Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

O.211

(01/2006)

SÉRIE O: SPÉCIFICATIONS DES APPAREILS DE MESURE

Appareils de mesure pour réseaux IP

Equipements de test et de mesure pour les essais au niveau de la couche IP

Recommandation UIT-T O.211

RECOMMANDATIONS UIT-T DE LA SÉRIE O

SPÉCIFICATIONS DES APPAREILS DE MESURE

Généralités	O.1–O.9
Accès pour la maintenance	O.10–O.19
Systèmes de mesure automatiques et semi-automatiques	O.20–O.39
Appareils de mesure des paramètres analogiques	O.40–O.129
Appareils de mesure des paramètres numériques et analogiques/numériques	O.130–O.199
Appareils de mesure des paramètres des canaux optiques	O.200–O.209
Appareils de mesure pour réseaux IP	**O.210–O.219**

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

Recommandation UIT-T O.211

Equipements de test et de mesure pour les essais au niveau de la couche IP

Résumé

Dans la présente Recommandation sont définis une signature de la mesure de la qualité de fonctionnement au niveau de la couche du protocole Internet (IPPMS, *IP performance measurement signature*) et les paquets de test destinés à la mesure de la qualité et de la disponibilité des services de réseau IP dans l'ensemble des domaines administratifs, dans les réseaux composites et au niveau des dispositifs hétérogènes. La signature IPPMS peut être employée pour assurer la configuration et la maintenance des réseaux employant tant la version 4 du protocole Internet (IPv4) que la version 6 (IPv6).

Source

La Recommandation UIT-T O.211 a été approuvée le 13 janvier 2006 par la Commission d'études 4 (2005-2008) de l'UIT-T selon la procédure définie dans la Recommandation UIT-T A.8.

Mots clés

Mesure active, qualité de fonctionnement de réseau.

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

Recommandation UIT-T O.211

Equipements de test et de mesure pour les essais au niveau de la couche IP

1 Domaine d'application

Afin d'assurer la configuration et la maintenance des réseaux employant le protocole Internet (IP, *Internet protocol*), il est souhaitable de disposer d'un format normalisé commun de paquets IP de test de sorte qu'il puisse y avoir *interopérabilité* des équipements d'essai et comparaison des résultats de mesure. Les mesures de la qualité de fonctionnement des réseaux et des services, employant la version 4 du protocole Internet (IPv4) et la version 6 (IPv6), exigent, pour différents types de paquets (type-P), l'interopérabilité des équipements des divers constructeurs. Sont concernées dans l'ensemble des domaines administratifs ou dans les réseaux composites les mesures des paramètres définis dans les Recommandations UIT-T Y.1540 [4] et M.2301 [1] (taux d'erreurs sur les paquets IP (IPER, *IP packet error ratio*), taux de perte de paquets IP (IPLR, *IP packet loss ratio*), temps de transfert des paquets IP (IPTD, *IP packet transfer delay*), variation du temps de propagation des paquets IP (IPDV, *IP packet delay variation*), bloc de perte grave de paquets IP (IPSLB, *IP packet severe loss block*), taux de reclassement des paquets IP (IPRR, *IP packet reordering ratio*)). Le format des paquets devrait faciliter non seulement l'exécution des mesures au sein des domaines d'opérateurs mais aussi l'identification du responsable des essais chargé de la mesure.

Ceci est analogue aux prescriptions, précédemment énoncées dans les Recommandations UIT-T O.181 [2] et O.191 [3], qui ont été faites au niveau de la couche de réseau à hiérarchie numérique plésiochrone (PDH, *plesiochronous digital hierarchy*)/hiérarchie numérique synchrone (SDH, *synchronous digital hierarchy*) (couche 1) et en mode de transfert asynchrone (ATM, *asynchronous transfer mode*) (couche 2). Le paquet de test doit contenir les informations appropriées que nécessite la mesure des principaux paramètres de performance des réseaux définis dans les Recommandations UIT-T Y.1540 [4] et M.2301 [1].

La présente Recommandation porte sur la mesure de la qualité des services de réseau IP.

Les techniques de mesure doivent aussi permettre la prise en charge des critères mesurables définis par les Commissions d'études 2, 4, 9, 12, 13, 15 et 16 de l'UIT-T, par le groupe de travail T1A1 de l'Alliance pour des solutions industrielles de télécommunication (ATIS, *Alliance for telecommunications industry solutions*), par le groupe de travail chargé de l'harmonisation des télécommunications et du protocole Internet dans l'ensemble des réseaux (TIPHON, *Telecommunications and Internet protocol harmonization over networks*) de l'Institut européen des normes de télécommunication (ETSI, *European telecommunications standards institute*), par l'Institut européen de recherche et d'études stratégiques pour les télécommunications (EURESCOM, *European institute for research and strategic studies in telecommunications*), par le Projet de partenariat de la troisième génération (3GPP, *Third generation partnership project*) et par le Groupe de travail d'ingénierie Internet (IETF, *Internet engineering task force*).

Le but recherché est de normaliser la signature de la mesure de la qualité de fonctionnement en mode IP (IPPMS, *IP performance measurement signature*) et les paquets de test destinés à la mesure de la qualité et de la disponibilité des services de réseau IP dans l'ensemble des domaines administratifs, dans les réseaux composites et au niveau des dispositifs hétérogènes. La couche IP prend en charge de très nombreux services en mode IP différents dont les prescriptions en matière de qualité de fonctionnement sont différentes. Les paquets de test doivent donc être, dans la mesure du possible, *représentatifs des services* acheminés par les couches IPv4 et/ou IPv6 au cours des essais de démarrage, de la maintenance, de la recherche de pannes ou de la surveillance des accords de niveau de service (SLA, *service level agreement*).

La présente Recommandation n'a pas pour objet de spécifier comment les mesures sont effectuées ni comment il y est mis fin, et encore moins de définir comment les résultats de mesures sont gérés. Néanmoins, la signature de la mesure doit pouvoir permettre d'identifier une mesure et son initiateur.

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.

[1] Recommandation UIT-T M.2301 (2002), *Objectifs de qualité de service et procédures de mise en service et de maintenance des réseaux à protocole Internet.*

[2] Recommandation UIT-T O.181 (2002), *Appareils utilisés pour l'évaluation des caractéristiques d'erreur sur les interfaces STM-N.*

[3] Recommandation UIT-T O.191 (2000), *Equipement d'évaluation des caractéristiques de transfert de cellules de la couche ATM.*

[4] 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.*

[5] Recommandation UIT-T Y.1541 (2006), *Objectifs de qualité de fonctionnement pour les services en mode IP.*

[6] Recommandation UIT-T Y.1241 (2001), *Prise en charge des services de type IP utilisant les capacités de transfert IP.*

[7] Recommandation UIT-T I.353 (1996), *Evénements de référence permettant de définir les paramètres de performance du RNIS et du RNIS-LB.*

[8] Recommandation UIT-T G.7041/Y.1303 (2005), *Procédure générique de tramage.*

[9] Recommandation UIT-T M.1400 (2004), *Désignations des interconnexions entre opérateurs de réseau.*

[10] IETF RFC 4148 (2005), *IP Performance Metrics (IPPM) Metrics Registry.*

[11] ISO 3166-1:1997, *Codes pour la représentation des noms de pays et de leurs subdivisions – Partie 1: Codes pays*.

3 Définitions

Les définitions suivantes sont reprises de la Rec. UIT-T Y.1241 [6].

3.1 service en mode IP: service fourni par le plan de service à un utilisateur final (par exemple un serveur (système final) ou un élément de réseau), qui utilise les capacités de transfert en mode IP ainsi que les fonctions de commande et de gestion associées, en vue de fournir les informations utilisateur spécifiées par les accords de niveau de service.

3.2 service de réseau IP: service de transmission de données au cours duquel les données transmises à travers l'interface entre l'utilisateur et le fournisseur sont acheminées sous la forme de paquets IP (protocole Internet), parfois appelés datagrammes. Ce service inclut l'utilisation des capacités de transfert en mode IP.

3.3 capacité de transfert en mode IP: ensemble des capacités de réseau fournies par la couche IP. Cette capacité peut être caractérisée par le contrat de trafic ainsi que par les attributs de qualité de fonctionnement pris en charge par les fonctions de commande et de gestion des couches de protocole sous-jacentes.

Dans la Rec. UIT-T Y.1540 [4] sont données les définitions suivantes du service en mode IP de bout en bout et du point de mesure (MP, *measurement point*).

3.4 service en mode IP de bout en bout: service qui, dans le cadre de la présente Recommandation, concerne le transfert de datagrammes IP produits par l'utilisateur (appelés dans la présente Recommandation paquets IP) entre deux serveurs terminaux spécifiés par leur adresse IP complète.

3.5 point de mesure: frontière entre un serveur et une liaison adjacente, au niveau de laquelle il est possible d'observer et de mesurer des événements de référence en matière de qualité de fonctionnement. Conformément à la Rec. UIT-T I.353 [7], les protocoles Internet normalisés peuvent être observés aux points de mesure de la qualité de fonctionnement en mode IP. Dans la Rec. UIT-T I.353 sont données d'autres informations sur les points de mesure pour services numériques.

3.6 type-P: notion indiquant le type de paquet, introduite dans la norme RFC 2330 en vue de la définition d'un cadre de mesure de la qualité de fonctionnement. Cette notion correspond à la suite de protocoles présents dans les en-têtes liés à la couche IP et à la couche en dessous de celle-ci (SUB-IP, *sub-IP layer*) du paquet. Un type-P correspond à une liste de noms d'identificateurs de protocoles. Les noms des identificateurs de protocoles pour le protocole Internet sont définis dans la norme RFC 2896 de l'IETF. A titre d'exemple, le type-P ip.udp.snmp diffère du type-P ip.ip6.udp.snmp parce que ce dernier ne correspond pas seulement à un paquet SNMP sur IPv6 mais aussi à un paquet IPv6 encapsulé sur IP. Cette définition n'est employée dans la présente Recommandation qu'en vue de donner des exemples clairs d'encapsulation.

3.7 signature de mesure de qualité de fonctionnement en mode IP: un paquet IP de test est un paquet IP normal qui contient un bloc normalisé de champs nécessaires à la mesure. Ce bloc de champs est appelé signature de mesure de qualité de fonctionnement en mode IP (IPPMS, *IP performance measurement signature*).

4 Abréviations

La présente Recommandation utilise les abréviations suivantes:

3GPP projet de partenariat de la troisième génération (*third generation partnership project*)

ATIS alliance pour des solutions industrielles de télécommunication (*Alliance for telecommunications industry solutions*)

ATM mode de transfert asynchrone (*asynchronous transfer mode*)

BGP protocole de passerelle limite (*border gateway protocol*)

CAC contrôle d'admission de connexion (*connection admission control*)

CIF format de l'identificateur du contrôleur (*controller identifier format*)

CRC contrôle de redondance cyclique (*cyclic redundancy check*)

CRC32	contrôle de redondance cyclique à 32 bits (*32-bit cyclic redundancy check*)
DiffServ	services différenciés (*differentiated services*)
DoS	déni de service (*denial of service)*
DSCP	point de code des services différenciés (*differentiated service code point*)
DST	destination
ETSI	Institut européen des normes de télécommunication (*European telecommunications standards institute*)
EURESCOM	Institut européen de recherche et d'études stratégiques pour les télécommunications (*European institute for research and strategic studies in telecommunications*)
FR	relais de trame (*frame relay*)
FTP	protocole de transfert de fichiers (*file transfer protocol*)
HTTP	protocole de transfert hypertexte (*hyper text transfer protocol*)
ICMP	protocole de messages de commande Internet (*Internet control message protocol*)
ID	identificateur
IETF	Groupe de travail d'ingénierie Internet (*Internet engineering task force*)
IntServ	service intégré (*integrated service*)
IP	protocole Internet (*Internet protocol*)
IPDR	taux de rejet des paquets IP (*IP packet discard rate*)
IPDV	variation du temps de propagation des paquets IP (*IP packet delay variation*)
IPER	taux d'erreurs sur les paquets IP (*IP packet error ratio*)
IPLR	taux de perte de paquets IP (*IP packet loss ratio*)
IPOD	domaine de l'opérateur IP (*IP operator domain*)
IPPM	mesure de qualité de fonctionnement en mode IP (*IP performance metrics*)
IPPMS	signature de mesure de qualité de fonctionnement en mode IP (*IP performance measurement signature*)
IPRTD	temps aller-retour des paquets IP (*IP packet round trip delay*)
IPRR	taux de reclassement des paquets IP (*IP packet reordering ratio*)
IPSLBR	taux de perte grave de paquets IP (*IP packet severe loss block ratio*)
IPTD	temps de transfert des paquets IP (*IP packet transfer delay*)
IPv4	version 4 du protocole Internet
IPv6	version 6 du protocole Internet
LL	couches inférieures (*lower layers*)
MIB	base d'informations de gestion (*management information base*)
MP	point de mesure (*measurement point*)
MPEG	Groupe d'experts des images animées (*moving picture experts Group*)
MTTR	temps moyen de réparation (*mean time to restore*)
NAT	traduction des adresses de réseau (*network address translation*)

NTP	point de terminaison de réseau (*network termination point*)
OBGR	routeur de passerelle frontière de l'opérateur (*operator border gateway router*)
PAM	mesure passive et active (*passive and active measurement*)
PAT	traduction des adresses de protocole (*protocol address translation*)
PDH	hiérarchie numérique plésiochrone (*plesiochronous digital hierarchy*)
PDU	unité de données protocolaire (*protocol data unit*)
PING	sondeur interréseau (Internet) de paquets (*packet internetwork (Internet) grouper*)
PPP	protocole point à point (*point-to-point protocol*)
QS	qualité de service
RMON	surveillance à distance du réseau (*remote network monitoring*)
RTP	protocole de transport en temps réel (*real time transport protocol*)
SDH	hiérarchie numérique synchrone (*synchronous digital hierarchy*)
SDU	unité de données de service (*service data unit*)
SLA	accord de niveau de service (*service level agreement*)
SN	numéro d'ordre (*sequence number*)
SRC	source
STM-N	module de transport synchrone de niveau N (*synchronous transport module, level N*)
SUB-IP	couche en dessous de la couche IP (*sub IP layer*)
TCP	protocole de commande de transmission (*transmission control protocol*)
TIPHON	harmonisation des télécommunications et du protocole Internet dans l'ensemble des réseaux (*telecommunications and Internet protocol harmonization over networks*)
TSC	contrôle du timbre horodateur (*timestamp control*)
TSF	format du timbre horodateur (*timestamp format*)
Tx	émetteur (*transmitter*)
UDP	protocole datagramme d'utilisateur (*user datagram protocol*)
VoIP	voix sur IP (*voice over IP*)

5 Considérations relatives à l'état actuel de la technique

5.1 Sondeur Internet de paquets et utilitaire Traceroute

En employant des méthodes simples telles que celle du sondeur interréseau (Internet) de paquets (PING, *packet internetwork (Internet) grouper*) du protocole de messages de commande Internet (ICMP, *Internet control message protocol*) ou celle de l'utilitaire Traceroute, on ne peut mesurer que les temps aller-retour des paquets IP (IPRTD, *IP packet round trip delay*), le temps dans un sens n'étant bien sûr pas exactement égal à la moitié du temps IPRTD dans un réseau en mode paquets. Deux autres problèmes se posent au sujet de l'emploi du sondeur PING, à savoir que la fonction de réponse au sondeur PING dans les routeurs est de plus en plus souvent désactivée pour réduire les attaques des pirates et les dénis de service, et que, même si elle est activée, le sondeur PING a la priorité la plus faible lors du traitement des paquets par le routeur. Les temps de propagation mesurés par le sondeur PING ne sont donc pas une mesure réelle des temps de

propagation rencontrés par le trafic des clients. En fait, le sondeur PING est seulement un outil permettant une vérification de la connectivité à un niveau de base, certes, mais une vérification bien utile quand même.

5.2 Solutions en vigueur de mesure active

Bien que les systèmes en vigueur de mesure de la qualité de fonctionnement des réseaux et des services en mode IP ne puissent s'appliquer simultanément aux produits de constructeurs différents, leur sémantique et leurs méthodes sont les mêmes. Le paquet de test est placé au-dessus d'un paquet IP normal. La suite de protocoles présents dans l'en-tête IP décrit le type du paquet (type-P). Des informations propres à la mesure sont insérées dans le paquet.

Les paquets de mesure diffèrent par la signification des champs, l'ordre des champs, leur nom, leur unité, leur dimension et l'emplacement des informations d'essai dans les données du paquet. Les champs communs correspondent aux éléments suivants:

– dispositif ayant envoyé le paquet;
– interface ayant envoyé le paquet;
– identificateur du flux auquel appartient le paquet;
– horodatage absolu correspondant au temps de l'envoi du paquet;
– numéro d'ordre du paquet;
– contrôle de redondance cyclique (CRC, *cyclic redundancy check*) ou contrôle CRC calculé pour des champs précédents ou pour le paquet IP entier.

Dans les implémentations en vigueur, les informations relatives aux tests sont insérées soit au début soit à la fin de l'unité de données de service (SDU, *service data unit*) du paquet IP de test.

La Recommandation doit inclure ces deux configurations.

6 Prescriptions s'appliquant à un paquet IP de test et avantages de sa normalisation

Dans la présente Recommandation est défini un format de paquet IP de test à employer lors des essais de configuration et de la maintenance des réseaux, afin d'éprouver les prescriptions en matière de qualité du transfert en mode IP des services en mesurant les critères IP définis dans les Recommandations UIT-T Y.1540 [4] et M.2301 [1].

Dans le présent paragraphe sont examinées les prescriptions générales s'appliquant à un paquet de test normalisé et les avantages qu'il présente.

6.1 Prescriptions générales

Dans la Rec. UIT-T M.2301 [1] sont décrites deux démarches fondamentales de mesure – avec intrusion et sans intrusion.

Les mesures avec intrusion emploient un flux de paquets IP de test pour créer un courant IP sur le chemin à éprouver. Ces paquets de test sont entrelacés entre les deux points de mesure (MP, *measurement point*) avec les flux de trafic normaux ou transmis comme un flux continu de trafic pseudoclient.

Les mesures sans intrusion font appel à l'une des deux méthodes suivantes:

– Surveillance et collecte des données de la base d'informations de gestion (MIB, *management information base*) à partir des éléments de réseau tels que les routeurs, en vue d'une évaluation de la qualité de fonctionnement et de la maintenance.
– Mesure de la qualité de fonctionnement des paquets IP client.

A l'aide des mesures sans intrusion, on ne surveille pas seulement les paquets IP client. On surveille les paquets IP de test comme s'ils faisaient partie du trafic habituel, d'où une démarche de mesure passive et active (PAM, *passive and active mesaurement*). On peut considérer qu'il s'agit d'un "mode mixte" où les paquets sont insérés avec intrusion mais où ils sont surveillés sans intrusion. A titre d'exemple, des sondes ne nécessitant pas d'intrusion, rattachées à des points de mesure clés dans le réseau, tels que les routeurs de passerelle, peuvent surveiller les paquets de test et mesurer la qualité de fonctionnement interdomaine.

Pour mesurer la qualité de service, il est important qu'il y ait interopérabilité des équipements des divers constructeurs et que la mesure du temps de propagation dans un sens et de la perte de paquets dans un sens puisse se faire dans l'ensemble des domaines administratifs et dans les réseaux composites pour des paquets de types-P différents.

En conséquence, la Recommandation doit inclure les deux points importants suivants:

– Lorsque l'on configure le réseau et exécute les essais de démarrage des services, il est essentiel d'employer un flux de paquets IP de test qui simule le type de services d'application devant être pris en charge.

– Les données IP ne sont jamais directement acheminées en mode IP. La circulation des données utilisateur se fait principalement au-dessus des couches de protocole datagramme d'utilisateur (UDP, *user datagram protocol*) ou de protocole de commande de transmission (TCP, *transmission control protocol*), mais pas uniquement.

6.2 Avantages de la normalisation d'un paquet IP de test

La normalisation d'un paquet IP de test présente de nombreux avantages:

– Les services en mode IP peuvent être configurés et démarrés de manière cohérente et la qualité de service (QS) peut être établie en fonction des accords de niveau de service (SLA, *service level agreement*).

– La qualité de fonctionnement du réseau et la qualité de service peuvent être surveillées de manière cohérente et les résultats de mesure peuvent être comparés aux accords SLA et reliés à ceux des différents points de mesure et instruments.

– L'interopérabilité des instruments des différents constructeurs peut être assurée.

– L'interopérabilité des mesures dans l'ensemble des domaines administratifs et dans les réseaux composites peut être assurée.

6.3 Interopérabilité

La définition du paquet IP de test doit être telle qu'il y ait interopérabilité des équipements des différents constructeurs afin que des mesures des critères puissent se faire dans l'ensemble des domaines administratifs et dans les réseaux composites.

Actuellement, dans un essai impliquant des équipements et/ou des domaines administratifs hétérogènes, l'identificateur de la mesure (essentiellement l'identification de la source) établi par la source est dénué de sens pour le collecteur.

Pour augmenter l'interopérabilité, le paquet IP de test doit acheminer des informations permettant d'identifier sans ambiguïté le contrôleur de la mesure.

6.4 Multidiffusion et mobilité en mode IP

Dans la définition il doit être tenu compte de la mesure de la qualité de fonctionnement des services de multidiffusion et des services mobiles en mode IP.

6.5 Coexistence des versions 4 et 6 du protocole Internet

Afin que la mesure de bout en bout puisse se faire, les paquets de test ne doivent pas dépendre de la version du protocole Internet, que ce soit la version 4 (IPv4) ou la version 6 (IPv6).

Les mécanismes de traduction des protocoles permettant de passer de la version IPv4 à la version IPv6 et la coexistence de ces deux versions sont des sources potentielles de non-interopérabilité des mesures.

Dans la mesure du possible, le paquet de test ne doit pas être rejeté par les mécanismes de traduction ou de transition IPv6/IPv4.

6.6 Protocole de transfert

Dans la Figure 1 est représenté un modèle en couches de la qualité de fonctionnement d'un service en mode IP, qui intègre les protocoles UDP et TCP décrits initialement dans la Rec. UIT-T Y.1540 [4].

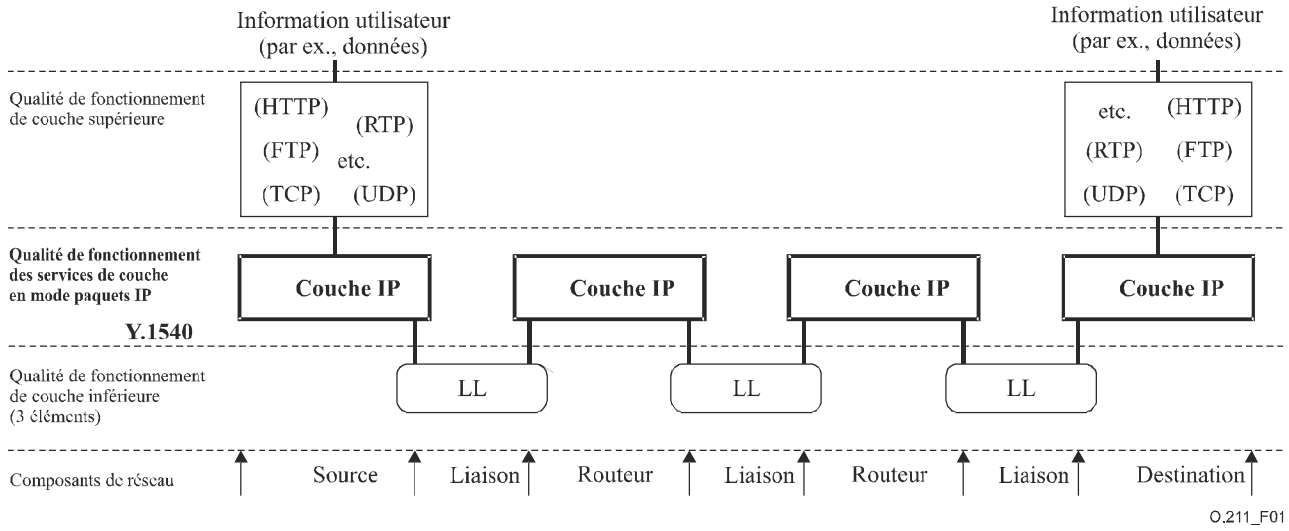

Figure 1/O.211 – Modèle en couches conforme à la Rec. UIT-T Y.1540 de la qualité de fonctionnement d'un service en mode IP – Exemple

Les données IP sont rarement directement acheminées au-dessus de la couche IP. Les informations utilisateur sont habituellement transportées au-dessus des couches UDP ou TCP. En conséquence, le paquet de test doit permettre la mesure de la qualité de fonctionnement des flux UDP et TCP.

Mais les informations utilisateur ne sont pas seulement acheminées au-dessus des couches UDP ou TCP. Actuellement, il existe 46 protocoles qui sont définis pour être encapsulés directement sur IP. La définition du paquet de test devrait, idéalement, permettre la mesure de la qualité de fonctionnement des réseaux et des services en mode IP qui reposent sur ces protocoles.

Il n'entre pas dans le cadre de la présente Recommandation de recenser les protocoles pour lesquels il conviendrait de mesurer la qualité de fonctionnement. Il faudrait par ailleurs tenir compte du fait que de nouveaux protocoles seront définis à l'avenir.

La Recommandation doit donc proposer au moins un paquet de test, souple d'utilisation, qui est destiné à mesurer la qualité de fonctionnement de tout protocole encapsulé directement au-dessus des couches IPv4 ou IPv6.

6.7 Paquet de test représentatif

Afin d'être représentatif d'un service en mode IP, un flux de paquet IP de test doit souvent respecter l'encapsulation de ce service.

La plupart des applications professionnelles, auxquelles il est accédé à partir des bureaux, sont disponibles après avoir traversé une étape de traduction des adresses de réseau (NAT, *network address translation*) ou une étape de traduction des adresses de protocole (PAT, *protocol address translation*) ou après avoir franchi un coupe-feu. Ces applications sont exécutées dans leur majorité au-dessus de la couche TCP, mais pas uniquement:

– Les paquets de test doivent traverser l'étape de traduction NAT/PAT et le coupe-feu comme le font les paquets des services en mode IP.

La qualité de service est principalement assurée au moyen des mécanismes de contrôle d'admission de connexion (CAC, *connection admission control*) qui définissent le point de code des services différenciés (DiffServ, *differentiated services*) dans l'en-tête de chacun des paquets IP. Les routeurs accordent les priorités aux paquets en fonction de la valeur de leurs points de code:

– Le mécanisme de contrôle CAC doit attribuer au paquet de test le même point de code que celui du service dont la qualité de fonctionnement doit être éprouvée par le paquet de test.

Puisque les services en mode IP ne sont pas directement encapsulés sur IP, il n'y a pas lieu de définir un paquet IP de test au niveau IP brut.

6.8 Relations avec d'autres organismes ou forums

L'objectif de la présente Recommandation est d'accroître l'interopérabilité opérationnelle. Pour l'essentiel, cela consiste à promouvoir la nécessité de disposer des mêmes paquets de mesure dans les divers organismes et forums et de réutiliser les normes déjà définies.

6.9 Critères mesurables et paramètres

Dans les Recommandations UIT-T Y.1540 [4] et M.2301 [1] sont définis les critères mesurables de qualité de fonctionnement et les objectifs en matière de qualité de fonctionnement pour les réseaux en mode IP.

Dans le paragraphe 6/M.2301 [1] sont présentées des méthodes de mesure et définis les critères pouvant être mesurés au moyen de paquets de test. La correspondance, mise à jour, est indiquée dans le Tableau 1:

Tableau 1/O.211 – Mesure avec et sans intrusion des paramètres de performance

Paramètre	Avec intrusion	Sans intrusion
IPTD	√	(Note)
IPDV	√	(Note)
IPER	√	√
IPLR	√	√
IPDR		√
NOTE – La variation du temps de propagation des paquets IP (IPDV, IP packet delay variation) et le temps de transfert des paquets IP (IPTD, IP packet transfer delay) peut être calculée à partir d'une mesure sans intrusion. A titre d'exemple, on détecte le même paquet et on le soumet à l'horodatage en deux endroits, puis on recueille les informations et on calcule la différence de temps. Ces techniques sont décrites dans les documents du Groupe de travail chargé de l'échantillonnage des paquets de l'IETF.		

6.9.1 Temps de transfert des paquets IP

Le temps de transfert des paquets IP (IPTD, *IP packet transfer delay*) est un critère mesurable de première importance défini au § 6.2/Y.1540 [4].

Les mesures de la qualité des temps de propagation se font entre deux points de mesure. L'essai consiste à envoyer, d'un bout à l'autre, un flux de paquets horodatés, répartis dans la circulation. On enregistre à quel moment chaque paquet est reçu.

On soustrait le temps d'émission de chaque paquet de son temps de réception pour obtenir le résultat, à savoir le temps IPTD pour ce paquet.

En conséquence, la signature de la mesure de la qualité de fonctionnement en mode IP doit disposer d'un champ d'horodatage absolu.

6.9.2 Variation du temps de propagation des paquets IP

Plusieurs définitions de la variation IPDV sont données dans la Rec. UIT-T Y.1540 [4]. A l'Appendice II/Y.1541 [5], elle est clairement définie comme étant la variation du temps de transfert en mode IP. Il y est employé la même définition que dans la norme RFC 3393.

Pour obtenir la variation IPDV, on soustrait la valeur du temps IPTD la plus petite, obtenue pour un intervalle de mesure, de la valeur IPTD la plus grande, obtenue pour ce même intervalle.

Afin de calculer les erreurs limites sur la mesure de la variation IPDV, la signature IPPMS de l'émetteur doit inclure un champ permettant d'acheminer la précision de l'horloge de l'émetteur.

6.9.3 Taux d'erreurs sur les paquets IP

Le taux d'erreurs sur les paquets IP (IPER, *IP packet error ratio*) est un critère mesurable d'importance secondaire défini au § 6.3/Y.1540 [4].

Les mesures de la qualité en matière d'erreurs se font entre deux points de mesure. L'essai consiste à envoyer, d'un bout à l'autre, un flux de paquets numérotés, répartis dans la circulation. Chaque paquet de test contient des bits de vérification d'erreurs. A l'extrémité où les paquets sont reçus, on vérifie s'ils comportent des erreurs et s'il en manque.

Pour obtenir le taux IPER, le nombre total de paquets erronés est enregistré, de même que le nombre total de paquets reçus. Le rapport des deux valeurs est égal au taux IPER.

Le paquet de test doit acheminer les informations permettant de détecter les erreurs sur les bits dans le paquet lorsqu'il effectue la mesure au niveau IP ou au niveau en dessous de celui-ci.

6.9.4 Taux de perte de paquets IP

Le taux de perte de paquets IP (IPLR, *IP packet loss ratio*) est un critère mesurable d'importance secondaire défini dans au § 6.4/Y.1540 [4].

Pour obtenir le taux IPLR, le nombre total de paquets manquants est enregistré, de même que le nombre total de paquets envoyés. Le rapport des deux valeurs est égal au taux IPLR.

En conséquence, la signature IPPMS doit inclure un champ permettant de numéroter les paquets dans le flux de paquets de test.

6.9.5 Taux de perte grave de paquets

Le taux de perte grave de paquets (IPSLBR, *IP packet severe loss block ratio*) est un critère mesurable d'importance secondaire défini dans au § 6.6/Y.1540 [4].

Le taux IPSLBR exige de longues périodes d'observation. Puisqu'elles peuvent être effectuées sur des liaisons à grande vitesse, elles nécessitent des numéros d'ordre élevés pour indiquer l'ordre des paquets de test. En conséquence, le numéro d'ordre de la signature IPPMS doit avoir une longueur de 32 ou de 64 bits.

6.9.6 Taux de reclassement des paquets IP

Le taux de reclassement des paquets IP (IPRR, *IP packet reordering ratio*) est défini à l'Appendice VII/Y.1540 [4].

Un paquet est incorrect ou reclassé lorsque son numéro d'ordre est inférieur à celui qui lui était destiné.

En conséquence, le numéro d'ordre du paquet dans la définition doit être suffisamment grand pour assurer la numérotation d'un grand nombre de paquets de test. Une longueur de 32 ou 64 bits est appropriée.

6.9.7 Périodes d'indisponibilité conformément à la Rec. UIT-T Y.1540

Dans la Rec. UIT-T Y.1540 sont définis les critères permettant de déclarer certaines périodes comme étant des périodes d'indisponibilité. Le service en mode IP, de bout en bout, est indisponible si le taux IPLR est supérieur ou égal à 75% au cours d'une période d'évaluation de 5 minutes. Ces valeurs sont données à titre provisoire.

L'horodatage doit être suffisamment long pour permettre l'enregistrement pendant une période de 5 minutes.

6.9.8 Considérations en matière de routage des paquets IP

A l'Appendice I/Y.1540 est introduite la nécessité de mesurer l'influence du routage en mode IP sur la qualité de fonctionnement dans ce mode.

Comme la durée de convergence pour le protocole de passerelle limite (BGP, *border gateway protocol*) est proche de 30 s, un champ d'horodatage d'une longueur de 64 bits est approprié.

6.9.9 Détection des paquets

La signature IPPMS doit prévoir un mode facilitant la détection des paquets de test dans les nœuds intermédiaires traversés par le flux des paquets de test.

7 Cadre pour les paquets destinés à la mesure de la qualité de fonctionnement en mode IP

Le but est de normaliser une signature de paquet afin de mesurer la qualité de fonctionnement et la disponibilité des réseaux et des services en modes IPv4 et IPv6 dans l'ensemble des domaines administratifs, dans les réseaux composites et au niveau des dispositifs hétérogènes.

La première étape consiste à définir un bloc d'informations commun, la signature IPPMS.

La deuxième étape consiste à spécifier les paquets de test conformément aux prescriptions et aux contraintes, la principale contrainte étant de tenir compte de l'emplacement de la signature IPPMS dans le paquet de test.

La définition du cadre doit se faire comme suit:

– Tenir compte de l'état de la mesure, tel qu'il est à ce moment.
– Définir un format assurant l'interopérabilité des plans de mesure des systèmes de mesure des différents constructeurs.
– Définir un format dont la dimension est suffisante pour identifier le contrôleur de la mesure afin de faciliter le dialogue entre les systèmes de mesure et la gestion de la mesure à l'avenir.
– Définir un format qui permette la mesure des paramètres de performance de l'UIT-T, fondés sur la définition des critères mesurables en matière de qualité de fonctionnement en mode IP, qui sont consignés dans la norme RFC 4148 [10].

– Définir un format qui permette la mesure de la qualité de fonctionnement des protocoles IP définis à l'avenir.
– Définir un paquet de test compatible avec le protocole IPv4, avec le protocole IPv6 et avec les deux simultanément.
– Définir un format de paquet de test voisin de celui des paquets envoyés par des applications IP concrètes.
– Définir un format de paquet de test qui puisse être reconnu et traité à grande vitesse.
– Définir un paquet de test qui permette aux constructeurs d'inclure des informations spécifiques tout en préservant l'interopérabilité.

7.1 Examen de l'emplacement de la signature IPPMS dans le paquet de test

La signature IPPMS est conçue pour être insérée soit au début soit à la fin du paquet, comme indiqué dans la Figure 2.

IP	Encaps 1	Encaps2...	Données	IPPMS Extensions	IPPMS
Suite d'en-têtes: Longueur variable			Longueur variable	Longueur variable	Longueur fixe

(a) Signature IPPMS à la fin de l'unité SDU IP

IP	Encaps 1	Encaps2...	IPPMS	IPPMS Extensions	Données	En-queue (le cas échéant)
Suite d'en-têtes: Longueur variable			Longueur fixe	Longueur variable	Longueur variable	Longueur variable

(b) Signature IPPMS au début de l'unité SDU d'application

Figure 2/O.211 – Possibilités de formats de paquet IP de test

Lorsque des informations relatives à l'essai sont insérées au début de l'unité de données de type-P, les émetteurs et les récepteurs doivent convenir du type-P avant la mesure.

Lorsque ces informations relatives à l'essai sont insérées à la fin du paquet IP, son emplacement ne dépend pas du type-P, à condition que cette unité PDU de type-P n'ait pas d'en-queue. En conséquence, les émetteurs, les nœuds intermédiaires et les récepteurs n'ont pas à convenir du type-P avant la mesure.

Exemple:

Dans l'exemple suivant, nous considérons un paquet de test pour le protocole de transport en temps réel (RTP, *real time transport protocol*). Son type-P est IP.UDP.RTP.

La signature IPPMS est placée au début de l'unité SDU de type-P

L'émetteur envoie le paquet de test suivant: IP.UDP.RTP.IPPMS.data. Etant donné que le récepteur dispose de capacités d'analyse du niveau UDP seulement, il recherchera la signature IPPMS au début de l'unité SDU UDP plutôt qu'au début de l'unité SDU RTP et, en conséquence, il ne décodera pas le paquet comme étant un paquet de test valable.

La signature IPPMS est placée à la fin du paquet IP

L'émetteur envoie le paquet de test suivant: IP.UDP.RTP.data.IPPMS. Le récepteur, recherchant la signature IPPMS à la fin de l'unité SDU IP, la reconnaîtra.

7.1.1 Signature placée à la fin de l'unité SDU IP

L'insertion de la signature IPPMS à la fin du paquet IP présente de nombreux avantages.

En effet, la spécification du paquet de test ne dépend d'aucun protocole situé au-dessus de la couche IP. En conséquence, il peut représenter tout paquet d'application.

Le paquet IP de test proposé dans la Figure 2 est constitué des éléments suivants:

– une suite d'en-têtes de protocoles IP (par exemple, ip.udp.snmp, ip6.tcp.http…);

– un bloc de données;

– une signature IPPMS.

7.1.2 Signature placée au début de l'unité SDU d'application

Le niveau de l'application détermine l'encapsulation IP et en conséquence l'emplacement de la signature IPPMS dans le paquet. L'insertion de la signature IPPMS au début d'une unité SDU d'application du paquet exige de décider de l'encapsulation nécessaire ou d'analyser la syntaxe des en-têtes de chaque paquet.

La plupart des données utilisateur sont acheminées au-dessus des couches UDP ou TCP.

7.1.2.1 Emplacement du champ de la signature IPPMS

Le champ de la signature IPPMS est situé directement après l'en-tête de l'application dans le paquet IP de test. Comme la longueur de l'en-tête est connue pour un type de point de mesure spécifique, il est très facile de trouver le début du champ de la signature IPPMS.

D'autres avantages du placement de la signature IPPMS directement après l'en-tête sont les suivants:

– alignement automatique à 32 bits simplifiant le traitement en parallèle;

– extension simple du champ normalisé de la signature IPPMS en y adjoignant des éléments d'informations propres au constructeur.

7.1.2.2 Relation entre les mécanismes de type-P et de qualité de service au niveau de la couche IP

Il est tenu compte des prescriptions propres aux services (par exemple, les priorités, les temps maximaux de propagation, etc.) en affectant les applications de bout en bout spécifiques à des classes de qualité de service différentes ou en réservant les ressources de réseau à ces applications exclusivement.

Les routeurs IP peuvent appliquer différents mécanismes en ce qui concerne la qualité de service, tels que ceux pour les services intégrés (IntServ) ou pour les services DiffServ, pour lesquels différentes règles de réexpédition sont appliquées aux différents flux (services IntServ) ou des paquets sont affectés à certaines classes de qualité de service (services DiffServ).

Les décisions de réexpédition pour les services IntServ sont fondées sur l'adresse IP de destination et le numéro du port.

La décision de réexpédition pour les services DiffServ, quant à elle, est fondée sur la valeur du champ du point de code des services différenciés (DSCP, *differentiated service code point*) dans l'en-tête IP. La valeur de ce champ est fixée par le contrôle d'admission de connexion d'un routeur à l'entrée du chemin. Cette valeur est obtenue en analysant l'en-tête du paquet.

7.1.2.3 Représentation au niveau de la couche IP des services de couches supérieures

Les seuls paramètres propres aux applications, à l'exception de l'adresse IP, du numéro de protocole, du numéro de port et du point de code DSCP, qui sont visibles au niveau de la couche IP, sont la longueur du paquet et la configuration du trafic.

Le paquet IP de test doit donc incorporer un champ de données de longueur variable à la suite de la signature IPPMS.

7.1.2.4 Structure d'en-tête fixe

Le paquet de test le plus simple, contenant toutes les informations susmentionnées, possède un format d'en-tête fixe qui comporte un en-tête IP normalisé suivi d'un en-tête UDP.

Ceci est conforme à ce qui se fait par ailleurs concernant les mesures actives dans les réseaux employant des trames (voir les Recommandations UIT-T M.2301 [1], O.181 [2] et O.191 [3]).

7.1.3 Paquet IP brut

L'IETF ne recommande pas d'envoyer des paquets IP bruts. La présente Recommandation propose donc d'employer le type UDP en tant que type-P du paquet de test.

7.1.4 Paquet UDP de test

Dans les applications où des datagrammes sont envoyés vers un serveur, il faut préciser une cible qui est plus spécifique que l'adresse IP, puisque les datagrammes sont normalement dirigés vers certains processus et non vers le système dans son ensemble.

Le protocole UDP, en employant les ports pour diriger les datagrammes, sert simplement de multiplexeur/démultiplexeur pour l'envoi et la réception de ceux-ci.

Le paquet de test IP/UDP a un unique format caractérisé par les éléments suivants:

– une structure d'en-tête fixe pour le paquet IP de test;

– un emplacement fixe de la signature IPPMS, directement après l'en-tête UDP.

Ce format de paquet permet la mesure de la qualité de service en mode IP de bout en bout, telle qu'elle est définie dans la Rec. UIT-T Y.1540 [4].

7.1.5 Protocole de commande de transfert

Les essais de qualité de fonctionnement au-dessus de la couche IP, telle que la qualité de fonctionnement des connexions TCP [4] peuvent exiger plus d'informations dans la trame d'essai.

Le présent paragraphe sera complété ultérieurement.

7.1.6 Paquet de test contenant seulement la signature IPPMS dans la charge utile de type-P

L'insertion d'un bloc de mesure soit au début soit à la fin d'une unité SDU de type-P ne diffère que par l'emplacement de la signature IPPMS dans le paquet.

Quand aucune donnée n'est présente dans l'unité SDU, la signature IPPMS est située tant au début qu'à la fin du paquet de test. Ceci est illustré dans la Figure 3.

Ce cas admet l'interopérabilité des deux modes d'encapsulation.

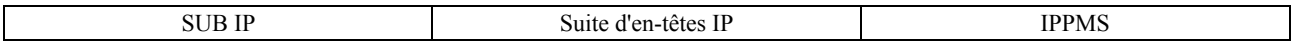

Figure 3/O.211 – Format commun de paquet de test

7.1.7 Résumé des utilisations possibles

Dans le Tableau 2 sont indiquées les diverses possibilités pour l'emplacement de la signature IPPMS dans le paquet de test et leur effet sur l'interopérabilité et la dimension du paquet.

Tableau 2/O.211 – Emplacement de la signature IPPMS

Emplacement de la signature IPPMS	Interoperabilité	Dimension du paquet
1) A la fin de la charge utile	Analyse inutile de la suite d'en-têtes complète	Quelconque
2) Au début de la charge utile	Analyse de la syntaxe de la suite d'en-têtes Connaissance de la structure des en-têtes éventuellement requise	Quelconque
3) Signature IPPMS = charge utile	Avec 1 et 2	Dimension du paquet différente de celle du paquet d'application Petite dimension du paquet seulement

7.1.8 Généralisation au cas de la mesure de la qualité de fonctionnement dans une classe de services

La mesure de la qualité de fonctionnement en mode IP peut nécessiter la présence d'une encapsulation en ce qui concerne le transport ou l'application afin de garantir que les paquets de test soient traités de la même manière que les paquets d'application normaux.

Pour mesurer la qualité de fonctionnement d'une application reposant sur un protocole spécifique, il est recommandé d'employer le format défini au § 7.1.6.

Un paquet de test RTP est présenté, à titre d'exemple, dans la Figure 4.

Figure 4/O.211 – Exemple de paquet de test RTP

On peut employer ce cadre dans les Recommandations où il faut définir des paquets de test pour mesurer la qualité de fonctionnement d'une application de réseau.

NOTE – Certaines encapsulations de protocoles nécessitent un en-queue. Dans ce cas, il peut être nécessaire d'analyser l'en-queue et l'en-tête pour déterminer l'emplacement de la signature IPPMS.

7.1.9 Autres utilisations éventuelles

La signature IPPMS définit un bloc d'informations, destiné à la mesure de la qualité de fonctionnement du réseau et de la disponibilité. En conséquence, il peut être employé pour la mesure de la qualité de fonctionnement des réseaux employant des trames. Dans ce cas, la signature IPPMS peut être insérée directement dans la trame brute sans aucun en-tête IP.

8 Spécification de la signature de la mesure de la qualité de fonctionnement en mode IP

Dans les paragraphes suivants est défini un format de paquet IP de test, y compris un format de trame, et sont données des considérations en matière de charge utile. Il peut en être fait usage pour les mesures avec intrusion de l'aptitude des réseaux IP à prendre en charge le niveau de la qualité de service et, comme stimulus, pour la surveillance sans intrusion de la qualité de fonctionnement en mode IP aux points clés dans le réseau. Il peut aussi en être fait usage pour la vérification des débits à la sortie lorsque les caractéristiques programmables sont mises sur la capacité de transfert IP choisie (contrat de trafic) pour un service d'application donné. Le dispositif d'essai doit disposer d'une connectivité en dessous de la couche IP pour être capable d'envoyer ou de recevoir le trafic IP de test et de mesurer la qualité de fonctionnement du réseau IP et la qualité de service. Ceci peut comporter divers formats de couches de liaison, notamment celles du protocole point à point (PPP, *point-to-point protocol*), du protocole à relais de trame (FR, *frame relay*), du mode de transfert asynchrone (ATM, *asynchronous transfer mode*), du protocole Ethernet, etc. En outre, le dispositif d'essai doit activer chaque service en mode IP avant de mesurer sa qualité.

Le type-P d'un paquet de test est défini par l'encapsulation en dessous de la couche IP et par la suite d'en-têtes IP du paquet.

8.1 Dimension du paquet IP de test

La dimension maximale d'un paquet IP est de 65 535 octets, la dimension par défaut commune étant de 570 octets. Chaque paquet comporte une suite d'en-têtes et des informations relatives à la charge utile. La dimension des suites d'en-têtes IP dépend de la version du protocole Internet et de l'application encapsulée. Le temps de la mise sous forme de paquets et du traitement diminue avec la dimension du paquet. Il s'agit de l'un des facteurs qui affectent la qualité de service.

La dimension des paquets influe sur les résultats obtenus pour la plupart des paramètres de qualité de fonctionnement en mode IP. Une gamme de dimensions de paquets peut être appropriée, parce que nombreux sont les flux dont la dimension varie considérablement. Par exemple, la voix sur IP (VoIP, *voice over IP*) fait appel à de courts paquets tandis que ceux qui sont employés par la vidéo sur IP sont beaucoup plus longs. L'évaluation est toutefois simplifiée avec une dimension unique de paquets, comme c'est le cas lors de l'évaluation de la variation IPDV ou des flux cible qui prennent en charge des sources à débit binaire constant, et il est donc recommandé de fixer la dimension du champ d'informations. Conformément à la définition du temps IPTD dans la Rec. UIT-T Y.1540 [4], le temps d'insertion des paquets est inclus dans les objectifs de performance qui concernent le temps IPTD. Dans la Rec. UIT-T Y.1541 [5], il est proposé d'employer des champs d'informations de 160 ou de 1500 octets, mais, quelle que soit leur dimension, il convient de l'indiquer. Par ailleurs, un champ d'informations de 1500 octets est recommandé pour l'évaluation des paramètres de qualité de fonctionnement IP lors des essais des couches inférieures, tels que la mesure des erreurs sur les bits. Il est suggéré que des paquets IP de test de longueurs fixes de 80, 160, 200, 600 et 1500 octets soient à disposition, en tant que capacité minimale, lors de la simulation du trafic voix sur IP, vidéo et vidéo conforme au Groupe d'experts des images animées (MPEG, *moving picture experts group*).

Pour satisfaire à ces différents besoins, le paquet de test comporte une zone de données qui fait généralement l'objet d'un bourrage pour avoir la longueur requise dans la mesure.

8.2 Durée de la mesure

Dans les Recommandations UIT-T Y.1541 [5] et M.2301 [1] est définie la qualité de fonctionnement en mode IP en fonction de la borne supérieure de chaque paramètre. Dans la Rec. UIT-T Y.1541 [5] il est proposé une durée d'évaluation de 1 minute pour le temps IPTD, la variation IPDV, le taux IPER et le taux IPLR, tandis que dans la Rec. UIT-T Y.1540 [4] il est proposé une durée de mesure de 5 minutes pour la mesure des critères de disponibilité. Dans les Recommandations de l'UIT-T et les procédures d'exploitation, la qualité de fonctionnement est mesurée sur des périodes de 15 minutes, 24 heures, 7 jours ou 1 mois.

Afin de tenir compte des contraintes relatives à la mesure des critères, le timbre horodateur de la signature IPPMS doit prévoir les deux usages différents suivants:

– Le premier usage concerne l'horodatage absolu pour la mesure de la qualité de fonctionnement des réseaux de bout en bout et de la qualité des services à travers divers types d'équipements.
– Le deuxième usage concerne l'horodatage relatif pour la mesure de la qualité de fonctionnement de la liaison.

8.3 Signature de la mesure de la qualité de fonctionnement en mode IP

La signature IPPMS a une longueur de 32 octets.

Elle est une combinaison des éléments d'information suivants:

– contrôle de la signature de la mesure de la qualité de fonctionnement en mode IP (Contrôle IPPMS);
– champ permettant d'identifier le critère à mesurer (Metric_ID);
– champ réservé à un usage ultérieur (Réservé);
– numéro d'ordre (Seq_Number);
– élément d'information sur le timbre horodateur d'émission (Tx_Timestamp);
– identificateur du contrôleur (Controller_ID);
– identificateur d'un flux de paquets de test (Flow_ID);
– champ de protection de la signature IPPMS (CRC32).

Afin de garantir une interopérabilité maximale, il est obligatoire de n'avoir qu'un seul format pour la signature des paquets de test et d'avoir un nombre minimal d'options.

Ci-après est indiquée une proposition de signature de paquet de test. Elle intègre toutes les prescriptions et a une dimension constante de 32 octets. Dans le Tableau 3 sont énumérés les champs de la signature IPPMS.

Tableau 3/O.211 – Eléments d'information de la signature IPPMS

Eléments d'information	Dimension (octets)
Contrôle	2
Metric_ID	1
Réservé	1
Seq_Number	4
Tx_Timestamp	8
Controller_ID	10
Flow_ID	2
CRC32	4

On obtient ainsi un format commun de la signature IPPMS, comme illustré dans la Figure 5.

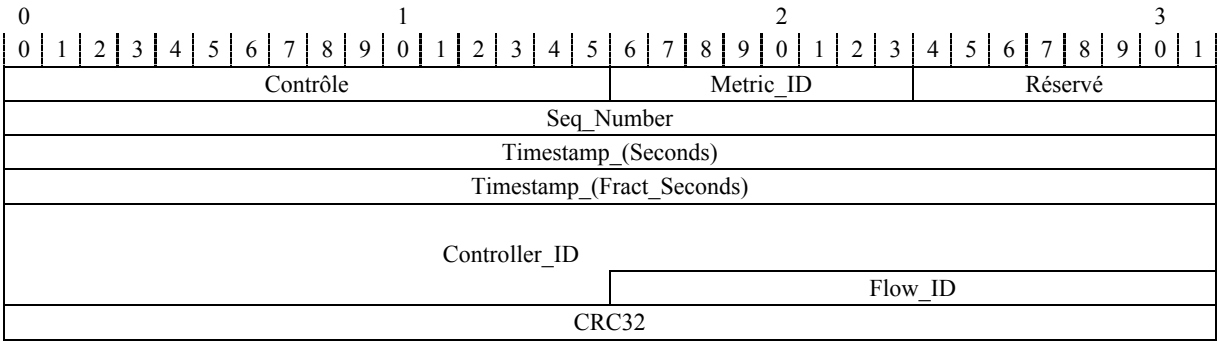

Figure 5/O.211 – Format de la signature IPPMS

8.4 Détails du format de la signature IPPMS

8.4.1 Champ de contrôle de la signature IPPMS (contrôle)

Le champ de contrôle de la signature IPPMS a une longueur de 2 octets. Il est composé de 6 champs:

– format du timbre horodateur (TSF, *timestamp format*);

– contrôle du timbre horodateur de l'horloge qui a envoyé le paquet (TSC, *timestamp control*);

– présence de l'extension (Ext);

– version de la signature IPPMS (Ver);

– format de l'identificateur du contrôleur (CIF, *controller identifier format*);

– champ réservé.

Dans le Tableau 4 sont données les dimensions des différents chanps.

Tableau 4/O.211 – Format de l'en-tête

Champs	Dimension (bits)
Format du timbre horodateur (TSF)	1
Contrôle du timbre horodateur (TSC)	3
Présence de l'extension (Ext)	1
Version (Ver)	2
Format de l'identificateur du contrôleur (CIF)	3
Réservé	6

8.4.1.1 Format du timbre horodateur (TSF)

Ce champ indique si la référence en ce qui concerne le temps du timbre horodateur est absolue ou non.

"0" indique qu'aucun horodatage absolu n'est employé.

"1" indique qu'un horodatage absolu est employé.

8.4.1.2 Contrôle du timbre horodateur (TSC)

Ce champ achemine la précision de l'horloge de l'émetteur. Les différentes valeurs sont énumérées dans le Tableau 5.

Tableau 5/O.211 – Contrôle du timbre horodateur

TSC	Valeur	Signification: la précision de l'horloge est meilleure que:
000	0	La valeur 0 veut dire qu'au moment où le paquet a été envoyé, la source n'était pas synchronisée avec une référence de temps absolue
001	1	10 ns
010	2	50 ns
011	3	500 ns
100	4	10 µs
101	5	50 µs
110	6	500 µs
111	7	≤10 ms

8.4.1.3 Présence de l'extension (Ext)

Ce champ a une longueur de 1 bit.

Des points de mesure peuvent être insérés dans le paquet de test des données propres au constructeur, tout en préservant l'interopérabilité des mesures. Le champ 'Ext' indique la présence d'une telle information.

La valeur 0 indique l'absence d'extension (valeur par défaut).

La valeur 1 indique la présence d'une extension.

Pour mesurer le taux IPER, l'extension doit être protégée au moyen d'une valeur de contrôle CRC32.

8.4.1.4 Version de la signature IPPMS (Ver)

Ce champ a une longueur de 2 bits.

Le champ version, nommé 'Ver', permet de définir jusqu'à quatre versions de signature IPPMS.

Habituellement, le champ 'Ver' a la valeur 0.

8.4.1.5 Format de l'identificateur de contrôle (CIF)

Ce champ a une longueur de 3 bits.

Il définit le type employé de l'identificateur de contrôle. Dans le Tableau 6 sont énumérées les différentes valeurs.

Tableau 6/O.211 – Format de l'identificateur de contrôle

CIF	Valeur	Signification: la valeur du contrôleur employé achemine:
000	0	Réservé
001	1	Un code d'opérateur
010	2	Un numéro d'entreprise de construction
011	3	L'adresse IPv4, le type de protocole et le port du contrôleur
100	4	Les dix premiers octets d'une adresse IPv6 du contrôleur
101	5	Les six derniers octets d'une adresse IPv6, le type de protocole et le port du contrôleur
110	6	Réservé au constructeur
111	7	Réservé

8.4.2 Identificateur des critères mesurables (Metric_ID)

Dans la norme RFC 4148 [10] est défini un registre initial des mesures des critères mesurables de qualité de fonctionnement en mode IP. Il s'agit d'un registre extensible tenu par l'Autorité chargée de l'attribution des numéros Internet (IANA, *Internet assigned numbers authority*), qui attribue à chaque critère mesurable, défini par le groupe de travail chargé des critères IPPM du Groupe de travail d'ingénierie Internet, un numéro d'identification.

L'identificateur Metric_ID a une longueur de un octet. Il achemine l'identificateur du critère IPPM correspondant au paramètre de performance à mesurer.

Une valeur 0 indique que le champ n'est pas employé (valeur par défaut).

Les paquets de test suivants peuvent acheminer la liste des critères (paramètres primaires et secondaires) à mesurer. Cela aide le récepteur à limiter la consommation des ressources.

8.4.3 Réservé

Ce champ a une longueur d'un octet.

Il n'est pas employé dans la version 0 de la signature IPPMS. Le récepteur ne doit pas tenir compte de sa valeur.

8.4.4 Numéro d'ordre (Seq_Number)

La mesure de la perte de paquets nécessite un numéro d'ordre pour recenser les paquets manquants dans la séquence de paquets reçus.

De plus en plus de services IP traversent les passerelles. Ils peuvent modifier les numéros d'ordre des paquets présents dans l'en-tête IP (par exemple, la valeur initiale). Le calcul des critères mesurables repose pour beaucoup sur l'analyse de l'ordre des paquets. Afin d'obtenir une suite fiable de résultats, il faut intégrer le numéro d'ordre dans la signature IPPMS. Le point de mesure doit avoir la possibilité de remplir et de lire le numéro d'ordre. Le numéro d'ordre de la signature IPPMS (Seq_Number) est augmenté d'une unité pour chaque trame d'essai dans une mesure.

Ce champ a une longueur de 32 bits. Il est obligatoire.

8.4.5 Timbre horodateur de l'émetteur (Tx_Timestamp)

Ce champ a une longueur de 64 bits.

Il est employé soit comme un compteur de substitution de 64 bits lorsque le fanion du format TSF de l'élément d'information de contrôle est mis sur 0, ou comme un timbre horodateur au point de terminaison de réseau (NTP, *network termination point*) lorsque le fanion du format TSF est mis sur 1.

8.4.5.1 'Seconds' au point NTP

Il s'agit d'une longueur de champ de 32 bits où sont indiquées les secondes du timbre horodateur au point NTP.

8.4.5.2 'Fract_Seconds' au point NTP

Il s'agit d'une longueur de champ de 32 bits où sont indiquées les fractions de seconde du timbre horodateur au point NTP.

8.4.6 Identificateur du contrôleur (Controller_ID)

Les dispositifs d'essai n'interagissent que s'ils appartiennent à la même entreprise de construction. Pour exécuter la mesure, ils insèrent trois champs, à savoir ceux des éléments suivants:

– dispositif ayant envoyé le paquet;

– interface ayant envoyé le paquet;

– identificateur du flux auquel appartient le paquet.

Un tel cadre ne convient pas à l'interopérabilité des dispositifs d'essai et à l'interopérabilité interdomaine, principalement parce que l'émetteur et le récepteur n'ont pas la même compréhension des notions 'dispositif', 'interface' et 'flux'. En conséquence, dans le cadre d'un essai entre 2 dispositifs d'essai de deux entreprises de construction différentes, chacun des dispositifs emploiera ses propres règles de numérotation pour identifier l'essai. L'interopérabilité est donc impossible, l'identificateur à fournir par le contrôleur de la mesure n'étant pas unique.

Afin qu'il puisse y avoir interopérabilité, il est nécessaire que l'identificateur de l'essai soit choisi par le contrôleur de l'essai. Un dispositif d'essai pouvant être employé simultanément par plusieurs contrôleurs, la signature IPPMS doit acheminer l'identification du contrôleur.

L'identificateur fournit à l'émetteur et au récepteur de la mesure une valeur non ambiguë permettant d'identifier le contrôleur de la mesure faite sur différents domaines administratifs.

Son type dépend de la valeur du champ CIF du champ de contrôle de la signature IPPMS (voir Tableau 6).

Sa valeur et son type varient, dans la suite de paquets, en fonction des paquets. Cela permet de transmettre l'identification complète du contrôleur et en conséquence l'identification du flux.

Plusieurs types sont définis pour identifier complètement le contrôleur de la mesure.

8.4.6.1 Code de l'opérateur

Le code de l'opérateur a une longueur de 10 octets. Son format est le suivant:

– 6 octets pour l'identificateur de l'opérateur défini dans la Rec. UIT-T M.1400 [9];

– 1 octet pour le caractère;

– 3 octets pour le code de pays défini dans la norme ISO 3166-1 [11].

8.4.6.2 Numéro de l'entreprise de construction

Il identifie le constructeur du point de mesure qui envoie les paquets. Cette information accroît l'interopérabilité opérationnelle des différents constructeurs.

Le numéro de l'entreprise de construction doit être mis sur 0 si ce champ n'est pas employé.

8.4.6.3 Adresse IPv4

Cette valeur achemine l'adresse, le type de protocole et le port du contrôleur.

8.4.6.4 Adresse IPv6

Cette valeur achemine l'adresse IPv6, le type de protocole et le port du contrôleur. Ceci se fait en 2 étapes décrites dans la définition du champ CIF (voir Tableau 6).

8.4.6.5 Informations propres au constructeur

Cette valeur achemine des informations propres au constructeur.

8.4.6.6 Utilisation interdomaine et interopérabilité

L'adresse IP du contrôleur et l'identificateur du flux assurent l'identification absolue de la mesure.

Le code de l'opérateur, le numéro de l'entreprise de construction et l'adresse IP du contrôleur sont obligatoires lorsque l'on exécute une mesure entre deux domaines administratifs ou deux constructeurs différents.

8.4.7 Identificateur du flux (Flow_ID)

La signature IPPMS doit inclure un identificateur du flux de paquets de test correspondant à la mesure.

Cet identificateur de flux identifie les paquets de test associés à une mesure.

Il a une longueur de 2 octets.

L'identificateur de flux est attribué par l'initiateur de la mesure.

8.4.8 Protection de la signature IPPMS (CRC32)

Ce champ a une longueur de 32 bits. Sa présence est obligatoire.

Il sert à protéger la signature IPPMS.

L'émetteur calcule une valeur de contrôle CRC32 pour la signature IPPMS et insère le résultat dans les quatre derniers octets du champ 'CRC32'.

Pour vérifier l'intégrité de la signature IPPMS le récepteur calcule aussi la valeur CRC32 et compare le résultat avec celle du champ 'CRC32'. Si les valeurs sont les mêmes, la signature IPPMS ne contient pas d'erreur sur les bits et le paquet reçu est classé comme étant un paquet de test.

Les nœuds intermédiaires peuvent utiliser ce champ pour détecter la présence d'une signature IPPMS dans un paquet.

Le calcul de la valeur CRC32 se fait au moyen du polynôme générateur, défini comme suit:

$$x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$$

Le calcul lui-même se fait selon la méthode décrite dans la Rec. UIT-T G.7041/Y.1303 [8].

9 Paquets IP de mesure pour les niveaux IPv4 et IPv6

Ci-après nous définissons 6 paquets de test satisfaisant à la prescription concernant la mesure de la qualité de fonctionnement de la couche IP entre deux points IP de mesure.

Une charge utile ne peut être directement encapsulée sur la couche IP. Donc, les paquets de test proposés sont en fait des paquets UDP comme illustré dans la Figure 6.

Figure 6/O.211 – Format du paquet de test UDP

Une longueur fixe pour les paquets facilite la détection et l'extraction de la signature IPPMS par les nœuds intermédiaires.

Les dimensions des paquets de test IPv4 sont au minimum les suivantes: 80, 160, 200, 600 et 1500 octets. Vingt octets étant réservés pour l'en-tête IPv4, 8 octets pour l'en-tête UDP et 32 octets pour la signature IPPMS, les nombres d'octets de bourrage correspondants sont respectivement 20, 100, 130, 530 et 1430. Pour améliorer le traitement à grande vitesse, il a été décidé de limiter le bourrage de façon générale à 32 octets. En conséquence, les dimensions des charges utiles employées sont de 52, 132, 164, 564 et 1464.

En outre, nous proposons un paquet de test UDP qui achemine seulement les 32 octets de la signature IPPMS.

9.1 Options en ce qui concerne la signature IPPMS

Le format de la signature IPPMS défini au § 8.3 assure une grande souplesse d'utilisation. Afin d'accroître l'interopérabilité au maximum, les réglages par défaut suivants doivent être appliqués:

– Il n'y a pas d'extension.

– Le champ CIF ne peut acheminer qu'un code d'opérateur (par exemple, interdomaine), et/ou l'adresse IPv4, le type de protocole et le port du contrôleur (par exemple, réparti), et/ou des informations propres au constructeur (par exemple, à usage local).

– La valeur du champ Metric_ID est 0. Le récepteur ne tient pas compte des autres valeurs.

– La configuration de remplissage est la suivante:
  - Toute configuration binaire peut être employée comme configuration de remplissage.
  - Pour les mesures du taux IPER, la configuration de remplissage doit être protégée au moyen du contrôle CRC32 défini au § 8.4.8 qui permet de détecter les erreurs. La valeur de contrôle CRC32 doit être calculée sur les N-4 premiers octets de la configuration de remplissage, où N est la longueur du champ de remplissage. Les 4 derniers octets du champ de remplissage correspondent à la valeur de contrôle CRC32.
  - Le récepteur ne doit pas tenir compte du champ de remplissage pour toutes les autres mesures.

La modification de ces réglages par défaut relève de la responsabilité de la personne chargée des essais et sort du cadre de la présente Recommandation.

9.2 Charge utile de 32 octets (avec la signature IPPMS seulement)

Ce paquet de test est décrit dans la Figure 7.

Figure 7/O.211 – Charge utile de 32 octets

9.3 Charge utile de 52 octets

Ce paquet de test est décrit dans la Figure 8.

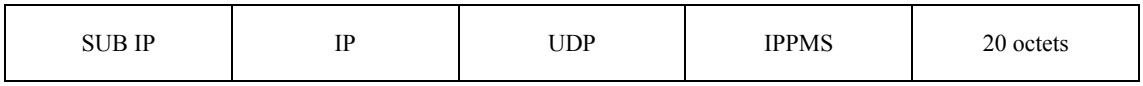

Figure 8/O.211 – Charge utile de 52 octets

9.4 Charge utile de 132 octets

Ce paquet de test est décrit dans la Figure 9.

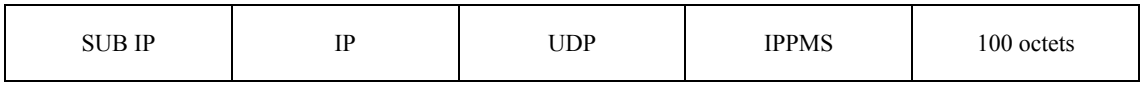

Figure 9/O.211 – Charge utile de 132 octets

9.5 Charge utile de 164 octets

Ce paquet de test est décrit dans la Figure 10.

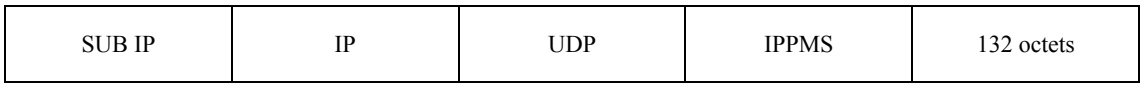

Figure 10/O.211 – Charge utile de 164 octets

9.6 Charge utile de 564 octets

Ce paquet de test est décrit dans la Figure 11.

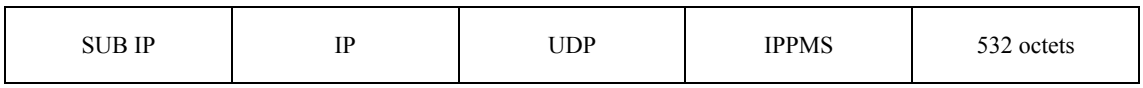

Figure 11/O.211 – Charge utile de 564 octets

9.7 Charge utile de 1464 octets

Ce paquet de test est décrit dans la Figure 12.

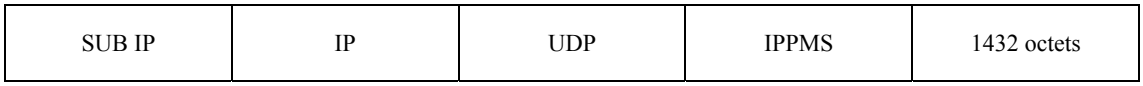

Figure 12/O.211 – Charge utile de 1464 octets

10 Sécurité

Dans la Rec. UIT-T M.2301 [1], il est indiqué qu'il convient de noter que la mesure de la qualité de fonctionnement avec intrusion occasionne un trafic supplémentaire à travers le réseau. Il faut donc veiller à ce que l'exécution de cet essai ne provoque ni encombrement ni perte résultante de paquets du client.

Pour éviter que les systèmes de mesure ne soient employés pour lancer des attaques, il faut impérativement proposer un mécanisme de sécurité permettant de contrôler l'accès à la mise en place des mesures de réseau.

Du point de vue de la sécurité du réseau, l'élément le plus vulnérable en ce qui concerne la sécurité dans une mesure de réseau est le paquet de test de contrôle. La normalisation d'une signature de paquet ne facilite pas la commande ordonnant à une sonde de lancer une attaque par déni de service (DoS, *denial of service*).

BIBLIOGRAPHIE

– IETF RFC 1305 (1992), *Network time protocol (Version 3) specification, implementation and analysis*.

– IETF RFC 2330 (1998), *Framework for IP performance metrics*.

– IETF RFC 2679 (1999), *A one-way delay metric for IPPM*.

– IETF RFC 2680 (1999), *A one-way packet loss metric for IPPM*.

– IETF RFC 2896 (2000), *Remote network monitoring MIB protocol identifier macros*.

– IETF RFC 3919 (2004), *Remote network monitoring (RMON) protocol identifiers for IPv6 and multi protocol label switching (MPLS)*.

– IETF RFC 3393 (2002), *IP packet delay variation metric for IP performance metrics (IPPM)*.

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
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	Gestion des télécommunications y compris le RGT et maintenance des réseaux
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, communication entre systèmes ouverts et sécurité
Série Y	Infrastructure mondiale de l'information, protocole Internet et réseaux de prochaine génération
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2006