Groupe de travail Réseau
**Request for Comments : 4412**
Catégorie : En cours de normalisation
Traduction Claude Brière de L'Isle

H. Schulzrinne, Columbia U.
J. Polk, Cisco Systems
février 2006

# Priorité de ressource de communications pour le protocole d'initialisation de session (SIP)

**Statut du présent mémoire**

Le présent document spécifie un protocole de normalisation Internet pour la communauté Internet, et appelle à des discussions et suggestions en vue de son amélioration. Prière de se rapporter à l'édition en cours des normes officielles du protocole Internet (STD 1) pour connaître l'état de la normalisation et le statut du présent protocole. La distribution du présent mémo n'est soumise à aucune restriction.

**Déclaration de copyright**



**Résumé**

Le présent document définit deux nouveaux champs d'en-tête du protcole d'initialisation de session (SIP, *Session Initiation Protocol*) pour la priorité de ressource de communication, à savoir , "Resource-Priority" et "Accept-Resource-Priority". Le champ d'en-tête "Resource-Priority" peut influencer le comportement des agents d'utilisateur SIP (comme des routeurs de téléphonie ou des téléphones IP) et des mandataires SIP. Il n'influence pas directement le comportement de transmission des routeurs IP.

## Table des matières

## 1. Introduction

En cas d'urgence, les ressources de communications (y compris les circuits téléphoniques, la bande passante IP, et les routeurs entre les réseaux à commutation de circuit et IP) peuvent subir de l'encombrement. L'encombrement peut survenir du fait d'une utilisation importante, de la perte de ressources causées par des désastres naturels ou causés par l'homme, et par des attaques contre le réseau lors de situations d'urgence causées par l'homme. Cet encombrement peut rendre difficile aux personnes chargées de l'assistance en cas d'urgence, la récupération, ou l'application de la loi pour coordonner leurs efforts. Alors que les réseaux IP deviennent partie intégrante des réseaux convergents ou hybrides, au côté des réseaux publics et privés à commutation de circuit (téléphone), il devient nécessaire de s'assurer que ces réseaux peuvent fournir une assistance durant de telles urgences.

Les usagers peuvent également vouloir interrompre leurs activités de communications de priorité inférieure et dédier leurs ressources de système d'extrémité aux tentatives de communications de priorité élevée si une demande de communications de priorité élevée parvient à leur système d'extrémité.

Il y a de nombreux services fondés sur IP qui peuvent fournir une assistance durant des urgences. Le présent mémoire ne couvre que les applications de communications en temps réel qui impliquent le protocole d'initialisation de session (SIP) [RFC3261], y compris la voix sur IP, les conférences multimédia, la messagerie instantanée, et la présence. Les applications SIP peuvent impliquer au moins cinq ressources différentes qui peuvent devenir rares et encombrées durant les urgences. Ces ressources incluent les ressources de routeurs, les ressources de réseau à commutation de circuit, les ressources de réseau IP, les ressources de système d'extrémité récepteur, et les ressources de mandataire SIP. Les ressources de réseau IP sont en dehors du domaine d'application de la signalisation SIP et ne seront donc pas prises ici en considération.

Même si les ressources à l'élément SIP lui-même ne sont pas raréfiées, un routeur SIP peut marquer les appels sortants avec une indication de priorité, par exemple, sur un message d'adresse initial (IAM, *Initial Address Message*) ISUP (ISDN User Part) généré par un routeur SIP avec le réseau téléphonique public commuté (RTPC).

Pour améliorer les réponses aux cas d'urgence, il est devenu nécessaire de donner des priorités à l'accès aux ressources à signalisation SIP durant les périodes de rareté de ressourced résultant d'une situation de crise. On appelle cela "priorité de ressource". Le mécanisme lui-même peut bien être en place en permanence, mais ne prendre matériellement effet sur le traitement des appels que durant les périodes de ressources rares.

Actuellement, SIP ne comporte pas de mécanisme qui permette à l'origine d'une demande d'indiquer à un élément SIP qu'il souhaite que la demande invoque une telle priorité de ressource. Pour répondre à ce besoin, le présent document ajoute un élément de protocole SIP qui marque certaines demandes SIP.

Le présent document définit (Section 3) deux nouveaux champs d'en-tête SIP pour la priorité de ressource de communications, appelés "Resource-Priority" et "Accept-Resource-Priority". Le champ d'en-tête "Resource-Priority"

PEUT être utilisé par les agents d'utilisateur SIP, incluant les passerelles et terminaux du réseau téléphonique public commuté (RTPC) et les serveurs mandataires SIP, pour influencer leur traitement des demandes SIP, incluant la priorité accordée aux appels du RTPC. Pour les passerelles RTPC, le comportement traduit en schémas analogiques dans le RTPC, par exemple, le mécanisme de priorité de la Recommandation UIT-T Q.735.3 [Q.735.3] dans les deux direction du RTPC à IP et de IP au RTPC. La Recommandation UIT-T I.255.3 [I.255.3] est un autre exemple.

Une demande SIP avec une indication de "Priorité de ressource" peut être traitée différemment dans ces situations :

1. La demande peut recevoir une priorité élevée pour l'accès aux ressources de passerelle RTPC, comme des circuits inter-urbains.
2. La demande peut interrompre des demandes de priorité inférieure sur un appareil d'utilisateur comme un téléphone IP.
3. La demande peut porter des informations provenant d'un domaine de priorité multi-niveaux dans le réseau téléphonique (par exemple, en utilisant les facilités de [Q.735.3]) à un autre, sans que les mandataires SIP eux-mêmes inspectent ou modifient les champs d'en-tête.
4. Dans les mandataires SIP et les agents d'utilisateur de boucle locale, les demandes de priorité supérieure peuvent déplacer les demandes de signalisation existantes ou outrepasser les limites de capacité de passerelle RTPC en effet pour des priorités inférieures.

Ce champ d'en-tête se rapporte, mais avec une sémantique différente, au champ d'en-tête "Priority" du paragraphe 20.26 de la [RFC3261]. Le champ d'en-tête "Priority" décrit l'importance que la demande SIP devrait avoir pour la personne qui reçoit ou son agent. Par exemple, cet en-tête peut être factorisé en décisions sur l'acheminement de l'appel à des appareils mobiles et assistants et sur l'acceptation de l'appel quand la destination est occupée. Le champ d'en-tête "Priority" n'affecte par exemple pas l'usage des ressources de passerelle RTPC ou de mandataire. De plus, tout client d'agent d'utilisateur (UAC, *User Agent Client*) peut affirmer une valeur de priorité de "toute" *(any)* et l'usage des valeurs du champ d'en-tête "Resource-Priority" est soumis à autorisation.

Bien que le champ d'en-tête "Resource-Priority" n'influence pas directement le comportement de transmission des routeurs IP ou l'utilisation des ressources de communications comme une priorité de transmission de paquet, les procédures pour utiliser ce champ d'en-tête pour causer une telle influence pourront être définies dans d'autres documents.

Les mises en œuvre existantes de la [RFC3261] qui ne participent pas au mécanisme de priorité de ressource suivent les règles normales de son paragraphe 8.2.2 : "Si un UAS ne comprend pas un champ d'en-tête dans une demande (c'est-à-dire, si le champ d'en-tête n'est pas défini dans cette spécification ou dans une extension prise en charge) le serveur DOIT ignorer ce champ d'en-tête et continuer le traitement du message". Donc, l'utilisation de ce mécanisme est entièrement invisible aux mises en œuvre existantes sauf si la demande inclut le champ d'en-tête "Require" avec l'étiquette d'option "resource-priority".

Le mécanisme décrit ici peut être utilisé pour la préparation des urgences dans les systèmes de télécommunications d'urgence, mais c'est seulement une petite partie d'un réseau de préparation d'urgences et ne se restreint pas à un tel usage.

Le mécanisme vise à satisfaire les exigences de la [RFC3487]. Il est structuré de telle sorte qu'il fonctionne dans tous les réseaux transparents à SIP et au protocole de transport en temps réel (RTP, *Real-Time Transport Protocol*) [RFC3550], définis dans la [RFC3487]. Dans de tels réseaux, tous les éléments de réseau et les mandataires SIP laissent passer inchangées les demandes SIP valides. C'est important car il est probable que ce mécanisme va souvent être déployé dans des réseaux où les réseaux voisins ne connaissent pas le mécanisme de priorité de ressource et ne fournissent pas de privilèges spéciaux à de telles demandes. La demande atteint alors une passerelle du RTPC ou un ensemble d'éléments SIP qui connaissent le mécanisme.

Par souci de concision, on se réfère aux mandataires SIP et aux agents d'utilisateur (UA) qui agissent sur le champ d'en-tête "Resource-Priority" comme à des acteurs RP.

Il sera probablement courant que le même élément SIP traite les demandes qui portent les champs d'en-tête "Resource-Priority" et celles qui ne les portent pas.

Les entités gouvernementales et les organismes de normalisation ont développé plusieurs schémas de priorité différents pour leurs réseaux. Les utilisateurs aimeraient être capables d'obtenir un traitement de priorité autorisé dans plusieurs de ces réseaux, sans changer de client SIP. Aussi, un seul appel peut traverser des éléments SIP qui sont gérés par des administrations différentes et soumis à des mécanismes de priorité différents. Comme il n'y a pas un ordre mondial pour ces priorités, on permet à chaque demande de contenir plus d'une valeur de priorité tirée de ces différentes listes de priorité, appelées un espace de noms dans le présent document. Normalement, chaque élément SIP ne prend en charge qu'un seul de

ces espaces de noms, mais on discute de ce qui se passe si un élément a besoin de prendre en charge plusieurs espaces de noms à la Section 8.

Comme l'obtention d'un accès prioritaire aux ressources offre des opportunités de dénier le service aux autres, on s'attend à ce que de tels appels prioritaires soient soumis à authentification et autorisation, en utilisant les mécanismes de sécurité SIP standard (Section 11) ou d'autres comme approprié.

Le reste de ce document est structuré comme suit : après la définition de la terminologie à la Section 2, on définit la syntaxe pour les deux nouveaux champs d'en-tête SIP à la Section 3 et on décrit le comportement de protocole à la Section 4. Les deux principaux mécanismes pour le traitement différencié des demandes SIP (à savoir, préemption et mise en file d'attente) sont décrits au paragraphe 4.5. Les conditions d'erreur sont traitées au paragraphe 4.6. Les paragraphes 4.7.1 à 4.7.3 détaillent le comportement des éléments SIP spécifiques. L'authentification par des tiers est brièvement résumée à la Section 5. La Section 6 décrit comment ces caractéristiques affectent les systèmes existants qui ne les prennent pas en charge.

Comme les appels peuvent traverser plusieurs domaines administratifs avec des espaces de noms différents ou plusieurs éléments avec le même espace de noms, il est fortement suggéré que tous ces domaines et éléments appliquent les mêmes algorithmes pour le même espace de noms, car autrement l'expérience de bout en bout des utilisateurs privilégiés peut être compromise.

Des exemples du protocole sont donnés à la Section 7. La Section 8 discute de ce qui arrive si une demande contient plusieurs espaces de noms ou si un élément peut traiter plus d'un espace de noms. La Section 9 énumère les informations que l'enregistrement d'un espace de noms doit fournir. La Section 10 définit les propriétés de cinq espaces de noms qui sont enregistrés par le présent document. Les questions de sécurité sont considérées à la Section 11, mais le présent document ne définit pas de nouveau mécanisme de sécurité. La Section 12 discute les considérations relatives à l'IANA et enregistre les paramètres relatifs au présent document.

## 2. Terminologie

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119], et indiquent les niveaux d'exigence pour les mises en œuvre conformes.

## 3. Champs d'en-tête SIP Resource-Priority et Accept-Resource-Priority

Cette section définit la syntaxe des champs d'en-tête "Resource-Priority" et "Accept-Resource-Priority" SIP. Le comportement est décrit à la Section 4.

### 3.1 Champs d'en-tête "Resource-Priority"

Le champ d'en-tête demande de "Resource-Priority" marque une demande SIP comme désirant un accès prioritaire à des ressources, comme décrit dans l'introduction.

Il n'est pas exigé par le protocole que toutes les demandes au sein d'un dialogue ou session SIP utilisent le champ d'en-tête "Resource-Priority". La politique administrative locale PEUT rendre obligatoire l'inclusion du champ d'en-tête "Resource-Priority" dans toutes les demandes. Les mises en œuvre de la présente spécification DOIVENT permettre que l'inclusion soit par une demande explicite de l'utilisateur, soit qu'elle soit automatique pour toutes les demandes.

La syntaxe du champ d'en-tête "Resource-Priority" est décrite ci-dessous. La production "token-nodot" est copiée de la [RFC3265].

```
Resource-Priority  = "Resource-Priority" HCOLON r-value *(COMMA r-value)
r-value  = espace de noms "." r-priority
espace de noms = token-nodot
r-priority = token-nodot
token-nodot = 1*( alphanum / "-"  / "!" / "%" / "*" / "_" / "+" / "`" / "'" / "~" )
```

Voici un exemple de champ d'en-tête "Resource-Priority" : Resource-Priority: dsn.flash

Le paramètre "r-value" dans le champ d'en-tête "Resource-Priority" indique la priorité de ressource désirée par le générateur de la demande. Chaque valeur de ressource (r-value) est formatée comme "espace de noms" "." "valeur de priorité". La valeur est tirée de l'espace de noms identifié par le jeton "espace de noms". Les espaces de noms et priorités sont des jetons ASCII insensibles à la casse qui ne contiennent pas de points. Donc, "dsn.flash" et "DSN.Flash", par exemple, sont équivalents. Chaque espace de noms a au moins une valeur de priorité. Les espaces de noms et valeurs de priorité au sein de chaque espace de noms DOIVENT être enregistrés par l'IANA (Section 12). Les enregistrements d'espace de noms initiaux sont décrits au paragraphe 12.5.

Comme une demande peut traverser plusieurs domaines administratifs avec plusieurs différents espaces de noms, il est nécessaire d'être capable d'énumérer plusieurs espaces de noms différents au sein du même message. Cependant, un espace de noms particulier NE DOIT PAS apparaître plus d'une fois dans le même message SIP. Cela peut être exprimé de façon équivalente comme des listes séparées par des virgules au sein d'un seul champ d'en-tête, comme plusieurs champs d'en-tête, ou comme leur combinaison. L'ordre des "r-values" au sein du champ d'en-tête n'a pas de signification. Donc, par exemple, les trois fragments d'en-tête suivants sont équivalents :

Resource-Priority: dsn.flash, wps.3
Resource-Priority: wps.3, dsn.flash
Resource-Priority: wps.3
Resource-Priority: dsn.flash

### 3.2 Champ d'en-tête "Accept-Resource-Priority"

Le champ d'en-tête de réponse "Accept-Resource-Priority" énumère les valeurs de ressource (r-values) qu'un agent d'utilisateur de serveur SIP accepte de traiter. (Cela n'implique pas qu'un appel avec de telles valeurs va trouver des ressources suffisantes et réussir.) La syntaxe du champ d'en-tête "Accept-Resource-Priority" est la suivante :

Accept-Resource-Priority = "Accept-Resource-Priority" HCOLON [r-value *(COMMA r-value)]

Voici un exemple : Accept-Resource-Priority: dsn.flash-override, dsn.flash, dsn.immediate, dsn.priority, dsn.routine

Certains domaines administratifs PEUVENT choisir de désactiver l'utilisation de l'en-tête "Accept-Resource-Priority" comme révélant trop d'informations sur ce domaine dans les réponses. Cependant, ce comportement N'EST PAS RECOMMANDÉ, car ce champ d'en-tête aide à corriger les problèmes.

### 3.3 Usage des champs d'en-tête "Resource-Priority" et "Accept-Resource-Priority"

Le tableau suivant étend les valeurs du Tableau 2 de la [RFC3261]. (La méthode PRACK, marquée PRA, est définie dans la [RFC3262], les méthodes SUBSCRIBE (marquée SUB) et NOTIFY (marquée NOT) dans la [RFC3265], la méthode UPDATE (UPD) dans la [RFC3311], la méthode MESSAGE (MSG) dans la [RFC3428], la méthode REFER (REF) dans la [RFC3515], la méthode INFO (INF) dans la [RFC2976], et la méthode PUBLISH (PUB) dans la [RFC3903].)

| **Champ d'en-tête** | **où** | **mandataire** | **INV** | **ACK** | **CAN** | **BYE** | **REG** | **OPT** | **PRA** |
|---|---|---|---|---|---|---|---|---|---|
| Resource-Priority | R | amdr | o | o | o | o | o | o | o |
| Accept-Resource-Priority | 200 | amdr | o | - | o | o | o | o | o |
| Accept-Resource-Priority | 417 | amdr | o | - | o | o | o | o | o |

| **Champ d'en-tête** | **où** | **mandataire** | **SUB** | **NOT** | **UPD** | **MSG** | **REF** | **INF** | **PUB** |
|---|---|---|---|---|---|---|---|---|---|
| Resource-Priority | R | amdr | o | o | o | o | o | o | o |
| Accept-Resource-Priority | 200 | amdr | o | o | o | o | o | o | o |
| Accept-Resource-Priority | 417 | amdr | o | o | o | o | o | o | o |

D'autres méthodes de demande PEUVENT définir leurs propres règles de traitement, sauf mention contraire, les receveurs PEUVENT ignorer ces champs d'en-tête.

### 3.4 Étiquette d'option "priorité de ressource"

Le présent document définit aussi l'étiquette d'option "priorité de ressource". Le comportement est décrit au paragraphe 4.3, et l'enregistrement par l'IANA est décrit au paragraphe 12.3.

# 4. Comportement des éléments SIP qui reçoivent des demandes de priorité

## 4.1 Introduction

Tous les agents d'utilisateur SIP et serveurs mandataires qui prennent en charge la présente spécification partagent un certain comportement, qu'on décrit au paragraphe 4.2. Le comportement quand on rencontre une étiquette d'option "priorité de ressource" dans un champ d'en-tête "Require" est décrit au paragraphe 4.3. Le paragraphe 4.4 décrit le traitement des demandes d'option. Les deux mécanismes fondamentaux de résolution de contention de ressource, préemption et mise en file d'attente, sont décrits au paragraphe 4.5. Le paragraphe 4.6 explique ce qui arrive quand les demandes échouent. Le comportement spécifique des clients d'agent d'utilisateur, des serveurs, et des serveurs mandataires est couvert au paragraphe 4.7.

## 4.2 Règles générales

Le champ d'en-tête "Resource-Priority" est potentiellement applicable à tout message de demande SIP. Au minimum, les mises en œuvre des types de demande suivants DOIVENT prendre en charge l'en-tête "Resource-Priority" pour être conformes à la présente spécification :

- o INVITE [RFC3261]
- o ACK [RFC3261]
- o PRACK [RFC3262]
- o UPDATE [RFC3311]
- o REFER [RFC3515]

Les mises en œuvre DEVRAIENT prendre en charge le champ d'en-tête "Resource-Priority" dans les types de demande suivants :

- o MESSAGE [RFC3428]
- o SUBSCRIBE [RFC3265]
- o NOTIFY [RFC3265]

Noter que ceci n'implique pas que toutes les mises en œuvre doivent prendre en charge toutes les méthodes de demande mentionnées.

Si un élément SIP reçoit le champ d'en-tête "Resource-Priority" dans une demande autre que celles mentionnées ci-dessus, l'en-tête PEUT être ignoré, conformément aux règles de la [RFC3261].

En bref, un acteur RP effectue les étapes suivantes quand il reçoit une demande avec priorité. Le comportement en présence d'erreur est décrit au paragraphe 4.6.

1. Si l'acteur RP ne reconnaît aucun des espaces de noms, il traite la demande comme si elle n'avait pas de champ d'en-tête "Resource-Priority".

2. Il s'assure que la demande est autorisée, conformément à la politique locale, à utiliser les niveaux de priorité indiqués. Si la demande n'est pas autorisée, il la rejette. Des exemples de politique d'autorisation sont discutés dans les Considérations sur la sécurité (Section 11).

3. Si la demande est autorisée et si des ressources sont disponibles (pas d'encombrement) il sert la demande comme normal. Si la demande est autorisée mais que les ressources ne sont pas disponibles (encombrement) soit il préempte d'autres sessions en cours, soit il insère la demande dans une file d'attente de priorité, comme décrit au paragraphe 4.5.

## 4.3 Usage de l'en-tête Require avec Resource-Priority

Suivant le comportement SIP standard, si une demande SIP contient le champ d'en-tête "Require" avec l'étiquette d'option "resource-priority", un agent d'utilisateur SIP DOIT répondre par un code 420 (Mauvaise extension) si il ne prend pas en charge les extensions SIP décrites dans ce document. Il mentionne ensuite "resource-priority" dans le champ d'en-tête "Non pris en charge" inclus dans la réponse.

L'utilisation de l'étiquette d'option "resource-priority" dans le champ d'en-tête "Proxy-Require" est NON RECOMMANDÉE.

### 4.4 Demande OPTIONS avec Resource-Priority

Une demande OPTIONS peut être utilisée pour déterminer si un élément prend en charge le mécanisme. Une mise en œuvre conforme DEVRAIT retourner un champ d'en-tête "Accept-Resource-Priority" dans les réponses OPTIONS énumérant toutes les valeurs de ressource valides, mais un acteur RP PEUT être configuré à ne pas retourner de telles valeurs ou à ne les retourner qu'aux demandeurs autorisées.

Suivant le comportement SIP standard , les réponses OPTIONS DOIVENT inclure le champ d'en-tête "Supported" qui inclut l'étiquette d'option "priorité de ressource".

Selon la Section 11 de la RFC3261, les mandataires qui reçoivent une demande avec une valeur de champ d'en-tête "Max-Forwards" de zéro PEUVENT répondre la demande OPTIONS, permettant à un UAC de découvrir les capacités à la fois du mandataire et des serveurs d'agent d'utilisateur.

### 4.5 Approches du traitement préférentiel des demandes

Les éléments SIP peuvent utiliser le mécanisme de priorité de ressource pour modifier divers comportements, comme l'acheminement des demandes, les exigences d'authentification, l'outrepassement des contrôles de capacité du réseau, ou l'enregistrement dans les journaux d'incidents. Le mécanisme de priorité de ressource peut influencer le traitement de la demande elle-même, le marquage des appels RTPC sortants à une passerelle, ou de la session créée par la demande. (On utilise ici les termes de session et d'appel de façon interchangeable, ce qui implique à la fois un flux de données continu entre deux parties ou plus. Les sessions sont établies par les dialogues SIP.)

On définit ci-dessous deux algorithmes courants, à savoir, préemption et mise en file d'attente de priorité. La préemption s’applique seulement aux sessions créées par les demandes SIP, tandis que le traitement des sessions et des demandes peut être soumis à la mise en file d'attente de priorité. Les deux algorithmes peuvent parfois être combinés dans le même élément, bien qu'aucun des espaces de noms décrits dans le présent document ne le fasse. Des algorithmes peuvent être définis pour chaque espace de noms ou, dans certains cas, peuvent être spécifiques d'un domaine administratif. Un autre comportement, comme un acheminement de demande ou des commandes de gestion de réseau, n'est pas défini par la présente spécification.

Naturellement, seuls les éléments SIP qui comprennent ce mécanisme, l'espace de noms et la valeur de ressource, effectuent ces algorithmes. Le paragraphe 4.6.2 discute de ce qui se passe si un acteur RP ne comprend pas les valeurs de priorité contenues dans une demande.

#### 4.5.1 Préemption

Un acteur RP qui suit une politique de préemption peut interrompre une session existante pour faire de la place pour une session entrante de priorité supérieure. Comme les sessions peuvent exiger des quantités différentes de bande passante ou un nombre différent de circuits, une seule session de priorité supérieure peut déplacer plus d'une session de priorité inférieure. Sauf notation contraire, les demandes ne préemptent pas les autres demandes de priorité égale. Comme noté plus haut, le traitement des demandes SIP lui-même n'est pas préempté. Donc, comme les mandataires ne gèrent pas les sessions, ils n'effectuent pas de préemption.

La [RFC4411] contient plus de détails et des exemples de ce comportement.

Le comportement de l'UAS sur la préemption est discuté au paragraphe 4.7.2.1.

#### 4.5.2 Mise en file d'attente de priorité

Dans une politique de mise en file d'attente de priorité, les demandes qui ne trouvent pas de ressources disponibles sont mises en file d'attente dans la queue allouée à la valeur de priorité. Sauf spécification contraire, les demandes sont mises en file d'attente dans l'ordre du premier arrivé, premier servi. Chaque valeur de priorité a sa propre file d'attente, ou plusieurs valeurs de priorité peuvent partager une seule file d'attente. Si une ressource devient disponible, l'acteur RP choisit la demande à partir de la file d'attente non vide de plus haute priorité conformément à la politique de service de file d'attente. Pour les politiques de premier arrivé, premier servi, la demande dans cette file d'attente qui est en attente depuis le plus longtemps est servie. Chaque file d'attente peut contenir un nombre fini de demandes en instance. Si la file d'attente par valeur de priorité pour une nouvelle demande arrivante est pleine, la demande est rejetée immédiatement, avec les codes

d'état spécifiés au paragraphe 4.6.5 et au paragraphe 4.6.6. De plus, une politique de mise en file d'attente de priorité PEUT imposer une limite de temps d'attente pour chaque classe de priorité, par laquelle les demandes qui excèdent un temps d'attente spécifié sont éjectées de la file d'attente et une réponse d'échec de 408 (Fin de temporisation de demande) est retournée au demandeur.

Finalement, un acteur RP PEUT imposer une limite globale de taille de file d'attente additionnant celle de toutes les files d'attentes et abandonner les demandes en attente de priorité inférieure avec une réponse d'échec de 408 (Fin de temporisation de demande). Cela n'implique pas de préemption, car la session n'a pas encore été établie.

Le comportement d'UAS pour la mise en file d'attente est discuté au paragraphe 4.7.2.2.

## 4.6 Conditions d'erreur

### 4.6.1 Introduction

Dans cette section, on décrit le comportement en présence d'erreurs qui est partagé par plusieurs types d'acteurs RP (incluant diverses instances d'UAS comme les passerelles de circuits interurbains, les passerelles de ligne, et les téléphones IP) et mandataires.

Une demande qui contient une indication de priorité de ressource peut échouer pour quatre raisons :
- o l'acteur RP ne comprend pas la valeur de priorité (paragraphe 4.6.2),
- o le demandeur n'est pas authentifié (paragraphe 4.6.3),
- o un demandeur authentifié n'est pas autorisé à faire une telle demande (paragraphe 4.6.4), ou
- o il y a des ressources insuffisantes pour une demande autorisée (paragraphe 4.6.5).

On traite ces cas d'erreur dans l'ordre dans lequel ils se produisent normalement dans le traitement des demandes avec des en-têtes "Resource-Priority". Cependant, cet ordre n'est pas obligatoire. Par exemple, un acteur RP qui sait qu'une certaine valeur de ressource ne peut pas être servie ou mise en file d'attente PEUT, selon la politique locale, s'abstenir d'autorisation, car cela ajouterait seulement de la charge de traitement sans changer le résultat.

### 4.6.2 Pas d'espace de nom ou de valeur de priorité connus

Si un acteur RP ne comprend pas une des valeurs de ressource dans la demande, le traitement dépend de la présence de l'étiquette d'option "Require" "priorité de ressource" :

1. Sans l'étiquette d'option, l'acteur RP traite la demande comme si elle ne contenait pas de champ d'en-tête "Resource-Priority" et la traite avec la priorité par défaut. Les valeurs de ressource qui ne sont pas comprises NE DOIVENT PAS être modifiée ou supprimées.

2. Avec l'étiquette d'option, il DOIT rejeter la demande avec un code de réponse a 417 (Priorité de ressource inconnue).

Faire du cas 1 la valeur par défaut est nécessaire car autrement il n'y aurait pas de moyen de faire aboutir un appel au cas où un mandataire sur le chemin de l'UAS ne partage pas d'espace de noms commun avec l'UAC, mais que l'UAC et l'UAS ont bien un espace de noms en commun.

En général, comme on l'a noté, une demande SIP peut contenir plus d'un champ d'en-tête "Resource-Priority". C'est nécessaire si une demande a besoin de traverser différents domaines administratifs, chacun ayant son propre ensemble de valeurs de ressource valides. Par exemple, l'espace de noms ETS pourrait être activé pour les réseaux du gouvernement des États Unis qui prennent aussi en charge les espaces de noms DSN et/ou DRSN pour la plupart des individus dans ces domaines.

Une réponse 417 (Priorité de ressource inconnue) PEUT, selon la politique locale, inclure un champ d'en-tête "Accept-Resource-Priority" énumérant les valeurs de ressource acceptables.

### 4.6.3 Échec d'authentification

Si la demande n'est pas authentifiée, une réponse 401 (Non autorisé) ou 407 (Authentification du mandataire exigée) est retournée afin de permettre au demandeur d'insérer les accréditifs appropriés.

#### 4.6.4 Échec d'autorisation

Si l'acteur RP reçoit une demande non authentifiée avec un espace de noms et une valeur de priorité qu'il reconnaît mais l'origine n'est pas autorisée pour ce niveau de service, l'élément DOIT retourner une réponse 403 (Interdit).

#### 4.6.5 Ressources insuffisantes

Des conditions de ressources insuffisantes peuvent se produire sur les serveurs mandataires et les serveurs d'agent d'utilisateur, normalement des passerelles de circuits interurbains, si un acteur RP reçoit une demande autorisée, a des ressources insuffisantes, et si la demande ne préempte pas une autre session ni n'est mise en file d'attente. Une demande peut échouer parce que l'acteur RP a soit une capacité de traitement insuffisante pour traiter la demande SIP, soit une bande passante ou capacité de circuits insuffisante pour établir la session demandée pour les demandes SIP créatrices de session.

Si la demande échoue parce que l'acteur RP ne peut pas traiter la charge de signalisation, l'acteur RP répond par 503 (Service indisponible).

Si il n'y a pas assez de bande passante, ou si il y a un nombre insuffisant de circuits, une réponse 488 (Non acceptable ici) indique que l'acteur RP rejette la demande à cause de l'indisponibilité du chemin de support, comme des ressources de passerelle insuffisantes. Dans ce cas, la [RFC3261] indique qu'une réponse 488 DEVRAIT inclure un champ d'en-tête "Warning" avec la raison du rejet ; le code d'avertissement 370 (Bande passante insuffisante) est typique.

Pour les systèmes qui mettent en œuvre la mise en file d'attente, si la demande est mise en file d'attente, l'UAS va retourner une réponse 408 (Fin de temporisation de la demande) si la demande excède la durée d'attente maximum configurée dans la file d'attente.

#### 4.6.6 Occupation

La contention de ressource se produit aussi quand une demande d'appel arrive à un UAS qui est incapable d'accepter un autre appel, parce que l'UAS a juste une ligne ou qu'il a des appels actifs sur toutes ses lignes. Si la demande d'appel indique une valeur de priorité égale ou inférieure comparée à tous les appels actifs présents sur l'UAS, celui-ci retourne une réponse 486 (Occupé ici).

Si la demande est plutôt mise en file d'attente, l'UAS va retourner un code 408 (Fin de temporisation de demande) si la demande excède la durée d'attente maximum configurée dans la file d'attente de l'appareil.

Si un mandataire obtient une réponse 486 (Occupé ici) sur toutes les branches, il peut alors retourner un code 600 (Occupé partout) en réponse à l'appelant.

### 4.7 Comportements spécifiques de l'élément

#### 4.7.1 Comportement de client d'agent d'utilisateur

Les UAC SIP qui prennent en charge la présente spécification DOIVENT être capables de générer le champ d'en-tête "Resource-Priority" pour les demandes qui exigent une priorité élevée d'accès aux ressources. Comme déclaré précédemment, l'UAC DEVRAIT être capable de générer plus d'une valeur de ressource dans une seule demande SIP.

À réception d'une réponse 417 (Priorité de ressource inconnue) l'UAC PEUT tenter une demande ultérieure avec la même valeur de ressource ou une valeur différente. Si c'est disponible, il DEVRAIT choisir des valeurs de ressource autorisées dans l'ensemble de valeurs retournées dans le champ d'en-tête "Accept-Resource-Priority".

##### 4.7.1.1 Comportement de client d'agent d'utilisateur avec un algorithme de préemption

Un UAC qui demande une valeur de priorité qui peut causer une préemption DOIT comprendre un champ d'en-tête Raison dans la demande BYE expliquant pourquoi la session a été terminée, comme expliqué dans la [RFC4411].

##### 4.7.1.2 Comportement de client d'agent d'utilisateur avec une politique de mise en file d'attente

Selon les règles standard du protocole SIP, un UAC DOIT être prêt à recevoir une réponse 182 (Mis en file d'attente) d'un acteur RP qui est actuellement en capacité, mais qui a mis la demande originale dans une file d'attente. Un UAC PEUT

indiquer l'état de cette file d'attente à l'utilisateur par une indication audio ou visuelle pour l'empêcher d'interpréter l'appel comme un échec.

### 4.7.2 Comportement du serveur d'agent d'utilisateur

L'effet précis de l'indication "Resource-Priority" dépend du type d'UAS, de l'espace de noms, et de la politique locale.

#### 4.7.2.1 Serveurs d'agent d'utilisateur et algorithme de préemption

Un UAS conforme à la présente spécification DOIT terminer une session établie avec un espace de noms valide et une valeur de priorité inférieure en faveur d'une nouvelle session établie avec un espace de noms valide et une valeur relative de priorité supérieure, sauf si la politique locale a activé une forme de capacité de mise en attente d'appel. Si une session est terminée, la méthode BYE est utilisée avec un champ d'en-tête "Raison" indiquant pourquoi et où la préemption a eu lieu.

Les mises en œuvre qui ont un certain nombre de choix quant à la manière de mettre en œuvre la préemption sur les téléphones IP avec la présence de plusieurs lignes, c'est-à-dire, avec des appareils qui peuvent traiter plusieurs sessions simultanées. Naturellement, si cet appareil a atteint le nombre de sessions simultanées, une de ces sessions doit être remplacée. Si l'appareil a des sessions en réserve, une mise en œuvre PEUT choisir d'alerter l'appelé à l'arrivée d'un appel de priorité plus élevée. Les détails peuvent aussi être réglés en local ou par la politique d'espace de noms.

La [RFC4411] fournit des informations supplémentaires dans le cas d'une terminaison délibérée ou administrative d'une session en incluant l'en-tête Raison dans le message BYE qui déclare pourquoi le BYE a été envoyé (dans ce cas, un événement de préemption). Les mécanismes du présent document permettent l'indication de où la terminaison s'est produite ("à l' UA", "dans une réservation", "à la passerelle IP/RTPC") et l'inclusion d'exemples de flux d'appel de chaque raison.

#### 4.7.2.2 Serveurs d'agent d'utilisateur et politique fondée sur la file d'attente

Un UAS conforme à la présente spécification DEVRAIT générer une réponse 182 (Mis en file d'attente) si les ressources de cet élément sont occupées, jusqu'à ce qu'il soit capable de traiter la demande et fournir une réponse finale. La fréquence de tels messages provisoires est gouvernée par la [RFC3261].

### 4.7.3 Comportement du mandataire

Les mandataires SIP PEUVENT ignorer le champ d'en-tête "Resource-Priority". Les mandataires SIP PEUVENT rejeter toute demande non authentifiée qui porte ce champ d'en-tête.

Quand le champ d'en-tête "Require" est inclus dans un message, il assure que dans un fourchement parallèle, seules les branches qui prennent en charge le mécanisme de priorité de ressource réussissent.

Si l'encapsulation S/MIME est utilisée conformément à la Section 23 de la RFC 3261, des considérations particulières s'appliquent. Comme indiqué au paragraphe 3.3, le champ d'en-tête "Resource-Priority" peut être modifié par les mandataires et donc est exempté des vérifications d'intégrité décrites au paragraphe 23.4.1.1 de la RFC 3261. Comme il peut être besoin qu'il soit inspecté ou modifié par les mandataires, ce champ d'en-tête DOIT aussi être placé dans le message "externe" si l'UAC veut que les serveurs mandataires soient capables d'agir sur les informations de l'en-tête. Des considérations similaires s'appliquent si des parties du message sont protégées en intégrité ou chiffrées comme décrit dans la [RFC3420].

Si S/MIME n'est pas utilisé, ou si le champ d'en-tête "Resource-Priority" est dans l'en-tête "externe", les mandataires SIP PEUVENT dégrader ou rehausser la "Priorité de ressource" d'une demande ou insérer un nouvel en-tête "Priorité de ressource" si c'est permis par la politique locale.

Si un mandataire à états pleins a autorisé un certain niveau de priorité de ressource, et si il offre un traitement différencié aux réponses contenant des niveaux de priorité de ressource, le mandataire DEVRAIT ignorer toute valeur supérieure contenue dans les réponses, pour empêcher des agents d'utilisateur complices de relever artificiellement le niveau de priorité.

Un mandataire SIP PEUT utiliser l'indication "Resource-Priority" dans ses décisions d'acheminement, par exemple, pour recibler sur un nœud SIP ou un URI SIP qui est réservé pour une priorité de ressource particulière.

Il n'y a pas de considérations particulières pour les mandataires lors du fourchement de demandes contenant une indication de priorité de ressource.

Autrement, le comportement de mandataire est le même que pour les serveurs d'agent d'utilisateur décrits au paragraphe 4.7.2.

## 5. Authentification de tiers

Dans certains cas, l'acteur RP peut n'être pas capable d'authentifier le demandeur ou de déterminer si un utilisateur authentifié est autorisé à faire une telle demande. Dans ces circonstances, l'entité SIP peut s'aider des mécanismes généraux de SIP qui ne sont pas spécifiques de cette application. Le mécanisme de gestion d'entité authentifiée [RFC3893] permet à un tiers de vérifier l'identité du demandeur et de la certifier à un acteur RP. Dans les réseaux à confiance mutuelle, le mécanisme d'identité certifiée SIP [RFC3325] peut aider l'acteur RP à déterminer l'identité du demandeur.

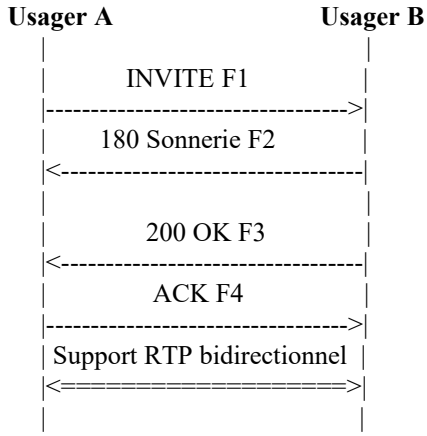
## 6. Rétro compatibilité

Le mécanisme de priorité de ressource décrit dans ce document est pleinement rétro compatible avec les systèmes SIP qui suivent la [RFC3261]. Les systèmes qui ne comprennent pas le mécanisme peuvent seulement délivrer la priorité de service standard, non élevée. Les serveurs d'agent d'utilisateur et mandataires peuvent ignorer tout champ d'en-tête "Resource-Priority" tout comme n'importe quel autre champ d'en-tête inconnu et traiter ensuite la demande comme toute autre demande. Naturellement, la demande peut quand même réussir.

## 7. Exemples

Le corps de message SDP et les échanges BYE et ACK sont les mêmes que dans la [RFC3665] et sont omis pour faire court.

### 7.1 Appel simple




Dans ce scénario, l'usager A achève directement un appel à l'usager B. L'appel de A à B est marqué avec une indication de priorité de ressource.

F1 INVITE Usager A -> Usager B

INVITE sip:UsagerB@biloxi.exemple.com SIP/2.0
Via: SIP/2.0/TCP client.atlanta.exemple.com:5060;branch=z9hG4bK74bf9
Max-Forwards: 70
From: BigGuy <sip:UsagerA@atlanta.exemple.com>;tag=9fxced76sl
To: LittleGuy <sip:UsagerB@biloxi.exemple.com>
Call-ID: 3848276298220188511@atlanta.exemple.com
CSeq: 1 INVITE

```
Resource-Priority: dsn.flash
Contact: <sip:UsagerA@client.atlanta.exemple.com;transport=tcp>
Content-Type: application/sdp
Content-Length: ...

  ...
```

F2 180 Sonnerie Usager B -> Usager A

```
SIP/2.0 180 Ringing
Via: SIP/2.0/TCP client.atlanta.exemple.com:5060;branch=z9hG4bK74bf9
  ;received=192.0.2.101
From: BigGuy <sip:UsagerA@atlanta.exemple.com>;tag=9fxced76sl
To: LittleGuy <sip:UsagerB@biloxi.exemple.com>;tag=8321234356
Call-ID: 3848276298220188511@atlanta.exemple.com
CSeq: 1 INVITE
Contact: <sip:UsagerB@client.biloxi.exemple.com;transport=tcp>
Content-Length: 0
```

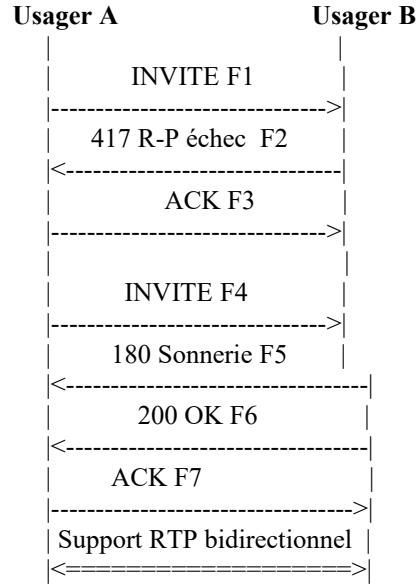
F3 200 OK Usager B -> Usager A

```
SIP/2.0 200 OK
Via: SIP/2.0/TCP client.atlanta.exemple.com:5060;branch=z9hG4bK74bf9
    ;received=192.0.2.101
From: BigGuy <sip:UsagerA@atlanta.exemple.com>;tag=9fxced76sl
To: LittleGuy <sip:UsagerB@biloxi.exemple.com>;tag=8321234356
Call-ID: 3848276298220188511@atlanta.exemple.com
CSeq: 1 INVITE
Contact: <sip:UsagerB@client.biloxi.exemple.com;transport=tcp>
Content-Type: application/sdp
Content-Length: ...

...
```

### 7.2 Le receveur ne comprend pas l'espace de noms

Dans cet exemple, l'UA receveur ne comprend pas l'espace de noms "dsn" et donc retourne un code d'état 417 (Priorité de ressource inconnue). On omet les détails de message pour les messages F5 à F7, car ils sont essentiellement les mêmes que dans le premier exemple.



F1 INVITE Usager A -> Usager B

```
INVITE sip:UsagerB@biloxi.exemple.com SIP/2.0
Via: SIP/2.0/TCP client.atlanta.exemple.com:5060;branch=z9hG4bK74bf9
Max-Forwards: 70
From: BigGuy <sip:UsagerA@atlanta.exemple.com>;tag=9fxced76sl
To: LittleGuy <sip:UsagerB@biloxi.exemple.com>
Call-ID: 3848276298220188511@atlanta.exemple.com
CSeq: 1 INVITE
Require: resource-priority
Resource-Priority: dsn.flash
Contact: <sip:UsagerA@client.atlanta.exemple.com;transport=tcp>
Content-Type: application/sdp
Content-Length: ...
 ...
```

F2 417 Resource-Priority échec  Usager B -> Usager A

```
SIP/2.0 417 Priorité de ressource inconnue
Via: SIP/2.0/TCP client.atlanta.exemple.com:5060;branch=z9hG4bK74bf9
    ;received=192.0.2.101
From: BigGuy <sip:UsagerA@atlanta.exemple.com>;tag=9fxced76sl
To: LittleGuy <sip:UsagerB@biloxi.exemple.com>;tag=8321234356
Call-ID: 3848276298220188511@atlanta.exemple.com
CSeq: 1 INVITE
Accept-Resource-Priority: q735.0, q735.1, q735.2, q735.3, q735.4
Contact: <sip:UsagerB@client.biloxi.exemple.com;transport=tcp>
Content-Type: application/sdp
Content-Length: 0
```

F3 ACK Usager A -> Usager B

```
ACK sip:UsagerB@biloxi.exemple.com SIP/2.0
Via: SIP/2.0/TCP client.atlanta.exemple.com:5060;branch=z9hG4bK74bd5
Max-Forwards: 70
From: BigGuy <sip:UsagerA@atlanta.exemple.com>;tag=9fxced76sl
To: LittleGuy <sip:UsagerB@biloxi.exemple.com>;tag=8321234356
Call-ID: 3848276298220188511@atlanta.exemple.com
CSeq: 1 ACK
Content-Length: 0
```

F4 INVITE Usager A -> Usager B

```
INVITE sip:UsagerB@biloxi.exemple.com SIP/2.0
Via: SIP/2.0/TCP client.atlanta.exemple.com:5060;branch=z9hG4bK74bf9
Max-Forwards: 70
From: BigGuy <sip:UsagerA@atlanta.exemple.com>;tag=9fxced76sl
To: LittleGuy <sip:UsagerB@biloxi.exemple.com>
Call-ID: 3848276298220188511@atlanta.exemple.com
CSeq: 2 INVITE
Require: resource-priority
Resource-Priority: q735.3
Contact: <sip:UsagerA@client.atlanta.exemple.com;transport=tcp>
Content-Type: application/sdp
Content-Length: ...
...
```

# 8. Traitement de plusieurs espaces de noms concurrents

## 8.1 Règles générales

Une seule demande SIP PEUT contenir des valeurs de ressource provenant de plusieurs espaces de noms. Comme noté précédemment, un acteur RP ignore tous les espaces de noms qu'il ne reconnaît pas. La présente spécification s'adresse seulement au cas où un acteur RP choisit alors une des valeurs de ressource restantes pour continuer, choisissant généralement celle qui a la valeur de priorité relative la plus forte.

Si un acteur RP comprend plusieurs espaces de noms, il DOIT créer un ordre local total sur toutes les valeurs de ressource à partir de ces espaces de noms, maintenant l'ordre relatif au sein de chaque espace de noms. Il est RECOMMANDÉ que le même ordre soit utilisé à travers un domaine administratif. Cependant, il n'est pas exigé qu'un tel ordre soit le même sur tous les domaines administratifs.

## 8.2 Exemples de rangements valides

Voici un ensemble d'exemples d'un acteur RP qui prend en charge deux espaces de noms, foo et bar. Les valeurs de priorité de Foo sont 3 (la plus forte) puis 2, et enfin 1 (la plus faible) et les valeurs de priorité de bar sont C (la plus forte) puis B, et enfin A (la plus faible).

Voici cinq listes d'ordres de priorité acceptables que peut utiliser l'élément SIP :

```
Foo.3      Foo.3      Bar.C    (plus haute priorité)
Foo.2      Bar.C      Foo.3
Foo.1  ou  Foo.2  ou  Foo.2
Bar.C      Bar.B      Foo.1
Bar.B      Foo.1      Bar.B
Bar.A      Bar.A      Bar.A    (plus faible priorité)
```

```
     Bar.C      (plus haute priorité)
     Foo.3  Bar.B   (tous deux traités avec égale priorité (FIFO))
ou   Foo.2  Bar.A   (tous deux traités avec égale priorité (FIFO))
     Foo.1      (plus faible priorité)
```

```
     Bar.C    (plus haute priorité)
     Foo.3
ou   Foo.2
     Foo.1    (plus faible priorité)
```

Dans le dernier exemple, Bar.A et Bar.B sont ignorés.

## 8.3 Exemples de rangements invalides

Sur la base de l'ordre de priorité des espaces de noms ci-dessus, les combinaisons suivantes sont des exemples d'ordres qui NE SONT PAS acceptables et NE DOIVENT PAS être configurables :

| **Exemple 1** | **Exemple 2** | **Exemple 3** | **Exemple 4** |
|---|---|---|---|
| Foo.3 | Foo.3 | Bar.C | Bar.C |
| Foo.2 | Bar.A | Foo.1 | Foo.1 Bar.B |
| Foo.1 ou | Foo.2 ou | Foo.3 ou | Foo.3 Bar.A |
| Bar.C | Bar.B | Foo.2 | Foo.2 |
| Bar.A | Foo.1 | Bar.A | |
| Bar.B | Bar.C | Bar.B | |

Ces exemples sont invalides car ils ne sont pas cohérents avec l'ordre interne des espaces de noms :

- dans l'exemple 1, Bar.A est de rang plus élevé que Bar.B,
- dans l'exemple 2, Bar.A est de rang plus élevé que Bar.B et Bar.C,
- dans l'exemple 3, Foo.1 est de rang plus élevé que Foo.2 et Foo.3,
- dans l'exemple 4, Foo.1 est de rang plus élevé que Foo.3 et Foo.2.

## 9. Enregistrement des espaces de noms

Les organisations qui envisagent l'utilisation du champ d'en-tête "Resource-Priority" devraient étudier si une combinaison existante d'espace de noms et de valeurs de priorité satisfait leurs besoins. Par exemple, les services de réponse aux situations d'urgence du monde entier discutent de l'utilisation de ce mécanisme pour le traitement préférentiel dans les futurs réseaux. Les juridictions DEVRAIENT tenter de réutiliser les espaces de noms existant enregistrés par l'IANA lorsque possible, car un des buts du présent document est de n'avoir pas des espaces de noms uniques par juridiction servant le même but, avec le même usage des niveaux de priorité. Cela va grandement augmenter l'interopérabilité et réduire les temps de développement, et probablement réduire la confusion à l'avenir si il y a un jour un besoin de transposer un espace de noms en un autre dans une fonction d'interopération.

On décrit ci-dessous les étapes nécessaires pour enregistrer un nouvel espace de noms.

Un nouvel espace de noms DOIT être défini dans une RFC sur la voie de la normalisation, suivant la politique "Action de normalisation" de la [RFC2434], et DOIT inclure les facettes suivantes :

- Il doit définir l'étiquette d'espace de noms, une unique étiquette d'espace de noms dans le registre IANA pour le champ d'en-tête SIP "Resource-Priority".
- Il doit énumérer les niveaux de priorité (c'est-à-dire, les valeurs de "r-priority") qu'utilise l'espace de noms. Noter que seules des listes finies sont permises, par exemple, pas d'entier ou de jeton sans contrainte.
- L'algorithme de priorité (paragraphe 4.5) qui identifie si l'espace de noms est à utiliser avec mise en file d'attente de priorité ("queue") ou préemption ("preemption"). Si la mise en file d'attente est utilisée, l'espace de noms PEUT indiquer si les demandes de priorité normale sont mises en file d'attente. Si il y a un nouvel "algorithme prévu" autre que préemption ou mise en file d'attente de priorité, l'algorithme doit être décrit, en prenant en compte tous les acteurs RP (UAC, UAS, mandataires).
- Un espace de noms peut soit faire référence à une liste de valeurs de priorité existante, soit définir une nouvelle liste finie de valeurs de priorité dans l'ordre de priorité relative pour l'enregistrement par l'IANA au sein du registre des paramètres des valeurs de priorité de la priorité de ressource SIP. De nouvelles valeurs de priorité NE DEVRAIENT PAS être ajoutées à une liste précédemment enregistrée par l'IANA associée à un espace de noms particulier, car cela peut causer des problèmes d'interopérabilité. Sauf spécification contraire, on suppose que toutes les valeurs de priorité confèrent une priorité supérieure à celle des demandes sans valeur de priorité.
- Tout nouveau code de réponse SIP unique pour ce nouvel espace de noms doit être expliqué et enregistré.
- Le document de référence doit spécifier et décrire tous nouveaux codes de champ d'en-tête d'avertissement (RFC 3261, paragraphe 27.2).
- Le document doit spécifier une nouvelle rangée dans le tableau suivant qui résume les caractéristiques de l'espace de noms et est inclus dans le registre IANA des espaces de noms de priorité de ressource :

| Espace de noms | Niveaux | Algorithme prévus | Code d'avertissement | Nouveau code de réponse | Référence |
|---|---|---|---|---|---|
| <étiquette> | <n ° des niveaux> | <préemption ou file d'attente> | <code d'avertissement> | <nouveau code> | <RFC> |

Si les informations sur les nouveaux codes de réponse, codes de rejet, ou comportement d'erreur sont omis, cela suppose que l'espace de noms ne définit pas de nouveau paramètre ou comportement.

## 10. Définitions des espaces de noms

### 10.1 Introduction

La présente spécification définit cinq espaces de noms uniques : DSN, DRSN, Q735, ETS, et WPS, constituant leur enregistrement auprès de l'IANA. Chaque enregistrement IANA contient les facettes définies à la Section 9. Pour les reconnaître, on étiquette les espaces de noms en majuscules, mais on notera que les noms d'espace de noms sont insensibles à la casse et sont généralement rendus en minuscules dans les demandes du protocole.

### 10.2 Espace de noms "DSN"

L'espace de noms DSN vient du nom d'un réseau du gouvernement américain nommé "Defense Switched Network".

L'espace de noms DSN a une liste finie de valeurs de priorité relatives, mentionnées ci-dessous de la plus faible à la plus forte priorité :

dsn.routine (plus faible)
dsn.priority
dsn.immediate
dsn.flash
dsn.flash-override (plus forte)

L'espace de noms DSN utilise l'algorithme de préemption (paragraphe 4.5.1).

### 10.3 Espace de noms "DRSN"

L'espace de noms DRSN vient du nom d'un réseau du gouvernement américain, appelé "Defense RED Switched Network".

L'espace de noms DRSN définit les valeurs de ressource suivantes, de la plus faible à la plus forte priorité :
drsn.routine (plus faible)
drsn.priority
drsn.immediate
drsn.flash
drsn.flash-override
drsn.flash-override-override (plus forte)

L'espace de noms DRSN utilise l'algorithme de préemption (paragraphe 4.5.1).

L'espace de noms DRSN diffère par un aspect algorithmique des espaces de noms DSN et Q735. Le comportement pour la valeur de priorité "flash-override-override" diffère des autres valeurs. Normalement, les demandes ne préemptent pas celles de priorité égale, mais une nouvelle demande "lash- override-override" arrivante va en déplacer une autre de priorité égale si les ressources sont insuffisantes. Ceci peut aussi être exprimé en disant que les demandes "flash-override-override" se défendent elles-mêmes comme seulement "flash-override".

### 10.4 Espace de noms "Q735"

Q.735.3 [Q.735.3] a été créé pour être une version commerciale de la spécification opérationnellement équivalente de DSN pour la préséance et la préemption multi niveaux (MLPP, *Multi-Level Precedence and Preemption*). L'espace de noms Q735 est défini ici de la même manière. L'espace de noms Q735 définit les valeurs de ressource suivantes,de la plus faible priorité à à la plus forte :
(plus faible)
q735.3
q735.2
q735.1
q735.0 (plus forte)

L'espace de noms Q735 opère conformément à l'algorithme de préemption (paragraphe 4.5.1).

### 10.5 Espace de noms "ETS"

L'espace de noms ETS tire indirectement son nom du service de télécommunications du gouvernement américain appelé "Service de télécommunications d'urgence du gouvernement" (GETS, *Government Emergency Telecommunications Service*) bien que l'organisation responsable du service GETS ait choisi l'acronyme "ETS" pour son service GETS sur IP, qui signifie "Service de Télécommunications d'urgence".

L'espace de noms ETS définit les valeurs de ressource suivantes, de la plus faible priorité à la plus forte :
ets.4 (plus faible)
ets.3
ets.2
ets.1
ets.0 (plus forte)

L'espace de noms ETS opère conformément à l'algorithme de mise en file d'attente de priorité (paragraphe 4.5.2).

### 10.6 Espace de noms "WPS"

L'espace de noms WPS tire son nom du service de priorité sans fil (Wireless Priority Service) défini dans le GSM et autres technologies sans fil. L'espace de noms WPS définit les valeurs de ressource suivantes, de la plus faible priorité à la plus forte :
wps.4 (plus faible)
wps.3
wps.2
wps.1
wps.0 (plus forte)

L'espace de noms WPS opère conformément à l'algorithme de mise en file d'attente de priorité (paragraphe 4.5.2).

## 11. Considérations sur la sécurité

### 11.1 Remarques générales

Tout mécanisme de priorité de ressource peut être trompé pour obtenir des ressources et donc dénier le service aux autres usagers. Un adversaire peut être capable de prendre le contrôle d'une passerelle RTPC particulière, causer de l'encombrement supplémentaire durant des urgences affectant le RTPC, ou dénier le service aux utilisateurs légitimes. Dans les systèmes d'extrémité SIP, tels que les téléphones IP, ce mécanisme pourrait terminer de façon inappropriée les sessions et appels existants.

Donc, alors que l'indication elle-même n'a pas à fournir une authentification séparée, les demandes SIP qui contiennent cet en-tête vont très probablement avoir des exigences d'authentification plus fortes que celles qui ne le contiennent pas.

Ces exigences d'authentification et d'autorisation s'étendent aux utilisateurs au sein du domaine administratif, car l'interconnexion ultérieure avec d'autres domaines administratifs peut invalider des hypothèses antérieures sur le niveau de confiance à accorder à l'usager.

On décrit ci-dessous les aspects d'authentification et d'autorisation, les exigences de confidentialité et de protection de la vie privée, la protection contre les attaques de déni de service, et les exigences d'anonymat. Naturellement, la discussion générale de la [RFC3261] s'applique.

Tous les agents d'utilisateur et serveurs mandataires qui prennent en charge la présente extension DOIVENT mettre en œuvre SIP sur TLS [RFC3546], le schéma d'URI 'sips' comme décrit au paragraphe 26.2 de la RFC 3261, et l'authentification par résumé [RFC2617] comme décrite à la Section 22 de la RFC 3261. De plus, les agents d'utilisateur qui prennent en charge la présente extension DEVRAIENT aussi mettre en œuvre S/MIME [RFC3851] comme décrit à la Section 23 de la RFC 3261 pour permettre la signature et la vérification de signature sur les demandes qui utilisent cette extension.

### 11.2 Authentification et autorisation

L'accès prioritaire au ressources de réseau et de système d'extrémité impose des exigences particulièrement strictes en matière de mécanismes d'authentification et d'autorisation, car l'accès prioritaire à des ressources peut impacter la stabilité et les performances globales du système et pas seulement juste le vol de, par exemple, un seul appel téléphonique.

Dans certaines conditions d'urgence, l'infrastructure du réseau, incluant ses mécanismes d'authentification et d'autorisation, peut être soumise à des attaques.

Étant donnée l'urgence durant des événement d'urgence, la détection statistique normale de fraude peut être moins efficace, plaçant donc un accent particulier sur une authentification fiable.

Les exigences courantes pour les mécanismes d'authentification s'appliquent, comme la résistance aux attaques en répétition, en copié-collé, et en dégradation.

L'authentification PEUT être fondée sur SIP ou utiliser d'autres mécanismes. L'utilisation de l'authentification par résumé et/ou S/MIME est RECOMMANDÉE pour l'authentification des UAS. L'authentification par résumé exige que les parties partagent un secret, limitant donc son utilisation à travers les domaines administratifs. Les systèmes SIP qui emploient la priorité de ressource DEVRAIENT mettre en œuvre S/MIME au moins pour l'intégrité, comme décrit à la Section 23 de la

[RFC3261]. Cependant, dans certains environnements, la réception d'une identité certifiée [RFC3325] à partir d'une entité de confiance peut être une autorisation suffisante. La Section 5 décrit une authentification par un tiers.

L'autorisation fondée sur les traits [RFC4484] "entraîne une assertion par un service d'autorisation des attributs associés à une identité" et peut être appropriée pour cette application. Avec l'autorisation fondée sur les traits, un élément de réseau peut directement déterminer, en inspectant le certificat, qu'une demande est autorisée à obtenir un type particulier de service, sans avoir à consulter un mécanisme de transposition qui convertit les identités d'utilisateur en autorisations.

L'autorisation peut se fonder sur des facteurs différents de l'identité de l'appelant, comme la destination demandée. Les espaces de noms PEUVENT aussi imposer des considérations particulières d'authentification ou d'autorisation qui sont plus strictes que les éléments de base décrits ici.

### 11.3 Confidentialité et intégrité

Les appels qui utilisent des niveaux élevés de priorité de ressource fournis par le champ d'en-tête "Resource-Priority" vont probablement être sensibles et avoir souvent besoin d'être protégés contre l'interception et l'altération. En particulier,les exigences de protection de la confidentialité des relations de communication peuvent être supérieures à celles pour les services commerciaux normaux. Pour SIP, les champs d'en-tête 'To', 'From', 'Organization', et 'Subject' sont des exemples d'informations particulièrement sensibles. Les systèmes DOIVENT mettre en œuvre le chiffrement au niveau transport en utilisant TLS et PEUVENT mettre en œuvre d'autres mécanismes de sécurité au niveau de la couche transport ou réseau. Les UAC DEVRAIENT utiliser l'URI "sips" pour demander une association de transport sûr à la destination.

Le champ d'en-tête "Resource-Priority" peut être porté dans l'en-tête de message SIP ou peut être encapsulé dans un fragment de message porté dans le corps de message SIP [RFC3420]. Pour être considérée comme une authentification valide pour les besoins de la présente spécification, les messages ou fragments SIP signés S/MIME DOIVENT contenir, au minimum, les champs d'en-tête Date, To, From, Call-ID, et Resource-Priority. L'encapsulation dans les parties de corps S/MIME permet à l'utilisateur de protéger ces champs d'en-tête contre l'inspection ou la modification par les mandataires. Cependant, dans de nombreux cas, les mandataires vont avoir besoin d'authentifier et autoriser la demande, de sorte que l'encapsulation va être indésirable.

La suppression d'un champ d'en-tête "Resource-Priority" ou la dégradation de sa valeur de priorité n'offre pas d'opportunités supplémentaires à un adversaire, car cette attaque par interposition pourrait simplement éliminer ou autrement invalider la demande SIP et donc empêcher la réalisation de l'appel.

Seuls les éléments SIP au sein du même domaine administratif de confiance qui emploient un canal sûr entre leurs éléments SIP vont faire confiance à un champ d'en-tête "Resource-Priority" qui n'est pas signé de façon appropriée. D'autres vont avoir besoin d'authentifier la demande indépendamment. Donc, l'insertion d'un champ d'en-tête "Resource-Priority" ou l'augmentation de la valeur de priorité n'a pas d'autre implication pour la sécurité que de causer l'échec d'une demande (voir la discussion du paragraphe précédent).

### 11.4 Anonymat

Certains usagers peuvent souhaiter rester anonymes pour la destination de la demande. L'anonymat pour les demandes avec priorité de ressource n'est pas différent de ce qui est fait pour toute autre demande SIP authentifiée. Pour les raisons notées plus haut, les usagers doivent s'authentifier à l'égard des éléments SIP qui portent la demande lorsque ils désirent le traitement de priorité de ressource. L'authentification peut se fonder sur les capacités et les noms, pas nécessairement leur état civil. En clair, ils peuvent rester anonymes à l'égard de la destination de la demande, en utilisant l'identité assurée par le réseau et le mécanisme général de confidentialité décrit dans la [RFC3323].

### 11.5 Attaques de déni de service

Comme on l'a noté, les systèmes décrits ici vont probablement être soumis à des attaques délibérées de déni de service (DoS) durant certains types d'urgences. Les attaques de DoS peut être lancées sur le réseau lui-même ainsi que sur son mécanisme d'authentification et d'autorisation. Comme on l'a noté, les systèmes devraient minimiser la quantité d'état, de calcul, et de ressources de réseau qu'un utilisateur non autorisé peut commander. Le système ne doit pas amplifier les attaques en causant la transmission de plus d'un paquet à une adresse réseau dont l'accessibilité n'a pas été vérifiée.

## 12. Considérations relatives à l'IANA

### 12.1 Introduction

Cette Section définit deux nouveaux en-têtes SIP (paragraphe 12.2), une étiquette d'option SIP (paragraphe 12.3), un nouveau code d'erreur 4xx (paragraphe 12.4), un nouveau registre au sein de la section paramètres SIP de l'IANA pour les espaces de noms "Resource-Priority" (paragraphe 12.5), et un nouveau registre au sein de la section paramètres SIP de l'IANA pour les priorités de ressource et les valeurs de priorité (paragraphe 12.6).

Des espaces de noms et valeurs de priorité supplémentaires DOIVENT être enregistrés auprès de l'IANA, comme décrit à la Section 9.

Le processus de changement de SIP [RFC3427] établit une politique pour l'enregistrement de nouveaux en-têtes d'extension SIP. Les espaces de noms de priorité de ressource et les valeurs de priorité ont des exigences d'interopérabilité similaires à celles des en-têtes d'extension SIP. Par conséquent, l'enregistrement de nouveaux espaces de noms de priorité de ressource et de valeurs de priorité exige la documentation dans une RFC en utilisant le processus d'approbation d'en-tête d'extension spécifié dans la RFC 3427.

Les politiques d'enregistrement des nouveaux espaces de noms sont définies à la Section 9.

### 12.2 Enregistrement par l'IANA des champs d'en-tête "Resource-Priority" et "Accept-Resource-Priority"

L'enregistrement pour le champ d'en-tête "Resource-Priority" est le suivant :
Numéro de RFC : 4412
Nom d'en-tête : 'Resource-Priority'
Forme compacte : aucune

L'enregistrement pour le champ d'en-tête "Accept-Resource-Priority" est le suivant :
Numéro de RFC : 4412
Nom d'en-tête : Accept-Resource-Priority
Forme compacte : aucune

### 12.3 Enregistrement par l'IANA de l'étiquette d'option de priorité de ressource

Numéro de RFC : 4412
Nom de l'étiquette d'option : "resource-priority"
Description : Indique ou demande de prendre en charge le mécanisme de priorité de ressource.

### 12.4 Enregistrement par l'IANA du code de réponse 417

Numéro de RFC : 4412
Code de réponse : 417
Phrase de raison par défaut : Priorité de ressource inconnue

### 12.5 Enregistrement par l'IANA de l'espace de noms "Resource-Priority"

Un nouveau registre ("espaces de noms "Resource-Priority"") dans la section Paramètres SIP de l'IANA a été créé, prenant une forme similaire au tableau ci-dessous :

| Espaces de noms | Niveaux | Algorithmes prévus | N. codes d'avertmt | N. code de rép. | Référence |
|---|---|---|---|---|---|
| dsn | 5 | préemption | non | non | [RFC4412] |
| drsn | 6 | préemption | non | non | [RFC4412] |
| q735 | 5 | préemption | non | non | [RFC4412] |
| ets | 5 | file d'attente | non | non | [RFC4412] |
| wps | 5 | file d'attente | non | non | [RFC4412] |

Légende :
Espace de noms : chaîne unique identifiant l'espace de noms.
Niveaux : nombre de valeurs de priorité au sein de l'espace de noms.
Algorithmes prévus : comportement opérationnel des éléments SIP qui mettent en œuvre cet espace de noms.

Nouveaux codes d'avertissement : ceux introduits par cet espace de noms.
Nouveaux codes de réponse ; nouveaux codes de réponse SIP introduits par cet espace de noms.
Référence : document de référence de l'IETF pour cet espace de noms.

### 12.6 Enregistrement par l'IANA des valeurs de priorité

Un nouveau registre ("Valeurs de priorité de "Resource-Priority") dans la section Paramètres SIP de l'IANA a été créé, prenant une forme similaire au tableau ci-dessous :

Espace de noms : drsn
Référence : RFC 4412
Valeurs de priorité (de la moindre à la plus grande) : "routine", "priority", "immediate", "flash", "flash-override", "flash-override-override"

Espace de noms : dsn
Référence : RFC 4412
Valeurs de priorité (de la moindre à la plus grande) : "routine", "priority", "immediate", "flash", "flash-override"

Espace de noms : q735
Référence : RFC 4412
Valeurs de priorité (de la moindre à la plus grande) : "4", "3", "2", "1", "0"

Espace de noms : ets
Référence : RFC 4412
Valeurs de priorité (de la moindre à la plus grande) : "4", "3", "2", "1", "0"

Espace de noms : wps
Référence : RFC 4412
Valeurs de priorité (de la moindre à la plus grande) : "4", "3", "2", "1", "0"

## 13. Remerciements

Merci à Ben Campbell, Ken Carlberg, Paul Kyzivat, Rohan Mahy, Allison Mankin, Xavier Marjou, Piers O'Hanlon, Mike Pierce, Samir Srivastava, et Dale Worley qui ont fourni d'utiles commentaires.
Les efforts de Dean Willis ont été d'un grand secours.
Martin Dolly, An Nguyen, et Niranjan Sandesara ont aidé pour les espaces de noms ETS et WPS.
Janet Gunn a aidé à améliorer le texte sur la priorité fondée sur la mise en file d'attente.

## 14. Références

### 14.1 Références normatives

[I.255.3] Union Internationale des Télécommunications, Recommandation I.255.3, "Réseau numérique à intégration de services (RNIS) - Structure générale et capacités de service - Préséance et préemption multi niveaux", juillet 1990.

[Q.735.3] Union Internationale des Télécommunications, Recommandation Q.735.3, "Description d'étape 3 pour les services supplémentaires de communauté d'intérêt utilant le système de signalisation n° 7 : préséance et préemption multi niveaux", mars 1993.

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

[RFC2434] T. Narten et H. Alvestrand, "Lignes directrices pour la rédaction d'une section Considérations relatives à l'IANA dans les RFC", BCP 26, octobre 1998. *(Rendue obsolète par la* RFC5226)

[RFC3261] J. Rosenberg et autres, "SIP : Protocole d'initialisation de session", juin 2002. (*Mise à jour par* 3265, 3853, 4320, 4916, 5393, 6665, 8217, 8760)

[RFC3262] J. Rosenberg et H. Schulzrinne, "Fiabilité des réponses provisoires dans le protocole d'initialisation de session (SIP)", juin 2002. *(P.S.)*

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

[RFC3311] J. Rosenberg, "Méthode UPDATE du protocole d'initialisation de session (SIP) ", octobre 2002.

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

[RFC3428] B. Campbell et autres, "Extension de messagerie instantanée pour le protocole d'initialisation de session (SIP) ", décembre 2002.

[RFC4411] J. Polk, "Extension de l'en-tête Reason pour les événements de préemption du protocole d'initialisation de session (SIP)", février 2006. *(P.S.)*

### 14.2 Références pour information

[RFC2617] J. Franks et autres, "Authentification HTTP : Authentification d'accès de base et par résumé", RFC 2617, juin 1999. *(DS.)*

[RFC2976] S. Donovan, "Méthode INFO pour SIP", octobre 2000. *(P.S., Remplacée par la* RFC6086)

[RFC3323] J. Peterson, "Mécanisme de confidentialité pour le protocole d'initialisation de session (SIP)", nov. 2002.

[RFC3325] C. Jennings, J. Peterson et M. Watson, "Extensions privées au protocole d'initialisation de session (SIP) pour l'assertion d'identité au sein de réseaux de confiance", novembre 2002. *(Information ; ; MàJ par* RFC8217)

[RFC3427] A. Mankin et autres, "Processus des changements au protocole d'initialisation de session (SIP)", BCP 67, décembre 2002. *(Remplacée par* RFC5727)

[RFC3487] H. Schulzrinne, "Exigences pour les mécanismes de priorité de ressource pour le protocole d'initialisation de session (SIP)", février 2003. *(Information)*

[RFC3515] R. Sparks, "Méthode Refer du protocole d'initialisation de session (SIP)", avril 2003. *(MàJ par* RFC8217)

[RFC3546] S. Blake-Wilson et autres, "Extensions à la sécurité de la couche Transport (TLS) ", juin 2003. *(Obsolète, voir* RFC4366)

[RFC3550] H. Schulzrinne, S. Casner, R. Frederick et V. Jacobson, "RTP : un protocole de transport pour les applications en temps réel", STD 64, juillet 2003. *(MàJ par* RFC7164, RFC7160, RFC8083, RFC8108)

[RFC3665] A. Johnston, S. Donovan, R. Sparks, C. Cunningham et K. Summers, "Exemples de flux d'appel de base du protocole d'initialisation de session (SIP)", BCP 75, décembre 2003.

[RFC3851] B. Ramsdell, "Spécification du message d'extensions de messagerie Internet multi-objets/sécurisé (S/MIME) version 3.1", juillet 2004. *(Obsolète, voir* RFC5751)

[RFC3893] J. Peterson, "Format de corps d'identité authentifiée (AIB) du protocole d'initialisation de session (SIP)", septembre 2004.

[RFC3903] A. Niemi, "Extension au protocole d'initialisation de session (SIP) pour la publication d'état d'événement", octobre 2004.

[RFC4484] J. Peterson, J. Polk, D. Sicker et H. Tschofenig, "Exigences d'autorisation fondées sur Trait pour le protocole d'initialisation de session (SIP)", août 2006. *(Information)*

## Adresse des auteurs

Henning Schulzrinne
Columbia University
Department of Computer Science
450 Computer Science Building
New York, NY 10027
US
téléphone : +1 212 939 7004
mél : hgs@cs.columbia.edu
URI : http://www.cs.columbia.edu

James Polk
Cisco Systems
2200 East President George Bush Turnpike
Richardson, TX 75082
US
mél : jmpolk@cisco.com

## Déclaration complète de droits de reproduction



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