Groupe de travail Réseau
Request for Comments : 4974
RFC mise à jour : 3473
Catégorie : sur la voie de la normalisation

D. Papadimitriou, Alcatel
A. Farrel, Old Dog Consulting
août 2007
Traduction Claude Brière de L'Isle

Extensions de signalisation RSVP-TE à MPLS généralisée (GMPLS) pour la prise en charge des appels

Résumé
Dans certaines topologies de réseau, il peut être avantageux de maintenir des associations entre les points d'extrémité et les points de transit clés pour prendre en charge une instance d'un service. Ces associations sont connues sous le nom d'appels.

Un appel ne fournit pas la connectivité réelle pour transmettre le trafic d'utilisateur, mais établit seulement une relation par laquelle des connexions ultérieures peuvent être établies. Dans le système MPLS généralisé (GMPLS) ces connexions sont connues sous le nom de chemins à commutation d'étiquettes (LSP, *Label Switched Path*).

Le présent document spécifie comment la signalisation GMPLS du protocole de réservation de ressources - ingénierie du trafic (RSVP-TE) peut être utilisée et étendue pour prendre en charge les appels. Ces mécanismes assurent une séparation complète et logique entre l'appel et la connexion.

Les mécanismes proposés dans ce document sont applicables à tout environnement (y compris les multi zones) et à tout type d'interface : commutation par paquets, couche 2, multiplexage temporel, lambda ou fibre.

Table des Matières

1. Introduction

Le présent document définit les procédures de protocole et les extensions pour prendre en charge les appels au sein de MPLS généralisé (GMPLS).

Un appel est une association entre des points d'extrémité et éventuellement entre des points de transit clés (tels que les frontières de réseau) à l'appui d'une instance d'un service. L'association de bout en bout est appelée un "appel", et l'association entre deux points de transit ou entre un point d'extrémité et un point de transit est appelée un "segment d'appel". Une entité qui traite un appel ou un segment d'appel est appelée un "gestionnaire d'appel".

Un appel ne fournit pas la connexité réelle pour transmettre le trafic d'utilisateur, mais établit seulement une relation par laquelle des connexions ultérieures peuvent être établies. Dans GMPLS, ces connexions sont connues sous le nom de chemins à commutation d'étiquettes (LSP, *Label Switched Path*). Le présent document ne modifie pas les procédures d'établissement de connexion définies dans les [RFC3473], [RFC4208] et [RFC5150]. Les connexions établies dans le cadre d'un appel suivent les règles définies dans ces documents.

Un appel peut être associé à zéro, une ou plusieurs connexions, et une connexion peut être associée à zéro ou un appel. Il faut donc une séparation complète et logique entre l'appel et la connexion.

L'architecture du réseau optique à commutation automatique (ASON) de l'UIT-T [G.8080] donne un exemple des exigences relatives aux appels et les exigences spécifiques relatives à la prise en charge des appels dans ce contexte figurent dans la [RFC4139]. Noter cependant que si les mécanismes décrits dans le présent document répondent aux exigences énoncées dans la [RFC4139], ils ont une applicabilité plus large.

Les mécanismes définis dans le présent document sont également applicables à toute interface de paquets (PSC), aux interfaces de couche 2 (L2SC), aux interfaces compatibles TDM, aux interfaces LSC ou aux interfaces FSC. Les mécanismes et les extensions de protocole sont rétrocompatibles et peuvent être utilisés pour la gestion d'appel où seuls les gestionnaires d'appels ont besoin de connaître les extensions de protocole.

1.1 Applicabilité à ASON

La [RFC4139] détaille les exigences relatives à la signalisation GMPLS pour satisfaire l'architecture ASON décrite dans [G.8080]. Les mécanismes décrits dans ce document satisfont aux exigences relatives aux appels décrites aux paragraphes 4.2 et 4.3 de la [RFC4139] et aux exigences supplémentaires relatives aux appels, décrites aux paragraphes 4.4, 4.7, et aux Sections 5 et 6 de la [RFC4139].

[ASON-APPL] décrit l'applicabilité des protocoles à l'architecture ASON.

2. Conventions utilisées dans ce document

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119].

De plus, le lecteur est supposé être familiarisé avec la terminologie utilisée dans les [RFC3471], [RFC3473], [RFC3477], et [RFC3945].

3. Exigences

3.1 Fonction d'appel de base

Le concept d'appel est utilisé pour fournir les capacités suivantes :
- Vérification et identification de l'initiateur de l'appel (avant l'établissement du LSP).
- Prise en charge de l'enchaînement virtuel avec divers composants de chemin de LSP.
- Association de plusieurs LSP à un seul appel (les aspects liés à la récupération sont détaillés dans les [RFC4426] et [RFC4872]).
- Facilitation des opérations du plan de contrôle en permettant un changement d'état opérationnel du LSP associé.

Les procédures et les extensions de protocole pour prendre en charge l'établissement d'appel et l'association des appels avec les connexions sont décrites à partir de la section 5 du présent document.

3.2 Séparation de l'appel et de la connexion

Une séparation complète et logique entre l'appel et la connexion est nécessaire. C'est-à-dire :
- Il DOIT être possible d'établir une connexion sans dépendre d'un appel.
- Il DOIT être possible d'établir un appel sans aucune connexion associée.
- Il DOIT être possible d'associer plus d'une connexion à un appel.
- La suppression de la dernière connexion associée à un appel NE DEVRAIT PAS entraîner la suppression automatique de l'appel, sauf dans le cadre d'une politique locale à l'entrée de l'appel.
- La signalisation d'une connexion associée à un appel NE DOIT PAS nécessiter la distribution ou la conservation d'informations relatives à l'appel (état) au sein du réseau.

3.3 Segments d'appel

Les capacités de segment d'appel DOIVENT être prises en charge.

Les procédures et les extensions du protocole de signalisation RSVP-TE (GMPLS) pour la prise en charge des segments d'appel sont décrites au paragraphe 7.3.1 du présent document.

4. Concepts et termes

Les concepts d'appel et de connexion sont également abordés dans l'architecture ASON [G.8080] et la [RFC4139]. Cette section n'est pas destinée à remplacer ces documents, mais constitue un bref résumé des termes et concepts clés.

4.1 Qu'est ce qu'un "appel" ?

Un appel est un accord entre des points d'extrémité, éventuellement en coopération avec les nœuds qui fournissent l'accès au réseau. L'établissement d'appel peut inclure l'échange de capacités, la politique, l'autorisation et la sécurité.

Un appel est utilisé pour faciliter et gérer un ensemble de connexions qui fournissent des services de données de bout en bout. Alors que les connexions nécessitent le maintien d'un état dans les nœuds situés le long du chemin des données dans le réseau, les appels n'impliquent pas la participation des nœuds de transit, si ce n'est pour transmettre les demandes de gestion d'appel sous forme de messages transparents.

Un appel peut être établi et maintenu indépendamment des connexions qu'il prend en charge.

4.2. Hiérarchie des appels, connexions, tunnels, et LSP

Il est clair qu'il existe une relation hiérarchique entre les appels et les connexions. Une ou plusieurs connexions peuvent être associées à un appel. Une connexion ne peut pas faire partie de plus d'un appel. Une connexion peut toutefois exister sans appel.

Dans RSVP-TERSVP-TE GMPLS [RFC3473], une connexion est identifiée par un tunnel GMPLS TE. Généralement, un tunnel est identifié avec un seul LSP, mais on devrait noter que pour la protection, l'équilibrage de charge, et beaucoup d'autres fonctions, un tunnel peut être pris en charge par plusieurs LSP parallèles. L'identification suivante reproduit cette hiérarchie.

- Les identifiants d'appel sont uniques dans le contexte de la paire d'adresses qui sont la source et la destination de l'appel.

- Les identifiants de tunnel sont uniques dans le contexte de la session (qui est la destination du tunnel). Les applications peuvent également trouver pratique de garder l'identifiant de tunnel unique dans le contexte d'un appel.

- Les identifiants de LSP sont uniques dans le contexte d'un tunnel.

Noter que la valeur Call_ID de zéro est réservée et NE DOIT PAS être utilisée pendant l'établissement d'un appel indépendant du LSP.

Dans la suite du présent document, les termes LSP et tunnel sont utilisés de manière interchangeable avec le terme connexion. Le cas d'un tunnel qui est pris en charge par plus d'un LSP est couvert implicitement.

4.3 Échange des capacités des liaisons d'accès

Dans un modèle superposé, il est utile pour le nœud d'entrée d'un LSP de connaître les capacités de la liaison entre le réseau et le réseau superposé distant. Dans le langage de la [RFC4208], le nœud d'entrée peut utiliser des informations sur la liaison entre le nœud central de sortie (CN) et le nœud de bordure distant (EN). Nous appelons cette liaison la liaison de réseau de sortie. Ces informations peuvent permettre au nœud d'entrée d'adapter sa demande de LSP à ces capacités et de mieux utiliser les ressources du réseau en fonction de ces capacités.

Par exemple, cela pourrait être utilisé dans les réseaux optiques transparents pour fournir des informations sur la disponibilité lambda sur les liaisons de réseau de sortie ou, lorsque le CN de sortie est capable de régénérer le signal, cela pourrait fournir un mécanisme de négociation des attributs de qualité du signal (tels que le taux d'erreur sur les bits). De même, dans les environnements d'acheminement multi domaines, cela pourrait être utilisé pour assurer la sélection de bout en bout des liaisons composantes (c'est-à-dire la négociation des attributs spatiaux) lorsque les liaisons TE ont été regroupées sur la base d'attributs spécifiques de la technologie.

Dans certains cas, la base de données d'ingénierie du trafic (TED, *Traffic Engineering Database*) peut contenir suffisamment d'informations pour que des décisions soient prises quant à la liaison de réseau de sortie à utiliser. Dans d'autres cas, la base de données d'ingénierie du trafic peut ne pas contenir ces informations et l'établissement de l'appel peut fournir un mécanisme approprié pour échanger des informations à cette fin. Le répondant à l'appel peut utiliser les paramètres d'appel pour sélectionner un sous-ensemble de liaisons de réseau de sortie disponibles entre la CN de sortie et l'EN distant, et peut signaler ces liaisons et leurs capacités dans la réponse d'appel afin que l'initiateur de l'appel puisse sélectionner une liaison appropriée.

Les paragraphes suivants indiquent les cas où la TED peut être utilisée et ceux où l'échange de paramètres d'appel peut être approprié.

4.3.1 Appels initiés par le réseau

Les appels initiés par le réseau surviennent lorsque l'entrée (et par conséquent la sortie) se situe dans le réseau et qu'il n'est peut-être pas nécessaire de distribuer des informations supplémentaires sur la capacité de la liaison en plus des informations distribuées par les extensions TE et GMPLS à l'IGP. En outre, il est possible que des extensions futures à ces IGP permettent la distribution d'informations plus détaillées, y compris les dégradations optiques.

4.3.2 Appels initiés par l'utilisateur

Les appels initiés par l'utilisateur surviennent lorsque l'entrée (et par conséquent la sortie) se situe en dehors du réseau. Les informations relatives aux liaisons de périphérie peuvent ne pas être visibles dans le réseau central, ni (et surtout) dans les autres nœuds de périphérie. Cela peut empêcher un entrant de demander des caractéristiques de LSP appropriées pour assurer la réussite de l'établissement du LSP.

Il existe plusieurs solutions à ce problème, incluant la définition de liaisons TE statiques (c'est-à-dire non annoncées par un protocole d'acheminement) entre les CN et les EN. Néanmoins, des procédures spéciales peuvent être nécessaires pour annoncer aux nœuds de bordure extérieurs au réseau des informations sur les liaisons du réseau de sortie sans annoncer également les informations spécifiques du contenu du réseau.

À l'avenir, lorsque les exigences relatives aux informations qui doivent être prises en charge seront mieux comprises, des extensions TE aux EGP pourront être définies pour assurer cette fonction, et de nouvelles règles pour la divulgation d'informations de TE entre les instances d'acheminement pourront être utilisées.

4.3.3 Utilisation de l'établissement d'appel

Lorsque les solutions IGP et EGP ne sont pas disponibles au niveau de l'interface utilisateur-réseau (UNI, *User-to-Network Interface*) il est toujours nécessaire de connaître les capacités des liaisons de périphérie distantes au niveau des nœuds de périphérie locaux.

La procédure d'établissement d'appel permet de découvrir les capacités des liaisons de périphérie des nœuds de périphérie distants avant de tenter d'établir des LSP.

- Le répondant à l'appel peut retourner des informations sur une ou plusieurs liaisons de réseau de sortie. Il peut renvoyer une liste complète des liaisons disponibles avec des informations sur les capacités des liaisons, ou filtrer la liste pour ne renvoyer que des informations sur les liaisons susceptibles de prendre en charge les connexions nécessaires à l'appel. Pour cette deuxième option, le répondantà l'appel doit déterminer les liaisons appropriées à partir des informations contenues dans la demande d'appel, notamment la destination de l'appel et le niveau de service (largeur de bande, protection, etc.) requis.

- Lorsqu'il reçoit une réponse d'appel, l'initiateur de l'appel doit déterminer les chemins pour les connexions (LSP) qu'il va établir. La manière dont il le fait sort du cadre du présent document puisqu'il s'agit d'un processus algorithmique spécifique de la mise en œuvre. Cependant, il peut prendre en entrée les informations sur les liaisons de réseau de sortie disponibles, telles qu'elles sont fournies dans la réponse à l'appel.

L'objet LINK_CAPABILITY est défini pour permettre l'échange de ces informations. Les informations incluses dans cet objet sont similaires à celles distribuées par les IGP compatibles GMPLS (voir la [RFC4202]).

5. Extensions au protocole pour les appels et les connexions

Cette section décrit les extensions de protocole nécessaires à la prise en charge de l'identification des appels et de la gestion des appels et des connexions. Les procédures d'utilisation de ces extensions de protocole sont décrites à la Section 6.

5.1. Établissement et suppression d'appel

Les appels sont établis indépendamment des connexions grâce à l'utilisation du message Notify. Le message Notify est un message ciblé et n'a pas besoin de suivre le chemin des LSP à travers le réseau.

L'établissement simultané d'un appel et d'une connexion (parfois appelé "portage") n'est pas pris en charge.

5.2 Identification d'appel

Dès que le concept d'appel est introduit, il est nécessaire de prévoir un moyen d'identifier l'appel. Cela devient particulièrement important lorsque les appels et les connexions sont séparés et que les connexions doivent contenir une référence à l'appel.

Un appel peut être identifié par une séquence d'octets d'une longueur considérable (mais non arbitraire). Un identifiant d'appel de 40 octets ne serait pas déraisonnable. Il n'appartient pas au présent document de fournir des règles de codage ou d'analyse des identifiants d'appel, mais il doit fournir un moyen approprié de communiquer les identifiants d'appel dans le

cadre du protocole. L'identification complète de l'appel est appelée identification longue d'appel.

L'identifiant d'appel n'est pertinent que pour les nœuds d'émission et de réception. La maintenance de cette information dans l'état de signalisation n'est obligatoire pour aucun nœud intermédiaire. Par conséquent, aucune modification des mises en œuvre de transit de la [RFC3473] n'est nécessaire et il n'y a pas de problème de rétro compatibilité. La compatibilité future est maintenue en utilisant les valeurs par défaut existantes pour indiquer qu'aucun traitement d'appel n'est nécessaire.

En outre, l'identifiant long d'appel n'est pas nécessaire dans le cadre de l'état de la connexion (LSP) même aux nœuds d'émission et de réception, tant qu'une certaine forme de corrélation est disponible. Cette corrélation est fournie par l'identifiant court d'appel.

5.2.1 Forme longue d'identification d'appel

L'identifiant long d'appel n'est requis que dans le message Notify utilisé pour établir l'appel. Il figure dans le champ "Nom de session" de l'objet SESSION_ATTRIBUTE du message Notify.

Une valeur unique par appel est insérée dans le champ "Nom de session" par l'initiateur de l'appel. Les nœuds centraux suivants PEUVENT inspecter cet objet et DOIVENT le transmettre de manière transparente à travers les interfaces réseau jusqu'à ce qu'il atteigne le nœud de sortie. Noter que la structure de ce champ PEUT faire l'objet d'un formatage supplémentaire en fonction de la ou des conventions de dénomination. Toutefois, la [RFC3209] définit le champ "Nom de la session" comme une chaîne d'affichage bourrée avec des zéros, de sorte que toute convention de formatage pour l'identifiant d'appel doit être limitée à cette portée.

5.2.2 Forme courte d'identification d'appel

Les connexions (LSP) associées à un appel doivent contenir une référence à l'appel - l'identifiant court de l'appel. Un nouveau champ est ajouté au protocole de signalisation pour identifier un LSP individuel avec l'appel auquel il appartient.

Le nouveau champ est un identifiant de 16 bits (unique dans le contexte de l'appariement d'adresses fourni par l'adresse du point de terminaison du tunnel et l'adresse de l'expéditeur de l'objet SENDER_TEMPLATE) qui DOIT être échangé dans le message Notify pendant l'initialisation de l'appel et qui est utilisé dans tous les messages de LSP ultérieurs qui sont associés à l'appel. Cet identifiant est connu sous le nom d'identifiant court d'appel et est codé comme décrit au paragraphe 5.2.3. L'identifiant d'appel NE DOIT PAS être utilisé au titre du traitement visant à déterminer la session à laquelle s'applique un message de signalisation RSVP. Cela ne pose aucun problème de rétro compatibilité puisque le champ réservé de l'objet SESSION défini dans la [RFC3209] NE DOIT PAS être examiné à la réception.

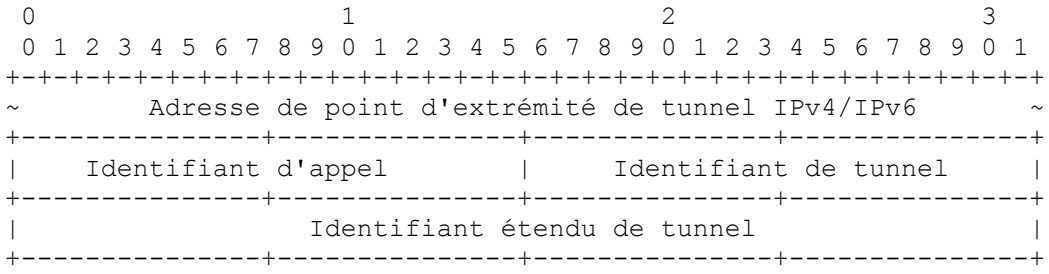
Dans le cas improbable de l'épuisement des identifiants courts d'appel, la politique locale du nœud déciderait des mesures spécifiques à prendre, mais pourrait inclure l'utilisation d'une deuxième adresse d'envoyeur. Les détails de la politique locale sortent du champ d'application du présent document.

5.2.3 Forme courte de codage d'identifiant d'appel

L'identifiant court d'appel est porté dans un champ de 16 bits de l'objet SESSION contenu dans le message Notify utilisé pendant l'établissement de l'appel et dans tous les messages pendant l'établissement et la gestion du LSP. Le champ utilisé était précédemment réservé (DOIT être réglé à zéro à l'émission et ignoré à la réception). Cela assure la rétro compatibilité avec les nœuds qui n'utilisent pas d'appels.

La figure ci-dessous montre la nouvelle version de l'objet.

Classe = SESSION, Numéro de classe = 1, Type de classe = 7(IPv4)/8(IPv6)



Adresse de point d'extrémité de tunnel IPv4/IPv6 : 32 bits/128 bits (voir la [RFC3209])

Identifiant d'appel : 16 bits. Identifiant de 16 bits utilisé dans l'objet SESSION qui reste constant sur la vie de l'appel. La valeur de l'identifiant d'appel DOIT être réglée à zéro quand il n'y a pas d'appel correspondant.

Identifiant de tunnel : 16 bits (voir la [RFC3209])

Identifiant étendu de tunnel : 32 bits/128 bits (voir la [RFC3209])

5.3 Objet LINK_CAPABILITY

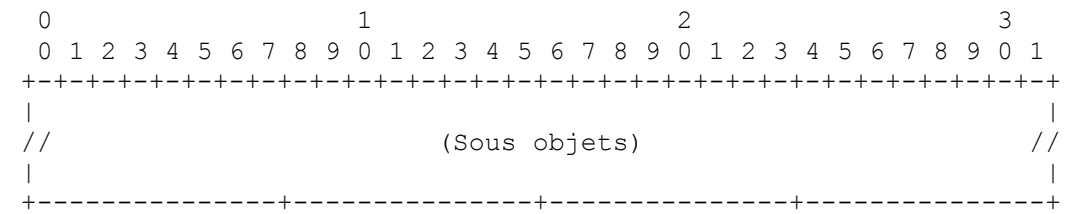
L'objet LINK_CAPABILITY est introduit pour prendre en charge l'échange de capacités de liaison pendant l'établissement de l'appel et PEUT être inclus dans un message Notify utilisé pour l'établissement de l'appel. Cet objet facultatif comprend les capacités de liaison locale d'une liaison reliant le nœud initiateur de l'appel (ou le nœud de terminaison de l'appel) au réseau. Le nœud spécifique est indiqué par l'adresse de source du message Notify.

La liaison signalée peut être une liaison unique ou une liaison en faisceau [RFC4201].

Le numéro de classe est choisi de manière à ce que les nœuds qui ne reconnaissent pas cet objet l'éliminent en silence. En d'autres termes, le bit de poids fort est à un et le bit suivant est à zéro.

Cet objet a le format suivant :

Numéro de classe = 133 (forme 10bbbbbb), Typede classe = 1



Le contenu de l'objet LINK_CAPABILITY est défini comme une série d'éléments de données de longueur variable appelés des sous objets. Le format des sous objets est défini dans la [RFC3209].

Les sous-objets suivants sont actuellement définis.
- Type 1 : l'adresse IPv4 de liaison locale d'une liaison ou d'un faisceau numéroté selon le format défini dans la [RFC3209].
- Type 2 : l'adresse IPv6 de liaison locale d'une liaison ou d'un faisceau numéroté selon le format défini dans la [RFC3209].
- Type 4 : l'identifiant de liaison locale d'une liaison ou d'un faisceau non numéroté en utilisant le format défini dans la [RFC3477].
- Type 64 : la bande passante maximale réservable correspondant à cette liaison ou à ce faisceau (voir la [RFC4201]).
- Type 65 : le descripteur de capacité de commutation d'interface (voir la [RFC4202]) correspondant à cette liaison ou à ce faisceau (voir aussi la [RFC4201]).

Note : de futures révisions du présent document pourront allonger la liste ci-dessus.

Une seule instance de cet objet PEUT être utilisée pour échanger les informations de capacité relatives à plus d'une liaison ou liaison groupée. Dans ce cas, l'ordre suivant DOIT être utilisé :
- chaque liaison DOIT être identifiée par un sous objet Identifiant (type 1, 2 ou 4)
- les sous objets Capacité (type 64 ou 65, et sous objets futurs) DOIVENT être placés après le sous-objet Identifiant pour la liaison ou faisceau auquel ils se réfèrent.

Plusieurs instances de l'objet LINK_CAPABILITY dans le même message de notification ne sont pas acceptées par la présente spécification. Si un message de notification contient plusieurs objets LINK_CAPABILITY, le receveur DEVRAIT traiter le premier comme d'habitude et ignorer les instances suivantes de l'objet.

5.4 Formats de message révisés

Le message Notify est amélioré pour prendre en charge l'établissement et la suppression des appels. Voir à la Section 6 la description des procédures.

5.4.1 Message Notify

Le message Notify est modifié dans l'établissement d'appel par l'ajout facultatif de l'objet LINK_CAPABILITY. En outre, l'objet SESSION_ATTRIBUTE est ajouté à la séquence <notifier la session> pour transporter l'identifiant long d'appel. La présence de l'objet SESSION_ATTRIBUTE PEUT être utilisée pour distinguer un message Notify utilisé pour la gestion d'appel, mais voir un autre mécanisme au paragraphe 5.5. Le <Notifier la liste des sessions> PEUT être utilisé pour établir simultanément plusieurs appels.

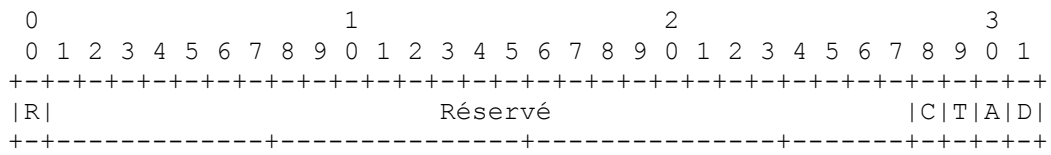
Le format du message Notify est le suivant :

```
<message Notify>  ::= <En-tête commun> [ <INTEGRITY> ]
                      [[ <MESSAGE_ID_ACK> | <MESSAGE_ID_NACK>]...]
                      [ <MESSAGE_ID> ]
                      <ERROR_SPEC>
                      <Notifier la liste des sessions>

<Notifier la liste des sessions> ::= [ <Notifier la liste des sessions> ] <Notifier la session>

<Notifier la session>  ::= <SESSION> [ <ADMIN_STATUS> ]
                           [ <POLICY_DATA>...]
                           [ <LINK_CAPABILITY> ]
                           [ <SESSION_ATTRIBUTE> ]
                           [ <descripteur de l'envoyeur> | <descripteur de flux> ]

<descripteur de l'envoyeur> ::= voir la [RFC3473]

<descripteur de flux> ::= voir la [RFC3473]
```

5.5 Objet ADMIN_STATUS

Les messages Notify échangés à des fins de contrôle et de gestion des appels comportent un nouveau bit spécifique (le bit Gestion d'appel ou C) dans l'objet ADMIN_STATUS.

La [RFC3473] indique que le format et le contenu de l'objet ADMIN_STATUS sont définis dans la [RFC3471]. Le nouveau bit "C" est ajouté pour le contrôle d'appel, comme indiqué ci-dessous.



Reflet (R) : 1 bit - voir la [RFC3471]
Gestion d'appel (C) : 1 bit. Ce bit est établi quand le message est utilisé pour contrôler et gérer un appel. Les procédures pour l'utilisation du bit C sont décrites à la Section 6.
Essai (T) : 1 bit - voir la [RFC3471]
Arrêt administratif (A) : 1 bit - voir la [RFC3471]
Suppression en cours (D) : 1 bit - voir la [RFC3471]

6. Procédures de prise en charge des appels et des connexions

6.1 Procédures d'établissement d'appel/connexion

Ce paragraphe décrit les étapes du traitement de l'établissement d'appel et de connexion.

Trois cas sont considérés :
- Un appel est établi sans connexion associée. On suppose que des connexions seront ajoutées à l'appel ultérieurement, mais ce n'est ni une exigence ni une contrainte.
- Une connexion peut être ajoutée à un appel existant. Cela peut se produire si l'appel a été établi sans aucune connexion associée, ou si une autre connexion est ajoutée à un appel qui a déjà une ou plusieurs connexions associées.
- Une connexion peut être établie sans référence à un appel (voir le paragraphe 6.4). Cela englobe la procédure d'établissement de LSP précédente.

Noter qu'un appel NE DOIT PAS être imposé à une connexion déjà établie. Pour ce faire, il faudrait modifier l'identifiant d'appel court dans l'objet SESSION des LSP existants, ce qui constituerait une modification de l'identifiant de session. Cela n'est pas autorisé par les spécifications de protocole existantes.

Les procédures de suppression d'appel et de connexion sont décrites au paragraphe 6.6.

6.2 Établissement d'appel

Un appel est établi avant et indépendamment de l'établissement du LSP (c'est-à-dire de la connexion).

L'établissement d'appel PEUT nécessiter la vérification de l'état de la liaison et la négociation de la capacité de la liaison entre le nœud d'entrée de l'appel et le nœud de sortie de l'appel. La procédure décrite ci-dessous n'est appliquée qu'une seule fois pour un appel et donc une seule fois pour l'ensemble des LSP associés à un appel.

Le message Notify (voir la [RFC3473]) est utilisé pour signaler la demande et la réponse d'établissement de l'appel. Le nouveau bit de gestion d'appel (C) dans l'objet ADMIN_STATUS est utilisé pour indiquer que cette notification gère un appel. Le message Notify est envoyé avec les adresses IPv4/IPv6 de source et de destination définies sur n'importe quelle adresse de nœud respectivement d'entrée/de sortie acheminable.

Au moins une session DOIT figurer dans la <notifier la liste des sessions> du message Notify. Afin de permettre une identification longue de l'appel, l'objet SESSION_ATTRIBUTE est ajouté à la <notifier la liste des sessions>. Noter que l'objet ERROR_SPEC n'est pas pertinent pour l'établissement de l'appel et qu'il DOIT porter le code d'erreur zéro ("Confirmation") pour indiquer qu'il n'y a pas d'erreur.

Pendant l'établissement d'appel, l'objet ADMIN_STATUS est envoyé avec les bits suivants établis. Les bits non énumérés DOIVENT être mis à zéro.

R - pour causer la réponse de la sortie
C - pour indiquer que le message Notify gère un appel.

Les objets SESSION, SESSION_ATTRIBUTE, SENDER_TEMPLATE, SENDER_TSPEC inclus dans le <Notifier la session> du message Notify sont construits comme suit.

- L'objet SESSION comprend comme adresse de point de terminaison du tunnel n'importe quelle adresse IPv4/IPv6 acheminable du nœud de terminaison de l'appel (sortie). L'identifiant d'appel est réglé à une valeur non nulle unique dans le contexte de l'appariement d'adresses fourni par l'adresse de point d'extrémité de tunnel et l'adresse d'envoyeur de l'objet SENDER_TEMPLATE (voir ci-dessous). Cette valeur sera utilisée comme identifiant court d'appel dans tous les messages pour les LSP associés à cet appel.

Noter que la valeur Call_ID de zéro est réservée et NE DOIT PAS être utilisée car elle sera présente dans les objets SESSION des LSP qui ne sont pas associés à des appels. L'identifiant de tunnel de l'objet SESSION n'est pas pertinent pour cette procédure et DOIT être mis à zéro. L'identifiant de tunnel étendu de l'objet SESSION n'est pas pertinent pour cette procédure et PEUT être fixé à zéro ou à une adresse du nœud d'entrée.

- L'objet SESSION_ATTRIBUTE contient des fanions de priorité. Actuellement, aucune utilisation de ces fanions n'est envisagée, mais des travaux futurs pourraient identifier un intérêt à l'attribution de priorités aux appels ; par conséquent, les champs Priority PEUVENT être réglés à des valeurs non nulles. Aucun des fanions de l'objet SESSION_ATTRIBUTE n'est pertinent pour ce processus et ce champ DEVRAIT être réglé à zéro. Le champ Nom de session est utilisé pour porter l'identifiant long d'appel, comme décrit à la Section 5.

- L'objet SENDER_TEMPLATE inclut comme adresse d'expéditeur n'importe quelle adresse IPv4/IPv6 acheminable du nœud initiateur de l'appel (entrée). L'identifiant de LSP n'est pas pertinent et devrait être mis à zéro.

- La valeur de bande passante insérée dans les objets SENDER_TSPEC et FLOWSPEC DOIT être ignorée à réception et DEVRAIT être mise à zéro à l'envoi.

De plus, les nœuds d'entrée/sortie qui doivent communiquer leurs capacités respectives de liaison locale peuvent inclure un objet LINK_CAPABILITY dans le message Notify.

Le receveur d'un message Notify peut déterminer s'il fait partie de la gestion d'appel ou s'il signale une erreur par la présence ou l'absence de l'objet SESSION_ATTRIBUTE dans le <notifier la liste des sessions>. Toutefois, il est possible d'obtenir une clarté totale en examinant le nouveau bit Gestion des appels (C) dans l'objet ADMIN_STATUS.

Noter que l'objet POLICY_DATA peut être inclus dans le <notifier la liste des sessions> et qu'il PEUT être utilisé pour identifier les accréditifs du demandeur, les numéros de compte, les limites, les quotas, etc. Cet objet est opaque pour RSVP, qui le transmet simplement au contrôle de politique lorsque nécessaire.

Les identifiants de message DOIVENT être utilisés lors de l'établissement de l'appel.

6.2.1 Acceptation de l'établisement d'appel

Un nœud qui reçoit un message Notify contenant l'objet ADMIN_STATUS avec les bits R et C établis est invité à établir un appel. Le receveur PEUT effectuer l'autorisation et la politique conformément aux exigences locales.

Si l'appel est acceptable, le receveur répond par un message Notify reflétant les informations de la demande d'appel, à deux exceptions près :
- Celui qui répond supprime tout objet LINK_CAPABLITY reçu et PEUT insérer un objet LINK_CAPABILITY qui décrit sa propre liaison d'accès.
- L'objet ADMIN_STATUS est envoyé avec le seul bit C établi. Tous les autres bits DOIVENT être mis à zéro.

Celui qui répond DOIT utiliser l'objet Identifiant de message pour garantir la fiabilité de la livraison de la réponse. Si aucun accusé de réception de l'identifiant du message n'est reçu après le nombre configuré de tentatives, celui qui répond DEVRAIT continuer à supposer que l'appel a été établi avec succès. Les procédures de survivance de l'appel sont traitées au paragraphe 6.7.

6.2.2. Échec et rejet de l'établissement d'appel

L'établissement de l'appel peut échouer ou être rejeté.

Si le message Notify ne peut pas être livré, l'envoyeur ne recevra pas d'accusé de réception de l'identifiant du message. Dans le cas où l'envoyeur a retransmis le message Notify un nombre configurable de fois sans recevoir d'accusé de réception de l'identifiant de message (comme décrit dans la [RFC2961]) l'initiateur DEVRAIT déclarer que l'appel a échoué et DEVRAIT envoyer une demande de suppression d'appel (voir le paragraphe 6.6).

Il est également possible qu'un accusé de réception d'identifiant de message soit reçu mais qu'aucun message Notification de réponse d'appel ne soit reçu. Dans ce cas, l'initiateur PEUT envoyer à nouveau la demande d'établissement d'appel un nombre configurable de fois (voir le paragraphe 6.7) avant de déclarer que l'appel a échoué. À ce stade, l'initiateur DOIT envoyer une demande de suppression d'appel (voir le paragraphe 6.6).

Si le message Notify ne peut pas être analysé ou est erroné, il PEUT y être répondu par un message Notify portant le code d'erreur 13 ("Classe d'objet inconnue") ou 14 ("Type de classe d'objet inconnu") en fonction de l'erreur détectée.

L'établissement d'appel PEUT être rejeté par le receveur pour des raisons de sécurité, d'autorisation ou de politique. Des codes d'erreur appropriés existent déjà dans la [RFC2205] et peuvent être utilisés dans l'objet ERROR_SPEC inclus dans le message Notify envoyé en réponse.

Les messages Notify de réponse d'une erreur DEVRAIENT également utiliser l'objet Identifiant de message pour assurer une livraison fiable. Aucune action ne devrait être effectuée en cas d'échec de réception d'un accusé de réception de l'identifiant de message après le nombre configuré de tentatives.

6.3 Ajout d'une connexion à un appel

Une fois qu'un appel a été établi, des LSP peuvent être ajoutés à l'appel. Puisque l'identifiant court d'appel fait partie de l'objet SESSION, tout LSP ayant la même valeur d'identifiant d'appel dans l'objet SESSION appartient au même appel, et le message Notify utilisé pour établir l'appel portait le même identifiant d'appel dans son objet SESSION.

Il n'y aura pas de confusion entre les LSP qui sont associés à un appel et ceux qui ne le sont pas, puisque la valeur d'identifiant d'appel DOIT être égale à zéro pour les LSP qui ne sont pas associés à un appel, et NE DOIT PAS être égale à zéro pour un identifiant d'appel valide.

Les LSP pour différents appels peuvent être distingués parce que l'identifiant de l'appel est unique dans le contexte de l'adresse de source (dans l'objet SENDER_TEMPLATE) et de l'adresse de destination (dans l'objet SESSION).

Les nœuds d'entrée et de sortie PEUVENT regrouper les LSP associés au même appel et les traiter en tant que groupe conformément aux exigences de mise en œuvre. Les nœuds de transit n'ont pas besoin d'être au courant de l'association de plusieurs LSP au même appel.

Le nœud d'entrée PEUT choisir d'établir le "nom de session" d'un LSP de manière à ce qu'il corresponde à l'identifiant long d'appel de l'appel associé.

Le bit C de l'objet ADMIN_STATUS NE DOIT PAS être établi sur les messages de LSP incluant les messages Notify qui appartiennent au LSP et DOIVENT être ignorés.

6.3.1 Ajout d'un LSP de direction inverse à un appel

Noter qu'une fois qu'un appel a été établi, il est symétrique. C'est-à-dire que chaque extrémité de l'appel peut ajouter des LSP à l'appel.

Une attention particulière est nécessaire lors de la gestion de LSP dans la direction inverse puisque les adresses dans les objets SESSION et SENDER_TEMPLATE sont inversées. Cependant, étant donné que l'identifiant court de l'appel est unique dans le contexte d'une paire d'adresses d'entrée et de sortie donnée, il peut être utilisé en toute sécurité pour associer le LSP à l'appel.

Noter que les appels étant définis ici comme symétriques, la question d'une éventuelle collision d'identifiants d'appel se pose. Ce point est discuté au paragraphe 6.5.

6.4 Établissement d'une connexion sans appel

Il reste possible d'établir des LSP conformément à la [RFC3473] sans les associer à un appel. Si l'identifiant court d'appel dans l'objet SESSION est réglé à zéro, il n'y a pas d'appel associé et le champ Nom de session dans l'objet SESSION_ATTRIBUTE DOIT être interprété simplement comme le nom de la session (voir la [RFC3209]).

Le bit C de l'objet ADMIN_STATUS NE DOIT PAS être établi dans les messages de contrôle des LSP, y compris dans les messages Notify relatifs aux LSP, et DOIT être ignoré lorsqu'il est reçu dans de tels messages.

6.5 Collision d'appels

Les appels étant symétriques, il est possible que les deux extrémités d'un appel tentent d'établir simultanément des appels avec le même identifiant long d'appel. Ce problème ne se pose que si les paires d'adresses de source et de destination correspondent. Cette situation peut être évitée en appliquant certaines règles au contenu de l'identifiant long d'appel, mais de tels mécanismes sortent du cadre du présent document.

Si un nœud qui a envoyé une demande d'établissement d'appel et n'a pas encore reçu lui-même de réponse reçoit une demande d'établissement d'appel avec le même identifiant long d'appel et des adresses de source/destination qui correspondent, il DEVRAIT procéder comme suit :
Si un nœud qui a envoyé une demande d'établissement d'appel et n'a pas encore reçu lui-même de réponse reçoit une demande d'établissement d'appel avec le même identifiant long d'appel et des adresses de source/destination qui correspondent, il DEVRAIT procéder comme suit :

- Si son adresse de source est numériquement supérieure à l'adresse de source distante, il DOIT rejeter le message reçu et

continuer à attendre une réponse à sa demande d'établissement.
- Si son adresse de source est numériquement inférieure à l'adresse de source distante, il DOIT éliminer l'état associé à l'établissement de l'appel qu'il a initié, et DOIT répondre à l'établissement de l'appel reçu.

Si un nœud reçoit une demande d'établissement d'appel comportant une paire d'adresses et un idenifiant long d'appel qui correspondent à un appel existant, le nœud DOIT renvoyer un message d'erreur (message Notify) avec le nouveau code d'erreur "Gestion d'appel" et la nouvelle valeur d'erreur "Appel dupliqué" en réponse à la nouvelle demande d'appel, et NE DOIT PAS apporter de modification à l'appel existant.

Une autre possibilité de conflit survient lorsque des identifiants courts d'appel sont attribués par une paire de nœuds pour deux appels distincts qui sont établis simultanément en utilisant des identifiants longs d'appel différents. Dans ce cas, un nœud reçoit une demande d'établissement d'appel portant un identifant court d'appel qui correspond à celui qu'il a précédemment envoyé pour la même paire d'adresses. Le traitement suivant DOIT être suivi :
- Si l'adresse de source du receveur est numériquement supérieure à l'adresse de source distante, le receveur renvoie une erreur (message Notify) avec le nouveau code d'erreur "Gestion d'appel" et la nouvelle valeur d'erreur "Conflit d'identifiant d'appel".
- Si l'adresse de source du receveur est numériquement inférieure à l'adresse de source distante, le receveur accepte et traite la demande d'appel. Il recevra un message d'erreur envoyé comme décrit ci-dessus et, à ce moment-là, il sélectionnera un nouvel identifiant court d'appel et enverra à nouveau la demande d'établissement d'appel.

6.6 Suppression d'appel/connexion

Comme pour l'établissement d'appel/connexion, il y a plusieurs cas à prendre en compte.
- Suppression d'une connexion d'un appel.
- Suppression de la dernière connexion d'un appel.
- Suppression d'un appel "vide".

Le cas de la suppression d'un LSP qui n'est pas associé à un appel n'a pas besoin d'être examiné car il suit exactement les procédures décrites dans la [RFC3473].

6.6.1 Retrait d'une connexion d'un appel

Un LSP associé à un appel peut être supprimé en utilisant les procédures standard décrites dans la [RFC3473]. Aucune procédure particulière n'est requise.

Noter qu'il n'est pas possible de supprimer un LSP d'un appel sans supprimer le LSP. Il n'est pas valide de changer l'identifiant court de l'appel de non zéro à zéro car cela implique une modification de l'objet SESSION, ce qui n'est pas autorisé.

6.6.2 Retrait de la dernière connexion d'un appel

Lorsque le dernier LSP associé à un appel est supprimé, la question se pose de savoir ce qu'il advient de l'appel. Étant donné qu'un appel peut exister indépendamment des connexions, il n'est pas toujours acceptable de dire que la suppression du dernier LSP d'un appel supprime l'appel.

La suppression du dernier LSP ne supprime pas l'appel et les procédures décrites dans le paragraphe suivant DOIVENT être utilisées pour supprimer l'appel.

6.6.3 Suppression d'un appel "vide"

Lorsque tous les LSP ont été retirés d'un appel, l'appel peut être supprimé ou laissé à la disposition de futurs LSP.

La suppression des appels s'effectue par l'envoi d'un message Notify comme pour l'établissement d'un appel, mais l'objet ADMIN_STATUS porte les bits R, D et C établis sur la demande de suppression et les bits D et C établis sur la réponse à la suppression. Les autres bits DOIVENT être mis à zéro.

Lorsqu'un message Notify est envoyé pour supprimer un appel et que l'initiateur ne reçoit pas le message Notify réfléchi correspondant (ou même éventuellement le message Ack ID) l'initiateur PEUT réessayer la demande de suppression en

utilisant les mêmes procédures de réessai que celles utilisées lors de l'établissement de l'appel. Si aucune réponse n'est reçue après une relance complète, le nœud supprimant l'appel PEUT déclarer l'appel supprimé, mais dans de telles circonstances, le nœud DEVRAIT éviter de réutiliser les identifiants longs ou courts d'appel pendant au moins cinq fois la période de rafraîchissement de notification.

6.6.4 Tentative de suppression d'un appel avec des connexions existantes

Si une demande Notify avec le bit D de l'objet ADMIN_STATUS établi est reçue pour un appel pour lequel des LSP existent encore, la demande DOIT être rejetée avec le code d'erreur "Gestion d'appel" et la valeur d'erreur "Des connexions existent encore". L'état de l'appel NE DOIT PAS être modifié.

6.6.5 Suppression d'un appel à partir de la sortie

Les appels étant symétriques, ils peuvent être supprimés à partir de l'entrée ou de la sortie.

Lorsque l'appel est "vide" (il n'a pas de LSP associé) il peut être supprimé par la sortie en envoyant un message Notify comme décrit ci-dessus.

Noter qu'il est possible que les deux extrémités d'un appel lancent la suppression de l'appel en même temps. Dans ce cas, le message Notify agissant comme une demande de suppression peut être interprété par son destinataire comme une réponse de suppression. Mais comme les messages Notify agissant comme des demandes de suppression portent le bit R établi dans l'objet ADMIN_STATUS, ils DOIVENT de toute façon faire l'objet d'une réponse. Si un message Notify de demande de suppression est reçu pour un identifiant d'appel inconnu, il y est néanmoins répondu par l'affirmative.

6.7 Survivance du plan de contrôle

La livraison des messages Notify est sécurisée par des accusés de réception d'identifiant de message, comme décrit dans les paragraphes précédents.

Les messages Notify fournissent une communication de bout en bout qui ne repose pas sur des chemins constants à travers le réseau. Les messages Notify sont acheminés conformément aux informations d'acheminement d'IGP. Il n'est donc pas nécessaire de prendre en compte la résilience du réseau (par exemple, faire avant de casser, protection, réacheminement rapide) bien que la résilience de bout en bout soit intéressante pour le redémarrage des nœuds et les réseaux complètement disjoints.

Des messages Notify périodiques DEVRAIENT être envoyés par l'initiateur et la terminaison de l'appel pour maintenir l'appel en vie et pour traiter le redémarrage du nœud d'entrée ou de sortie. La période pour ces retransmissions est une question locale, mais il est RECOMMANDÉ que cette période soit le double de la période de rafraîchissement la plus courte de tout LSP associé à l'appel. Lorsqu'il n'y a pas de LSP associé à un appel, il est RECOMMANDÉ à un LSR d'utiliser une période de rafraîchissement d'au moins une minute. Les messages Notify sont identiques à ceux envoyés comme si l'appel était établi pour la première fois, à l'exception de l'objet LINK_CAPABILITY, qui peut avoir changé depuis que l'appel a été établi pour la première fois, en raison, par exemple, de l'établissement de connexions, de défaillances de liaison ou de l'ajout de nouvelles liaisons composantes. Les informations sur le lien actuel sont utiles pour l'établissement de connexions ultérieures. Un nœud qui reçoit un message Notify de rafraîchissement portant le bit R dans l'objet ADMIN_STATUS DOIT répondre par une réponse Notify. Un nœud qui reçoit un message Notify de rafraîchissement (réponse ou demande) PEUT réinitialiser son temporisateur - ainsi, en fonctionnement normal, les rafraîchissements de Notify impliquent un seul échange par période de temps.

Un nœud (émetteur ou récepteur) qui n'est pas sûr de l'état d'un appel PEUT immédiatement envoyer un message Notify comme si il établissait l'appel pour la première fois.

L'absence de réception d'une demande de rafraîchissement de Notify n'a pas de signification particulière. Un nœud qui ne reçoit pas de demande de rafraîchissement de Notify peut envoyer sa propre demande de rafraîchissement de Notify pour établir l'état de l'appel. Si un nœud ne reçoit aucune réponse à une demande de rafraîchissement de Notify (y compris aucun accusé de réception d'ID de message) il PEUT supposer que le nœud distant est inaccessible ou indisponible. La décision de supprimer les LSP associés et l'appel relève de la politique locale.

Dans le cas où un nœud de bordure redémarre sans état préservé, il PEUT réapprendre l'état du LSP des nœuds adjacents et l'état d'appel des nœuds distants. Si un message Path ou Resv est reçu avec un identifiant d'appel non nul mais sans le bit C dans ADMIN_STATUS, et pour un identifiant d'appel qui n'est pas reconnu, il est RECOMMANDÉ que le receveur

suppose que l'établissement de l'appel est retardé et ignore le message reçu. Si l'établissement de l'appel ne se concrétise jamais, l'absence de rafraîchissement de l'état par le nœud qui redémarre entraînera la destruction des LSP. Facultativement, le receveur d'un tel message de LSP pour un identifiant d'appel inconnu peut renvoyer une erreur (message PathErr ou ResvErr) avec le code d'erreur "Gestion d'appel" et la valeur d'erreur "Identifiant d'appel inconnu".

7. Applicabilité des procédures d'appel et de connexion

Cette Section examine l'applicabilité des différentes procédures d'établissement d'appel aux points de référence NNI et UNI. Cette section est pour information et n'a pas pour but de prescrire ou d'empêcher d'autres options.

7.1 Appels initiés par le réseau

Étant donné que les propriétés de liaison et les autres attributs d'ingénierie du trafic sont probablement connus par le biais de l'IGP, l'objet LINK_CAPABILITY n'est généralement pas nécessaire.

Dans les réseaux multi-domaines, il est possible que les propriétés des liaisons d'accès et les autres attributs d'ingénierie du trafic ne soient pas connus car les domaines ne partagent pas ce type d'informations. Dans ce cas, le mécanisme d'établissement d'appel peut inclure l'objet LINK_CAPABILITY.

7.2 Appels initiés par l'utilisateur

Il est possible que les propriétés de la liaison d'accès et d'autres attributs d'ingénierie du trafic ne soient pas partagés dans le cœur de réseau. Dans ce cas, le mécanisme d'établissement d'appel peut inclure l'objet LINK_CAPABILITY.

En outre, le premier nœud au sein du réseau peut être responsable de la gestion de l'appel. Dans ce cas, le message Notify utilisé pour établir l'appel est adressé par le nœud de bordure du réseau de l'utilisateur au premier nœud du réseau central. En outre, ni l'identifiant long d'appel ni l'identifiant court d'appel ne sont fournis (la longueur du nom de session est réglée à zéro et la valeur de l'identifiant d'appel est réglée à zéro). Le message Notify est transmis au premier nœud du cœur, qui est chargé de générer les identifiants longs et courts d'appel avant d'envoyer le message au point d'extrémité d'appel distant (qui est connu grâce à l'objet SESSION).

De plus, lorsqu'il est utilisé dans un contexte de superposition, le premier nœud du cœur est autorisé (voir la [RFC4208]) à remplacer le nom de session attribué par le nœud d'entrée et transmis dans le message Path. Dans le cas de la gestion d'appel, le premier nœud central :

1) PEUT insérer un identifiant long d'appel dans le nom de session d'un message Path.
2) DOIT remplacer le nom de session par celui émis à l'origine par le nœud côté utilisateur lorsqu'il renvoie le message Resv au nœud d'entrée.

7.3 Gestionnaires d'appel externes

Des agents tiers de gestion d'appel peuvent être utilisés pour appliquer la politique et l'autorisation à un point qui n'est ni l'initiateur ni la terminaison de l'appel. L'exemple précédent en est un cas particulier, mais le processus et les procédures sont identiques.

7.3.1 Segments d'appel

Des segments d'appel existent entre un ensemble de gestionnaires d'appels externes par défaut et configurés le long d'un chemin entre les nœuds d'entrée et de sortie, et utilisent les protocoles décrits dans le présent document.

Les techniques utilisées par un fournisseur de services donné pour identifier quels gestionnaires d'appel externes de son réseau devraient traiter un appel donné sortent du cadre du présent document.

Un gestionnaire d'appel externe utilise l'acheminement IP normal pour acheminer le message Notify au gestionnaire d'appel externe suivant. Les messages Notify (demandes et réponses) sont donc encapsulés dans des paquets IP qui identifient les gestionnaires d'appel externes envoyeur et receveur, mais les adresses utilisées pour identifier l'appel (l'adresse de l'envoyeur dans l'objet SENDER_TEMPLATE et l'adresse du point d'extrémité du tunnel dans l'objet SESSION) continuent d'identifier les points d'extrémité de l'appel.

8. Non prise en charge de l'identifiant d'appel

Il est important que les procédures décrites ci-dessus fonctionnent de manière aussi transparente que possible avec les nœuds existants qui ne prennent pas en charge les extensions décrites.

De toute évidence, il n'est pas nécessaire d'envisager le cas où l'initiateur de l'appel ne prend pas en charge l'initiation de l'établissement de l'appel.

8.1 Non prise en charge par les gestionnaires d'appel externes

Il est peu probable qu'un initiateur d'appel soit configuré pour envoyer des demandes de notification d'établissement d'appel à un gestionnaire d'appel externe, y compris au premier nœud du cœur, si ce nœud ne prend pas en charge l'établissement d'appel.

Un nœud qui reçoit une demande d'établissement d'appel inattendue va entrer dans l'une des catégories suivantes :
- Le nœud ne prend pas en charge RSVP. Le message ne sera pas livré ou ne recevra pas de réponse. Aucun accusé de réception de l'identifiant du message ne sera envoyé. L'initiateur réessaie puis abandonne.
- Le nœud prend en charge RSVP ou RSVP-TE mais pas GMPLS. Le message sera livré mais ne sera pas compris. Il sera éliminé. Aucun accusé de réception de l'identifiant du message ne sera envoyé. L'initiateur réessaie, puis abandonne.
- Le nœud prend en charge GMPLS mais pas la gestion d'appel. Le message sera remis, mais l'analyse échouera en raison de la présence de l'objet SESSION_ATTRIBUTE. Un accusé de réception de l' identifiant du message peut être envoyé avant l'échec de l'analyse. Quand l'analyse échoue, le message Notify peut être éliminé, auquel cas l'initiateur va réessayer puis abandonner ; sinon, une erreur d'analyse peut être générée et renvoyée dans un message Notify, ce qui va indiquer à l'initiateur que la gestion d'appel n'est pas prise en charge.

8.2 Non prise en charge par un nœud de transit

Les nœuds de transit NE DEVRAIENT PAS examiner les messages Notify qui ne leur sont pas adressés. Cependant, ils verront les identifiants courts d'appel dans tous les messages pour tous les LSP associés aux appels.

Les spécifications précédentes déclarent que ces champs DEVRAIENT être ignorés à réception et DOIVENT être transmis à zéro. Cela pourrait être interprété par certaines mises en œuvre comme signifiant que les champs devraient être mis à zéro avant que les objets ne soient transmis. Dans ce cas, l'établissement d'un LSP ne sera pas possible. Si un des champs est mis à zéro dans le message Path ou Resv, le message Resv parviendra à l'initiateur avec le champ mis à zéro, ce qui indique à l'initiateur qu'un nœud du réseau empêche la gestion d'appel. L'utilisation de chemins explicites peut contribuer à atténuer ce problème en évitant de tels nœuds. En fin de compte, cependant, il peut s'avérer nécessaire de mettre à niveau les nœuds incriminés pour qu'ils puissent traiter ces extensions de protocole.

8.3. Non prise en charge par le nœud de sortie

Il est peu probable que l'on tente d'établir un appel vers un nœud distant qui ne prend pas en charge les appels.

Si le nœud de sortie ne prend pas en charge la gestion d'appel par le message Notify, il réagira (comme décrit au paragraphe 8.1) de la même manière qu'un gestionnaire d'appels externe.

9. Considérations sur la sécurité

Se référer à chacun des documents référencés dans les paragraphes qui suivent pour une description des considérations de sécurité applicables aux fonctionnalités fournies.

9.1 Considérations sur la sécurité de l'appel et de la connexion

L'établissement d'appel est vulnérable aux attaques par usurpation d'identité et par déni de service. Comme l'établissement d'appel utilise des messages Notify, le processus peut être protégé par l'utilisation de l'objet INTEGRITY pour sécuriser ces messages comme décrit dans les [RFC2205] et [RFC3473]. Les déploiements où la sécurité est une préoccupation DEVRAIENT utiliser ce mécanisme.

Les mises en œuvre et les déploiements PEUVENT en outre protéger l'échange d'établissement d'appel en utilisant des mécanismes de sécurité de bout en bout tels que ceux fournis par IPsec (voir les [RFC4302] et [RFC4303]) ou en utilisant la sécurité RSVP [RFC2747].

Noter en outre qu'il serait souhaitable d'utiliser le processus d'établissement d'appel indépendant, dans lequel l'appel est établi séparément des LSP, pour appliquer un niveau supplémentaire d'authentification et de politique pour les LSP de bout en bout, au-delà de ce qui est disponible avec l'établissement de LSP sans appel, bond par bond. Cependant, le faire exige un travail supplémentaire pour établir des associations de sécurité entre homologue et gestionnaire d'appel qui satisfassent aux exigences de la [RFC4107]. Le mécanisme décrit dans le présent document devrait répondre à ce cas d'utilisation lorsqu'il est associé à ce travail supplémentaire. L'application de ce mécanisme au cas d'utilisation de l'authentification et de la politique avant la normalisation d'une solution de sécurité est inappropriée et en dehors de l'applicabilité actuelle du mécanisme.

La fréquence de l'établissement d'appel dépend de l'application et est difficile à généraliser. L'échange de clés pour les échanges de messages liés à l'appel est donc quelque chose qui devrait être configuré ou arrangé dynamiquement dans les différents déploiements selon les conseils de la [RFC4107]. Noter que la relation de signalisation RSVP-TE distante entre les points d'extrémité d'appel n'est pas différente de la relation de signalisation entre les LSR qui établissent un LSP. C'est-à-dire, les LSR ne sont pas nécessairement adjacents au sens IP dans le plan de contrôle dans les deux cas. L'échange de clés doit donc être considéré comme une procédure à distance et non comme une procédure d'un seul bond. Il existe plusieurs procédures pour l'échange automatique de clés à distance, et IKEv2 [RFC4306] est particulièrement suggéré dans la [RFC3473].

10. Considérations relatives à l'IANA

10.1 Objets RSVP

Un nouvel objet RSVP est introduit. L'IANA a fait une allocation dans le registre "Paramètres RSVP" en utilisant le sous registre "Noms, numéros, et types de classes".

o Objet LINK_CAPABILITY

Numéro de classe = 133 (forme 10bbbbbb). Le numéro de classe est choisi de telle façon que les nœuds qui ne reconnaissent pas cet objet l'éliminent en silence. C'est-à-dire que le bit de poids fort est établi et le bit suivant est à zéro.

Type de classe = 1 (Capacités de liaison TE). L'objet LINK_CAPABILITY n'est défini que pour inclusion dans les messages Notify. Voir au paragraphe 5.3 du présent document.

L'IANA tient une liste des sous objets qui peuvent être portés dans cet objet. Cette liste est tenue dans l'entrée de registre pour l'objet LINK_CAPABILITY comme il est de pratique courante pour les sous objets des autres objets RSVP. Pour chaque sous objet, l'IANA mentionne :
- le numéro de type du sous objet,
- le nom du sous objet,
- la référence qui indique où le sous objet est défini.

La liste initiale des sous objets est donnée au paragraphe 5.3 du présent document.

10.2 Codes et valeurs d'erreur RSVP

Un nouveau code d'erreur RSVP et de nouvelles valeurs d'erreur sont introduits. L'IANA a procédé à des attributions à partir du registre "Paramètres RSVP" en utilisant le sous-registre "Codes d'erreur et sous codes de valeurs d'erreur définis globalement".

o Codes d'erreur : Gestion d'appel (valeur 32)
o Valeurs d'erreur :
  - Conflit de gestion d'appel/d'identifiant d'appel (valeur 1)
  - La gestion d'appel/connexion existe encore (valeur 2)
  - Gestion d'appel/identifiant d'appel inconnu (valeur 3)
  - Gestion d'appel/appel dupliqué (valeur 4)

10.3 Bits d'objet RSVP ADMIN_STATUS

La [RFC4872] demandait que l'IANA gère les bits de l'objet RSVP ADMIN_STATUS. Un nouveau sous registre "Fanions d'information d'état administratif" du registre "Paramètres de signalisation GMPLS" a été créé.

Le présent document définit un nouveau bit, le bit C, à retracer dans ce sous registre. Le numéro de bit 28 a été alloué. Voir le paragraphe 5.5 du présent document.

11. Remerciements

Les auteurs tiennent à remercier George Swallow, Yakov Rekhter, Lou Berger, Jerry Ash, et Kireeti Kompella de leurs très utiles apports et commentaires sur la révision précédente de ce document.

Merci à Lyndon Ong et Ben Mack-Crane des longues discussions durant et après le dernier appel du groupe de travail, et à Deborah Brungard pour sa relecture finale détaillée.

Merci à Suresh Krishnan pour la revue de GenArt, et à Magnus Nystrom pour les discussions sur la sécurité.

Des commentaires utiles ont été reçus durant la revue de l'IESG de Brian Carpenter, Lars Eggert, Ted Hardie, Sam Hartman, et Russ Housley.

12. Références

12.1 Références normatives

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. *(MàJ par* RFC8174)

[RFC2205] R. Braden, éd., L. Zhang, S. Berson, S. Herzog, S. Jamin, "Protocole de réservation de ressource (RSVP) -- version 1, spécification fonctionnelle", septembre 1997. (*MàJ par* RFC2750, RFC3936, RFC4495, RFC6780)) *(P.S.)*

[RFC2747] F. Baker, B. Lindell, M. Talwar, "Authentification cryptographique RSVP", janvier 2000. (*MàJ par* RFC3097) *(P.S.)*

[RFC2961] L. Berger et autres, "Extensions de réduction de redondance de rafraîchissement pour RSVP", avril 2001. (*MàJ par* RFC5063) *(P.S.)*

[RFC3209] D. Awduche, et autres, "RSVP-TE : Extensions à RSVP pour les tunnels LSP", décembre 2001. (*Mise à jour par* RFC3936, RFC4420, RFC4874, RFC5151, RFC5420, RFC6790)

[RFC3471] L. Berger, éd., "Commutation d'étiquettes multi-protocoles généralisée (GMPLS) : description fonctionnelle de la signalisation", janvier 2003. (*MàJ par* RFC4201, RFC4328, RFC4872, RFC8359) *(P.S.)*

[RFC3473] L. Berger, "Extensions d'ingénierie de protocole - trafic de signalisation de réservation de ressource (RSVP-TE) de commutation d'étiquettes multi-protocoles généralisée (GMPLS)", janvier 2003. *(P.S., MàJ par 4003, 4201, 4420, 4783, 4784, 4873, 4974, 5063, 5151,* 8359)

[RFC3477] K. Kompella, Y. Rekhter, "Signalisation des liaisons non numérotées dans le protocole de réservation de ressource – ingénierie du trafic (RSVP-TE)", janvier 2003. *(P.S.)*

[RFC3945] E. Mannie, éd., "Architecture de commutation d'étiquettes multi-protocoles généralisée (GMPLS)", octobre 2004. *(P.S.)*

[RFC4201] K. Kompella et autres, "Faisceaux de liaisons dans l'ingénierie du trafic MPLS", octobre 2005. *(P.S.)*

[RFC4202] K. Kompella et autres, "Extensions d'acheminement pour la prise en charge de la commutation généralisée d'étiquettes multi-protocoles (GMPLS)", octobre 2005. *(P.S.)*

[RFC4208] G. Swallow et autres, "Interface usager-réseau (UNI) de commutation généralisée d'étiquettes multiprotocoles (GMPLS) : prise en charge du protocole de réservation de ressource - ingénierie du trafic (RSVP-TE) pour le modèle de recouvrement", octobre 2005. *(P.S.)*

[RFC4302] S. Kent, "En-tête d'authentification IP", décembre 2005. *(P.S.)*

[RFC4303] S. Kent, "Encapsulation de charge utile de sécurité dans IP (ESP)", décembre 2005. (*Remplace* RFC2406) *(P.S.)*

[RFC4306] C. Kaufman, "Protocole d'échange de clés sur Internet (IKEv2)", décembre 2005. *(Obsolète, voir la* RFC5996)

[RFC4426] J. Lang et autres, "Spécification fonctionnelle de récupération du protocole généralisé de commutation d'étiquettes multiprotocoles (GMPLS)", mars 2006. *(P.S.)*

[RFC4872] P. Lang et autres, "Extensions RSVP-TE pour la prise en charge de la récupération de commutation d'étiquettes multi protocole généralisée (GMPLS) de bout en bout", mai 2007. *(P.S. ; MàJ* RFC3471 ; *MàJ par* RFC4873, RFC6780, RFC9270*.)*

12.2 Références pour information

[ASON-APPL] Drake, J., Papadimitriou, D., Farrel, A., Brungard, D., Ali, Z., Ayyangar, A., Ould-Brahim, H., and D. Fedyk, "Generalized MPLS (GMPLS) RSVP-TE Signalling in support of Automatically Switched Optical Network (ASON), Travail en cours, juillet 2005.

[RFC4107] S. Bellovin, R. Housley, "Lignes directrices pour la gestion des clés de chiffrement", juin 2005. (BCP0107)

[RFC4139] D. Papadimitriou et autres, "Exigences pour l'utilisation de la signalisation de MPLS généralisé (GMPLS) et extensions pour les réseaux optiques à commutation automatique (ASON)", juillet 2005. *(Information)*

[RFC5150] A. Ayyangar et autres, "Raccordement de chemin à commutation d'étiquette avec la commutation généralisée d'étiquettes multiprotocoles à ingénierie de trafic (GMPLS-TE)", février 2008. *(P.S.)*

[G.8080] Recommandation UIT-T G.8080/Y.1304, "Architecture pour le réseau optique à commutation automatique (ASON)," november 2001 (et révision de janvier 2003).Voir à http://www.itu.int.

Adresse des auteurs

John Drake
Boeing Satellite Systems
2300 East Imperial Highway
El Segundo, CA 90245
mél : John.E.Drake2@boeing.com

Deborah Brungard (AT&T)
Rm. D1-3C22 - 200 S. Laurel Ave.
Middletown, NJ 07748, USA
mél : dbrungard@att.com

Zafar Ali (Cisco)
100 South Main St. #200
Ann Arbor, MI 48104, USA
mél : zali@cisco.com

Arthi Ayyangar (Nuova Systems)
2600 San Tomas Expressway
Santa Clara, CA 95051
mél : arthi@nuovasystems.com

Don Fedyk (Nortel Networks)
600 Technology Park Drive
Billerica, MA, 01821, USA
mél : dwfedyk@nortel.com

Adresses de contact

Dimitri Papadimitriou
Alcatel-Lucent,
Fr. Wellesplein 1,
B-2018 Antwerpen, Belgium
téléphone : +32 3 240-8491
mél : dimitri.papadimitriou@alcatel-lucent.be

Adrian Farrel
Old Dog Consulting
téléphone : +44 (0) 1978 860944
mél : adrian@olddog.co.uk

Déclaration complète de droits de reproduction

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