Groupe de travail Réseau
Request for Comments : 4783
RFC mise à jour : 3473
Catégorie : Sur la voie de la normalisation

Y. Rekhter, Juniper Networks
décembre 2006

Traduction Claude Brière de L'Isle

GMPLS – communication des informations d'alarme

Résumé
Le présent document décrit une extension à la signalisation de commutation généralisée d'étiquettes multi protocoles (GMPLS, *Generalized Multi-Protocol Label Switching*) pour prendre en charge la communication des informations d'alarme. La signalisation GMPLS prend déjà en charge le contrôle de rapport d'alarme, mais pas la communication des informations d'alarme. Le présent document présente à la fois une description fonctionnelle et les spécificités de GMPLS-RSVP pour une telle extension. Le présent document propose aussi la modification de l'objet RSVP ERROR_SPEC.

Le présent document met à jour la RFC 3473, "Extensions d'ingénierie de protocole - trafic de signalisation de réservation de ressource (RSVP-TE) de commutation d'étiquettes multi-protocoles généralisée (GMPLS)" par l'ajout de nouveaux éléments de protocole facultatifs. Il ne change pas, et est pleinement rétro compatible avec les procédures spécifiées dans la RFC 3473.

Table des matières

1. Introduction

La signalisation GMPLS fournit des mécanismes qui peuvent être utilisés pour contrôler les rapports d'alarmes associées à

un chemin à commutation d'étiquettes (LSP, *Label Switched Path*). Cette prise en charge est fournie via des informations d'état administratif [RFC3471] et l'objet Admin_Status [RFC3473]. Ces mécanismes contrôlent seulement si le rapport d'alarme est inactivé. Aucune disposition n'est prise pour la communication des informations d'alarme au sein de GMPLS.

L'extension décrite dans le présent document définit comment les informations d'alarme associées à un LSP GMPLS peuvent être communiquées le long du chemin du LSP. La communication en amont et en aval est prise en charge. La valeur de la communication de telles informations d'alarme est qu'elles sont ensuite disponibles à chaque nœud le long du LSP pour les besoins d'affichage et de diagnostic. Les informations d'alarme peuvent aussi être utiles dans certains scénarios de protection du trafic, mais de telles utilisations sortent du domaine d'application du présent document. La communication d'alarme est prise en charge via un nouvel objet, de nouveaux TLV Erreur/informations d'alarme, et un nouveau bit Informations d'état administratif

La communication des alarmes, comme décrite dans le présent document, est contrôlable au niveau du LSP. Une telle communication peut être utile au sein de configurations de réseau où tous les nœuds ne prennent pas en charge la communication à un utilisateur pour rapporter les alarmes et/ou la communication est nécessaire pour prendre en charge des applications spécifiques. La prise en charge de cette fonctionnalité est facultative.

La communication des alarmes au sein de GMPLS n'implique aucune modification de comportement pour le traitement des alarmes, ou pour la communication des alarmes en dehors de GMPLS. De plus, l'extension décrite dans le présent document n'est pas destinée à remplacer une technique (existante) de propagation de fautes du plan des données.

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].

1.1. Fondements

Les problèmes avec l'état du plan des données peuvent souvent être détectés en associant des composants matériels du plan des données. Ces problèmes du plan des données sont normalement filtrés sur la base du temps écoulé et de la politique locale. Les problèmes qui passent le processus de filtrage sont normalement soulevés comme des alarmes. Ces alarmes sont disponibles pour affichage à l'opérateur. Elles peuvent aussi être collectées centralement par des moyens qui sortent du domaine d'application du présent document.

Tous les problèmes du plan des données ne causent pas la fermeture immédiate du LSP. De plus, il peut être désiré, en particulier dans les réseaux de transport optiques, de conserver un LSP et communiquer les informations d'alarme pertinentes même quand l'état du plan des données est complètement défaillant.

Bien que les informations d'erreur puissent être rapportées en utilisant les messages PathErr, ResvErr, et Notify, ces messages indiquent normalement un problème de l'état de signalisation et peuvent seulement rapporter un problème à la fois. Cela rend difficile de corréler tous les problèmes qui peuvent être associés à un seul LSP et de permettre à un opérateur qui examine l'état d'un LSP d'avoir une vue de la liste complète des problèmes actuels. Cette situation est exacerbée par l'absence de tout moyen de communiquer qu'un problème a été résolu et que l'alarme correspondante a été levée.

Les extensions définies dans le présent document permettent à un opérateur ou un composant logiciel d'obtenir une liste complète des alarmes en cours associées à toutes les ressources utilisées pour prendre en charge un LSP. Les extensions assurent aussi que cette liste est mise à jour et synchronisée avec l'état réel des alarmes dans le réseau. Finalement, les extensions rendent la liste disponible pour chaque nœud traversé par un LSP.

2. Communication des informations d'alarme

Un nouvel objet est introduit pour porter les détails des informations d'alarme. Les détails des informations d'alarme sont très semblables aux informations d'erreur portées dans les objets existants ERROR_SPEC. Pour cette raison, la communication des informations d'alarme utilise un format qui se fonde sur la communication des informations d'erreur.

Le nouvel objet introduit pour porter les détails des informations d'alarme est appelé un objet ALARM_SPEC. Cet objet a le même format que l'objet ERROR_SPEC, mais utilise un nouveau C-Num pour éviter la sémantique du traitement d'erreur. Aussi, des TLV supplémentaires sont définis pour les objets IF_ID ALARM_SPEC pour prendre en charge la

communication des informations relatives à une alarme spécifique. Ces TLV peuvent aussi être utiles quand il sont inclus dans des objets ERROR_SPEC, par exemple, quand l'objet ERROR_SPEC est porté dans un message Notify.

Bien que les détails des informations d'alarme soient comme les détails de la communication d'erreur existante, la sémantique du traitement diffère. Les informations d'alarme vont normalement se rapporter à des changements de l'état du plan des données, sans changement de l'état de contrôle. Les informations d'alarme vont toujours être associées aux LSP en place. De telles informations vont aussi normalement être très utiles aux opérateurs et applications autres que de traitement du protocole de plan de contrôle. Finalement, alors que les informations d'erreur sont communiquées dans de messages PathErr, ResvErr, et Notify [RFC3473], les informations d'alarme vont être portées dans des messages Path et Resv.

Les messages Path sont utilisés pour porter les informations d'alarme aux nœuds en aval, et les messages Resv sont utilisés pour porter les informations d'alarme aux nœuds en amont. L'intention de l'envoi des informations d'alarme à la fois en amont et en aval est de fournir la même visibilité sur les informations d'alarme en tout point le long d'un LSP. La communication de plusieurs alarmes associées à un LSP est prise en charge. Dans ce cas, plusieurs objets ALARM_SPEC vont être portés dans les messages Path ou Resv.

L'ajout des informations d'alarme aux messages Path et Resv est contrôlé via un nouveau bit Informations d'état administratif. Les informations d'état administratif sont portées dans l'objet Admin_Status.

3. Détails de GMPLS-RSVP

Cette Section donne la spécification de GMPLS-RSVP [RFC3473] pour la communication des informations d'alarme. La communication des informations d'alarme est FACULTATIVE. Cette Section s'applique aux nœuds qui prennent en charge la communication des informations d'alarme.

3.1 Objets ALARM_SPEC

Les objets ALARM_SPEC utilisent le même format que l'objet ERROR_SPEC, mais avec le numéro de classe 198 (alloué par l'IANA sous la forme 11bbbbbb, selon le paragraphe 3.1.4).

- Classe = 198, C-Type = 1. Réservé. (La valeur de C-Type est définie pour ERROR_SPEC, mais n'est pas définie pour être utilisée avec ALARM_SPEC.)

- Classe = 198, C-Type = 2. Réservé. ((La valeur de C-Type est définie pour ERROR_SPEC, mais n'est pas définie pour être utilisée avec ALARM_SPEC.)

- Objet IPv4 IF_ID ALARM_SPEC : Classe = 198, C-Type = 3. Même définition que IPv4 IF_ID ERROR_SPEC [RFC3473].

- Objet IPv6 IF_ID ALARM_SPEC : Classe = 198, C-Type = 4. Même définition que IPv6 IF_ID ERROR_SPEC [RFC3473].

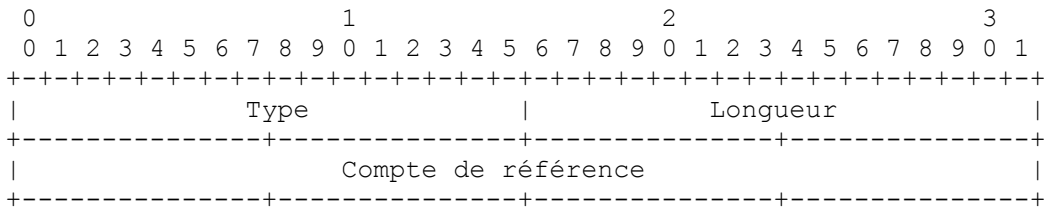
3.1.1 TLV IF_ID ALARM_SPEC (et ERROR_SPEC)

Les nouveaux TLV suivants sont définis pour être utilisés avec les objets IPv4 et IPv6 IF_ID ALARM_SPEC. Ils peuvent aussi être utilisés avec les objets IPv4 et IPv6 IF_ID ERROR_SPEC. Voir au paragraphe 9.1.1 de la [RFC3471] la définition originale de ces valeurs. Noter que la longueur fournie ci-dessous est pour le TLV total. Tous les TLV définis dans cette section sont FACULTATIFS.

Les TLV définis DOIVENT suivre tout TLV identifiant une interface. Aucune règle ne s'applique à l'ordre relatif des TLV définis dans cette section.

Type	**Longueur**	**Description**
512	8	REFERENCE_COUNT *(compte de référence)*
513	8	SEVERITY *(sévérité)*
514	8	GLOBAL_TIMESTAMP *(horodatage global)*
515	8	LOCAL_TIMESTAMP *(horodatage local)*
516	variable	ERROR_STRING *(chaîne d'erreur)*

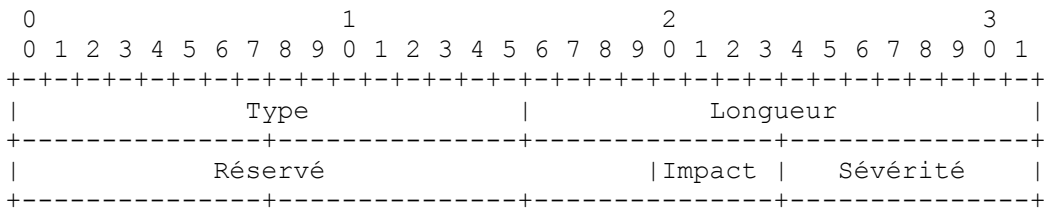
La TLV Compte de référence a le format suivant :



Compte de référence : 32 bits
C'est le nombre de fois que cette alarme a été répétée comme déterminé par le nœud rapporteur. Ce champ NE DOIT PAS être réglé à zéro, et les TLV reçus avec ce champ réglé à zéro DOIVENT être ignorés.

Un seul TLV Compte de référence peut être inclus dans un objet.

Le TLV Sévérité a le format suivant :



Réservé : 20 bits
Ce champ est réservé. Il DOIT être réglé à zéro à l'émission, DOIT être ignoré à réception, et DOIT être transmis inchangé et non examiné par les nœuds de transit.

Impact : 4 bits
Indique l'impact de l'alarme indiquée dans le TLV. Voir dans [M.20] une discussion générale sur la classification des défaillances. Les valeurs suivantes sont définies dans le présent document. Les détails de leur sémantique peuvent être trouvés dans [M.20].

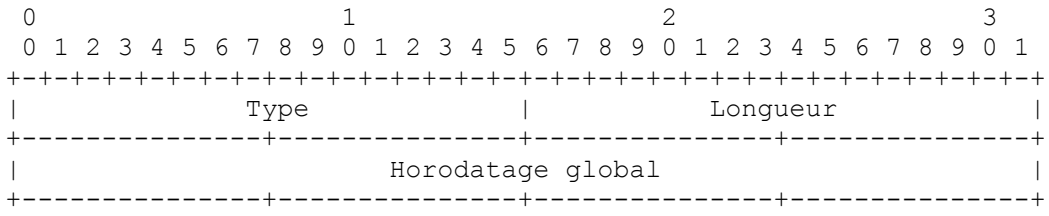
Valeur	**Définition**
0	Impact non spécifié
1	Service non affecté (le trafic de données n'est pas interrompu)
2	Service affecté (le trafic des données est interrompu)

Sévérité : 8 bits
Indique l'impact de l'alarme indiquée dans le TLV. Voir dans la [RFC3877] et [M.3100] plus d'informations sur la sévérité. Les valeurs suivantes sont définies dans le présent document. Les détails de leur sémantique peuvent être trouvés dans la [RFC3877] et [M.3100]:

Valeur	**Définition**
0	Supprimée
1	Indéterminée
2	Critique
3	Majeure
4	Mineure
5	Avertissement

Un seul TLV Sévérité peut être inclus dans un objet.

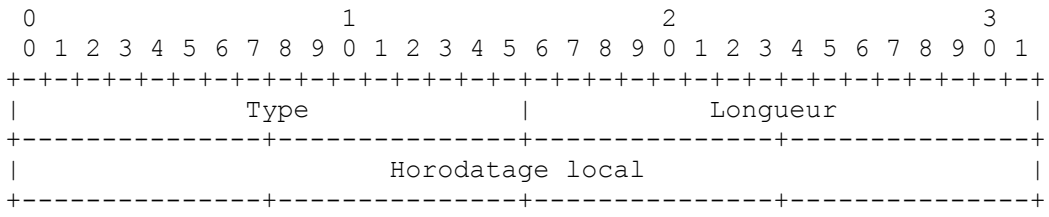
Le TLV Horodatage global a le format suivant :



Horodatage global : 32 bits
Entier non signé à virgule fixe qui indique le nombre de secondes depuis 00:00:00 UT le 1er janvier 1970 selon l'horloge du nœud qui a généré ce TLV. Ce temps PEUT inclure des secondes sautées si elles sont utilisées par l'horloge locale et DEVRAIT contenir la même valeur de temps qu'utilisé par le nœud quand l'alarme est rapportée par d'autres systèmes (comme dans le plan de gestion) si l'heure mondiale est utilisée dans ces rapports.

Un seul TLV Horodatage global peut être inclus dans un objet.

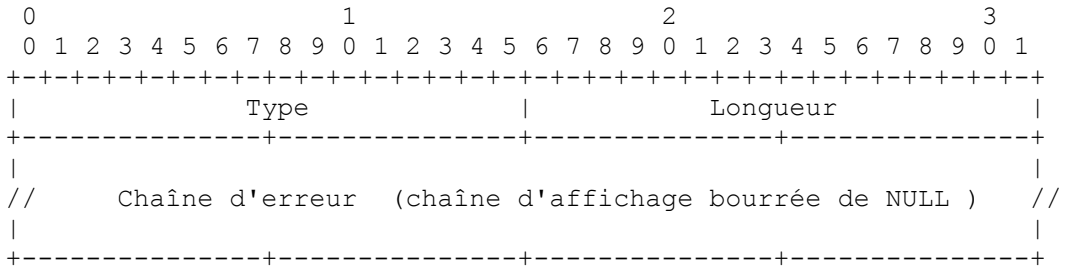
Le TLV Horodatage local a le format suivant :



Horodatage local : 32 bits
Nombre de secondes rapporté par l'horloge du système local au moment de la détection de l'alarme associée sur le nœud qui génère ce TLV. Ce nombre est supposé avoir une signification dans le contexte du nœud générateur. Par exemple, il peut indiquer le nombre de secondes depuis le réamorçage du nœud ou peut être une représentation locale d'une horloge en temps réel non synchronisée.

Un seul TLV Horodatage local peut être inclus dans un objet.

Le TLV Chaîne d'erreur a le format suivant :



Chaîne d'erreur : 32 bits minimum (variable)
Chaîne de caractères en US-ASCII, représentant le type d'erreur/alarme. Cette chaîne est bourrée jusqu'à la prochaine limite de quatre octets en utilisant des caractères nuls. Le bourrage de nuls n'est pas exigé quand la chaîne est alignée sur 32 bits. Le contenu de la chaîne d'erreur dépend de la mise en œuvre. Voir les types de conditions mentionnés dans les appendices de [GR833] et une liste d'exemples de chaînes. Noter que la longueur inclut le bourrage.

Plusieurs TLV Chaîne d'erreur peuvent être inclus dans un objet.

3.1.2 Procédures

Ce paragraphe s'applique aux nœuds qui prennent en charge la communication des informations d'alarme. Les objets ALARM_SPEC sont portés dans les messages Path et Resv. Plusieurs objets ALARM_SPEC PEUVENT être présents.

Les nœuds qui prennent en charge les extensions définies dans le présent document DEVRAIENT mémoriser toutes les

informations d'alarme provenant des objets ALARM_SPEC reçus pour les utiliser ultérieurement. Tous les objets ALARM_SPEC reçus dans les messages Path DEVRAIENT être passés non modifiés en aval dans les messages Path correspondants. Tous les objets ALARM_SPEC reçus dans des messages Resv DEVRAIENT être passés non modifés en amont dans les messages Resv correspondants. Les objets ALARM_SPEC sont fusionnés dans les messages Resv transmis en incluant une copie de tous les objets ALARM_SPEC reçus dans les messages Resv correspondants.

Pour annoncer des informations d'alarme locales, un nœud génère un objet ALARM_SPEC pour chaque alarme et l'ajoute aux messages Path et Resv pour le LSP impacté.

Dans tous les cas, les valeurs appropriées d'adresse de nœud en erreur, code d'erreur, et valeurs d'erreur DOIVENT être réglées (voir ci-dessous la discussion sur les codes d'erreur et valeurs d'erreur). Comme les fanions InPlace et NotGuilty n'ont de signification que dans les objets ERROR_SPEC, ils NE DEVRAIENT PAS être établis. Les TLV DEVRAIENT être inclus dans l'objet ALARM_SPEC pour identifier l'interface, si il en est une, associée à l'alarme. Les TLV définis dans la [RFC3471] pour identifier les interfaces dans l'objet IF_ID ERROR_SPEC [RFC3473] DEVRAIENT être utilisés à cette fin, mais on notera que les TLV de type 4 et 5 (interfaces composantes) sont déconseillés par la [RFC4201] et NE DEVRAIENT PAS être utilisés. Les TLV DEVRAIENT aussi être inclus pour indiquer la sévérité (TLV Sévérité) l'heure (TLV Horodatage global et/ou Horodatage local) et une (brève) chaîne (TLV Chaîne d'erreur) associée à l'alarme. Le TLV Compte de référence PEUT aussi être inclus pour indiquer le nombre de fois qu'une alarme a été répétée au nœud rapporteur. Les objets ALARM_SPEC reçus d'autres nœuds ne sont pas impactés par l'ajout des objets locaux ALARM_SPEC, c'est-à-dire, ils continuent d'être traités comme décrit ci-dessus. Le choix de la ou des alarmes à annoncer et à omettre est une affaire de politique locale, et peut être configurable par l'utilisateur.

Il y a deux façons d'indiquer l'heure. Un TLV horodatage global est utilisé pour fournir une référence de temps absolu pour l'occurrence d'une alarme. Les TLV Horodatage local est utilisé pour fournir la référence de temps pour l'occurrence d'une alarme relative aux autres informations annoncées par le nœud. L'horodatage global DEVRAIT être utilisé sur les nœuds qui conservent une référence de temps absolu. Les deux TLV d'horodatage PEUVENT être utilisés simultanément.

Noter que les objets ALARM_SPEC NE DEVRAIENT PAS être ajoutés aux états Path et Resv des LSP qui sont dans l'état "communication d'alarme inhibée". Les objets ALARM_SPEC PEUVENT être ajoutés à l'état de LSP qui sont dans un état "désactivé administrativement". Ces états sont indiqués par les bits I et A de l'objet Admin_Status ; voir au paragraphe 3.2.

Pour supprimer les informations d'alarme locales, un nœud supprime simplement les objets ALARM_SPEC générés localement correspondants des messages Path et Resv sortants. Un nœud PEUT modifier un objet ALARM_SPEC généré en local.

Le traitement normal des messages de rafraîchissement et de déclenchement s'applique aux messages Path ou Resv qui contiennent des objets ALARM_SPEC. Noter que des changements dans les objets ALARM_SPEC d'un message au suivant peuvent inclure une modification du contenu d'un objet ALARM_SPEC spécifique, ou un changement du nombre d'objets ALARM_SPEC présents. Tous les changements dans les objets ALARM_SPEC DEVRAIENT être traités comme des messages déclencheurs.

Manquer à suivre les directives ci-dessus, en particulier celles marquées "DEVRAIT" et "NE DEVRAIENT PAS", peut résulter en ce que les informations d'alarme ne soient pas correctement ou entièrement communiquées.

3.1.3 Codes et valeurs d'erreur

Les codes et valeurs d'erreur utilisés dans les objets ALARM_SPEC sont les mêmes que ceux utilisés dans les objets ERROR_SPEC. De nouvelles valeurs de code d'erreur à utiliser pour les deux objets ERROR_SPEC et ALARM_SPEC peuvent être allouées pour prendre en charge des types d'alarmes définis par d'autres normes.

Dans le présent document, on définit un nouveau code d'erreur. Le code d'erreur utilise la valeur 31 et est appelé "Alarms". Les valeurs utilisées dans le champ Valeur d'erreur quand le code d'erreur est "Alarms" sont les mêmes que les valeurs définies dans la convention textuelle IANAItuProbableCause de IANA-ITU-ALARM-TC-MIB dans la MIB Alarmes [RFC3877]. Noter que ces valeurs sont gérées par l'IANA ; voir http://www.iana.org.

3.1.4 Rétro compatibilité

La prise en charge des objets ALARM_SPEC est FACULTATIVE. Les nœuds qui ne les prennent pas en charge (en accord avec les règles définies dans la [RFC2205]) passent les objets non modifiés à travers le nœud, parce que l'objet

ALARM_SPEC a un C-Num de la forme 11bbbbbb.

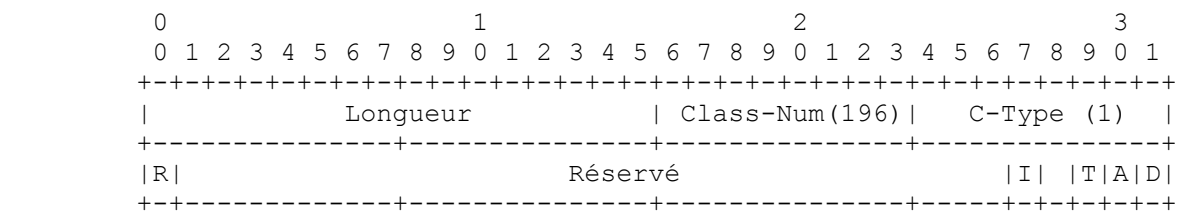
Cela permet que les informations d'alarme soient collectées et examinées dans un réseau construit à partir d'une collection de nœuds dont certains prennent en charge la communication des informations d'alarme, et certains autres ne le font pas.

3.2 Contrôle de la communication d'alarme

La communication des informations d'alarme est contrôlée via des informations d'état administratif portées dans l'objet Admin_Status. Un nouveau bit est défini, appelé le bit I, qui indique quand la communication de l'alarme doit être désactivée. La définition de ce bit ne modifie pas les procédures définies à la Section 7 de la [RFC3473].

3.2.1 Objet Admin_Status mis à jour

Le format de l'objet Admin_Status est mis à jour pour inclure le bit I :



Communication d'alarme désactivée (I) : 1 bit. Quand il est établi, cela indique que la communication d'alarme est désactivée pour le LSP et que les nœuds NE DEVRAIENT PAS ajouter d'informations d'alarme locales.

Voir au paragraphe 7.1 de la [RFC3473] la définition des autres bits.

3.2.2 Procédures

Le bit I peut être établi et mis à zéro en utilisant les procédures définies aux paragraphes 7.2 et 7.3 de la [RFC3473]. Un nœud qui reçoit (ou génère) un objet Admin_Status avec les bits A ou I établis (à 1) DEVRAIT supprimer toutes les informations d'alarme générées en local des messages Path et Resv sortants du LSP correspondant. Quand un nœud reçoit (ou génère) un objet Admin_Status avec les bits A et I à zéro (0) et que des informations d'alarme locales sont présentes, il DEVRAIT ajouter les informations d'alarme locales aux messages Path et Resv sortants du LSP correspondant.

Le traitement des objets ALARM_SPEC non générés en local NE DOIT PAS être impacté par le contenu de l'objet Admin_Status ; c'est-à-dire que les objets ALARM_SPEC reçus DOIVENT être transmis inchangés sans considération des réglages reçus ou transmis des bits I et A. Noter que selon la [RFC3473], l'absence de l'objet Admin_Status est équivalente à recevoir un objet contenant une valeur toute de zéros (0).

Le comportement de traitement relatif au bit I PEUT être outrepassé localement sur la base de la configuration.

Quand on génère de messages Notify pour des LSP avec le bit I établi, les TLV décrits dans le présent document PEUVENT être ajoutés à l'objet ERROR_SPEC envoyé dans le message Notify.

3.3 Formats de message

Ce paragraphe présente les formats relatifs au message RSVP tel que modifié par le présent document. Les formats spécifiés dans la [RFC3473] servent de base à ces formats. Les objets sont mentionnés dans l'ordre suggéré.

Le format d'un message Path est le suivant :

```
<Message Path> ::=  <En-tête commun> [ <INTEGRITY> ]
                    [ [<MESSAGE_ID_ACK> | <MESSAGE_ID_NACK>] ... ]
                    [ <MESSAGE_ID> ]
                    <SESSION> <RSVP_HOP>
                    <TIME_VALUES>
```

[<EXPLICIT_ROUTE>]
<LABEL_REQUEST>
[<PROTECTION>]
[<LABEL_SET> ...]
[<SESSION_ATTRIBUTE>]
[<NOTIFY_REQUEST>]
[<ADMIN_STATUS>]
[<POLICY_DATA> ...]
[<ALARM_SPEC> ...]
<descripteur de l'envoyeur>

<descripteur de l'envoyeur> n'est pas modifié par le présent document.

Le format d'un message Resv est le suivant :

<Message Resv> ::= <En-tête commun> [<INTEGRITY>]
[[<MESSAGE_ID_ACK> | <MESSAGE_ID_NACK>] ...]
[<MESSAGE_ID>]
<SESSION> <RSVP_HOP>
<TIME_VALUES>
[<RESV_CONFIRM>] [<SCOPE>]
[<NOTIFY_REQUEST>]
[<ADMIN_STATUS>]
[<POLICY_DATA> ...]
[<ALARM_SPEC> ...]
<STYLE> <Liste de descripteurs de flux>

<Liste de descripteurs de flux> n'est pas modifié par le présent document.

3.4 Relations avec UNI GMPLS

La [RFC4208] définit comment GMPLS peut être utilisé dans un modèle de recouvrement pour fournir une interface utilisateur-réseau (UNI, *User-to-Network Interface*). Dans ce modèle, des restrictions peuvent être appliquées aux informations qui sont signalées entre un nœud de bordure et un nœud de cœur. Cette restriction permet au réseau de cœur de limiter les informations qui sont visibles en dehors du cœur. Cette restriction peut être faite pour des raisons de confidentialité, de protection de la vie privée, ou de sécurité. Elle peut aussi être faite pour des raisons de fonctionnement, par exemple, si l'information n'est applicable que dans le réseau de cœur.

Les extensions décrites dans le présent document sont candidates au filtrage comme décrit dans la [RFC4208]. En particulier, les observations suivantes s'appliquent.

- Un nœud de cœur d'entrée ou de sortie PEUT filtrer les alarmes provenant du cœur GMPLS à un LSP UNI client-nœud. Ce peut être pour protéger des informations sur le réseau de cœur, ou pour indiquer que le réseau de cœur effectue ou a achevé des actions de récupération pour le LSP GMPLS.

- Un nœud de cœur d'entrée ou de sortie PEUT modifier les alarmes provenant du cœur GMPLS quand il envoie à un LSP UNI client-nœud. Ceci peut faciliter la capacité du client UNI de comprendre la défaillance et son effet sur le plan des données, et permettre au client UNI de prendre les actions correctives de façon plus appropriée.

- De même, un nœud de cœur de sortie PEUT choisir de ne pas demander de rapport d'alarme sur les messages Path qu'il envoie en aval au réseau de recouvrement.

3.5 Relations avec GMPLS E-NNI

GMPLS peut être utilisé à l'interface externe de réseau à réseau (E-NNI) ; voir la [RFC5787]. À cette interface, des restrictions peuvent être appliquées aux informations qui sont signalées entre un nœud cœur de sortie et un d'entrée.

Cette restriction permet au réseau cœur d'entrée de limiter les informations qui sont visibles en dehors de son réseau cœur. Cette restriction peut être faite pour des raisons de confidentialité, de protection de la vie privée, ou de sécurité. Elle peut

aussi être faite pour des raisons de fonctionnement, par exemple, si l'information n'est applicable que dans le réseau de cœur.

Les extensions décrites dans le présent document sont candidates au filtrage comme décrit dans la [RFC5787]. En particulier, les observations suivantes s'appliquent.

- Un nœud de cœur d'entrée ou de sortie PEUT filtrer les alarmes internes du réseau cœur. Ce peut être pour protéger les informations sur le réseau interne ou pour indiquer que le réseau cœur effectue ou a achevé des actions de récupération pour ce LSP.

- Un nœud de cœur d'entrée ou de sortie PEUT modifier les alarmes internes du réseau cœur. Cela peut faciliter à l'échange de trafic E-NNI (c'est-à-dire, au nœud de cœur de sortie) la compréhension de la défaillance et de ses effets sur le plan des données, et la prise des actions correctives d'une manière plus appropriée ou prolonger les alarmes générées en amont/en aval comme approprié.

- De façon similaire, un nœud cœur d'entrée/sortie PEUT choisir de ne pas demander de rapport d'alarme sur les messages Path qu'il envoie en aval.

4. Considérations sur la sécurité

Certains opérateurs peuvent considérer les informations d'alarme comme sensibles. Pour prendre en charge des environnements où c'est le cas, les mises en œuvre DEVRAIENT permettre à l'utilisateur de désactiver la génération des objets ALARM_SPEC, ou de les filtrer ou les corréler aux frontières de domaine.

Le présent document n'introduit aucune considération de sécurité supplémentaire. Voir dans la [RFC3473] les considérations de sécurité pertinentes.

On peut noter que si les considérations de sécurité de la [RFC3473] sont violées, les informations d'alarme peuvent être usurpées. Une telle usurpation serait tout au plus ennuyeuse et causerait une légère dégradation des performances du plan de contrôle dans la mesure où les détails ne sont fournis que pour information et ne résultent pas en des actions de protocole au delà de l'échange des messages pour convoyer les informations. Si la sécurité du protocole peut être violée suffisamment pour permettre de falsifier les informations d'alarme, alors des dommages considérablement plus intéressants et excitants peuvent être causés en falsifiant les autres éléments des messages de protocole.

8. Considérations relatives à l'IANA

L'IANA a alloué de nouvelles valeurs pour les espaces de noms définis dans le présent document et repris dans cette section.

5.1 Nouvel objet RSVP

L'IANA a fait les allocations suivantes dans la section "Noms, numéros, et types de classes" du registre "RSVP PARAMETERS" situé à http://www.iana.org/assignments/rsvp-parameters

Une nouvelle classe nommée ALARM_SPEC (198) a été créée dans la gamme 11bbbbbb avec les valeurs suivantes :

- Classe = 198, C-Type = 1
  RFC 4783
  Réservé. (La valeur de C-Type est définie pour ERROR_SPEC, mais n'est pas définie pour ALARM_SPEC.)

- Classe = 198, C-Type = 2
  RFC 4783
  Réservé. (La valeur de C-Type est définie pour ERROR_SPEC, mais n'est pas définie pour ALARM_SPEC.)

- Objet IPv4 IF_ID ALARM_SPEC : Classe = 198, C-Type = 3
  RFC 4783
  Même définition que pour IPv4 IF_ID ERROR_SPEC [RFC3473].

o Objet IPv6 IF_ID ALARM_SPEC : Classe = 198, C-Type = 4
RFC 4783
Même définition que IPv6 IF_ID ERROR_SPEC [RFC3473].

L'objet ALARM_SPEC utilise le code d'erreur et les valeurs d'erreur provenant de l'objet ERROR_SPEC.

5.2 Nouveaux types d'identifiant d'interface

L'IANA a fait les allocations suivantes dans la section "Types d'identifiant d'interface" du registre "Paramètres de signalisation GMPLS" situé à http://www.iana.org/assignments/gmpls-sig-parameters :

Code	Longueur	Nom	Référence
512	8	REFERENCE_COUNT	RFC 4783
513	8	SEVERITY	RFC 4783
514	8	GLOBAL_TIMESTAMP	RFC 4783
515	8	LOCAL_TIMESTAMP	RFC 4783
516	variable	ERROR_STRING	RFC 4783

5.3 Nouveau registre pour les champs de bits d'objet Admin-Status

L'IANA a créé une nouvelle section intitulée "Fanions d'informations d'état administratif" dans le registre "Paramètres de signalisation GMPLS" situé à http://www.iana.org/assignments/gmpls-sig-parameters et fait les allocations suivantes :

Valeur	Nom	Référence
0x80000000	Reflect (R)	[RFC3473/RFC3471]
0x00000010	Inhibit Alarm Communication (I)	RFC 4783
0x00000004	Testing (T)	[RFC3473/RFC3471]
0x00000002	Administratively down (A)	[RFC3473/RFC3471]
0x00000001	Deletion in progress (D)	[RFC3473/RFC3471]

5.4 Nouveau code d'erreur RSVP

L'IANA a fait les allocations suivantes dans la section "Codes et valeurs d'errreur" du registre "Paramètres RSVP" situé à http://www.iana.org/assignments/rsvp-parameters :

31 Alarms RFC 4783

Les sous codes de valeur d'erreur pour ce code d'erreur ont des valeurs et significations identiques aux valeurs et significations définies dans la convention textuelle IANAItuProbableCause de la MIB IANA-ITU-ALARM-TC-MIB des alarmes [RFC3877]. Noter que ces valeurs sont déjà gérées par l'IANA.

6. Références

6.1 Références normatives

[M.3100] Recommandation UIT-T M.3100, "Modèle générique d'informations réseau", 1995.

[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.)*

[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)

[RFC3877] S. Chisholm, D. Romascanu, "Base de données d'informations de gestion d'alarmes", septembre 2004. *(P.S.)*

6.2 Références pour information

[GR833] Bellcore, "Network Maintenance: Network Element and Transport Surveillance Messages" (GR-833-CORE), Issue 3, February 1999.

[M.20] Recommandation UIT-T M.20, "Philosophie de la maintenance des réseaux de télécommunication", octobre 1992.

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

[RFC5787] D. Papadimitriou, "Extensions des protocoles d'acheminement OSPFv2 pour l'acheminement sur les réseaux optiques à commutation automatique (ASON)", mars 2010. *(Expérimentale)*

7. Remerciements

Des commentaires et apports précieux ont été reçus d'un certain nombre de personnes, incluant Wes Doonan, Bert Wijnen pour la référence DISMAN, et Tom Petch qui a commencé l'interaction du groupe de travail DISMAN. On remercie aussi David Black, Lars Eggert, Russ Housley, Dan Romascanu, et Magnus Westerlund de leurs précieux commentaires.

8. Contributeurs

La liste descontributeurs est par ordre alphabétique.

Deborah Brungard
AT&T Labs, Room MT D1-3C22
200 Laurel Avenue
Middletown, NJ 07748, USA
mél : dbrungard@att.com

Igor Bryskin
Movaz Networks, Inc.
7926 Jones Branch Drive
McLean VA, 22102, USA
mél : ibryskin@movaz.com

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

Dimitri Papadimitriou (Alcatel)
1 rue Francis Wellesplein
B-2018 Antwerpen, Belgium
téléphone : +32 3 240-8491
mél : dimitri.papadimitriou@alcatel.be

Arun Satyanarayana
Cisco Systems, Inc
170 West Tasman Dr.
San Jose, CA 95134 USA
mél : asatyana@cisco.com

Adresse de l'éditeur

Lou Berger
LabN Consulting, L.L.C.
téléphone : +1 301-468-9228
mél : lberger@labn.net

Déclaration complète de droits de reproduction

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