Groupe de travail Réseau
Request for Comments : 2474
RFC rendues obsolètes : 1455, 1349
Catégorie : En cours de normalisation
Traduction Claude Brière de L'Isle

K. Nichols, Cisco Systems
S. Blake, Torrent Networking Technologies
F. Baker, Cisco Systems
D. Black, EMC Corporation
décembre 1998

Définition du champ Services différenciés (DS) dans les en-têtes IPv4 et IPv6

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

Résumé

Les améliorations de services différenciés au protocole Internet sont destinées à permettre une discrimination de service mesurable dans l'Internet sans qu'il soit besoin de l'état flux par flux et de la signalisation à chaque bond. Divers services peuvent être construits à partir d'un petit ensemble de blocs de construction bien définis qui sont déployés dans les nœuds du réseau. Les services peuvent être de bout en bout ou intra domaine ; ils incluent à la fois ceux qui peuvent satisfaire à des exigences de performances quantitatives (par exemple, la bande passante de crête) et ceux qui se fondent sur la performance relative (par exemple, la différenciation de "classe"). Les services peuvent être construits par une combinaison de :
- réglage de bits dans un champ d'en-tête IP aux frontières du réseau (frontières de systèmes autonomes, frontières administratives internes, ou hôtes),
- utilisation de ces bits pour déterminer comment sont transmis les paquets par les nœuds à l'intérieur du réseau, et
- conditionnement des paquets marqués aux frontières du réseau conformément aux exigences ou règles de chaque service.

Les exigences ou règles de chaque service doivent être établies au moyen de mécanismes de politique administrative qui sortent du domaine d'application du présent document. Un nœud de réseau conforme aux services différenciés comporte un classeur qui sélectionne les paquets sur la base de la valeur du champ DS, ainsi qu'un mécanisme de gestion de mémoire tampon et de programmation des paquets capable de délivrer le traitement spécifique de transmission du paquet indiqué par la valeur du champ DS. Le réglage du champ DS et le conditionnement du comportement dans le temps des paquets marqués a seulement besoin d'être effectué aux frontières du réseau et sa complexité peut varier.

Le présent document définit le champ d'en-tête IP, appelé le champ DS *(differentiated services)*. Dans IPv4, il définit la disposition de l'octet TOS *(type de service)* ; dans IPv6, de l'octet de classe de trafic. De plus, est défini un ensemble de base de traitements de transmission de paquet, ou de comportements par bond.

Pour une compréhension complète des services différenciés, voir aussi l'architecture des services différenciés [ARCH].

Table des matières

Définition du champ Services différenciés (DS) dans les en-têtes IPv4 et IPv6.....1
1. Introduction.....2
2. Terminologie utilisée dans le document.....3
3. Définition du champ Services différenciés.....4
4. Définitions historiques du codet et exigences de PHB.....5
4.1 PHB par défaut.....5
4.2 Utilisation passée et future du champ de préséance IP.....6
4.2.1 Brève histoire et évolution de Préséance IP.....6
4.2.2 Englobement de Préséance IP dans les codets de sélecteur de classe.....6

4.3 Résumé....7
5. Lignes directrices de normalisation du comportement bond par bond....8
6. Considérations relatives à l'IANA....8
7. Considérations sur la sécurité....9
7.1 Vol et déni de service....9
7.2 IPsec et interactions de tunnelage....9
8. Remerciements....10
9. Références....10

1. Introduction

Les services différenciés sont destinés à fournir un cadre de travail et des blocs de construction pour permettre la mise en place d'une discrimination mesurable des services dans l'Internet. L'approche des services différenciés vise à accélérer le développement en séparant l'architecture en deux composants majeurs, l'un d'eux qui est très bien compris et l'autre qui commence tout juste à être compris. En cela, nous sommes guidés par le concept original de l'Internet lorsque la décision a été prise de séparer les composants de transmission et d'acheminement. La transmission de paquet est la tâche relativement simple qui doit être effectuée aussi vite que possible paquet par paquet. La transmission utilise l'en-tête de paquet pour trouver une entrée dans un tableau d'acheminement qui détermine l'interface de sortie du paquet. L'acheminement établit les entrées dans ce tableau et peut avoir besoin de refléter une gamme de politiques de transit et autres ainsi que de garder la trace des défaillances de l'acheminement. Les tableaux d'acheminement sont maintenus par un sous produit des tâches de transmission. De plus, l'acheminement est la tâche la plus complexe et il n'a pas cessé d'évoluer ces vingt dernières années.

De façon analogue, l'architecture des services différenciés contient deux composants principaux. L'un est le comportement très bien compris dans le chemin de transmission, et l'autre est le composant plus complexe et toujours évolutif de l'allocation et de la politique sous-jacente qui configure les paramètres utilisés dans le chemin de transmission. Les comportements du chemin de transmission incluent le traitement différentiel et la réception des paquets individuels, tels que mis en œuvre par les disciplines de mise en file d'attente de service et/ou de gestion de file d'attente. Ces comportements au niveau du bond sont utiles et exigés dans les nœuds du réseau pour effectuer le traitement différencié des paquets indépendamment de la façon dont sont construits les services de bout en bout ou intra domaine. On se focalisera sur la sémantique générale du comportement plutôt que sur les mécanismes spécifiques utilisés pour les mettre en œuvre dans la mesure où ces comportements vont évoluer moins vite que le mécanisme.

Les comportements et mécanismes par bond à choisir paquet par paquet peuvent être développés aujourd'hui dans les nœuds de réseau et c'est l'aspect de l'architecture des services différenciés qui sera traité en premier. De plus, le chemin de transmission peut exiger qu'une certaine surveillance, régulation et mise en forme soient effectuées sur le trafic réseau conçu pour recevoir un traitement particulier afin de mettre en application les exigences associées à la délivrance de ce traitement particulier. Les mécanismes de cette sorte de conditionnement du trafic sont également très bien compris. Un large développement de tels conditionneurs de trafic est aussi important pour permettre la construction des services, bien que leur utilisation réelle dans la construction des services puisse évoluer avec le temps.

La configuration des éléments de réseau sur le point de savoir quels paquets reçoivent un traitement particulier et quelles sortes de règles appliquer à l'utilisation des ressources est beaucoup moins bien comprise. Néanmoins, il est possible de développer des services différenciés utiles dans les réseaux en utilisant des politiques simples et des configurations statiques. Comme décrit dans [ARCH], il y a un certain nombre de moyens pour conjuguer les comportements par bond et les conditionneurs de trafic pour créer des services. Dans le processus, une expérience supplémentaire est obtenue pour conduire des politiques et des allocations plus complexes. Les comportements de base du chemin de transmission peuvent rester les mêmes alors qu'évoluent les composants de l'architecture. Les expériences de la construction de tels services vont continuer pendant un certain temps, et donc la normalisation de cette construction est prématurée. De plus, beaucoup des détails de la construction des services sont couverts par des accords réglementaires entre différentes entités professionnelles et ceci est très loin des domaines d'intervention de l'IETF.

Le présent document se concentre sur les composants du chemin de transmission. Dans le chemin de transmission du paquet, les services différenciés sont réalisés par la transposition du codet contenu dans un champ de l'en-tête du paquet IP en un traitement de transmission particulier, ou comportement par bond (PHB, *per-hop behavior*), sur chaque nœud du réseau le long de ce chemin. Les codets peuvent être choisis parmi un ensemble de valeurs obligatoires définies plus loin dans le présent document, dans un ensemble de valeurs recommandées qui seront définies dans des documents à venir, ou qui peuvent avoir une signification purement locale. Il est prévu que les PHB soient mis en œuvre en utilisant une gamme de disciplines de file d'attente de services et/ou de gestion de file d'attente sur la file d'attente de l'interface de sortie d'un nœud de réseau : par exemple un service de file d'attente à pondération comparative (WRR, *weighted round-robin*) ou une

gestion de file d'attente à préférence d'extraction.

Le marquage est effectué par les conditionneurs de trafic aux frontières du réseau, y compris les bordures du réseau (routeur du premier bond ou hôte de source) et les frontières administratives. Les conditionneurs de trafic peuvent inclure les primitives du marquage, les mesures, la politique et le formatage (ces mécanismes sont décrits dans [ARCH]). Les services sont réalisés par l'utilisation d'une classification particulière des paquets et des mécanismes de conditionnement du trafic aux frontières couplés avec l'enchaînement des comportements par bond le long du chemin de transit du trafic. Un objectif de l'architecture des services différenciés est de spécifier ces blocs de construction en vue de l'extension future, aussi bien du nombre et du type des blocs de construction que des services construits à partir d'eux.

La terminologie utilisée dans le présent mémoire est définie à la Section 2. La définition du champ des services différenciés (champ DS) est donnée à la Section 3. Dans la Section 4, est exposé le désir d'une rétrocompatibilité partielle avec l'utilisation actuelle du champ de préséance IPv4. Comme solution, on introduit les PHB de codet de sélecteur de classe et de conformité au sélecteur de classe. La Section 5 présente des lignes directrices pour la normalisation du comportement par bond. La Section 6 expose les lignes directrices pour l'allocation des codets. La Section 7 traite les considérations pour la sécurité.

Le présent document est une brève description du champ DS et de ses utilisations. Il est destiné à être lu conjointement à l'architecture des services différenciés [ARCH].

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTAIF" dans le présent document sont à interpréter comme décrit dans la [RFC2119].

2. Terminologie utilisée dans le document

Agrégat de comportement : collection de paquets dont le même codet traverse une liaison dans une direction particulière. Les termes "agrégat" et "agrégat de comportement" sont utilisés de façon interchangeable dans le présent document.

Classeur : entité qui choisit les paquets sur la base du contenu des en-têtes de paquet selon des règles définies.

Codet de sélecteur de classe : un des huit codets dans la gamme ' xxx000' (où 'x' peut être égal à '0' ou '1'). Les codets de sélecteur de classe sont exposés au paragraphe 4.2.2.

PHB conforme au sélecteur de classe : comportement par bond satisfaisant aux exigences de PHB de sélecteur de classe du paragraphe 4.2.2.2.

Codet : valeur spécifique de la portion DSCP du champ DS. Les codets recommandés DEVRAIENT se transposer en PHB spécifiques, normalisés. Plusieurs codets PEUVENT se transposer en le même PHB.

Frontière de services différenciés : bordure d'un domaine DS, où les classeurs et les conditionneurs de trafic vont vraisemblablement être déployés. Une frontière de services différenciés peut être redivisée en nœuds d'entrée et de sortie, où les nœuds d'entrée/sortie sont les nœuds aval/amont d'une liaison frontière dans une direction de trafic donnée. Une frontière de service différencié se trouve normalement à l'entrée du routeur de premier bond (ou nœud de réseau) conforme aux services différenciés que traversent les paquets d'un hôte, ou à la sortie du routeur ou nœud de réseau conforme aux services différenciés du dernier bond que traversent les paquets avant d'arriver à un hôte. Ceci est parfois appelé la frontière d'un routeur d'extrémité. Une frontière de services différenciés peut être colocalisée avec un hôte, sous réserve de la politique locale. Aussi appelée frontière DS.

Conforme aux services différenciés : en conformité aux exigences spécifiées dans le présent document. Aussi appelé conforme DS.

Domaine des services différenciés : portion contiguë de l'Internet sur laquelle un ensemble cohérent de politiques de services différenciés est administré de façon coordonnée. Un domaine de services différenciés peut représenter des domaines administratifs ou systèmes autonomes différents, des régions de confiance différentes, des technologies de réseau différentes (par exemple, cellule/trame), des hôtes et des routeurs, etc. Aussi appelé domaine DS.

Champ de services différenciés : octet de TOS de l'en-tête IPv4 ou octet de classe de trafic de l'en-tête IPv6 lorsqu'il est interprété conformément à la définition donnée dans le présent document. Aussi appelé champ DS.

Mécanisme : mise en œuvre d'un ou plusieurs comportements par bond selon un algorithme particulier.

Microflux : une seule instance d'un flux de paquets d'application à application qui est identifiée par une adresse de source, une adresse de destination, un identifiant de protocole, un accès de source et un accès de destination (le cas échéant).

Comportement par bond (PHB, *Per-hop Behavior*) : description du traitement de transmission observable de l'extérieur appliqué dans un nœud conforme aux services différenciés à un agrégat de comportement. La description d'un PHB DEVRAIT être suffisamment détaillée pour permettre la construction de services prévisibles, comme exposé dans [ARCH].

Groupe de comportement par bond : ensemble d'un ou plusieurs PHB qui ne peuvent être spécifiés et mis en œuvre de façon significative que simultanément, du fait de contraintes communes s'appliquant à tous les PHB dans l'ensemble, tels qu'un service de file d'attente ou une politique de gestion de file d'attente. Aussi appelé groupe de PHB.

Conditionnement du trafic : fonctions de contrôle qui peuvent s'appliquer à un agrégat de comportement, à un flux d'application, ou à un autre sous-ensemble de trafic fonctionnellement utile, par exemple des mises à jour de l'acheminement. Cela PEUT inclure la mesure, la régulation, la mise en forme, et le marquage des paquets. Le conditionnement du trafic est utilisé pour mettre en application les accords entre les domaines et conditionner le trafic à recevoir un service différencié au sein d'un domaine en marquant les paquets avec les codets appropriés dans le champ DS et en surveillant et altérant les caractéristiques temporelles de l'agrégat si nécessaire. Voir [ARCH].

Conditionneur de trafic : entité qui effectue les fonctions de conditionnement du trafic et qui PEUT contenir des instruments de mesure, des régulateurs, des formateurs, et des marqueurs. Les conditionneurs de trafic sont normalement développés dans les nœuds frontières de DS (c'est-à-dire, pas dans les nœuds intérieurs d'un domaine DS).

Service : description du traitement global du trafic (ou d'un sous-ensemble du trafic) d'un consommateur à travers un domaine particulier, à travers un ensemble de domaines DS interconnectés, ou de bout en bout. Les descriptions de service sont couvertes par des politiques administratives et les services sont construits en appliquant le conditionnement de trafic pour créer des agrégats de comportement qui rencontrent un PHB connu à chaque nœud au sein du domaine DS. Plusieurs services peuvent être pris en charge par un seul comportement par bond utilisé de concert avec une gamme de conditionneurs de trafic.

Pour résumer, les classeurs et les conditionneurs de trafic sont utilisés pour choisir les paquets qui sont à ajouter aux agrégats de comportement. Les agrégats reçoivent un traitement différencié dans un domaine DS et les conditionneurs de trafic PEUVENT altérer les caractéristiques temporelles de l'agrégat pour se conformer à une exigence. Le champ DS d'un paquet est utilisé pour désigner l'agrégat de comportement du paquet et est utilisé ultérieurement pour déterminer le traitement de transmission que va recevoir le paquet. Un classeur d'agrégat de comportement qui peut choisir un PHB, par exemple une discipline de service de file d'attente de sortie différenciée, fondée sur le codet contenu dans le champ DS DEVRAIT être inclus dans tous les nœuds de réseau d'un domaine DS. Les classeurs et les conditionneurs de trafic aux frontières DS sont configurés conformément à une spécification de service, objet de politique administrative qui sort du domaine d'application du présent document.

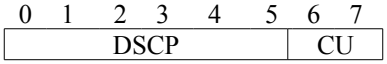
Des définitions de services différenciés supplémentaires sont données dans [ARCH].

3. Définition du champ Services différenciés

On définit un champ d'en-tête de remplacement, appelé le champ DS, qui est destiné à subroger les définitions existantes de l'octet TOS d'IPv4 [RFC791] et l'octet Classe de trafic d'IPv6 [IPv6].

Six bits du champ DS sont utilisés comme codet (DSCP) pour choisir le PHB qu'un paquet rencontre à chaque nœud. Un champ de deux bits actuellement inutilisé (CU) est réservé et sa définition et son interprétation sortent du domaine d'application du présent document. La valeur des bits CU est ignorée par les nœuds conformes aux services différenciés lors de la détermination du comportement par bond à appliquer à un paquet reçu.

La structure du champ DS est présentée ci-dessous :



DSCP : codet de services différenciés
CU ; non utilisé actuellement *(currently unused)*

Dans une notation de valeur DSCP 'xxxxxx' (où 'x' peut être égal à '0' ou '1') utilisée dans le présent document, le bit le plus

à gauche signifie le bit 0 du champ DS (comme indiqué ci-dessus), et le bit le plus à droite signifie le bit 5.

Les développeurs devraient noter que le champ DSCP fait six bits. Les nœuds conformes à DSCP DOIVENT choisir les PHB par confrontation sur la totalité du champ de 6 bits du DSCP, par exemple, en traitant la valeur du champ comme un tableau indexé utilisé pour choisir un mécanisme de traitement d'un paquet particulier qui a été mis en œuvre dans cet appareil. La valeur du champ CU DOIT être ignorée par le choix de PHB. Le champ DSCP est défini comme champ non structuré pour faciliter la définition de comportements par bond futurs.

À quelques exceptions près notées plus loin, la transposition des codets en PHB DOIT être configurable. Un nœud conforme à DS DOIT prendre en charge l'équivalent logique d'un tableau de transposition configurable des codets en PHB. Les spécifications de PHB DOIVENT inclure un codet par défaut recommandé, qui DOIT être unique pour les codets dans l'espace standard (voir à la Section 6). Les mises en œuvre devraient prendre en charge les transpositions recommandées de codet de PHB dans leur configuration par défaut. Les opérateurs peuvent choisir d'utiliser des codets différents pour un PHB, soit en plus, soit à la place de celui recommandé par défaut. Noter que si les opérateurs font ce choix, le re-marquage des champs DS peut être nécessaire aux frontières administratives même si les mêmes PHB sont mis en œuvre des deux côtés de la frontière. Voir dans [ARCH] des précisions sur le re-marquage.

Les exceptions à la configurabilité générale sont les codets 'xxx000' et sont notées aux paragraphes. 4.2.2 et 4.3.

Les paquets reçus avec un codet non reconnu DEVRAIENT être transmis comme s'ils étaient marqués du comportement par défaut (voir la Section 4), et leurs codets ne devraient pas être changés. De tels paquets NE DOIVENT PAS causer de disfonctionnement du nœud de réseau.

La structure du champ DS montré ci-dessus est incompatible avec la définition existante de l'octet TOS IPv4 dans la [RFC791]. La présomption est que les domaines DS se protègent par le re-marquage des nœuds de frontière, comme devraient le faire les réseaux qui utilisent les désignations de préséance de la RFC 791. La procédure de fonctionnement correcte DEVRAIT suivre la [RFC791], qui déclare : "Si l'utilisation réelle de ces désignations de préséance pose un problème à un réseau particulier, il est de la responsabilité de ce réseau de contrôler les accès et l'utilisation de ces désignations de préséance." Valider la valeur du champ DS aux frontières DS est sensé dans tous les cas car un nœud amont peut facilement le régler à une valeur arbitraire. Les domaines DS qui ne sont pas isolés par des nœuds frontière convenablement configurés peuvent fournir des services totalement imprévus.

Les nœuds PEUVENT réécrire le champ DS en tant que de besoin pour fournir un service local ou de bout en bout souhaité. Les spécifications des traductions du champ DS aux frontières DS font l'objet des accords de niveau de service entre les fournisseurs de services et les utilisateurs, et sont en dehors du domaine d'application du présent document. Les PHB normalisés permettent aux fournisseurs de services de construire leurs offres à partir d'un ensemble bien connu de traitements de transmission de paquets dont on peut s'attendre qu'ils soient présents dans les équipements de nombreux fabricants.

4. Définitions historiques du codet et exigences de PHB

Le champ DS aura une rétrocompatibilité limitée avec les pratiques actuelles, telles que décrites dans la présente section. La rétrocompatibilité est traitée de deux façons. D'abord, il y a des comportements par bonds qui sont déjà d'une utilisation très largement répandue (par exemple, ceux qui satisfont aux exigences de mise en file d'attente selon la préséance d'IPv4 spécifiées dans la [RFC1812]), et nous souhaitons permettre la poursuite de leur utilisation dans les nœuds conformes à DS. De plus, certains codets correspondent à une utilisation historique du champ Préséance IP et on réserve ces codets pour être transposés en des PHB qui satisfont aux exigences générales spécifiées au paragraphe 4.2.2.2, bien que les PHB de services différenciés spécifiques dont ces codets sont la transposition PUISSENT avoir des spécifications supplémentaires.

Il ne sera pas essayé de maintenir la rétrocompatibilité avec les bits de "DTR" ou de TOS de l'octet de type de service d'IPv4, défini dans la [RFC791].

4.1 PHB par défaut

Un PHB par "défaut" DOIT être disponible dans un nœud conforme DS. C'est le comportement courant de transmission au mieux disponible dans les routeurs existants normalisé par la [RFC1812]. Quand aucun autre accord n'est en place, on suppose que les paquets appartiennent à cet agrégat. De tels paquets PEUVENT être envoyés dans un réseau sans adhérer à des règles particulières et le réseau va livrer autant de ces paquets qu'il est possible et aussitôt que possible, sous réserve des autres contraintes de politique de ressources. Une mise en œuvre raisonnable de ce PHB serait une discipline de mise en file d'attente qui envoie les paquets de cet agrégat chaque fois que la liaison de sortie n'est pas prise pour satisfaire un

autre PHB. Une politique raisonnable pour la construction des services s'assurerait que l'agrégat n'était pas "affamé". Cela pourrait être mis en application par un mécanisme qui dans chaque nœud réserverait des ressources minimales (par exemple, de mémoire tampon, de bande passante) pour les agrégats de comportement par défaut. Cela permet à l'envoyeur qui n'est pas habilité aux services différenciés de continuer à utiliser le réseau de la même façon qu'aujourd'hui. L'impact de l'introduction des services différenciés dans un domaine sur les attentes de service de ses utilisateurs et homologues est une affaire complexe qui implique des décisions de politique de la part du domaine et sort du domaine d'application du présent document. Le codet RECOMMANDÉ pour le PHB par défaut est le schéma binaire ' 000000' ; la valeur '000000' DOIT être transposée en un PHB qui satisfait à ces spécifications. Le codet choisi pour le comportement par défaut est compatible avec la pratique existante [RFC791]. Lorsqu'un codet n'est pas transposé en un PHB normalisé ou d'utilisation locale, il DEVRAIT être transposé dans le PHB par défaut.

Un paquet marqué initialement pour le comportement par défaut PEUT être re-marqué avec un autre codet lorsqu'il passe une frontière de domaine DS, de telle sorte qu'il va être transmis en utilisant un PHB différent au sein de ce domaine, éventuellement soumis à un accord négocié entre les domaines homologues.

4.2 Utilisation passée et future du champ de préséance IP

On souhaite maintenir une certaine forme de rétrocompatibilité avec les utilisations actuelles du champ Préséance IP : les bits 0-2 de l'octet TOS IPv4. Il existe des routeurs qui utilisent le champ Préséance IP pour sélectionner différents traitement de transmission par bond d'une façon semblable à l'utilisation proposée ici pour le champ DSCP. Et donc, une architecture de simple prototype de services différenciés peut être rapidement déployée par une configuration appropriée de ces routeurs. De plus, les systèmes IP d'aujourd'hui comprennent la localisation du champ Préséance IP, et donc si ces bits sont utilisés de façon similaire à celle dont sont développés les équipements conformes à DS, des échecs significatifs ne devraient vraisemblablement pas se produire durant un développement précoce. En d'autres termes, la strict conformité à DS n'a pas besoin d'être totale, même au sein du réseau d'un seul fournisseur de services si les bits 0-2 du champ DSCP sont employés de façon similaire aux utilisations actuelles du champ Préséance IP, ou qui les englobe.

4.2.1 Brève histoire et évolution de Préséance IP

Le champ Préséance IP est en quelque sorte un précurseur du champ DS. Préséance IP, et le champ Préséance IP, ont été définis pour la première fois dans la [RFC791]. Les valeurs que peuvent prendre les trois bits du champ Préséance IP ont été allouées à diverses utilisations, qui incluent le trafic de contrôle du réseau, le trafic d'acheminement, et divers niveaux de privilège. Le moindre niveau de privilège était destiné au "trafic de routine". Dans la [RFC791], la notion de Préséance était vaguement défini comme "Une mesure indépendante de l'importance de ce datagramme." Toutes les valeurs du champ Préséance IP n'étaient pas supposées avoir une signification à travers les frontières, par exemple, "La désignation de la préséance du contrôle réseau est destinée à être utilisée seulement au sein d'un réseau. L'utilisation et le contrôle réels de cette désignation dépend de chaque réseau." [RFC791]

Bien que les premiers IMP BBN aient mis en œuvre le dispositif Préséance, les premiers routeurs commerciaux et le code de transmission IP d'UNIX ne le faisaient généralement pas. À mesure que les réseaux devenaient plus complexes et que croissaient les exigences des consommateurs, les fabricants de routeurs commerciaux ont développé des moyens de mettre en œuvre diverses sortes de services de mise en file d'attente qui incluaient une priorité de mise en file d'attente, qui était généralement fondée sur des politiques codées dans des filtres sur les routeurs, qui examinaient les adresses IP, les numéros de protocole IP, les accès TCP ou UDP, et d'autres champs d'en-tête. La Préséance IP était une des options que pouvaient examiner de tels filtres.

En bref, la Préséance IP est largement déployée et largement utilisée, même si ce n'est pas exactement de la manière prévue dans la [RFC791]. Cela a été reconnu dans la [RFC1122], qui déclare qu'alors que l'utilisation du champ Préséance IP est valide, l'allocation spécifique des priorités dans la [RFC791] a simplement un caractère historique.

4.2.2 Englobement de Préséance IP dans les codets de sélecteur de classe

Une spécification des traitements de transmission de paquet sélectionnés par le champ Préséance IP devrait aujourd'hui être assez générale ; probablement pas suffisamment spécifique pour construire des services prévisibles à partir du cadre de travail des services différenciés. Pour préserver une rétrocompatibilité partielle avec les utilisations actuelles connues du champ Préséance IP sans sacrifier la souplesse future, nous avons suivi l'approche de description des exigences minimales sur un ensemble de PHB qui sont compatibles avec la plupart des traitements de transmission installés sélectionnés par le champ Préséance IP. De plus, nous donnons un ensemble de codets qui DOIVENT se transposer en PHB en satisfaisant ces exigences minimales. Les PHB auxquels se transposent ces codets PEUVENT avoir une liste de spécifications plus détaillées en plus des celles qui sont déclarées exigées ici. D'autres codets PEUVENT se transposer en ces mêmes PHB. On désigne cet ensemble de codets comme codets de sélecteur de classe, et les exigences minimales pour les PHB auxquels ces

codets peuvent se transposer sont appelées exigences de PHB de sélecteur de classe.

4.2.2.1 Le codet Sélecteur de classe

Une spécification des traitements de transmission de paquet sélectionnés par les valeurs du champ DS de 'xxx000|xx', ou DSCP = 'xxx000' et du sous-champ CU non spécifié, est réservée comme ensemble des codets de sélecteur de classe. Les PHB auxquels se transposent ces codets DOIVENT satisfaire aux exigences de PHB de sélecteur de classe en plus de préserver les exigences du PHB par défaut sur le codet '000000' (paragraphe 4.1).

4.2.2.2 Exigences du PHB Sélecteur de classe

On se réfère à un codet de sélecteur de classe qui a une plus grande valeur numérique qu'un autre codet de sélecteur de calasse comme ayant un ordre relatif supérieur alors qu'un codet de sélecteur de classe avec plus petite valeur numérique que celle d'un autre codet de sélecteur de classe est dit avoir un ordre relatif inférieur. L'ensemble des PHB dans lequel se transposent les huit codets de sélecteur de classe DOIT donner au moins deux classes de transmission de trafic indépendantes, et les PHB choisis par un codet de sélecteur de classe DEVRAIENT donner aux paquets une probabilité de transmission à temps qui ne soit pas inférieure à celle données aux paquets marqués avec un codet de sélecteur de classe d'ordre relatif inférieur, dans des conditions de fonctionnement et de charge de trafic raisonnables. Un paquet éliminé est considéré comme un cas extrême de retard de transmission. De plus, les PHB sélectionnés par les codets '11x000' DOIVENT donner aux paquets un traitement préférentiel de transmission par comparaison avec le PHB sélectionné par le codet '000000' pour préserver l'usage courant des valeurs de Préséance IP '110' et '111' pour le trafic d'acheminement.

Ensuite, les PHB sélectionnés par des codets de sélecteur de classes distincts DEVRAIENT être transmis indépendamment ; c'est-à-dire que les paquets marqués par des codets de sélecteur de classe différents PEUVENT être réordonnés. Un nœud de réseau PEUT mettre en application des limites sur la quantité des ressources du nœud qui peuvent être utilisée par chacun de ces PHB.

Les groupes de PHB dont la spécification satisfait à ces exigences sont appelés des PHB conformes au sélecteur de classe.

Les exigences de PHB de sélecteur de classe sur le codet '000000' sont compatibles avec celles énumérées pour le PHB par défaut au paragraphe 4.1.

4.2.2.3 Utilisation des exigences du PHB Sélecteur de classe pour la compatibilité avec Préséance IP

Un nœud de réseau conforme à DS peut être développé avec un ensemble d'un ou plusieurs groupes de PHB conformes au sélecteur de classe. Le présent document établit que l'ensemble des codets 'xxx000' DOIT se transposer en un tel ensemble de PHB. Comme il est aussi possible de transposer plusieurs codets au même PHB, le fabricant ou l'administrateur de réseau PEUT configurer le nœud de réseau pour transposer les codets en PHB sans égard aux bits 3-5 du champ DSCP pour donner un réseau compatible avec l'utilisation historique de Préséance IP. Et donc, par exemple, le codet '011010' se transposerait en le même PHB que le codet '011000'.

4.2.2.4 Exemple de mécanismes de mise en œuvre de groupes de PHB conformes au sélecteur de classe

Les PHB conformes au sélecteur de classe peuvent être réalisés par divers mécanismes, incluant une mise en file d'attente à priorité stricte, une mise en file d'attente à pondération équitable (WFQ, *weighted fair queueing*), WRR, ou ses variantes [RPS, HPFQA, DRR], ou la mise en file d'attente fondée sur la classe (CBQ, *Class-Based Queuing*) [CBQ]. La distinction entre les PHB et les mécanismes est décrite en plus grand détail à la Section 5.

Il est important de noter que ces mécanismes pourraient être disponibles à travers d'autres PHB (normalisés ou non) qui sont disponibles dans l'équipement d'un fabricant particulier. Par exemple, des documents futurs pourront normaliser un groupe de PHB à mise en file d'attente selon la priorité stricte pour un ensemble de codets recommandé. Un administrateur de réseau pourrait configurer ces routeurs pour sélectionner les PHB de mise en file d'attente selon la priorité stricte avec les codets 'xxx000' conformément aux exigences du présent document.

Comme autre exemple, un autre vendeur pourrait employer un mécanisme CBQ dans ses routeurs. Le mécanisme CBQ pourrait être utilisé pour mettre en œuvre les PHB de mise en file d'attente selon la priorité stricte aussi bien qu'un ensemble de PHB conformes au sélecteur de classe avec une plus large gamme de dispositifs qui seraient disponibles dans un ensemble de PHB qui ne font rien de plus que satisfaire aux exigences minimales de PHB de sélecteur de classe.

4.3 Résumé

Le présent document définit les codets 'xxx000' comme codets de sélecteur de classe, et les PHB sélectionnés par ces codets DOIVENT satisfaire aux exigences de PHB de sélecteur de classe décrites au paragraphe 4.2.2.2. Ceci est fait pour préserver un niveau utile de rétrocompatibilité avec les utilisations actuelles du champ Préséance IP dans l'Internet sans limiter indûment la souplesse pour l'avenir. De plus, le codet '000000' est utilisé comme valeur de PHB par défaut pour

l'Internet et, comme telle, n'est pas configurable. Les sept codets de sélecteur de classe différents de zéro restants ne sont configurables que dans la mesure où ils se transposent en des PHB qui satisfont aux exigences du paragraphe 4.2.2.2.

5. Lignes directrices de normalisation du comportement bond par bond

Les caractéristiques du comportement d'un PHB sont à normaliser, et non les algorithmes ou les mécanismes particuliers utilisés pour les mettre en œuvre. Un nœud peut avoir un ensemble (éventuellement grand) de paramètres qui peuvent être utilisés pour contrôler comment les paquets sont programmés sur une interface de sortie (par exemple, N files d'attentes séparées avec des priorités, des longueurs de file d'attente, des pondérations round-robin, des algorithmes d'abandon, des pondérations et seuils de préférence d'abandon, etc. réglables). Pour illustrer la distinction entre un PHB et un mécanisme, on mentionnera que les PHB conformes au sélecteur de classe peuvent être mis en œuvre par plusieurs mécanismes, parmi lesquels : mise en file d'attente à priorité stricte, WFQ, WRR, ou leurs variantes [HPFQA, RPS, DRR], ou CBQ [CBQ], isolément ou en combinaison.

Les PHB peuvent être spécifiés individuellement, ou comme un groupe (un seul PHB est un cas particulier de groupe de PHB). Un groupe de PHB consiste normalement en un ensemble de deux PHB ou plus, qui ne peuvent être significativement spécifiés et mis en œuvre que simultanément, du fait de contraintes communes qui s'appliquent à chaque PHB du groupe, telle qu'une politique de service de mise en file d'attente ou de gestion de file d'attente. Une spécification de groupe de PHB DEVRAIT décrire les conditions dans lesquelles un paquet peut être re-marqué pour sélectionner un PHB au sein du groupe. Il est RECOMMANDÉ que les mises en œuvre de PHB n'introduisent pas de changement de l'ordre des paquets au sein d'un micro flux. Les spécifications de groupe de PHB DOIVENT identifier toutes les implications possibles de changement d'ordre des paquets qui pourraient survenir pour chaque PHB individuel, et qui pourraient survenir si différents paquets au sein d'un micro flux sont marqués pour des PHB différents au sein du groupe.

Seuls les comportements par bond qui ne sont pas décrits dans un PHB standard existant, et ont été mis en œuvre, déployés, et se sont révélés utilises DEVRAIENT être normalisés. Comme l'expérience actuelle des services différenciés est assez limitée, il est prématuré de faire des hypothèses sur la spécification exacte de ces comportements par bond.

Chaque PHB normalisé DOIT avoir un codet associé RECOMMANDÉ, alloué à partir d'un espace de 32 codets (voir la Section 6). La présente spécification a laissé de la place dans l'espace des codets pour permettre une évolution, et donc l'espace défini ('xxx000') est intentionnellement clairsemé.

Les fabricants d'équipements de réseau ou toute liberté pour offrir tous les paramètres et capacités qu'ils estiment utiles et vendables. Lorsqu'un PHB particulier, normalisé, est mis en œuvre dans un nœud, le fabricant PEUT utiliser l'algorithme de son choix qui satisfait à la définition du PHB conformément à la norme. Les capacités du nœud et sa configuration particulière déterminent les différentes façons dont les paquets peuvent être traités.

Les fournisseurs de services ne sont pas obligés d'utiliser les mêmes mécanismes ou configurations de nœud pour activer la différenciation de service au sein de leurs réseaux, et ils ont toute liberté pour configurer les paramètres des nœuds de la façon qui leur paraît appropriée pour leurs offres de service et leurs objectifs d'ingénierie du trafic. Avec le temps, certains comportements par bond communs vont vraisemblablement évoluer (c'est-à-dire, ceux qui sont particulièrement utiles pour la mise en œuvre des services de bout en bout) et ils POURRONT être associés à des codets de PHB EXP/LU particuliers dans le champ DS, permettant l'utilisation à travers les frontières de domaines (voir la Section 6). Ces PHB sont les candidats à la normalisation future.

Il est RECOMMANDÉ que les PHB normalisés soient spécifiés conformément aux lignes directrices établies dans [ARCH].

6. Considérations relatives à l'IANA

Le champ DSCP au sein du champ DS est capable de convoyer 64 codets distincts. L'espace des codets est divisé en trois groupes pour les besoins de l'allocation et la gestion des codets : un groupe de 32 codets RECOMMANDÉS (groupe 1) à allouer par action de normalisation comme défini dans [CONS], un groupe de 16 codets (groupe 2) à réserver pour utilisation expérimentale ou locale (EXP/LU) comme défini dans [CONS], et un groupe de 16 codets (groupe 3) qui sont au départ disponibles pour utilisation expérimentale ou locale, mais qui devraient de préférence être utilisés pour des allocations normalisées si le groupe 1 se trouvait épuisé. Les groupes sont définis dans le tableau suivant (où 'x' se réfère soit à '0' soit à '1') :

Groupe	Espace des codets	Politique d'allocation
1	xxxxx0	Action de normalisation
2	xxxx11	EXP/LU
3	xxxx01	EXP/LU (*)

(*) pourra être utilisé pour des allocations d'action de normalisation futures en tant que de besoin

Le présent document alloue huit codets RECOMMANDÉS ('xxx000') qui sont tirés du groupe 1 ci-dessus. Ces codets DOIVENT être transposés, non pas à des PHB spécifiques, mais aux PHB qui satisfont "au moins" aux exigences établies au paragraphe 4.2.2.2 pour fournir un niveau minimum de rétrocompatibilité avec la Préséance IP telle que définie dans la [RFC791] et comme utilisée dans certains équipements actuels.

7. Considérations sur la sécurité

La présente section considère les questions de sécurité soulevées par l'introduction des services différenciés, principalement les attaques potentielle de déni de service, et le vol de service potentiel qui s'y rattache par du trafic non autorisé (paragraphe 7.1). Le paragraphe 7.2 traite du fonctionnement des services différenciés en présence d'IPsec, y compris son interaction avec le mode tunnel IPsec et les autres protocoles de tunnelage. Voir dans [ARCH] un traitement plus extensif des problèmes de sécurité soulevés par l'architecture globale des services différenciés.

7.1 Vol et déni de service

Le but principal des services différenciés est de permettre que soient fournis différents niveaux de service pour les flux de trafic sur une infrastructure de réseau commune. Diverses techniques peuvent être utilisées pour l'atteindre, mais le résultat final sera que certains paquets reçoivent un service différent (par exemple, meilleur) que d'autres. L'application du trafic du réseau à des comportements spécifiques qui résultent en un service différent (par exemple, meilleur ou pire) est indiqué principalement par le codet DS, et donc un agresseur peut être capable d'obtenir un meilleur service en modifiant le codet pour des valeurs qui indiquent des comportements utilisés pour les services améliorés en injectant des paquets avec de telles valeurs de codets. Poussé à la limite, un tel vol de service devient une attaque de déni de service lorsque le trafic modifié ou injecté épuise les ressources disponibles pour le transmettre ainsi que les autres flux de trafic.

La défense contre cette classe d'attaques de vol et de déni de service consiste en la combinaison du conditionnement du trafic aux frontières du domaine DS avec la sécurité et l'intégrité de l'infrastructure réseau au sein d'un domaine DS. Les nœuds de frontière de domaine DS DOIVENT s'assurer que tout le trafic entrant dans le domaine est marqué avec les valeurs de codets appropriées au trafic et au domaine, à marquer à nouveau le trafic avec de nouvelles valeurs de codets si nécessaire. Ces nœuds frontière de DS sont la principale ligne de défense contre les attaques de vol et de déni de service fondées sur des codets modifiés, car le succès d'une telle attaque indique que les codets utilisés par le trafic attaquant étaient inappropriés. Une importante instance d'un nœud frontière est que tout nœud qui génère du trafic au sein d'un domaine DS est le nœud frontière initial pour ce trafic. Les nœuds intérieurs d'un domaine DS s'appuient sur les codets DS pour associer le trafic aux PHB de transmission, et NE SONT PAS OBLIGÉS de vérifier les valeurs des codets avant de les utiliser. Il en résulte que les nœuds intérieurs dépendent du fonctionnement correct des nœuds frontière du domaine DS pour empêcher l'arrivée de trafic avec des codets inappropriés ou un excès de niveaux approvisionnés qui interromprait le fonctionnement du domaine.

7.2 IPsec et interactions de tunnelage

Le protocole IPsec, tel que défini dans [ESP, AH], n'inclut pas le champ DS de l'en-tête IP dans ses calculs cryptographiques (dans le cas du mode tunnel, c'est le champ DS de l'en-tête IP sortant qui n'est pas inclus). Et donc la modification du champ DS par un nœud de réseau n'a pas d'effet sur la sécurité de bout en bout IPsec, parce qu'elle ne peut pas causer l'échec d'une vérification d'intégrité IPsec. Par conséquent, IPsec ne fournit aucune défense contre les modifications du champ DS par un adversaire (c'est-à-dire, une attaque par interposition), car la modification de l'adversaire n'aura pas d'effet sur la sécurité de bout en bout d'IPsec.

Le mode tunnel d'IPsec fournit la sécurité du champ DS de l'en-tête IP encapsulé. Un paquet IPsec en mode tunnel contient deux en-têtes IP : un en-tête externe fourni par le nœud d'entrée du tunnel et un en-tête interne encapsulé fourni par la source d'origine du paquet. Lorsque un tunnel IPsec est hébergé (en tout ou en partie) sur un réseau à services différenciés, les nœuds de réseau intermédiaires opèrent sur le champ DS de l'en-tête externe. Au nœud de sortie du tunnel, le traitement IPsec comporte le retrait de l'en-tête externe et la transmission du paquet (si c'est requis) en utilisant l'en-tête interne. Le

protocole IPsec EXIGE que le champ DS de l'en-tête interne ne soit pas changé par ce processus de décapsulation pour garantir que les modifications du champ DS ne puissent pas être utilisées pour lancer des attaque de vol ou déni de service à travers un point d'extrémité de tunnel IPsec. Le présent document n'apporte pas de changement à cette exigence. Si l'en-tête IP interne n'a pas été traité par un nœud frontière de DS pour le domaine DS du nœud de sortie du tunnel, le nœud de sortie du tunnel est le nœud frontière pour le trafic qui sort du tunnel, et donc il DOIT s'assurer que le trafic résultant a les codets DS appropriés.

Lorsque le traitement de décapsulation de sortie du tunnel IPsec comporte une vérification d'intégrité cryptographique suffisamment forte du paquet encapsulé (où "suffisamment" est déterminé par la politique de sécurité locale), le nœud de sortie du tunnel peut en toute sécurité supposer que le champ DS dans l'en-tête interne a la même valeur que celle qu'il avait au nœud d'entrée du tunnel. Une importante conséquence en est que des liaisons par ailleurs non sécurisées au sein d'un domaine DS peuvent être sécurisées par un tunnel IPsec suffisamment fort. Cette analyse et ses implications s'appliquent à tout protocole de tunnelage qui effectue des vérifications d'intégrité, mais le niveau d'assurance du champ DS de l'en-tête interne dépend de la force de la vérification d'intégrité effectuée par le protocole de tunnelage. En l'absence d'assurance suffisante sur un tunnel qui a pu transiter par des nœuds en dehors du domaine DS en cours (ou est vulnérable par ailleurs), le paquet encapsulé DOIT être traité comme si il arrivait à une frontière avec l'extérieur du domaine DS.

8. Remerciements

Les auteurs tiennent à remercier le groupe de travail services différenciés pour les discussions qui ont aidé à donner forme au présent document.

9. Références

[AH] S. Kent et R. Atkinson, "En-tête d'authentification IP", RFC 2402, novembre 1998. *(Rendue obsolète par les RFC 4302 et 4303)*

[ARCH] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang et W. Weiss, "Architecture pour services différenciés", RFC 2475, décembre 1998.

[CBQ] S. Floyd and V. Jacobson, "Link-sharing and Resource Management Models for Packet Networks", IEEE/ACM Transactions on Networking, Vol. 3 no. 4, pp. 365-386, août 1995.

[CONS] T. Narten et H. Alvestrand, "Lignes directrices pour la rédaction d'une section de considérations relatives à l'IANA dans les RFC", RFC 2434, octobre 1998. *(Rendue obsolète par la RFC 5226)*

[DRR] M. Shreedhar et G. Varghese, "Efficient Fair Queueing using Deficit Round Robin", Proc. ACM SIGCOMM 95, 1995.

[ESP] S. Kent et R. Atkinson, "Encapsulation de charge utile de sécurité IP (ESP)", RFC 2406, novembre 1998. *(Rendue obsolète par les RFC 4303 et 4835)*

[HPFQA] J. Bennett et Hui Zhang, "Hierarchical Packet Fair Queueing Algorithms", Proc. ACM SIGCOMM 96, août 1996.

[IPv6] S. Deering et R. Hinden, "Protocole Internet, spécification de la version 6 (IPv6)", RFC 2460, décembre 1998.

[RFC791] J. Postel, éditeur, "Protocole Internet", STD 5, RFC 791, septembre 1981.

[RFC1122] R. Braden, "Exigences pour les hôtes Internet – couches de communication", STD 3, RFC 1122, octobre 1989. *(Mise à jour par les RFC 2474, 3168, 3260 et 4379)*

[RFC1812] F. Baker, éditeur, "Exigences pour les routeurs d'IP version 4", RFC 1812, juin 1995. *(Mise à jour par la RFC 2644)*

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, RFC 2119, mars 1997.

[RPS] D. Stiliadis and A. Varma, "Rate-Proportional Servers: A Design Methodology for Fair Queueing Algorithms", IEEE/ ACM Trans. on Networking, avril 1998.

Adresse des auteurs

Kathleen Nichols
Cisco Systems
170 West Tasman Drive
San Jose, CA 95134-1706
Phone: +1-408-525-4857
EMail: kmn@cisco.com

Steven Blake
Torrent Networking Technologies
3000 Aerial Center, Suite 140
Morrisville, NC 27560
Phone: +1-919-468-8466 x232
EMail: slblake@torrentnet.com

Fred Baker
Cisco Systems
519 Lado Drive
Santa Barbara, CA 93111
Phone: +1-408-526-4257
EMail: fred@cisco.com

David L. Black
EMC Corporation
35 Parkwood Drive
Hopkinton, MA 01748
Phone: +1-508-435-1000 x76140
EMail: black_david@emc.com

Déclaration complète de droits de propriété intellectuelle