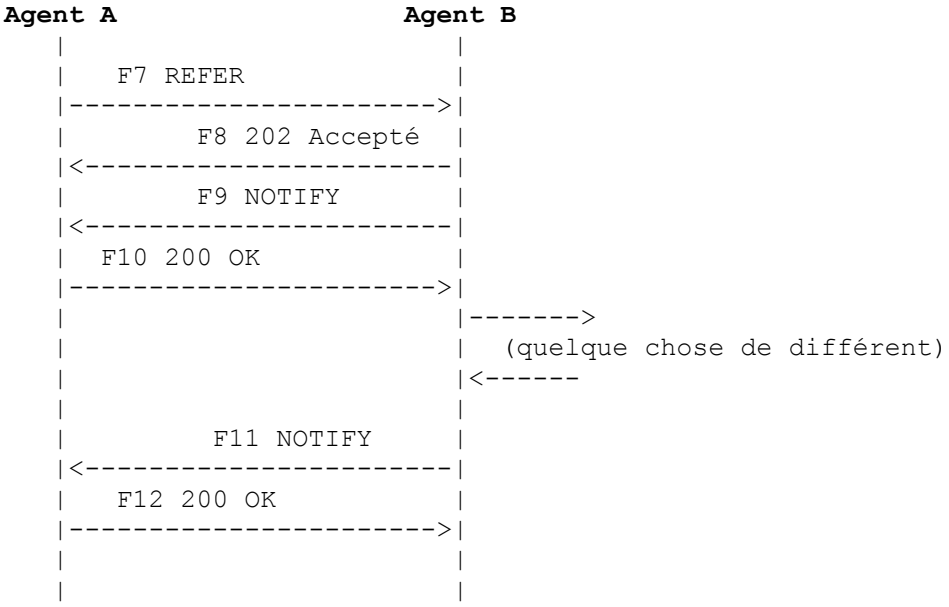
Event: refer
Subscription-State: terminated;reason=noresource
Contact: sip:b@atlanta.example.com
Content-Type: message/sipfrag;version=2.0
Content-Length: 16
SIP/2.0 200 OK

Message six (F6)

SIP/2.0 200 OK
Via: SIP/2.0/UDP agentb.atlanta.example.com;branch=z9hG4bK9323394234
To: <sip:a@atlanta.example.com>;tag=193402342
From: <sip:b@atlanta.example.com>;tag=4992881234
Call-ID: 898234234@agenta.atlanta.example.com
CSeq: 1993403 NOTIFY
Contact: sip:a@atlanta.example.com
Content-Length: 0

4.2 REFER multiples dans un dialogue

Le message un ci-dessus donne le jour à un dialogue d'abonnement implicite. Supposons que l'agent A produise un second REFER à l'intérieur de ce dialogue :



Message sept (F7)

REFER sip:b@atlanta.example.com SIP/2.0
Via: SIP/2.0/UDP agenta.atlanta.example.com;branch=z9hG4bK9390399231
To: <sip:b@atlanta.example.com>;tag=4992881234
From: <sip:a@atlanta.example.com>;tag=193402342
Call-ID: 898234234@agenta.atlanta.example.com
CSeq: 93809824 REFER
Max-Forwards: 70
Refer-To: (some different URI)
Contact: sip:a@atlanta.example.com
Content-Length: 0

Message huit (F8)

SIP/2.0 202 Accepted
Via: SIP/2.0/UDP agenta.atlanta.example.com;branch=z9hG4bK9390399231
To: <sip:b@atlanta.example.com>;tag=4992881234
From: <sip:a@atlanta.example.com>;tag=193402342
Call-ID: 898234234@agenta.atlanta.example.com
CSeq: 93809824 REFER
Contact: sip:b@atlanta.example.com
Content-Length: 0

Message neuf (F9)

NOTIFY sip:a@atlanta.example.com SIP/2.0
Via: SIP/2.0/UDP agentb.atlanta.example.com;branch=z9hG4bK9320394238995
To: <sip:a@atlanta.example.com>;tag=193402342
From: <sip:b@atlanta.example.com>;tag=4992881234
Call-ID: 898234234@agenta.atlanta.example.com
CSeq: 1993404 NOTIFY
Max-Forwards: 70
Event: refer;id=93809824
Subscription-State: active;expires=(dépend de l'URI Refer-To)
Contact: sip:b@atlanta.example.com
Content-Type: message/sipfrag;version=2.0
Content-Length: 20
SIP/2.0 100 Trying

Message dix (F10)

SIP/2.0 200 OK
Via: SIP/2.0/UDP agentb.atlanta.example.com;branch=z9hG4bK9320394238995To:
<sip:a@atlanta.example.com>;tag=193402342
From: <sip:b@atlanta.example.com>;tag=4992881234
Call-ID: 898234234@agenta.atlanta.example.com
CSeq: 1993404 NOTIFY
Contact: sip:a@atlanta.example.com
Content-Length: 0

Message onze (F11)

NOTIFY sip:a@atlanta.example.com SIP/2.0
Via: SIP/2.0/UDP agentb.atlanta.example.com;branch=z9hG4bK2994a93eb-fe
To: <sip:a@atlanta.example.com>;tag=193402342
From: <sip:b@atlanta.example.com>;tag=4992881234
Call-ID: 898234234@agenta.atlanta.example.com
CSeq: 1993405 NOTIFY
Max-Forwards: 70
Event: refer;id=93809824
Subscription-State: terminated;reason=noresource
Contact: sip:b@atlanta.example.com
Content-Type: message/sipfrag;version=2.0
Content-Length: 16
SIP/2.0 200 OK

Message douze (F12)

SIP/2.0 200 OK
Via: SIP/2.0/UDP agentb.atlanta.example.com;branch=z9hG4bK2994a93eb-fe
To: <sip:a@atlanta.example.com>;tag=193402342
From: <sip:b@atlanta.example.com>;tag=4992881234
Call-ID: 898234234@agenta.atlanta.example.com
CSeq: 1993405 NOTIFY
Contact: sip:a@atlanta.example.com

Content-Length: 0

5. Considérations sur la sécurité

Les considérations sur la sécurité décrites à la Section 26 de la [RFC3261] s'appliquent à la transaction REFER. En particulier, les exigences de mise en œuvre et les considérations du paragraphe 26.3 visent à sécuriser une transaction SIP générique. Une considération particulière s'attache aux politiques d'autorisation appliquées aux demandes REFER et à l'utilisation de message/sipfrag pour porter les résultats de la demande référencée.

5.1 Construction d'un URI Refer-To

Ce mécanisme s'appuie sur la fourniture des informations de contact pour la ressource visée en référence avec la partie référencée. Il faut veiller à fournir un URI convenablement restreint si la ressource référencée devait être protégée.

5.2 Considérations d'autorisation pour REFER

Comme décrit au paragraphe 2.4.2, une mise en œuvre peut recevoir une demande REFER avec un URI Refer-To contenant un schéma arbitraire. Par exemple, un usager pourrait être référencé à un service en ligne tel qu'un MUD en utilisant un URI telnet. Un service d'utilisateur pourrait renvoyer un usager à une page de la Toile de suivi d'ordre en utilisant un URI HTTP. Le paragraphe 2.4.2 permet à un agent d'utilisateur de rejeter une demande REFER lorsque il ne peut pas traiter le schéma référencé. Il exige aussi que l'agent d'utilisateur obtienne l'autorisation de son usager avant de tenter d'utiliser l'URI. Généralement, cela peut se faire en invitant l'usager avec l'URI complet et une question telle que "Souhaites vous accéder à cette ressource (O/N)". Bien sûr, les URI peuvent être d'une longueur arbitraire et sont à l'occasion construits avec une intention malveillante, de sorte qu'il faut faire attention à éviter des surprises même dans l'affichage de l'URI lui-même (comme un affichage partiel ou un échec). De plus, il faut faire attention à exposer autant d'informations que possible sur la référence à l'usager pour atténuer le risque d'être entraîné à une décision dangereuse. Par exemple, l'en-tête Refer-To peut contenir une nom d'affichage avec l'URI. Rien n'assure que les propriétés impliquées par ce nom d'affichage sont partagées par l'URI. Par exemple, le nom d'affichage contient "sûr" ou "président" alors que l'URI indique sip:agent59@telemarketing.example.com. Donc, l'invite de l'usager avec le nom d'affichage seul est insuffisant.

Dans certains cas, l'usager peut donner l'autorisation pour certaines demandes REFER par avance en fournissant une politique à l'agent d'utilisateur. Ceci est approprié, par exemple, pour un transfert d'appel, comme exposé dans la [RFC5589]. Ici, une demande REFER correctement authentifiée au sein d'un dialogue SIP existant à un URI sip:, sips:, ou tel: peut être accepté à travers une politique sans obtenir de façon interactive l'autorisation de l'usager. De même, il peut être approprié d'accepter un REFER correctement authentifié à un URI HTTP si le référant est sur une liste explicite de référents approuvés. En l'absence d'une telle autorisation fournie à l'avance, l'usager doit fournir de façon interactive l'autorisation de référencer la ressource indiquée.

Pour voir le danger d'une politique qui accepte et agit aveuglément sur un URI HTTP, considérons par exemple, un serveur de la Toile configuré à n'accepter que les demandes de clients derrière le pare-feu d'une petite organisation. Comme il se tient dans l'environnement douillet où la petite organisation fait confiance à tous ses membres et a peu de sécurité interne, le serveur de la Toile est fréquemment en retard de maintenance, le laissant vulnérable aux attaques par des URI de construction malveillante (résultant peut-être en du code arbitraire fourni dans l'URI). Si un UA SIP à l'intérieur de ce pare-feu a accepté aveuglément une référence à un URI HTTP arbitraire, un attaquant à l'extérieur du pare-feu pourrait compromettre le serveur de la Toile. D'un autre côté, si l'utilisateur de l'UA doit prendre une action positive (telle que de répondre à une invite) avant d'agir sur cet URI, le risque est réduit au même niveau que celui de l'usager qui clique sur l'URI dans un navigateur de la Toile ou dans un message électronique.

La conclusion du paragraphe ci-dessus se généralise aux URI de schéma arbitraire. Un agent qui prend des actions automatiques pour accéder à un URI avec un certain schéma risque d'être utilisé pour attaquer indirectement un autre hôte qui est vulnérable à certaines fautes de la sécurité qui se rapportent à ce schéma. Ce risque et le potentiel de dommages à cet autre hôte est augmenté lorsque l'hôte et l'agent résident derrière un point commun de mise en application de politique tel qu'un pare-feu. De plus, cet agent augmente son exposition aux attaques de déni de service par épuisement de ressources, en particulier si chaque action automatique implique d'ouvrir une nouvelle connexion.

Les agents d'utilisateur devraient faire attention lorsque ils traitent un URI arbitraire sur des services tiers tels que ceux fournis par certains systèmes d'exploitation modernes, en particulier si l'agent d'utilisateur ne connaît pas le schéma et ses possibles ramifications pour utiliser les protocoles qu'il indique. L'opportunité de violation du principe de moindre surprise est très élevé.

5.3 Considérations sur l'utilisation de message/sipfrag

L'utilisation des corps message/sipfrag pour retracer les progrès et résultats d'une demande REFER est extrêmement puissante. Une utilisation inattentive de cette capacité peut compromettre la confidentialité et le secret. Voici deux exemples simples, un peu forcés, pour montrer le potentiel de dommages.

5.3.1 Circonvenir la confidentialité

Supposons qu'Alice a un agent d'utilisateur qui accepte les demandes REFER à des URI SIP INVITE, et des NOTIFY au référant des progrès de l'INVITE en copiant chaque réponse à l'INVITE dans le corps d'un NOTIFY.

Supposons de plus que Carol a une raison pour éviter Mallory et a configuré son système sut son mandataire pour n'accepter les appels que d'un certain ensemble de gens de confiance (parmi lesquels Alice) de sorte que Mallory n'apprenne pas quand elle est là, ou quel agent d'utilisateur elle utilise en fait.

Mallory peut envoyer un REFER à Alice, avec un URI Refer-To qui indique Carol. Si Alice peut joindre Carol, le 200 OK qu'envoie Carl est retourné à Mallory dans un NOTIFY, lui faisant savoir non seulement que Carol est là, mais aussi l'adresse IP de l'agent qu'elle utilisé.

5.3.2 Circonvenir le secret

Supposons qu'Alice, avec le même agent d'utilisateur que ci-dessus, travaille dans une société qui fonctionne avec le plus gros appareil SIP jamais inventé - le SIP FOO. La société a travaillé pendant des mois à construire l'appareil et le matériel de commercialisation, gardant soigneusement l'idée secrète, et même le nom de l'idée (car un FOO est une de ces choses que n'importe qui pourrait faire si on en avait juste l'idée le premier). FOO est prêt et fonctionne, et tout le monde dans la société peut l'utiliser, mais il n'est pas disponible en dehors du pare-feu de la société.

Mallory a entendu des rumeurs selon lesquelles la société d'Alice est sur une grosse affaire, et s'est même débrouillé pour mettre la main sur un URI dont il soupçonner qu'il pourrait être en rapport avec cela. Il envoie un REFER à ALICE avec le mystérieux URI et lorsque Alice se connecte au FOO, Mallory obtient des NOTIFY avec des corps contenant "Server: FOO/v0.9.7".

5.3.3 Limiter les failles

Pour chacun de ces cas, et en général, retourner un sous-ensemble soigneusement choisi des informations disponibles sur les progrès de la référence à travers les NOTIFY atténue le risque. La mise en œuvre minimale décrite au paragraphe 2.4.5 expose moins les informations sur ce qu'a fait l'agent qui opère sur la demande REFER, et sera moins probablement un outil utile pour des utilisateurs malveillants .

5.3.4 Considérations de couper, coller, et duplication

Le mécanisme défini dans la présente spécification n'est pas directement susceptible d'abus par la copie des corps message/sipfrag à partir des demandes NOTIFY et leur insertion, en tout ou partie, dans de futures demandes NOTIFY associées au même REFER ou à un REFER différent. Sous la présente spécification, l'agent qui répond à la demande REFER a le complet contrôle du contenu des corps des NOTIFY qu'il envoie. Il n'y a pas de mécanisme qui soit défini ici qui exige que cet agent transmette de bonne foi une information provenant de la partie référencée. Donc, conserver un corps pour une répétition ultérieure ne donne pas à l'agent la capacité d'affecter le mécanisme défini dans ce document chez son correspondant plus qu'il ne l'a sans ce corps. De même, la capture d'un corps message/sipfrag par un espion ne lui donnera pas plus de capacité d'affecter ce mécanisme qu'il n'en aurait sans cela.

De futures extensions peuvent faire peser des contraintes supplémentaires sur l'agent qui répond à REFER pour permettre d'utiliser une partie du corps de message/sipfrag dans un NOTIFY pour faire des déclarations comme "J'ai contacté la partie que vous m'avez référencée, et en voici une preuve cryptographique". Ces déclarations pourraient être utilisées pour affecter le comportement de l'UA receveur. Ce type d'extension devra définir des mécanismes supplémentaires pour se protéger contre les attaques fondées sur la copie.

6. Éléments d'historique

À l'origine, cette méthode était motivée par l'application de transfert d'appel. Elle a commencé comme TRANSFER, et a ensuite été généralisée en REFER, cette méthode s'est améliorée avec le concept BYE/Also concept du projet expiré ietf-sip-cc-01 en dissociant les transferts du traitement de BYE. Ces changements facilitent la récupération des échecs de

transfert et précisent la gestion d'état dans les entités participantes.

Les premières versions de ce travail exigeaient que l'agent qui répond à REFER attende jusqu'à ce que s'achève l'action référencée avant d'envoyer une réponse finale au REFER. Cette réponse finale reflétait le succès ou l'échec de l'action référencée. Cela était infaisable à cause des règles de temporisation de transaction définies pour les demandes non INVITE dans la [RFC3261]. Un REFER doit toujours recevoir une réponse finale immédiate (dans la durée de vie d'une transaction non INVITE).

7. Considérations relatives à l'IANA

Le présent document définit un nouveau nom de méthode SIP (REFER), un nouveau nom de champ d'en-tête SIP avec une forme compacte (respectivement Refer-To et r) et un paquetage d'événement (refer).

Ce qui suit a été ajouté au sous-registre method sous http://www.iana.org/assignments/sip-parameters.

REFER : [RFC3515]

Les informations suivantes ont aussi été ajoutées au sous-registre d'en-têtes sous http://www.iana.org/assignments/sip-parameters.

Nom d'en-tête : Refer-To
Forme compacte : r
Référence : RFC 3515

La présente spécification enregistre un paquetage d'événement, fondé sur les procédures d'enregistrement définies dans la [RFC3265]. Les informations qui suivent sont exigées pour un tel enregistrement :

Nom du paquetage : refer
Paquetage ou gabarit de paquetage : C'est un paquetage.
Spécification publiée : RFC 3515
Personne à contacter : Robert Sparks, rsparks@dynamicsoft.com

8. Remerciements

Le présent document est le produit de la collaboration du groupe de travail SIP.

9. Références

[RFC3261] J. Rosenberg et autres, "SIP : Protocole d'initialisation de session", juin 2002. (*Mise à jour par* RFC3265, RFC3853, RFC4320, RFC4916, RFC5393, RFC6665))

[RFC3265] A.B. Roach, "Notification d'événement spécifique du protocole d'initialisation de session (SIP)", juin 2002. (*MàJ par* RFC6446) (*Remplacée par la* RFC6665)

[RFC3420] R. Sparks, "message/sipfrag de type de support Internet", novembre 2002.

[RFC5589] R. Sparks, A. Johnston, éd., D. Petrie, "Contrôle du transfert d'appel dans le protocole d'initialisation de session (SIP)", juin 2009. (BCP0149)

10. Considérations de propriété intellectuelle

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 le 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.

11. Adresse de l'auteur

Robert J. Sparks
dynamicsoft
5100 Tennyson Parkway
Suite 1200
Plano, TX 75024
USA
mél : rsparks@dynamicsoft.com

12. Déclaration complète de droits de reproduction

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