UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T Y.1291

(05/2004)

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

SÉRIE Y: INFRASTRUCTURE MONDIALE DE L'INFORMATION, PROTOCOLE INTERNET ET RÉSEAUX DE NOUVELLE GÉNÉRATION

Aspects relatifs au protocole Internet – Architecture, accès, capacités de réseau et gestion des ressources

Cadre architectural pour la prise en charge de la qualité de service dans les réseaux en mode paquet

Recommandation UIT-T Y.1291

RECOMMANDATIONS UIT-T DE LA SÉRIE Y

INFRASTRUCTURE MONDIALE DE L'INFORMATION, PROTOCOLE INTERNET ET RÉSEAUX DE NOUVELLE GÉNÉRATION

INFRASTRUCTURE MONDIALE DE L'INFORMATION	
Généralités	Y.100–Y.199
Services, applications et intergiciels	Y.200–Y.299
Aspects réseau	Y.300–Y.399
Interfaces et protocoles	Y.400–Y.499
Numérotage, adressage et dénomination	Y.500–Y.599
Gestion, exploitation et maintenance	Y.600–Y.699
Sécurité	Y.700–Y.799
Performances	Y.800–Y.899
ASPECTS RELATIFS AU PROTOCOLE INTERNET	
Généralités	Y.1000–Y.1099
Services et applications	Y.1100–Y.1199
Architecture, accès, capacités de réseau et gestion des ressources	**Y.1200–Y.1299**
Transport	Y.1300–Y.1399
Interfonctionnement	Y.1400–Y.1499
Qualité de service et performances de réseau	Y.1500–Y.1599
Signalisation	Y.1600–Y.1699
Gestion, exploitation et maintenance	Y.1700–Y.1799
Taxation	Y.1800–Y.1899
RÉSEAUX DE LA PROCHAINE GÉNÉRATION	
Cadre général et modèles architecturaux fonctionnels	Y.2000–Y.2099
Qualité de service et performances	Y.2100–Y.2199
Aspects relatifs aux services: capacités et architecture des services	Y.2200–Y.2249
Aspects relatifs aux services: interopérabilité des services et réseaux dans les réseaux de nouvelle génération	Y.2250–Y.2299
Numérotage, nommage et adressage	Y.2300–Y.2399
Gestion de réseau	Y.2400–Y.2499
Architectures et protocoles de commande de réseau	Y.2500–Y.2599
Sécurité	Y.2700–Y.2799
Mobilité généralisée	Y.2800–Y.2899

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T Y.1291

Cadre architectural pour la prise en charge de la qualité de service dans les réseaux en mode paquet

Résumé

La présente Recommandation définit un cadre architectural pour la prise en charge de la qualité de service dans les réseaux en mode paquet. Un cadre architectural repose essentiellement sur un ensemble de mécanismes de réseaux génériques (ou modules de qualité de service) qui régissent la réponse du réseau à une demande de service (le cas échéant propre à un élément de réseau) ou qui assurent la signalisation entre éléments de réseau, ou encore qui gèrent et contrôlent le trafic dans un réseau. Répartis dans trois plans logiques (à savoir le plan contrôle, le plan données et le plan gestion) les modules peuvent être utilisés conjointement de façon à offrir différentes solutions pour assurer l'effet global satisfaisant produit par la performance de différents services requis par un ensemble d'applications, tels que les services de transfert de données et de conférence multimédia.

Source

La Recommandation Y.1291 de l'UIT-T a été approuvée le 7 mai 2004 par la Commission d'études 13 (2001-2004) de l'UIT-T selon la procédure définie dans la Recommandation UIT-T A.8.

AVANT-PROPOS

L'UIT (Union internationale des télécommunications) est une institution spécialisée des Nations Unies dans le domaine des télécommunications. L'UIT-T (Secteur de la normalisation des télécommunications) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un Membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux responsables de la mise en œuvre de consulter la base de données des brevets du TSB.

TABLE DES MATIÈRES

		Page
1	Domaine d'application	1
2	Références normatives	1
3	Définitions	2
4	Abréviations et acronymes	2
5	Introduction	3
6	Modules de qualité de service	4
7	Mécanismes du plan contrôle	5
7.1	Contrôle d'admission	5
7.2	Routage en fonction de la qualité de service	5
7.3	Réservation de ressources	7
8	Mécanismes du plan données	7
8.1	Gestion de la mise en file d'attente (ou en mémoire tampon)	7
8.2	Mécanisme de prévention des encombrements	8
8.3	Mécanisme de mise en file d'attente et de programmation	9
8.4	Mécanisme de marquage des paquets	10
8.5	Mécanisme de classification du trafic	10
8.6	Mécanisme d'organisation du trafic	10
8.7	Mécanisme de formage du trafic	10
9	Mécanismes du plan gestion	11
9.1	Accord sur les niveaux de service	11
9.2	Mesure et enregistrement du trafic	11
9.3	Mécanisme de rétablissement du trafic	11
9.4	Politiques	12
10	Interactions entre les modules	12
10.1	Signalisation de la qualité de service	13
10.2	Mécanismes intraplans	14
10.3	Mécanisme interplans	14
11	Considérations de sécurité	15
11.1	Plan données	15
11.2	Plan gestion et plan contrôle	15
11.3	Signalisation de la qualité de service	15
12	Approches types	16
12.1	IntServ	16
12.2	DiffServ	16
12.3	MPLS	17
12.4	Qualité de service dynamique IPCablecom	17

Page

Annexe A – Niveaux de priorité du trafic 18

Appendice I – Approche globale de qualité de service basée sur un contrôle indépendant des ressources 20

I.1 Souplesse d'implémentation des réseaux par paquets avec prise en charge de la commutation MPLS 21

I.2 Souplesse d'implémentation des réseaux par paquets sans prise en charge de la commutation MPLS 22

I.3 Souplesse d'implémentation en cas de contrôle de ressources réparties 22

Appendice II – Système de renforcement des priorités 23

BIBLIOGRAPHIE 24

Recommandation UIT-T Y.1291

Cadre architectural pour la prise en charge de la qualité de service dans les réseaux en mode paquet

1 Domaine d'application

La présente Recommandation définit un cadre architectural pour la prise en charge de la qualité de service dans les réseaux en mode paquet. Un cadre architectural repose essentiellement sur une série de modules de qualité de service répartis dans trois plans logiques (à savoir le plan contrôle, le plan données et le plan gestion) de manière à contrôler la performance du réseau, même dans l'hypothèse d'un conflit de ressources. En définitive les modules doivent contribuer à obtenir "l'effet global produit par la performance d'un service qui détermine le degré de satisfaction de l'usager (du service)".

2 Références normatives

La présente Recommandation se réfère à certaines dispositions des Recommandations UIT-T et textes suivants qui, de ce fait, en sont partie intégrante. Les versions indiquées étaient en vigueur au moment de la publication de la présente Recommandation. Toute Recommandation ou tout texte étant sujet à révision, les utilisateurs de la présente Recommandation sont invités à se reporter, si possible, aux versions les plus récentes des références normatives suivantes. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut d'une Recommandation:

– Recommandation UIT-T E.360.1 (2002), *Routage en fonction de la qualité de service et méthodes associées d'ingénierie du trafic pour les réseaux multiservice IP, ATM et TDM – Cadre général*.

– Recommandation UIT-T E.360.2 (2002), *Routage en fonction de la qualité de service et méthodes associées d'ingénierie du trafic – Méthodes de routage d'appel et de routage de connexion*.

– Recommandation UIT-T E.360.3 (2002), *Routage en fonction de la qualité de service et méthodes associées d'ingénierie du trafic – Méthodes de gestion des ressources en fonction de la qualité de service*.

– Recommandation UIT-T E.360.4 (2002), *Routage en fonction de la qualité de service et méthodes associées d'ingénierie du trafic – Méthodes et prescriptions de gestion des tables de routage*.

– Recommandation UIT-T E.360.5 (2002), *Routage en fonction de la qualité de service et méthodes associées d'ingénierie du trafic – Méthodes de routage de transport*.

– Recommandation UIT-T E.360.6 (2002), *Routage en fonction de la qualité de service et méthodes associées d'ingénierie du trafic – Méthodes de gestion de la capacité*.

– Recommandation UIT-T E.360.7 (2002), *Routage en fonction de la qualité de service et méthodes associées d'ingénierie du trafic – Prescriptions opérationnelles d'ingénierie du trafic*.

– Recommandation UIT-T E.361 (2003), *Prise en charge du routage en fonction de la qualité de service aux fins de l'interfonctionnement des classes de qualité de service à travers les diverses techniques de routage*.

– Recommandation UIT-T E.860 (2002), *Accord sur les niveaux de service: cadre général*.

– Recommandation UIT-T G.114 (2003), *Temps de transmission dans un sens*.

– Recommandation UIT-T G.1000 (2001), *Qualité de service des communications: cadre et définitions*.

– Recommandation UIT-T G.1010 (2001), *Catégories de qualité de service multimédia pour l'utilisateur final*.

– Recommandation UIT-T I.350 (1993), *Aspects généraux relatifs à la qualité de service et à la performance des réseaux numériques, y compris les RNIS*.

– Recommandation UIT-T J.112 (1998), *Systèmes de transmission pour services interactifs de télévision par câble*.

– Recommandation UIT-T J.162 (2004), *Protocole réseau de signalisation d'appel pour la fourniture de services à temps critique sur les réseaux de télévision par câble utilisant des câblo-modems*.

– Recommandation UIT-T J.163 (2004), *Qualité de service dynamique pour la fourniture de services à temps critique sur les réseaux de télévision par câble utilisant des câblo-modems*.

– Recommandation UIT-T J.170 (2002), *Spécifications de la sécurité sur IPCablecom*.

– Recommandation UIT-T J.174 (2002), *Qualité de service interdomaniale IPCablecom*.

– Recommandation UIT-R M.1079-2 (2003), *Exigences imposées à la qualité globale et à la qualité de service pour les télécommunications mobiles internationales-2000 (IMT-2000)*.

– Recommandation UIT-T X.805 (2003), *Architecture de sécurité pour les systèmes assurant des communications de bout en bout*.

– Recommandation UIT-T Y.1221 (2002), *Gestion du trafic et des encombrements dans les réseaux en mode IP*.

– Recommandation UIT-T Y.1540 (2002), *Service de communication de données par protocole Internet – Paramètres de performance pour le transfert de paquets IP et la disponibilité de ce service*.

– Recommandation UIT-T Y.1541 (2002), *Objectifs de qualité de fonctionnement pour les services en mode IP*.

3 Définitions

La présente Recommandation ne définit pas de nouveaux termes.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations suivantes:

DiffServ services différenciés (*differentiated services*)

DQoS qualité de service dynamique (*dynamic QoS*)

IETF groupe de travail d'ingénierie Internet (*Internet engineering task force*)

IntServ services intégrés (*integrated services*)

LSP chemin commuté avec étiquette (*label switched path*)

MPLS commutation multiprotocolaire par étiquetage (*multiple protocol label switching*)

MTA adaptateur de terminal multi média (*multimedia terminal adaptor*)

QS qualité de service

RSVP protocole de réservation de ressource (*resource reservation protocol*)

SLA accord de niveau de service (*service level agreement*)

UIT-T Union internationale des télécommunications – Secteur de la normalisation des télécommunications

5 Introduction

La qualité de service (QS) consiste en définitive à prendre en charge les caractéristiques et les propriétés d'applications spécifiques. Or, des applications différentes peuvent avoir des besoins très différents. Pour la télémédecine par exemple, la précision des données acheminées est plus importante que le délai global ou la variation du temps de transmission des paquets (c'est-à-dire la gigue), tandis que pour la téléphonie Internet, la gigue et le délai sont des éléments essentiels dont la valeur doit être réduite au minimum. Un certain nombre de Recommandations de l'UIT-T traitent de la qualité de service. Aux termes de la Rec. UIT-T E.800 la qualité de service désigne: "l'effet global produit par la performance d'un service qui détermine le degré de satisfaction de l'usager". Pour la Rec. UIT-T E.800, la prise en charge, l'exploitabilité, la servibilité et la sécurité font toutes partie intégrante de la performance d'un service, de telle sorte que le domaine d'application de cette définition de la qualité de service est exhaustif. A partir de la notion de qualité de service de la Rec. UIT-T E.800, la Rec. UIT-T G.1000 subdivise la performance de service (ou la qualité de service) en plusieurs composantes fonctionnelles et la rattache à la performance du réseau, telle qu'elle est définie dans les Recommandations UIT-T I.350, Y.1540 et Y.1541. La Rec. UIT G.1010 complémentaire de la Rec. UIT-T G.1000 indique des exigences concernant les applications axées sur l'utilisateur final en les classant par grandes catégories (interactivité, tolérance des erreurs). Parmi les normes connexes et en ce qui concerne les applications ou les paramètres de performance spécifiques, la Rec. UIT-R M.1079-2, définit les spécifications applicables aux réseaux d'accès IMT-2000 en matière de qualité vocale/de données de bout en bout, comme de performance, tandis que la Rec. UIT-T G.114 spécifie les limites du délai de transmission dans le cas des communications dans un réseau numérique.

L'obtention de la performance de réseau requise exige la présence dans le réseau de certains mécanismes, lesquels visent à contrôler et à fournir différentes réponses de service, même en cas de conflit de ressources. Le Document RFC 2990 de l'IETF récapitule les caractéristiques potentielles de la réponse de service contrôlée suite à une demande spécifique: *cohérente et prévisible à un niveau identique ou supérieur à une valeur minimale garantie ou fixée à l'avance*. Par exemple, en cas de conflit de ressources ou d'encombrement du réseau, le maintien de la réponse de service escomptée exige la mise en œuvre de plusieurs moyens à différentes échelles de temps, depuis les moyens requis pour assurer une planification judicieuse du réseau fondée sur des caractéristiques du trafic au cours d'une longue période, jusqu'aux moyens nécessaires à un contrôle différentiel de l'attribution et de l'admission des ressources, fondé sur les conditions actuelles de charge du réseau. Ces différents mécanismes (par exemple une méthode de la signalisation indiquant le niveau souhaité de performance du réseau) font l'objet du cadre architectural pour la prise en charge de la qualité de service. En particulier, la présente Recommandation définit une série de mécanismes génériques de réseau pour la qualité de service et propose une structure appropriée. Enfin les mécanismes de réseau sont utilisés conjointement afin d'obtenir l'effet global satisfaisant produit par la réalisation des qualités de service adaptées aux besoins d'une vaste gamme d'applications. L'aspect indépendant des applications du cadre architectural le distingue des architectures de qualité de service spécifiques des applications, notamment celles définies dans la Rec. UIT-T H.360 propre aux applications multimédias.

6 Modules de qualité de service

Le cadre architectural de la qualité de service repose sur un ensemble de mécanismes de réseau génériques pour le contrôle de la réponse de service du réseau à une demande, qui peut être spécifique à un élément de réseau, ou pour la signalisation entre éléments de réseau ou encore pour le contrôle et la gestion du trafic dans un réseau. (On notera que le fonctionnement des modules ne doit pas être assimilé à un fonctionnement de bout en bout.) Tel qu'indiqué à la Figure 1, les modules sont organisés en trois plans:

– le plan contrôle qui contient les mécanismes relatifs aux itinéraires par lesquels circule le trafic utilisateur. Ces mécanismes comprennent le contrôle d'admission, le routage en fonction de la QS et la réservation de ressources;

– le plan données, qui comprend les mécanismes concernant directement le trafic utilisateur. Parmi ces mécanismes figurent la gestion des mémoires tampon, la prévention des encombrements, le marquage des paquets, la mise en file d'attente et la programmation, la classification, l'organisation et le formage du trafic;

– le plan gestion qui regroupe des mécanismes d'exploitation, d'administration et de gestion du réseau. Parmi ces mécanismes figurent l'accord sur les niveaux de service, le rétablissement, la taxation et l'enregistrement du trafic et enfin l'organisation du trafic.

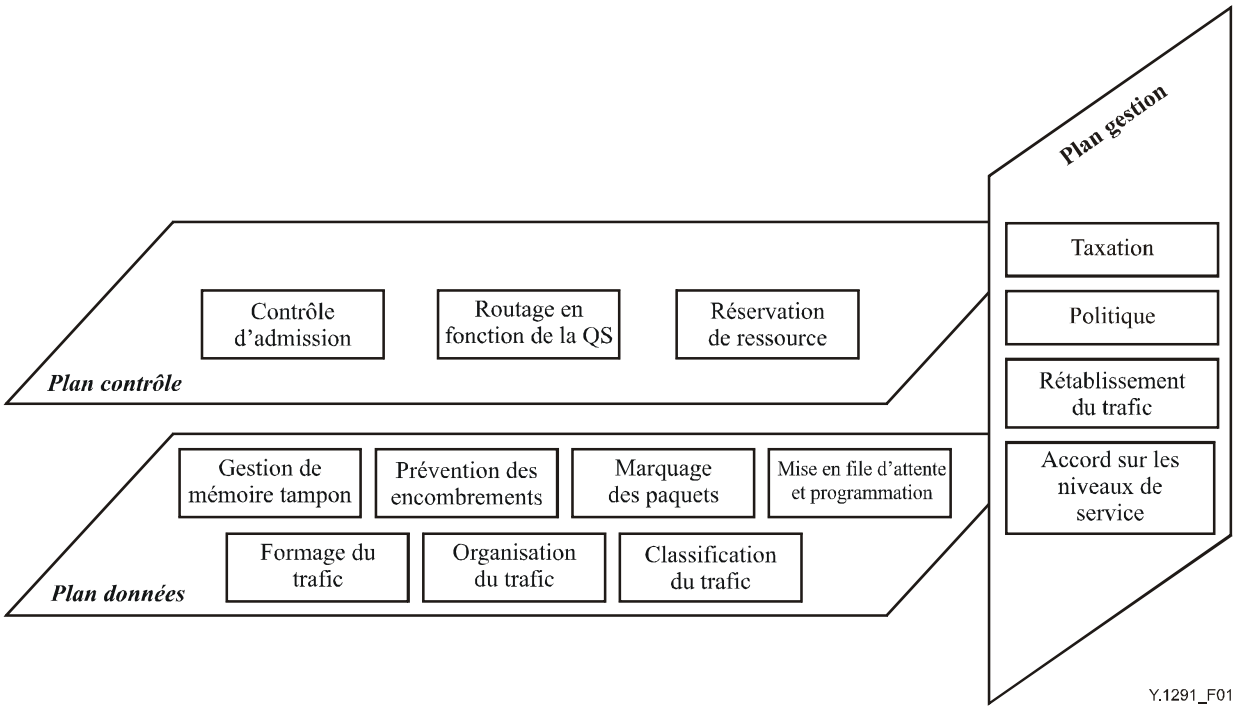


Figure 1/Y.1291 – Cadre architectural pour la prise en charge de la qualité de service

Un module de qualité de service peut être spécifique à un nœud de réseau (comme pour la gestion de mémoire tampon) ou applicable à un segment de réseau, comme par exemple dans le cas du routage en fonction de la qualité de service). Dans ce dernier cas en particulier une signalisation entre les nœuds de réseau s'impose, indépendamment du fait qu'ils fassent partie d'un segment de réseau, c'est-à-dire une signalisation de bout en bout, d'un bout à une extrémité, d'une extrémité à une extrémité ou d'un réseau à un réseau. La signalisation peut s'effectuer dans l'un de ces trois plans logiques. Lorsque la signalisation s'effectue dans le plan contrôle ou le plan gestion, elle comporte l'utilisation d'un protocole approprié. Du fait de ses propriétés spécifiques, la présente Recommandation considère la signalisation comme un élément des interactions entre les modules de qualité de service et traite cette question dans le paragraphe correspondant.

Il importe de signaler le caractère logique du cadre architectural pour la prise en charge de la qualité de service, lequel ne pose aucune condition quant aux modalités de réalisation d'un module; en tant que telle, l'implémentation d'un module peut être par exemple répartie ou centralisée. Les paragraphes ci-après décrivent de façon plus détaillée la réalisation des modules en fonction des plans.

7 Mécanismes du plan contrôle

7.1 Contrôle d'admission

Ce mécanisme contrôle le trafic admis dans le réseau. Normalement les critères d'admission résultent de l'organisation choisie [Document RFC 2753 de l'IETF]. Le fait que le trafic soit admis ou non dépend de la conclusion préalable d'un accord sur les niveaux de service. En outre, la décision peut dépendre de la disponibilité adéquate de ressources réseau, de sorte que le trafic nouvellement admis ne provoque pas une surcharge et une détérioration du service sur le trafic en cours. Pour un prestataire de services, il convient d'admettre le trafic maximal, en maintenant le même niveau de qualité de service (y compris les niveaux escomptés de performance des transactions et de fiabilité/disponibilité du service) pour le trafic existant.

Les mécanismes d'admission des appels liés à la performance des transactions sont généralement fondés sur les valeurs de certains paramètres ou sur des mesures. Le mécanisme dit paramétrique calcule les limites les plus défavorables d'un ensemble de mesures (par exemple, perte de paquet, retard et gigue) concernant les paramètres du trafic; il permet d'obtenir une qualité de service *fiable* pour des services en temps réel. Ce mécanisme est normalement mis en œuvre par une demande de réservation de ressources afin d'obtenir les ressources nécessaires pour l'établissement du flux de trafic. L'Appendice I donne un exemple de méthode QS mettant à profit ce type de contrôle d'admission.

Par contre, le mécanisme fondé sur des mesures utilise des mesures effectuées sur le trafic existant, préalablement à une décision d'admission. Il ne garantit pas un débit ou des niveaux limites fiables des pertes de paquet, du retard ou de la gigue et convient à l'établissement d'une qualité de service *non stabilisée* ou relative. Cette approche comporte en général une utilisation plus importante des ressources réseau par comparaison à l'approche paramétrique. L'Appendice II donne une présentation récapitulative d'une méthode expérimentale de prise en charge de la qualité de service sur la base de mesures. On notera qu'il est théoriquement possible d'adopter une approche hybride consistant par exemple à utiliser des mesures pour mettre à jour les ressources disponibles dans le cadre de l'approche paramétrique.

L'observation des prescriptions de fiabilité/disponibilité de service au cours d'une période spécifiée, pour les types de transaction négociés dans l'accord SLA, peut également faire appel au mécanisme de contrôle d'admission. En particulier, la fiabilité/disponibilité de service requise peut être demandée en terme de niveau de priorité pour le contrôle d'admission, ce qui ensuite détermine l'établissement d'une "connexion" ou d'une liaison de type chemin commuté avec étiquette. Les systèmes de contrôle d'admission privilégient les flux et trafics (par exemple pour les communications d'urgence) jugés critiques par un prestataire de services en période d'encombrement. La définition d'une priorité de contrôle d'admission est un moyen de privilégier les chemins LSP hautement prioritaires par rapport aux itinéraires LSP de moindre priorité.

L'Annexe A spécifie les niveaux de priorité en matière de contrôle d'admission.

7.2 Routage en fonction de la qualité de service

Au sens étroit, le routage en fonction de la qualité de service désigne le choix d'un itinéraire conforme aux exigences de qualité de service d'un flux de données. Selon toute vraisemblance, l'itinéraire choisi n'est pas l'itinéraire classique le plus court. Suivant les particularités et le nombre de mesures de la qualité de service impliqués, les calculs nécessaires au choix de l'itinéraire risquent

de comporter un coût prohibitif lorsque la taille du réseau augmente. Aussi les systèmes de routage selon la qualité de service utilisés dans la pratique considèrent-ils essentiellement les cas comportant une seule mesure (par exemple largeur de bande ou retard) ou deux mesures de la qualité de service (par exemple, coût-retard, coût-largeur de bande et largeur de bande-retard)[1]. Pour simplifier davantage le calcul d'itinéraires, il existe différentes stratégies de routage. Selon les modalités de mise à jour des informations d'état et d'exécution de la recherche d'itinéraires possibles, il existe différentes stratégies notamment le routage selon la source, le routage réparti et le routage hiérarchique [Chen]. En outre, en fonction du mode de traitement des différentes mesures de la qualité de service, des stratégies telles que le classement des mesures et le filtrage séquentiel permettent d'obtenir une optimisation globale, tout en réduisant la complexité des mesures [RFC 2386 de l'IETF].

Le processus de sélection de l'itinéraire implique la connaissance des spécifications et les caractéristiques de qualité de service du flux de données (qui changent fréquemment) et d'information concernant la disponibilité des ressources réseau (exprimée en mesures standards telles que la largeur de bande disponible et le retard). Ces données sont généralement obtenues et réparties au moyen des protocoles de signalisation. Par exemple, le protocole de réservation de ressources [Document RFC 2205 de l'IETF] peut servir à acheminer les spécifications et les caractéristiques d'un flux de données, les extensions OSPF étant définies dans le Document RFC 2676 de l'IETF pour la disponibilité des ressources. Par comparaison au routage par le premier conduit ouvert le plus court, qui détermine les itinéraires optimaux en fonction d'une mesure relativement constante (par exemple le nombre de bonds ou le coût), le routage en fonction de la qualité de service implique des calculs d'itinéraires plus fréquents et plus complexes et un trafic de signalisation plus important [Apostolopoulos].

Il importe de signaler que le routage en fonction de la qualité de service fournit un moyen de déterminer un itinéraire uniquement susceptible de prendre en charge la performance prescrite. Afin de garantir la performance sur un itinéraire sélectionné, ce type de routage doit être utilisé parallèlement à un mécanisme de réservation de ressources le long de l'itinéraire en question.

Le routage en fonction de la qualité de service peut en outre être étendu à l'ingénierie du trafic. (Avec des caractéristiques de trafic qui évoluent lentement sur une longue période de temps et en présence d'une forte granularisation des flux de trafic, l'ingénierie du trafic inclut la gestion du trafic, la gestion de la capacité, la mesure du trafic et sa modélisation, la modélisation du réseau et l'analyse de la performance.) A cet effet, la sélection du routage intègre fréquemment différentes contraintes telles que les attributs du trafic, les contraintes du réseau et les contraintes d'organisation [Document RFC 3272 de l'IETF]. Ce type de routage généralisé en fonction de la qualité de service est qualifié également de routage basé sur les contraintes, qui permet de choisir un itinéraire en contournant les points encombrés (ou de partager la charge) et d'améliorer l'utilisation globale du réseau tout en automatisant l'application des politiques d'ingénierie du trafic.

Les Recommandations UIT-T de la série E.360.x étudient et recommandent des méthodes de contrôle de la réponse d'un réseau aux besoins du trafic et aux autres stimuli tels que les défaillances de liaison ou de nœud. En particulier, les méthodes décrites dans les Recommandations de la série E.360.x portent notamment sur le routage des appels et des connexions, la gestion des ressources selon la qualité de service, la gestion des tables de routage, le routage de transport dynamique, la gestion de la capacité et les besoins en matière d'exploitation. La Rec. UIT-T E.361 spécifie les fonctions de routage en fonction de la qualité de service et les paramètres connexes, tels que l'attribution de largeur de bande et sa protection, les priorités d'acheminement, les priorités de mise en file d'attente et l'identification de la catégorie de service. De plus, la Rec. UIT-T E.361

[1] Certaines de ces mesures ont un caractère additif et d'autres sont limitatives (contraignantes), par exemple, le retard et le coût sont additifs tandis que la largeur de bande est contraignante. Ces considérations sont importantes dans le cadre de l'élaboration d'algorithmes d'acheminement applicables.

prescrit différentes méthodes de signalisation des paramètres de routage en fonction de la qualité de service dans des réseaux n'utilisant pas les mêmes technologies de routage.

7.3 Réservation de ressources

Ce mécanisme met de côté les ressources réseau prescrites sur demande afin d'obtenir les performances réseau voulues. La suite donnée à une demande de réservation est étroitement liée au mécanisme de contrôle d'admission. Aussi tous les éléments pris en compte dans le contrôle d'admission interviennent-ils également dans ce cas. Toutefois une condition nécessaire pour satisfaire à une demande de réservation tient généralement à la disponibilité de ressources réseau suffisantes.

La nature exacte d'une réservation de ressources dépend des spécifications en matière de performance du réseau et de la conception de réseau particulière permettant de répondre à cette demande. Par exemple, selon la conception *IntServ*, les flux simplex sont prioritaires et se caractérisent par des paramètres définissant un système de comptage de jetons; les réservations amorcées par le destinataire sont effectuées à la demande en fonction des besoins de débit de pointe propre à garantir des valeurs limites du retard. Indépendamment des particularités, il importe pour les prestataires de services de pouvoir facturer l'utilisation des ressources réservées. La réservation de ressources exige donc la prise en charge de procédures d'authentification, de comptabilisation et de règlement entre les différents prestataires de services. Aussi la réservation de ressources fait-elle généralement appel à un protocole spécialement conçu, tel que le protocole RSVP [Document RFC 2205 de l'IETF].

La réservation de ressources peut être conçue comme une fonctionnalité répartie ou centralisée. L'écart entre la disponibilité réelle et la disponibilité prévue en ressources constitue un problème majeur et il faut veiller à utiliser l'information la plus actualisée, pour que l'application demandant la réservation dispose effectivement des différentes ressources requises notamment en matière de nœuds et de liaisons.

8 Mécanismes du plan données

8.1 Gestion de la mise en file d'attente (ou en mémoire tampon)

La gestion de la mise en file d'attente ou en mémoire tampon consiste à choisir parmi les paquets à transmette ceux qu'il faut mettre en mémoire et ceux qui doivent être abandonnés. Parmi les principaux objectifs de la gestion de la mise en file d'attente figure la limitation au minimum de la longueur de la file d'attente en régime permanent, sans néanmoins sous-utiliser la liaison et tout en évitant le phénomène de verrouillage (monopolisation de l'espace de la file d'attente par une seule connexion ou un seul flux [Document RFC 2309 de l'IETF]). Les différents systèmes de gestion des files d'attente se distinguent principalement par les critères d'abandon des paquets et de choix des paquets à abandonner. Le recours aux files d'attente multiples introduit une diversification supplémentaire, par exemple selon le mode de répartition des paquets entre les différentes files.

Un critère courant d'abandon des paquets est la fixation d'une taille maximale de la file d'attente. Les paquets sont abandonnés lorsque la taille maximale est atteinte. Le choix des paquets abandonnés dépend des règles fixées à cet effet, par exemple:

– l'abandon des derniers paquets arrivés est la stratégie la plus courante;
– l'abandon des paquets les premiers arrivés conserve les derniers arrivés au détriment de ceux qui sont en tête de queue;
– l'abandon de type aléatoire conserve les derniers paquets arrivés au détriment d'un paquet choisi au hasard dans la file. Ce système est parfois coûteux puisqu'il implique un déplacement dans la file.

Le choix d'un système d'abandon des paquets uniquement lorsque la file d'attente atteint sa longueur maximale tend à maintenir la file d'attente dans cet état pendant un temps relativement long, ce qui risque d'avoir un effet catastrophique dans le cas d'un trafic par rafales. Il existe des systèmes qui utilisent un critère plus dynamique fondé non sur la taille maximale de la file d'attente et autorisant par conséquent une gestion active de cette file. L'un des principaux systèmes de ce type est le système dit de détection précoce aléatoire (RED, *random early detection*) [Floyd], qui par ailleurs facilite la résolution du problème posé par la longueur maximale de la file et permet d'éviter les encombrements. Le système RED abandonne les paquets (entrants) de façon probabiliste, en fonction de la longueur moyenne estimée de la file d'attente. La probabilité d'abandon augmente en fonction de la longueur moyenne estimée de cette file. Autrement dit, lorsque la file est restée pratiquement vide au cours de la période qui vient de s'écouler, les paquets entrants sont généralement conservés; par contre, si récemment la file est restée pratiquement pleine la plupart du temps, les paquets entrants sont susceptibles d'être abandonnés. Plus précisément, le système RED considère deux valeurs seuils de la longueur moyenne de la file d'attente: la première spécifie la longueur moyenne au-dessous de laquelle aucun paquet n'est abandonné; l'autre indique la longueur moyenne à partir de laquelle tous les nouveaux paquets sont abandonnés. Pour une file d'attente de longueur moyenne comprise entre ces deux valeurs seuils, la probabilité d'abandon du paquet entrant est proportionnelle à la longueur moyenne. L'efficacité du système RED dépend naturellement du choix pertinent des paramètres utilisés. Aucun jeu de paramètres ne fonctionne de façon parfaitement adaptée à tous les types de trafic et à tous les scénarios d'encombrement. Il existe donc deux variantes du système RED, à savoir:

– la détection RED de flux (FRED) [Lin *et al.*, 1997], qui ajoute un contrôle supplémentaire au système RED en appliquant aux flux un traitement différentiel des abandons de paquets en fonction de leur utilisation de la mémoire tampon. Si dans la file d'attente le nombre de paquets issus d'un flux particulier est inférieur à un seuil propre au flux en question, un paquet provenant du même flux et qui vient d'arriver ne sera pas abandonné; sinon, il sera susceptible de l'être pour favoriser les flux dont la mémoire tampon contient moins de paquets. Par comparaison au système RED, le système FRED est plus souple dans la mesure où il évite que les flux utilisent une fraction inférieure à leur juste part de la mémoire tampon et de la largeur de bande de la liaison;
– le système RED pondéré ajoute au système RED un contrôle supplémentaire en réalisant un traitement différentiel des abandons de paquets selon leur degré de priorité. La probabilité d'abandon d'un paquet est d'autant plus faible que la priorité de ce dernier est élevée.

8.2 Mécanisme de prévention des encombrements

L'encombrement d'un réseau survient lorsque le trafic atteint ou approche la capacité limite d'acheminement de ce réseau, faute de ressources suffisantes, notamment de largeur de bande de la liaison et d'espace de mémoire tampon. Le fait que les files d'attente du routeur (ou du commutateur) soient toujours pleines et que les routeurs commencent à abandonner des paquets est un signe d'encombrement. L'abandon de paquets entraîne une retransmission, d'où une intensification du trafic et une aggravation de l'encombrement. Cette réaction en chaîne risquerait d'entraîner un arrêt progressif du réseau et une réduction à zéro de son débit. L'utilisation de mémoire tampon très importante semble intuitivement devoir éviter les encombrements dus à une capacité mémoire insuffisante. Nagle [1987] a néanmoins démontré le contraire. En effet le long délai de mise en file d'attente des paquets, dû à l'importance de la mémoire tampon, nécessite leur retransmission et provoque ainsi un encombrement. La prévention des encombrements implique la mise en œuvre de moyens plus robustes, qui maintiennent la charge du réseau au-dessous de sa capacité, et autorisent ainsi son exploitation à un niveau de performance acceptable, sans réduction grave de sa capacité en période d'encombrement.

Un système classique de prévention des encombrements consiste, en cas d'encombrement effectif ou imminent, à réduire le trafic d'entrée du réseau sur l'initiative de l'expéditeur, [Jacobson, 1988]. Sauf indication explicite, la perte de paquet ou la fin d'une temporisation sont considérées normalement comme une indication implicite d'encombrement du réseau. Les modalités de fermeture partielle de la source de trafic dépendent des particularités des protocoles de transport. Dans le cas d'un protocole à fenêtrage, comme le protocole TCP, on procède par réduction multiplicative de taille de la fenêtre.

En principe, la priorité non critique du contrôle d'admission d'un usager permet de réduire le trafic. En effet, il est alors possible de conserver un niveau de service normal pour tout le trafic de priorité plus élevée.

Lorsque l'encombrement diminue, l'expéditeur peut ensuite intensifier prudemment le trafic.

Pour éviter le risque de retards excessifs imputables aux retransmissions suite à des pertes de paquet, des systèmes de notification explicite des encombrements (ECN, *explicit congestion notification*) ont été récemment mis au point. Le Document RFC 3168 de l'IETF spécifie un système ECN pour les protocoles IP et TCP qui constitue un exemple de système de gestion dynamique de la mémoire tampon; le marquage des paquets et non leur abandon signale alors un encombrement du réseau destinataire.

A réception d'un paquet ayant subi un encombrement, un hôte doté du système ECN répond pratiquement de la même façon qu'à réception d'un paquet abandonné.

8.3 Mécanisme de mise en file d'attente et de programmation

Pour résumer, ce mécanisme détermine les paquets à transmettre ou à émettre sur une liaison sortante. Le trafic d'arrivée est introduit dans un système de files d'attente, constitué généralement de plusieurs files et d'un programmateur. La gestion de ce système suit des règles préalablement définies de mise en attente et d'ordonnancement. Il existe à cet effet plusieurs méthodes de base:

– premier arrivé, premier servi (FIFO, *first-in, first out*): les paquets sont placés dans une file d'attente unique et servis dans leur ordre d'arrivée;
– gestion équitable de files: les paquets sont classés en plusieurs flux et attribués à des files affectées aux flux respectifs correspondants. Les files sont ensuite servies à tour de rôle. Les files vides sont sautées. La gestion équitable des files est également appelée gestion des files flux par flux;
– desserte prioritaire: les paquets sont d'abord classés, puis placés dans des files de priorités différentes. Les paquets sont programmés à partir de la tête d'une file donnée uniquement si toutes les files de priorité plus élevée sont vides. A l'intérieur de chacune des files prioritaires les paquets sont programmés dans l'ordre premier arrivé, premier servi;
– gestion équitable pondérée: les paquets sont classés en plusieurs flux et attribués à des files d'attente affectées à leurs flux respectifs. A chaque file est attribué un pourcentage de la largeur de bande de sortie en fonction des besoins de largeur de bande du flux correspondant. En distinguant des paquets de longueur variable, cette méthode évite également d'attribuer davantage de largeur de bande aux paquets plus importants par comparaison aux paquets plus petits;
– mise en file d'attente en fonction de la catégorie : les paquets sont classés dans différentes catégories de service, puis affectés à des files qui correspondent à chaque catégorie. Un pourcentage différent de la largeur de bande de sortie peut être affecté à chacune des files, celles-ci étant servies à tour de rôle (les files vides sont sautées).

8.4 Mécanisme de marquage des paquets

Il est possible de marquer les paquets en fonction de la catégorie de service particulière dont ils feront l'objet dans le réseau, selon le type de paquet considéré. Généralement effectué par un nœud d'extrémité, le marquage des paquets implique l'attribution normalisée d'une valeur à un champ d'en-tête réservé à cet effet. (Par exemple, le type de service de l'en-tête IP ou les bits EXP de l'en-tête MPLS [Document RFC 3032 de l'IETF] sert à codifier les caractéristiques observables de l'extérieur des routeurs avec les mécanismes *DiffServ* [RFC 2474 de l'IETF] ou *MPLS-DiffServ* [RFC 3270 de l'IETF]). Lorsque le marquage est effectué par un hôte, il doit être vérifié et peut être modifié si nécessaire par un nœud d'extrémité. Parfois, des valeurs spéciales peuvent servir à marquer des paquets non conformes qui seront éventuellement abandonnés ultérieurement en cas d'encombrement. Le degré de priorité des paquets peut également être renforcé ou réduit selon les résultats de certaines mesures.

L'hôte ou le nœud d'extrémité doivent procéder à une configuration dynamique des critères de marquage des paquets; les protocoles COPSP de service commun de politique ouverte (COPS, *common open policy service protocol*) (Document RFC 2748 de l'IETF) ou RSVP de réservation de ressources sont utilisables à cet effet; avec le protocole RSVP, l'entité de marquage peut interroger le réseau quant au marquage à appliquer aux paquets d'un flux particulier. [Document RFC 2996 de l'IETF].

8.5 Mécanisme de classification du trafic

La classification du trafic peut s'effectuer au niveau du flux ou des paquets. A l'extrémité du réseau, l'entité chargée de la classification du trafic examine normalement les champs multiples d'un paquet (par exemple les quintuplets associés à un flux IP), puis détermine l'agrégat auquel le paquet appartient et l'accord correspondant sur les niveaux de service.

8.6 Mécanisme d'organisation du trafic

L'organisation du trafic consiste à déterminer si le trafic à acheminer est conforme, bond par bond, aux politiques ou aux contrats préalablement négociés. Normalement, les paquets non conformes sont abandonnés. Les expéditeurs peuvent être informés des paquets abandonnés, les causes correspondantes peuvent être établies, et des accords sur les niveaux de service peuvent assurer ultérieurement leur conformité.

8.7 Mécanisme de formage du trafic

Le formage du trafic désigne le contrôle du débit et du volume du trafic entrant dans le réseau. L'entité chargée du formage du trafic met en mémoire tampon les paquets non conformes, jusqu'à ce que l'agrégat correspondant soit conforme au trafic; le trafic ainsi obtenu comporte moins de rafales que le trafic d'origine et s'avère donc plus prévisible. Un formage doit souvent être effectué entre les nœuds de sortie et d'entrée.

Il existe deux grandes méthodes de formage du trafic: le compteur à fuite (ou "godet à fuite") et le compteur à jetons (ou "godet à jetons"). L'algorithme du compteur à fuite utilise un compteur à fuite afin de réguler le débit du trafic à la sortie d'un nœud. Indépendamment du débit d'arrivée, le compteur à fuite maintient constant le débit de sortie. Tous les paquets en surdébit sont mis à l'écart. Deux paramètres caractérisent cette méthode et sont généralement configurables par l'usager. La taille du godet et le débit de transmission.

D'autre part, la méthode du compteur à jetons peut assurer une régulation plus souple du débit du trafic à la sortie d'un nœud. Elle autorise la sortie des paquets dès leur arrivée, à condition qu'ils possèdent un nombre de *jetons* suffisant. Les jetons sont générés à un certain débit et déposés dans le godet à jetons jusqu'à ce qu'il soit plein moyennant un certain volume de trafic (un certain nombre d'octets peuvent quitter un nœud). Aucun paquet ne peut être transmis, si le godet ne contient pas de jeton. Par contre, plusieurs jetons peuvent être consommés simultanément pour

permettre le passage de rafales. Cette méthode, contrairement à celle du compteur à fuite ne comporte pas de politique de rejet. Elle laisse ainsi le soin au système de gestion de la mémoire tampon de décider du sort des paquets lorsque le godet est plein. La méthode du compteur à jetons se caractérise par deux paramètres généralement configurables par l'usager: la taille du godet et le débit de production de jetons.

Ces deux méthodes peuvent être utilisées conjointement. En particulier, il est possible de former le trafic dans un premier temps en appliquant la méthode du compteur à jetons, puis celle du compteur de fuite afin d'éliminer les rafales préjudiciables. Il est également possible d'utiliser en tandem deux compteurs à jetons.

9 Mécanismes du plan gestion

9.1 Accord sur les niveaux de service

Un accord sur les niveaux de service (SLA, *service level agreement*) désigne généralement l'accord conclu entre un usager et un prestataire de services, qui spécifie le niveau de disponibilité, de servibilité, de performance, d'exploitation ou d'autres attributs. Il peut comporter différents aspects à caractère commercial (tels que la tarification), outre la partie technique intitulée spécification de niveau de service (SLS) [Document RFC 3198 de l'IETF]; la spécification SLS indique notamment une série de paramètres et les valeurs correspondantes définissant le service fourni par un réseau au trafic d'un usager. Les paramètres de la spécification SLS peuvent être à caractère général, comme ceux définis dans la Rec. UIT-T Y.1540, ou technique, tels que les paramètres de trafic et de performance des architectures *IntServ* ou *DiffServ*. Globalement, la Rec. UIT-T E.860 définit un cadre SLA général adapté à un environnement multifournisseur.

9.2 Mesure et enregistrement du trafic

La mesure du trafic désigne la surveillance des caractéristiques temporelles (par exemple, débit) d'un flux de trafic, par rapport au profil de trafic convenu. Elle implique l'observation des caractéristiques en un point donné du réseau, ainsi que la collecte et l'enregistrement des informations utiles en vue de l'analyse du trafic et des actions éventuelles à engager. Selon le niveau de conformité constaté, un dispositif de mesure peut invoquer un traitement approprié (par exemple abandon ou formage) du flux de paquets.

9.3 Mécanisme de rétablissement du trafic

Dans le présent contexte le rétablissement du trafic est défini comme la réaction d'atténuation produite par un réseau lors d'une défaillance; il doit être considéré au niveau de plusieurs couches. Au bas de la pile, les réseaux optiques offrent maintenant la possibilité d'assurer au niveau de la longueur d'onde une fonctionnalité dynamique de protection et de rétablissement en anneau et en treillis. Au niveau de la couche SONET/SDH la fiabilité est assurée grâce à la commutation de protection automatique (APS, *automatic protection switching*), et par des architectures autorégénératrices en anneau et en treillis. L'architecture ATM offre des capacités analogues. Les mécanismes de reroutage sont généralement mis en œuvre au niveau de la couche IP pour rétablir le service à la suite d'une défaillance de liaison et de nœud; il peut s'agir d'un reroutage de bout en bout ou local (reroutage rapide). Le reroutage au niveau de la couche IP intervient à la suite d'une période de convergence d'acheminement dont l'achèvement peut exiger un délai de quelques secondes à plusieurs minutes. Le mécanisme de commutation multiprotocolaire par étiquetage permet à présent un rétablissement au niveau de la couche IP préalablement à la convergence.

On distingue deux types de défaillances de réseau:

- défaillance de nœud: défaillance d'un élément de réseau (carte routeur) au niveau d'un nœud ou d'une administration de réseau; elle est généralement résolue par la mise au point de dispositifs de redondance au sein des éléments de réseau afin de réduire au minimum

l'impact d'une défaillance. Des défaillances catastrophiques telles que les pannes d'alimentation électrique et les catastrophes naturelles risquent néanmoins de provoquer la mise hors service de tout un nœud de réseau. Auquel cas, le trafic de transit peut être réacheminé par des liaisons de réserve prévues autour du nœud défaillant;

- défaillance de liaison de transport: défaillance d'une liaison (par exemple T1, OC-3) entre deux nœuds de réseau. En général la panne d'une liaison peut être due à une défaillance d'un élément de liaison (carte de ligne) (qui peut ensuite affecter une liaison particulière) ou de façon plus grave, un sectionnement de fibre (qui risque alors de perturber un nombre important de liaisons). Les prestataires de services peuvent mettre au point des capacités de réserve supplémentaires afin d'atténuer l'impact de ce type de défaillance et rétablir les flux de trafic jusqu'à ce que l'incident soit corrigé.

Il y a lieu de noter que certains de ces éléments concernent généralement une couche spécifique et que les couches multiples impliquées doivent être soigneusement prises en considération dans la conception d'ensemble. Par exemple, une défaillance de liaison au niveau de la couche Physique risque d'affecter plusieurs liaisons et plusieurs itinéraires au niveau de la couche IP.

Comme dans le cas du contrôle d'admission, certains flux de trafic associés à des services sensibles peuvent exiger une priorité de rétablissement supérieure à d'autres. Un prestataire de services doit prévoir des niveaux adéquats de ressources de réserve de façon à garantir la conformité aux accords sur les niveaux de service en période de rétablissement. Parmi les paramètres mesurant la capacité de rétablissement du service figurent le temps et le coefficient de rétablissement. On trouvera à l'Annexe A la description détaillée des niveaux de priorité.

9.4 Politiques

Les politiques désignent un ensemble de règles permettant généralement d'administrer, de gérer et de contrôler l'accès aux ressources du réseau. Elles peuvent se rapporter spécifiquement aux besoins du prestataire ou traduire les dispositions de l'accord conclu entre l'usager et le prestataire de services, dans lequel peuvent figurer des prescriptions de fiabilité et de disponibilité pendant une certaine période de temps et différentes exigences en matière de qualité de service. Les prestataires de services peuvent s'appuyer sur certaines politiques pour implémenter des mécanismes appropriés dans le plan contrôle et dans le plan données. Parmi les applications potentielles figurent l'acheminement en fonction d'une politique (qui consiste à diriger un flux de paquets vers un port de destination sans tableau d'acheminement), les politiques de filtrage de paquets (marquage ou abandon de paquets en fonction d'une politique de classement), l'enregistrement de paquets (autorisant les usagers à enregistrer des flux de paquets spécifiés) et les politiques relatives à la sécurité.

Différents événements peuvent déclencher des décisions concernant les politiques. Certaines sont liées au trafic et d'autres non. Les modalités détaillées dépendent généralement des particularités des applications. Le Document RFC 2748 de l'IETF, par exemple, spécifie un protocole simple d'interrogation et de réponse applicable aux échanges d'informations relatifs aux politiques entre un serveur de politique (ou point de décision relatif aux politiques) et son client (ou point d'application d'une politique).

10 Interactions entre les modules

Une approche globale en matière de qualité de service fait appel normalement à plusieurs modules dans le plan contrôle, dans le plan données et dans le plan gestion. Aussi les paramètres de la qualité de service doivent-ils faire l'objet d'un échange de données entre les différents modules. Ces paramètres comprennent la performance de transaction au niveau paquet (par exemple retard et perte de paquet) et la fiabilité/disponibilité de service escomptée en termes de niveaux de priorité de trafic pour des fonctions de réseau particulières telles que le contrôle d'admission et le

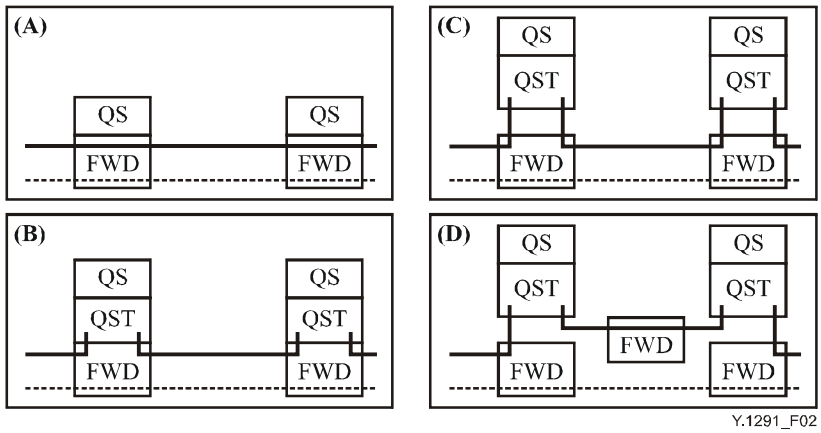
rétablissement du trafic. La signalisation et les consultations de bases de données constituent des exemples de mécanismes d'acheminement de ces paramètres.

10.1 Signalisation de la qualité de service

La signalisation de la qualité de service sert principalement à l'acheminement des spécifications de performance des applications (ou du réseau), à la réservation de ressources dans tout le réseau ou la communication de routes de qualité de service. Selon que l'information de signalisation fait partie du trafic de données associé, la signalisation de la qualité de service peut s'effectuer dans la bande ou hors bande:

– signalisation dans la bande: le signal de qualité de service fait partie du trafic de données associé, généralement présenté dans un champ d'en-tête particulier (par exemple le champ TOS dans le protocole IPv4 par exemple dans *DiffServ* et 802.1p) des paquets de données. Dans le plan données, la signalisation dans la bande n'introduit pas de trafic supplémentaire dans le réseau et n'entraîne pas de délai d'établissement pour le trafic de données. Ce type de signalisation ne convient évidemment pas à la réservation de ressources ou au routage en fonction de la qualité de service, qui doit intervenir a priori avant toute transmission de données;

– signalisation hors bande: le signal de qualité de service, acheminé dans des paquets spécialisés, est distinct du trafic de données associé. En outre, la signalisation de la qualité de service peut se faire bond par bond ou de bout en bout. Dans le cas de la signalisation bond par bond (Cas B de la Figure 2), l'information de signalisation est susceptible d'être modifiée par des nœuds intermédiaires. Puisqu'elle introduit dans le réseau un trafic supplémentaire la signalisation hors bande implique un surdébit pour l'obtention de la performance de réseau requise. En outre, elle comporte l'utilisation d'un protocole de signalisation ainsi qu'un traitement supplémentaire au-dessus de la couche Réseau, ce qui tend à ralentir les réponses par comparaison à la signalisation dans la bande. Toutefois, la signalisation hors bande se prête naturellement à la réservation de ressources ou au routage en fonction de la qualité de service.



QS fonctions de signalisation de qualité de service autres que la fonction QST
QST fonction de terminaison de la signalisation de la qualité de service
FWD fonction de transmission de données
——— itinéraire de signalisation de la qualité de service
---------- itinéraire de données

Figure 2/Y.1291 – Exemple de différentes formes de signalisation selon la qualité de service

De manière analogue, selon que l'itinéraire de signalisation est étroitement lié à l'itinéraire des données associées, la signalisation de la qualité de service peut être considérée comme couplée ou découplée de l'itinéraire:

– signalisation couplée à l'itinéraire: les messages de signalisation de la qualité de service sont acheminés uniquement par les nœuds potentiellement situés sur l'itinéraire de données. La signalisation dans la bande est par définition couplée à l'itinéraire, tandis que la signalisation hors bande ne l'est pas nécessairement. La signalisation couplée à l'itinéraire implique nécessairement que les nœuds de signalisation soient co-implantés avec les routeurs. Une configuration de ce type présente d'une part l'avantage de réduire le coût global de traitement de la signalisation (puisqu'il démultiplie les tâches d'acheminement dans la couche Réseau), mais d'autre part l'inconvénient d'un manque de souplesse pour la modernisation des routeurs ou pour l'intégration d'entités de contrôle (par exemple serveurs de politiques) non situées sur l'itinéraire de données (ou pour l'utilisation de méthodes d'acheminement non traditionnelles). Lorsqu'un mécanisme de couplage à l'itinéraire implique un protocole de signalisation, les routeurs doivent prendre en charge le protocole et pouvoir traiter les messages de signalisation correspondants. Le protocole RSVP est un exemple de protocole de signalisation couplée à l'itinéraire;
– signalisation découplée de l'itinéraire: les messages de signalisation de la qualité de service sont acheminés par des nœuds que l'on ne suppose pas situés sur l'itinéraire de données. En temps que telle seule la signalisation hors bande peut être découplée de l'itinéraire. La signalisation découplée de l'itinéraire implique que l'entité d'extrémité de la signalisation de qualité de service soit réservée et distincte de l'entité émettrice, qui est normalement située dans des routeurs. Contrairement à la signalisation couplée et à l'itinéraire, l'avantage de cette solution réside dans la souplesse de déploiement et de modernisation des nœuds de signalisation indépendamment des routeurs ou dans l'intégration des entités de contrôle non situées sur l'itinéraire de données; elle a en revanche l'inconvénient d'une complexité accrue et d'un coût majoré de l'ensemble des tâches de traitement et d'exploitation. Les cas C et D de la Figure 2 illustrent la configuration de signalisation découplée de l'itinéraire.

10.2 Mécanismes intraplans

Ce sujet doit faire l'objet d'un complément d'étude.

10.3 Mécanisme interplans

Plan contrôle et plan données

Mappage de la classe de qualité de service de la Rec. UIT-T Y.1541 sur les points de code de service différenciés (DSCP)

L'Appendice VI/Y.1541 décrit l'association des classes de qualité de service de la Rec. UIT-T Y.1541 avec les comportements domaine par domaine (PDB, *per domain behaviour*) du modèle *DiffServ*:

- comportements PDB basés sur le comportement de réexpédition accélérée: Y.1541 Classes 0 et 1
- comportements PDB basés sur le comportement de réexpédition assurée: Y.1541 Classes 2, 3 et 4
- comportements PDB basés sur le comportement par défaut/au mieux: Y.1541 Classe 5

11 Considérations de sécurité

En règle générale, la Rec. UIT-T X.805 définit une architecture de sécurité de réseau intéressante pour l'étude des propriétés de sécurité et pour la mise au point de garantie vis-à-vis des modules et des solutions de qualité de service.

11.1 Plan données

Sur le plan données, le trafic est généralement traité en fonction des données d'en-tête de paquet. Il est possible de marquer les paquets en attribuant une valeur à un champ d'en-tête désigné. Ils peuvent être également classés en fonction de la valeur de plusieurs champs de l'en-tête de paquet (par exemple les quintuplets IP). Le formage, l'organisation et la mise en file d'attente du trafic sont alors possibles sur la base de la classification et du marquage des paquets. En temps que telle l'intégrité des en-têtes de paquet est essentielle à la validité et à la sécurité de la méthode adoptée en matière de qualité de service. Il faut empêcher la modification et la fabrication malveillante de données d'en-têtes de paquet.

Il importe par ailleurs de signaler qu'en dépit de la possibilité pour un hôte ou un nœud de réseau quelconque de réaliser ou de modifier un marquage de paquet, il est intéressant que le marquage soit effectué par un nœud d'extrémité. Celui-ci dispose en général d'une relation de confiance avec les nœuds centraux; aussi, en cas de marquage par un hôte, il doit être vérifié et le cas échéant modifié par un nœud d'extrémité.

11.2 Plan gestion et plan contrôle

Le plan gestion et le plan contrôle traitent le trafic au niveau flux ou agrégat. Un flux est également identifié et décrit au moyen, par exemple, des quintuplets IP ou d'une étiquette MPLS dans l'en-tête de paquet, qui reste inchangée tout au long du cycle de vie du flux.

Le contrôle d'admission réalisé au niveau des nœuds d'extrémité contribue à éviter les usurpations d'identité et l'encombrement imputable à un trafic non autorisé. Les nœuds d'extrémité peuvent recevoir la confiance des nœuds centraux et peuvent avoir une vision de l'utilisation globale des ressources réseau. Réalisé de façon centralisée ou répartie, le contrôle d'admission doit inclure les tâches d'authentification et d'autorisation.

La réservation de ressources est étroitement liée au contrôle d'admission. Une demande de réservation peut être lancée par un hôte d'extrémité ou un nœud de prise en charge du service situé dans le réseau. Les demandes malveillantes de ressources risquent d'entraîner une réservation illicite excessive, un épuisement des ressources, puis un déni de service (refus de service). Il est souhaitable de prévoir des garanties contre les demandes malveillantes de ce type.

En règle générale les mécanismes de sécurité du réseau, tels que les passerelles et les mécanismes de détection d'intrus, peuvent contribuer à protéger les interfaces de réseau, indépendamment de la qualité de service. De plus les entités chargées des tâches d'authentification sont dotées de protections contre les attaques de déni de service.

11.3 Signalisation de la qualité de service

Pour protéger contre les attaques d'interception, de modification et de fabrication, la signalisation de la qualité de service doit faire appel à des mécanismes d'authentification et d'intégrité tels que RIPEMD160 ou SHA-1 (algorithme de hachage sécurisé n° 1). Le recours à des mécanismes de sécurité peut avoir des implications en termes de performance. Puisque le trafic de signalisation est normalement nettement inférieur au trafic de données, les répercussions en matière de performance du réseau imputables à la signalisation sécurisée hors bande (ou découplée de l'itinéraire) doivent être moindres par comparaison à la signalisation sécurisée dans la bande (ou couplée à l'itinéraire). De plus, les entités responsables de la signalisation doivent être protégées contre les attaques de déni de service.

12 Approches types

Afin d'illustrer les modalités d'interaction des modules de QS et l'élaboration de différentes approches de qualité de service, le présent paragraphe décrit quatre méthodes normalisées: services intégrés (*IntServ*), services différenciés (*DiffServ*), commutation multiprotocolaire par étiquetage (MPLS, *multi-protocol label switching*) et qualité de service dynamique IPCablecom. (Il est à noter que le Document RFC 2998 intègre les approches IntServ et DiffServ.) Les Appendices I et II donnent des exemples des approches plus globales à caractère évolutif qui commencent à faire leur apparition.

12.1 IntServ

Conçue essentiellement pour la prise en charge des applications sensibles au temps de transfert en temps réel, l'approche *IntServ* (voir par exemple, le [Document RFC 1633 de l'IETF]) s'appuie sur la constatation selon laquelle un flux à un débit légèrement supérieur à son débit de données comporte un temps de transfert limité, le réseau étant alors en mesure de garantir la limite du temps de transfert d'un flux par une réservation de ressources flux par flux. Cette approche permet à une application, avant d'envoyer des données, de signaler dans un premier temps au réseau la demande de service voulue, indiquant notamment ses caractéristiques détaillées (profil de trafic, largeur de bande et temps de transfert prescrits). Le réseau détermine ensuite s'il peut attribuer des ressources appropriées (par exemple, en termes de largeur de bande ou d'espace de mémoire tampon) pour assurer le niveau de performance requis de la demande de service. L'application doit attendre l'obtention d'une réponse positive à la demande avant de commencer à envoyer des données. Dans la mesure où l'application observe son profil de trafic, le réseau remplit son engagement de service en maintenant l'état de réservation flux par flux et en appliquant des principes évolués de mise en file d'attente (par exemple, gestion équitable pondérée des files d'attente) pour le partage des liaisons. Les modules de qualité de service adaptés à l'approche *IntServ* incluent le contrôle d'admission, la mise en file d'attente, la réservation de ressources, la classification du trafic et l'organisation du trafic. En particulier, le protocole de signalisation RSVP est appliqué à la réservation de ressources. Le réseau peut accepter ou refuser une demande de réservation via le mécanisme de contrôle d'admission, en fonction de la disponibilité de ressources. Une demande de réservation aboutie conduit à la mise en place des états appropriés au niveau des nœuds sensibles au protocole RSVP. L'accès aux informations d'état et à des différents objets de données configurés (et donc relativement statiques) autorise l'interaction des différents modules.

12.2 DiffServ

Le principe sur lequel repose l'approche *DiffServ* considère un paquet en fonction de sa classe de service telle qu'elle est codée dans son en-tête IP. Le prestataire de services conclut avec chaque usager un accord sur les niveaux de service (ou une spécification de niveau de service) qui spécifie, notamment, le volume de trafic susceptible d'être envoyé par un usager selon une classe de service déterminée. Le trafic qui en résulte est classé (paquet par paquet) en un petit nombre de classes ou de flux agrégés; il est organisé à la frontière du réseau ou du prestataire de services. Une fois le trafic introduit dans le réseau, les routeurs l'acheminent en lui appliquant un traitement différencié. A l'inverse de l'approche *IntServ*, il ne s'agit pas d'un traitement flux par flux, mais uniquement en fonction de la classe de service indiquée. L'ensemble du réseau est configuré de façon à observer tous les accords conclus sur les niveaux de service. Les modules concernés (notamment gestion des mémoires tampon, marquage des paquets, accord sur les niveaux de service, mesure et enregistrement du trafic, organisation du trafic, formage et programmation du trafic) interagissent entre eux de façon relativement statique, essentiellement par l'intermédiaire d'objets de données configurés.

12.3 MPLS

Initialement conçue pour assurer l'interfonctionnement des réseaux IP et ATM (ou à relais de trames), la commutation multiprotocolaire par étiquetage (MPLS [Document RFC 3031 de l'IETF]) permet d'accélérer substantiellement le cheminement des paquets, grâce à l'utilisation d'étiquettes courtes de type couche 2. Dès qu'un paquet est introduit dans le réseau MPLS, une classe d'équivalence pour la transmission (FEC, *forward equivalence class*) lui est attribuée une fois pour toute, et codée en tant que chaîne de longueur fixe (étiquette). L'étiquette accompagne le paquet lors de sa transmission vers le bond suivant; elle sert alors d'index dans un tableau préconfiguré permettant d'identifier le prochain bond, ainsi qu'une nouvelle étiquette. L'ancienne étiquette est remplacée par la nouvelle et le paquet est transmis au prochain bond. Le processus se poursuit jusqu'à ce que le paquet atteigne sa destination. Autrement dit, la transmission de paquets dans un réseau MPLS est entièrement déterminée par les étiquettes, puisque les paquets auxquels la même classe d'équivalence pour la transmission a été attribuée sont transmis de la même façon. De plus, les étiquettes n'ont une signification que pour la paire de routeurs qui partage une liaison et, uniquement dans un sens, de l'expéditeur vers le récepteur. Toutefois, le récepteur choisit l'étiquette et négocie sa sémantique au moyen d'un protocole de distribution d'étiquettes. Dans sa version de base, la commutation MPLS est particulièrement intéressante du point de vue de l'ingénierie du trafic. Pour assurer une prise en charge explicite de la qualité de service, la commutation MPLS utilise certains éléments des approches *IntServ* et *DiffServ*. Le protocole de distribution d'étiquettes par exemple peut s'appuyer sur un protocole de réservation de ressources [Document RFC 3209 de l'IETF]; ce protocole permet de réserver les ressources réseau requises, ainsi qu'un chemin commuté avec étiquette, au cours de sa phase d'établissement de façon à garantir la qualité de service des paquets empruntant cet itinéraire. De plus, puisque l'étiquette et certains bits EXP de l'en-tête <d'encapsulation spécifique> qui la contiennent servent à représenter les classes de services différenciés, les paquets de la même classe d'équivalence pour la transmission peuvent faire l'objet du traitement *DiffServ* [Document RFC 3270 de l'IETF]. Les modules concernés par la commutation multiprotocolaire par étiquetage comprennent la gestion de mémoire tampon, le marquage des paquets, le routage en fonction de la qualité de service, la mise en file d'attente, la réservation de ressources ainsi que la classification et le formage du trafic. Ils interagissent par l'intermédiaire des informations d'état d'itinéraire commuté par étiquette installées dans chaque nœud MPLS par un protocole de distribution d'étiquettes et au moyen d'objets de données configurés.

12.4 Qualité de service dynamique IPCablecom

La Rec. UIT-T J.163 spécifie une approche fondée sur la réservation de ressources dynamiques flux par flux, de façon à prendre en charge les applications multimédias interactives par le réseau d'accès IPCablecom. Le réseau d'accès relie l'adaptateur de terminal multimédia au nœud d'accès, tel qu'il est défini dans la Rec. UIT-T J.112. Des ressources sont attribuées sur le réseau J.112 à chacun des flux associés à une session d'application et un abonné déterminés, après autorisation et authentification.

La qualité de service dynamique est fondée essentiellement sur les portes de qualité de service dynamique (DQoS) et sur les contrôleurs de porte. Grâce au protocole COPS spécifié dans le Document RFC 2748 de l'IETF, le contrôleur de porte contrôle l'existence et le fonctionnement des portes.

Les portes DQoS sont installées sur le nœud d'accès entre le réseau J.112 et une dorsale IP au moyen des fonctions de classification et de filtrage paquet J.112. Monodirectionnelle par définition, une porte DQoS est une entité logique associée à une session. Lorsqu'une porte est "fermée", les données en transit dans le réseau J.112 peuvent être soit abandonnées soit recevoir simplement le service "au mieux", selon la politique du prestataire.

Le contrôleur de porte est mis en place sur le serveur de gestion d'appel, qui gère normalement les sessions multimédias lancées par les adaptateurs de terminal multimédias au moyen de la signalisation d'appel contrôlée par le réseau (telle qu'elle est définie dans la Rec. UIT-T J.162) ou de la signalisation d'appel répartie (définie dans le Document RFC 3261 de l'IETF). Le contrôleur décide de la création comme de l'ouverture d'une porte. L'ouverture d'une porte implique un contrôle d'admission à réception d'une demande de gestion de ressources (au moyen du protocole RSVP) et d'une réservation de ressources au fur et à mesure des besoins du réseau. Il y a lieu de noter que la réservation de ressources s'effectue en deux phases. A la fin de la première phase, les ressources sont réservées, mais les adaptateurs MTA ne peuvent pas encore en disposer. C'est seulement à la fin de la deuxième phase que les portes créées au niveau des nœuds d'accès et que les ressources sont disponibles pour les adaptateurs MTA. Le modèle de réservation et d'engagement garantit la disponibilité des ressources avant que l'ouverture d'une session soit signalée à l'entité d'extrémité; il garantit en outre que les ressources sont engagées seulement au moment où elles sont nécessaires.

Les modules concernés par l'approche de qualité de service dynamique IPCablecom comprennent le contrôle d'admission, la mise en file d'attente, la réservation de ressources, la classification du trafic, ainsi que l'organisation du trafic et la politique correspondante. La réservation et l'engagement de ressources font respectivement appel aux protocoles de signalisation RSVP et COPS. Le réseau peut accepter ou rejeter une demande de réservation, par le biais du contrôle d'admission, selon la disponibilité de ressources ou la politique en vigueur. A la suite une demande de réservation aboutie conduit à l'installation des états appropriés au niveau des nœuds sensibles au protocole RSVP. Les modules interagissent par accès aux informations d'état et à différents objets donnés configurés.

Annexe A

Niveaux de priorité du trafic

Les niveaux escomptés de qualité pour les services des réseaux par paquet peuvent être envisagés de deux points de vue. Les classes de transaction spécifiées dans différentes Recommandations UIT-T telles que la Rec. UIT-T Y.1541 pour les services IP et I.356 pour les services ATM fixent les objectifs de performance des paquets de transaction (par exemple, perte de paquet et temps de transfert). Ces classes couvrent un vaste éventail de services, notamment d'applications vocales, de données et multimédias. Les paramètres correspondants définissent des niveaux de performance acceptables (paquets perdus) pour chaque classe de transaction. Les priorités escomptées en matière de fiabilité impliquent la configuration de la liaison ou de la "connexion", par exemple, le chemin commuté avec étiquette, en commutation MPLS, permettant d'acheminer dans le réseau une transaction de paquets. Les mécanismes mis en œuvre pour atteindre ces objectifs de qualité de service comprennent différentes méthodes de routage des appels et des connexions, ainsi que les méthodes d'attribution de ressources selon la qualité de service (attribution de largeur de bande, routage par priorité, mise en file d'attente par priorité et rétablissement de transport). La présente annexe a pour objet la fiabilité de ces chemins commutés avec étiquette, exprimée sous la forme d'un niveau de priorité, ainsi que la nécessité de spécifier des niveaux de priorité pour la signalisation de la qualité de service.

La définition de priorités de trafic contribue dans une large mesure à assurer aux usagers des réseaux de télécommunication un niveau acceptable de fiabilité/disponibilité des services. Par exemple, dans un contexte de catastrophe naturelle ou d'attaque de terroristes, les communications d'urgence doivent faire l'objet du plus haut niveau de priorité disponible en matière de contrôle d'admission sur les réseaux téléphoniques publics commutés, ce niveau de priorité est exceptionnel.

La fiabilité/disponibilité requise peut être demandée en termes de niveau de priorité pour une fonction de réseau particulière, qui détermine ensuite l'établissement d'un itinéraire commuté avec étiquette. La mise au point de réseaux par paquets implique deux fonctions réseau du point de vue des priorités:

- le contrôle d'admission de connexion: les politiques de contrôle d'admission privilégient les flux de trafic jugés plus importants par un prestataire de service (communications d'urgence par exemple) en période d'encombrement. Les priorités de contrôle d'admission constituent un moyen de privilégier des chemins commutés avec étiquette selon leur niveau de priorité;
- rétablissement: on définit de façon générale le rétablissement comme une mesure d'atténuation adoptée par un réseau en cas de défaillance. Parmi les méthodes de récupération sur défaillance figurent la commutation de protection automatique pour la protection des lignes/itinéraires et les méthodes de rétablissement de maillage partagé. Les flux de trafic de services à temps critique peuvent exiger un rétablissement de priorité supérieure. Ce type de flux de trafic peut alors être routé par un itinéraire commuté avec étiquette doté d'un niveau de priorité de rétablissement convenablement "marqué".

L'établissement de priorité de trafic doit autoriser la souplesse maximale d'implémentation du point de vue des prestataires de service. Les niveaux de priorité doivent répondre aux conditions suivantes:

- le nombre total de classes de priorité doit être limité afin d'assurer l'évolutivité du système;
- il convient d'éviter les subdivisions à l'intérieur de toute classe de priorité à des fins de simplicité;
- les niveaux de priorité sont relatifs et ne sont pas associés à des paramètres particuliers (par exemple, temps de rétablissement) ni à leurs valeurs;
- pour leurs offres de services les prestataires doivent être autorisés à choisir le nombre de niveaux de priorité parmi les niveaux possibles. Par conséquent, ils peuvent établir des accords sur les niveaux de service (SLA) concernant le traitement de toute classe de priorité, à l'intention de leurs usagers y compris d'autres prestataires de service (interface réseau-réseau).

Pour le trafic de service à l'usager, on distingue quatre niveaux de priorité du point de vue du contrôle d'admission de connexion:

- priorité critique: niveau de priorité exceptionnel réservé aux communications d'urgence à l'intention de tous les prestataires de service, nationaux et internationaux;
- priorité élevée: parmi les exemples de service figurent les services publics, les principaux clients commerciaux, les réseaux privés virtuels;
- priorité normale: à titre d'exemple les services vocaux résidentiels;
- priorité par défaut/au mieux: parmi les exemples de service figurent ceux des fournisseurs d'accès Internet.

Du point de vue ou à des fins de rétablissement du réseau, on distingue trois niveaux de priorité: élevé, normal, et par défaut/au mieux. On peut également citer les exemples de services présentés ci-dessus: notamment les situations d'urgence exigent en principe un niveau de priorité élevé.

Tel qu'indiqué plus haut, un prestataire peut faire des offres de services prioritaires spécifiques en fonction des capacités réseau disponibles et des besoins des usagers; il peut ainsi choisir de proposer des services comportant les quatre priorités de connexion définies ci-dessus, mais seulement deux priorités de rétablissement (haute et normale). D'autre part, un simple fournisseur d'accès Internet peut convenir de proposer uniquement les priorités d'admission de connexion critique et par défaut/au mieux, et la priorité de rétablissement par défaut/au mieux.

Appendice I

Approche globale de qualité de service basée sur un contrôle indépendant des ressources

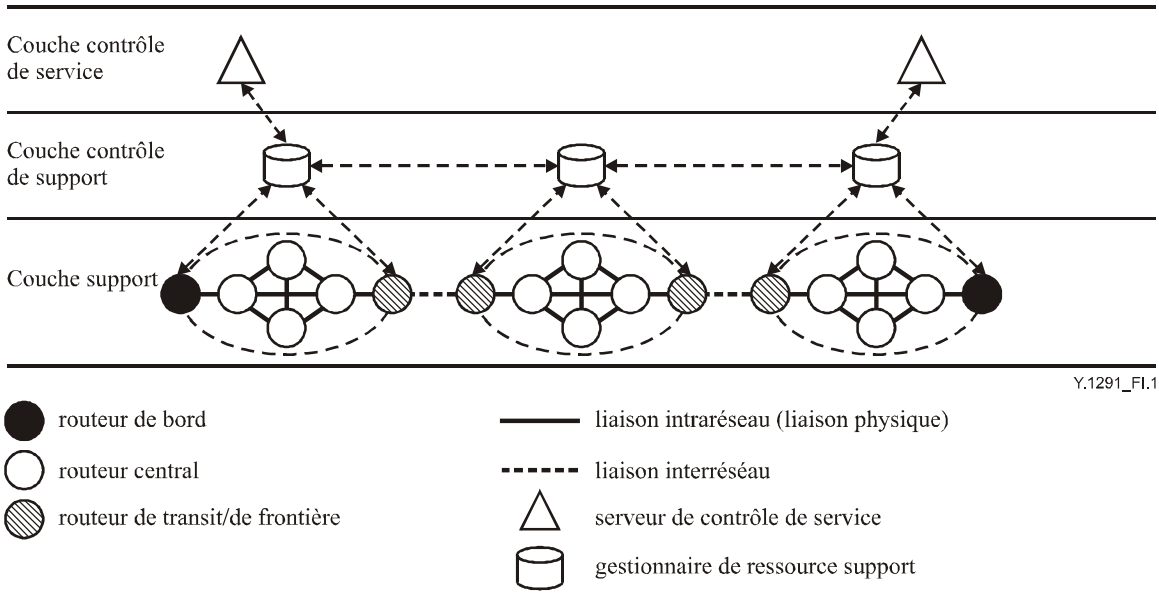


Figure I.1/Y.1291 – Démarche globale de qualité de service fondée sur un contrôle indépendant des ressources

Pour prendre en charge des services comportant différentes exigences de performance sur un seul réseau central IP et pour garantir la qualité de service en mode connexion et en temps réel (téléphonie Internet par exemple), une démarche globale de qualité de service fondée sur un contrôle indépendant des ressources a été élaborée, tel qu'indiqué à la Figure I.1. Cette approche fait conjointement appel à la commutation MPLS, à la méthode DiffServ, à l'ingénierie du trafic et à la gestion des politiques.

Les services exigeant une garantie de qualité de service sont classés par grands types de services (par exemple vocaux) ou selon les niveaux de traitement QS (EF). Afin de faciliter la gestion et la stabilité du réseau, le réseau central IP d'un fournisseur d'accès au réseau est divisé en plusieurs domaines administratifs. Cette division est souple et n'est pas nécessairement identique à celle des domaines de routage. Par exemple, un domaine administratif peut être réduit au point de contenir un seul routeur d'extrémité ou suffisamment étendu pour contenir tout le réseau d'un opérateur.

Un gestionnaire de ressource support (BRM, *bearer resource manager*) désigne une fonction indépendante de contrôle des ressources qui gère l'ensemble des ressources support dans chaque domaine administratif et pourrait être installé dans un ou plusieurs boîtiers. Le gestionnaire BRM enregistre et entretient la base de données sur la topologie et les ressources réseau (NTRD, *network topology and resource database*). En s'appuyant sur les données des NTRD, le gestionnaire BRM procède à l'intérieur du domaine à la sélection des trajets, à l'attribution des ressources et au contrôle d'admission relatif à un flux de service. Les gestionnaires BRM de différents domaines interagissent par le biais de la signalisation afin d'assurer le contrôle des ressources relatif aux flux d'application interdomaines. De plus, un gestionnaire BRM peut assurer également des fonctions telles que la gestion des politiques, la gestion des accords sur les niveaux de service, la taxation du trafic sur les itinéraires commutés avec étiquette et l'interface avec les serveurs AAA d'authentification, d'autorisation et de comptabilité.

Plusieurs types de serveurs de contrôle de service (SCS, *service control servers*) assurent le contrôle des différentes demandes de service (par exemple signalisation d'appel vocal), l'identification du point de départ et d'arrivée de chaque demande de service, la traduction des numéros (ou des noms) en adresses IP, puis l'envoi des demandes de ressources au gestionnaire BRM du domaine d'origine. Dans le cas de services comportant des exigences de qualité de service, mais dépourvus de serveurs de contrôle de service (par exemple services point à point), les hôtes peuvent lancer une demande de service QS par l'intermédiaire du protocole RSVP ou d'autres protocoles de signalisation de la QS. En l'occurrence, le protocole RSVP sert uniquement aux demandes de garantie de qualité de service formulées par les hôtes; or, les routeurs n'ont pas besoin de ce protocole pour procéder aux réservations de ressources flux par flux. L'équipement mis en œuvre pour traiter les demandes de service QS des hôtes peut être considéré comme un type particulier de serveur SCS.

Un gestionnaire BRM reçoit les demandes de ressource du serveur SCS provenant de son domaine administratif ou d'un autre gestionnaire BRM. Après traitement il notifie les réponses au serveur SCS. Simultanément, en cas d'acceptation d'une demande de ressources correspondant à un flux de service, le gestionnaire BRM notifie l'identification du flux, l'itinéraire et les attributs de qualité de service au routeur d'extrémité côté entrée. Le routeur d'extrémité côté entrée identifie, classe, marque, organise, forme et encapsule les paquets d'un flux au moyen des informations de qualité de service spécifiées par le gestionnaire BRM.

Pour les flux de service acheminés par plusieurs fournisseurs d'accès au réseau, il existe généralement entre ces derniers des passerelles d'application et des routeurs de frontière; les ressources de la liaison fixe et les accords SLA interréseaux spécifiés assurent leur interconnexion. Différents fournisseurs d'accès au réseau peuvent mettre en œuvre plusieurs mécanismes de qualité de service au sein de leurs réseaux. Dans ce cas, les gestionnaires BRM gèrent uniquement les ressources de liaison intraréseau, tandis que les passerelles d'application ou les routeurs de frontière gèrent les ressources de liaison interréseaux, en vertu des accords SLA spécifiés, tandis qu'une passerelle d'application ou un routeur de frontière fait office de routeur d'extrémité d'entrée ou de sortie.

Les modules appropriés associés à cette approche comprennent pratiquement tous les modules représentés à la Figure 1. Le gestionnaire BRM fait office de plan contrôle et de plan gestion matériellement indépendants. Les modules interagissent essentiellement par la signalisation flux par flux et sur la base d'une gestion de ressource propre à chaque réseau support logique. Il existe une interface de signalisation entre le plan contrôle et le plan données.

I.1 Souplesse d'implémentation des réseaux par paquets avec prise en charge de la commutation MPLS

On suppose en l'occurrence que les réseaux de base IP prennent en charge la commutation MPLS sensible au mécanisme DiffServ.

La technologie MPLS LSP est mise en œuvre afin de préconfigurer un réseau support logique (LBN, *logical bearer network*) pour chaque classe de service utilisant le réseau IP infrastructurel, manuellement ou automatiquement, par le protocole RSVP-TE ou CR-LDP. Pour les flux de service d'une classe déterminée, la sélection de l'itinéraire, l'attribution de ressources, le contrôle d'admission et la transmission des étiquettes sont pris en charge dans le cadre d'un seul et même réseau support logique. La planification de la topologie et la réservation de largeur de bande de chaque réseau support logique dépendent des données de taxation et de prévision du trafic, des politiques administratives et des accords SLA, dont l'ajustement peut se faire automatiquement ou manuellement selon les besoins de protection des itinéraires LSP, de modification de la capacité ou d'optimisation de la performance du réseau conformément aux contraintes d'ingénierie du trafic.

Dans les limites des ressources résiduelles des réseaux sous-jacents par paquets, le trafic BE sans spécification de qualité de service reste acheminé et transmis par les méthodes classiques de routage et de transmission IP, avec ou sans mécanisme DiffServ.

Le gestionnaire BRM enregistre et entretient une base de données sur la topologie et les ressources réseau (NTRD, *network topology and resource database*) pour chaque réseau support logique. En fonction des NTRD et des politiques adoptées, le gestionnaire BRM effectue à l'intérieur du domaine la sélection des itinéraires, l'attribution des ressources et le contrôle d'admission, pour un flux de service à l'intérieur du réseau support logique correspondant. Comme pour les ressources restantes des réseaux sous-jacents par paquets, le gestionnaire BRM pourrait également procéder aux tâches d'attribution de ressource et de contrôle d'admission.

L'information d'itinéraire QS pour un flux spécifié par un gestionnaire BRM se compose d'une pile d'étiquettes multicouches représentant un ensemble de chemins LSP concaténés. Le routeur d'extrémité encapsule les paquets avec cette pile d'étiquettes, grâce à laquelle les routeurs de transit intermédiaires transmettent les paquets d'un flux le long de l'itinéraire spécifié compte tenu de la pile d'étiquettes et des priorités indiquées.

I.2 Souplesse d'implémentation des réseaux par paquets sans prise en charge de la commutation MPLS

Le contrôle d'admission et la réservation de ressources sont impliqués de façon dynamique avec réservation des ressources liaison par liaison; la couche support n'a alors pas besoin de la capacité MPLS. Le routage et la transmission de l'ensemble du trafic sont contrôlés par les protocoles classiques de routage IP et par le mécanisme IP Diffserv.

Le gestionnaire BRM est déployé afin de gérer directement l'ensemble des ressources de liaison physique à l'intérieur de chaque domaine administratif. Il détient et entretient une base de données NTRD. En fonction des données de la NTRD, le gestionnaire BRM procède à l'exploration du routage, à la réservation de ressources liaison par liaison et au contrôle d'admission pour chaque flux exigeant une QS garantie. Lorsqu'un flux est admis avec un niveau de priorité élevé, il ne perturbe pas les autres flux de trafic.

I.3 Souplesse d'implémentation en cas de contrôle de ressources réparties

Dans ce cas, les réseaux supports logiques sont constitués de liaisons virtuelles (appelées conduits QS) reliant les paires de routeurs d'extrémité d'entrée et de sortie, dans un domaine de réseau. Un conduit QoS est établi afin d'acheminer des flux agrégés d'un service ou d'une classe spécifique de qualité de service.

Si la fonction BRM est implémentée dans des routeurs d'extrémité, le contrôle des ressources flux par flux est réparti aux bords. La fonction de contrôle de ressources (RCF, *resource control fonction*) assurée dans les routeurs d'extrémité met à jour le tableau d'état des ressources des conduits QS correspondants et procède par conséquent aux tâches de contrôle d'admission et d'attribution de ressources. Elle traite par ailleurs la signalisation de qualité de service.

Le système de gestion du réseau peut implémenter un ajustement manuel ou automatique à moyen terme ou à long terme des conduits QS.

Appendice II

Système de renforcement des priorités

Le système de renforcement des priorités (PPS, *priority promotion scheme*) est un nouveau système de contrôle du trafic encore au stade expérimental. En bref, le système PPS met à profit une forme de contrôle d'admission pour réaliser une qualité de service de bout en bout dans un réseau par paquets. Les principales applications d'un système de ce type concernent les services multimédias interactifs, tels que la téléphonie par Internet, les conversations vidéo et la visioconférence. En particulier, le système repose sur la mesure de bout en bout des ressources réseau par les systèmes d'extrémité. Avant l'établissement d'une session ou même pendant une session, le système d'extrémité source détecte, mesure ou vérifie la disponibilité des ressources réseau en envoyant des paquets d'un niveau de priorité inférieur d'une unité à celui des paquets normaux. Il en résulte une modification de la valeur du point de code des services différenciés (DSCP, *DiffServ Code Point*) des paquets IP suivants: la priorité est renforcée ou accrue afin de mieux établir la session, abaissée pour laisser des ressources à la disposition des sessions actuelles ou modifiée de manière à ce que le nombre de paquets ne dépasse pas la capacité disponible. Le réseau, c'est-à-dire les liaisons de sortie des routeurs ou les commutateurs L2, est simplement censé prendre en charge le type de contrôle de priorité classe par classe associé à l'architecture DiffServ. L'observation par tous les systèmes d'extrémité du comportement ci-dessus permet d'obtenir une qualité de service de bout en bout, sans devoir maintenir des états flux par flux dans les nœuds de réseau.

BIBLIOGRAPHIE

[IETF RFC 1633] BRADEN (R.), *et al*.: Integrated Services in the Internet Architecture: an Overview, juin 1994.

[IETF RFC 2205] BRADEN (R.), *et al*.: Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification, septembre 1997.

[IETF RFC 2309] BRADEN (R.), *et al*.: Recommendations on Queue Management and Congestion Avoidance in the Internet, avril 1998.

[IETF RFC 2386] CRAWLEY (E.), *et al*.: A Framework for QoS-based Routing in the Internet, août 1998.

[IETF RFC 2474] NICHOLS (K.), *et al*.: Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers, décembre 1998.

[IETF RFC 2748] DURHAM (D.), *et al*.: The COPS (Common Open Policy Service) Protocol, janvier 2000.

[IETF RFC 2753] YAVATKAR (R.), *et al*.: A Framework for Policy-based Admission Control, janvier 2000.

[IETF RFC 2990] HUSTON (G.): Next Steps for the IP QoS Architecture, novembre 2000.

[IETF RFC 2996] BERNET (Y.): Format of the RSVP DCLASS Object, novembre 2000.

[IETF RFC 2998] BERNET (Y.), *et al*.: A Framework for Integrated Services Operation over Diffserv Networks, novembre 2000.

[IETF RFC 3031] ROSEN (E.), *et al*.: Multiprotocol Label Switching Architecture, janvier 2001.

[IETF RFC 3032] ROSEN (E.), *et al*.: MPLS Label Stack Encoding, janvier 2001.

[IETF RFC 3198] WESTERINEN (A.), *et al*.: Terminology for Policy-Based Management, novembre 2001.

[IETF RFC 3209] AWDUCHE (D.), *et al*.: RSVP-TE: Extensions to RSVP for LSP Tunnels, décembre 2001.

[IETF RFC 3261] ROSENBERG (J.), *et al*.: SIP: Session Initiation Protocol, juin 2002.

[IETF RFC 3270] LE FAUCHEUR (F.), *et al*.: Multi-Protocol Label Switching (MPLS) Support of Differentiated Services, mai 2002.

[IETF RFC 3272] AWDUCHE (D.): Overview and Principles of Internet Traffic Engineering, mai 2002.

[Jacobson, 1988] JACOBSON (V.): Congestion Avoidance and Control*, Proceedings of ACM SIGCOMM'88*, pp. 314-329, août 1988.

[Lin *et al*., 1997] LIN (D.), MORRIS (R.): Dynamics of Random Early Detection*, Proceedings of ACM SIGCOMM'97*, pp. 127-138, septembre 1997.

[Chen] CHEN (Shigang), NAHRSTEDT (Klara): An Overview of Quality-of-Service Routing for the Next Generation High-Speed Networks: Problems and Solutions*, IEEE Network, Special Issue on Transmission and Distribution of Digital Video*, Vol. 12, No. 6, pp. 64-79, novembre/décembre 1998.

[Apostolopoulos] APOSTOLOPOULOS (D.), *et al*.: Intra domain QoS Routing in IP Networks: A Feasibility and Cost Benefit Analysis, *IEEE Network*, Vol. 13, No. 5, pp. 42, septembre/octobre 1999.

[Floyd] FLOYD (S.), JACOBSON (V.): Random Early Detection Gateways for Congestion Avoidance, *IEEE/ACM Transactions on Networking*, Vol. 1, No. 4, pp. 397-413, août 1993.

[Nagle] NAGLE (J.): On Packet Switches with Infinite Storage. *IEEE Trans. on communications*, Vol. COM-35, pp. 435-438. avril 1987.

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série B	Moyens d'expression: définitions, symboles, classification
Série C	Statistiques générales des télécommunications
Série D	Principes généraux de tarification
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	RGT et maintenance des réseaux: systèmes de transmission, circuits téléphoniques, télégraphie, télécopie et circuits loués internationaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	Réseaux de données et communication entre systèmes ouverts
Série Y	**Infrastructure mondiale de l'information, protocole Internet et réseaux de nouvelle génération**
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2005