

Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

H.248.40

(01/2007)

SÉRIE H: SYSTÈMES AUDIOVISUELS ET
MULTIMÉDIAS

Infrastructure des services audiovisuels – Procédures de
communication

**Protocole de commande de passerelle:
Paquetage de détection d'inactivité des
données d'application**

Recommandation UIT-T H.248.40

RECOMMANDATIONS UIT-T DE LA SÉRIE H
SYSTÈMES AUDIOVISUELS ET MULTIMÉDIAS

CARACTÉRISTIQUES DES SYSTÈMES VISIOPHONIQUES	H.100–H.199
INFRASTRUCTURE DES SERVICES AUDIOVISUELS	
Généralités	H.200–H.219
Multiplexage et synchronisation en transmission	H.220–H.229
Aspects système	H.230–H.239
Procédures de communication	H.240–H.259
Codage des images vidéo animées	H.260–H.279
Aspects liés aux systèmes	H.280–H.299
Systèmes et équipements terminaux pour les services audiovisuels	H.300–H.349
Architecture des services d'annuaire pour les services audiovisuels et multimédias	H.350–H.359
Architecture de la qualité de service pour les services audiovisuels et multimédias	H.360–H.369
Services complémentaires en multimédia	H.450–H.499
PROCÉDURES DE MOBILITÉ ET DE COLLABORATION	
Aperçu général de la mobilité et de la collaboration, définitions, protocoles et procédures	H.500–H.509
Mobilité pour les systèmes et services multimédias de la série H	H.510–H.519
Applications et services de collaboration multimédia mobile	H.520–H.529
Sécurité pour les systèmes et services multimédias mobiles	H.530–H.539
Sécurité pour les applications et services de collaboration multimédia mobile	H.540–H.549
Procédures d'interfonctionnement de la mobilité	H.550–H.559
Procédures d'interfonctionnement de collaboration multimédia mobile	H.560–H.569
SERVICES À LARGE BANDE ET MULTIMÉDIAS TRI-SERVICES	
Services multimédias à large bande sur VDSL	H.610–H.619

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

Recommandation UIT-T H.248.40

Protocole de commande de passerelle: Paquetage de détection d'inactivité des données d'application

Résumé

La présente Recommandation décrit le principe de détection d'inactivité des données d'application dans les connexions de transport IP en général, p. ex. afin d'éviter une éventuelle situation d'interblocage si le verrouillage a été réglé mais qu'aucun train de données d'application n'arrive de l'extérieur afin de s'y ancrer. La solution est fondée sur un événement de détection d'arrêt (ou de non-démarrage) des données d'application.

Source

La Recommandation UIT-T H.248.40 a été approuvée le 13 janvier 2007 par la Commission d'études 16 (2005-2008) 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 développeurs de consulter la base de données des brevets du TSB sous <http://www.itu.int/ITU-T/ipr/>.

© UIT 2007

Tous droits réservés. Aucune partie de cette publication ne peut être reproduite, par quelque procédé que ce soit, sans l'accord écrit préalable de l'UIT.

TABLE DES MATIÈRES

	Page
1	Domaine d'application 1
2	Références..... 1
3	Termes et définitions 1
4	Abréviations..... 1
5	Conventions 2
6	Paquetage de détection d'inactivité des données d'application..... 2
6.1	Propriétés..... 2
6.2	Événements..... 2
6.3	Signaux 3
6.4	Statistiques..... 3
6.5	Codes d'erreur..... 3
6.6	Procédures 4
Appendice I – Exemple d'un cas de figure en téléphonie RTP 5	
I.1	Introduction 5
I.2	Abréviations 5
I.3	Hypothèses 5
I.4	Exemple de logique de détection..... 5
I.5	Recommandations relatives aux réglages des temporisations..... 6
Appendice II – Exemple d'un cas de figure relatif à la détection d'un interblocage dans des scénarios de verrouillage IP 7	
II.1	Introduction 7
II.2	Hypothèses 8
II.3	Exemple de logique de détection..... 8
II.4	Recommandations relatives aux réglages des temporisations..... 8
Appendice III – Exemple d'un cas de figure relatif à la détection d'une session en attente de téléphonie RTP 10	
III.1	Introduction 10
III.2	Abréviations 10
III.3	Terminaison incorrecte d'une session de téléphonie RTP..... 10
III.4	Relation entre "session RTP en attente" et "terminaison H.248 en attente".... 11
Bibliographie..... 12	

Recommandation UIT-T H.248.40

Protocole de commande de passerelle: Paquetage de détection d'inactivité des données d'application

1 Domaine d'application

La présente Recommandation permet à un contrôleur de passerelle média de demander à celle-ci de détecter le fait qu'aucun flux de données d'application en protocole IP n'est passé depuis un certain temps par une terminaison particulière ou par un train particulier. La capacité de détecter si un flux de données d'application en protocole IP est arrêté ou n'a pas commencé sert à éviter un interblocage dans des scénarios de verrouillage. Cette capacité peut également servir à détecter des supports en attente.

La présente Recommandation définit un événement associé à un ou plusieurs duplets IP. Un duplet individuel est représenté par la paire <adresse IP, port IP> d'un flux IP présent dans un train ou dans une terminaison H.248. L'ensemble des conditions relatives à la détection d'inactivité est associé à des événements d'arrivée et/ou de départ de paquet IP pour tous les duplets d'un train/d'une terminaison. La situation des arrivées ou des départs – selon le cas – des paquets est commandée par un paramètre spécialisé (appelé "*direction*" (sens du flux)).

La flexibilité des configurations logiques de détection d'inactivité permet d'utiliser le paquetage H.248.40 pour diverses applications (voir également les appendices).

2 Références

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.

[UIT-T H.248.1] Recommandation UIT-T H.248.1 (2005), *Protocole de commande de passerelle: Version 3*.

3 Termes et définitions

Néant.

4 Abréviations

La présente Recommandation utilise les abréviations suivantes:

ADID	détection d'inactivité des données d'application (<i>application data inactivity detection</i>)
IP	protocole Internet (<i>Internet protocol</i>)
MG	passerelle média (<i>media gateway</i>)
MGC	contrôleur de passerelle média (<i>media gateway controller</i>)
NAPT	conversion d'adresse et de port réseau (<i>network address and port translation</i>)
RTCP	protocole de commande RTP (<i>RTP control protocol</i>)

RTP protocole de transport en temps réel (*real-time transport protocol*)
RTSP protocole d'écoulement en temps réel (*real-time streaming protocol*)

5 Conventions

Néant.

6 Paquetage de détection d'inactivité des données d'application

Nom du paquetage: Paquetage de détection d'inactivité des données d'application
Identificateur du paquetage: *adid*, 0x009c
Description: Ce paquetage permet au contrôleur MGC d'être averti lorsque la passerelle MG a détecté qu'aucun flux de données d'application IP n'a été détecté dans une terminaison ou dans un train.
Version: 1
Extension: Néant

6.1 Propriétés

Néant.

6.2 Événements

6.2.1 Détection d'arrêt de flux IP

Nom de l'événement: Détection d'arrêt de flux IP
Identificateur de l'événement: *ipstop* (0x0001)
Description: Cet événement détecte s'il n'y a eu aucun flux de données d'application sensibles au sens pendant un intervalle de temps déterminé (temps de détection). S'il a été indiqué que de multiples ports IP sont associés à un flux (p. ex. des flux RTP et RTCP), la détection d'absence de flux de données d'application doit être effectuée sur tous les ports avant que l'événement soit enclenché. Appliqué au niveau d'une terminaison, l'événement *adid/ipstop* doit être signalé quand il a été déterminé que les données d'application ont stoppé dans tous les trains associés à cette terminaison.

Si le signalement initial de l'événement a été effectué, si cet événement reste actif et si le temps de détection s'écoule sans détection de données d'application, l'événement est signalé de nouveau, ce qui peut se produire plusieurs fois.

Cet événement doit être détecté quel que soit le mode du train de données. Par exemple, même si le train est réglé à *SendOnly* et que des paquets soient reçus, cette condition sera prise en compte.

6.2.1.1 Paramètres de descripteur d'événement (*EventDescriptor*)

6.2.1.1.1 Temps de détection

Nom du paramètre: Temps de détection
Identificateur du paramètre: *dt* (0x0001)

Description: Intervalle de temps après lequel, si aucun flux de données d'application n'est détecté, l'événement de détection d'arrêt de flux IP est enclenché. La passerelle MG vérifie, dans les intervalles du temps de détection *dt*, si du trafic de données d'application s'est produit. Si aucune donnée d'application n'est arrivée, alors l'événement *adid/ipstop* est enclenché.

NOTE – Il peut en résulter un dépassement du temps de détection écoulé entre l'arrêt du flux de données IP et la détection de l'événement.

Type: Entier
Facultatif: Oui (si la valeur par défaut est fournie).
Valeurs possibles: Tout nombre positif de secondes.
Valeur par défaut: Fournie

6.2.1.1.2 Sens (*direction*)

Nom du paramètre: Sens
Identificateur du paramètre: dir (0x0002)
Description: Avec ce paramètre, le contrôleur MGC indique à la passerelle MG quel sens du flux de données devrait être surveillé afin de détecter l'inactivité. Le sens entrant signifie que les données viennent de l'extérieur du contexte. Le sens sortant signifie que les données vont vers l'extérieur du contexte. Si le sens est réglé à "BOTH", la passerelle MG produira l'événement si aucune donnée n'est envoyée ni reçue par la terminaison, à destination/en provenance de l'extérieur du contexte pendant l'intervalle de temps de détection *dt*.

Type: Enumération
Facultatif: Oui
Valeurs possibles: "IN" (0x0001) Sens entrant
"OUT" (0x0002) Sens sortant
"BOTH" (0x0003) Dans les deux sens
Valeur par défaut: "Both"

6.2.1.2 Paramètres de descripteur d'Événements observés (ObservedEventsDescriptor)

Néant.

6.3 Signaux

Néant.

6.4 Statistiques

Néant.

6.5 Codes d'erreur

Néant.

6.6 Procédures

Afin de détecter l'inactivité des données d'application, le contrôleur MGC devrait régler l'événement *adid/ipstop* sur un "temps de détection" approprié et sur le "sens" approprié dans le train/la terminaison H.248 applicable. L'événement *adid/ipstop* est signalé au contrôleur MGC:

- Si le contrôleur MGC a réglé le paramètre *dir* à "IN" et si aucun paquet de données IP n'a été reçu par la passerelle MG en provenance du réseau dans ce train/cette terminaison à l'expiration du temps de détection (*dt*).
- Si le contrôleur MGC a réglé le paramètre *dir* à "OUT" et si aucun paquet de données IP n'a été envoyé par la passerelle MG au réseau dans ce train/cette terminaison à l'expiration du temps de détection (*dt*).
- Si le contrôleur MGC a réglé le paramètre *dir* à "BOTH" et si aucun paquet de données IP n'a été envoyé ni reçu à destination/en provenance du réseau dans ce train/cette terminaison à l'expiration du temps de détection (*dt*).

Dès réception d'un message NOTIFY.req contenant l'événement *adid/ipstop*, le contrôleur MGC devrait prendre la mesure appropriée.

L'action enclenchée au niveau du contrôleur MGC peut avoir à prendre en compte:

- des éléments de service (p. ex. des applications unilatérales, un microphone coupé dans des services de conférence, etc.);
- des réglages de configuration d'un service support (p. ex. activation du mode de suppression de silence en cas de téléphonie conversationnelle, sessions RTP sans protocole RTCP, etc.);
- des configurations de terminaison H.248 (p. ex. une propriété de mode de train mise à la valeur "Inactive").

Il est recommandé de régler le temps de détection (*dt*) d'un temporisateur à une valeur appropriée, p. ex. à un multiple de la moitié du temps d'aller-retour ou à un multiple du temps typique entre arrivées de paquets. Le temps moyen entre arrivées peut être propre à l'application IP (p. ex. selon le type de codec). Il peut aussi dépendre du taux d'utilisation du protocole de verrouillage de trames au niveau applicatif (p. ex. temps de mise en paquets RTP, intervalle de transmission RTCP, etc.). Ce temps moyen peut également être propre au service (p. ex. microphone coupé en cas de téléphonie RTP, ou écoulement suspendu en cas de flux multimédia régi par protocole RTSP).

Appendice I

Exemple d'un cas de figure en téléphonie RTP

(Cet appendice ne fait pas partie intégrante de la présente Recommandation)

I.1 Introduction

La présente Recommandation peut être appliquée à des terminaisons éphémères, qui sont utilisées afin de réaliser un service de téléphonie RTP (VoRTP) entre deux correspondants. L'intervalle de transmission des paquets RTP est ici beaucoup plus petit que la granularité du temporisateur "ipstop/dt".

Cet appendice décrit la détection d'un événement d'"arrêt de média RTP" qui se rapporte à l'événement d'arrivée/ou de départ d'un paquet RTP ou RTCP.

I.2 Abréviations

Cet appendice utilise les abréviations suivantes:

FIB	base d'informations de réacheminement (IP) (<i>IP forwarding information base</i>)
IPLR	taux de perte de paquets IP (<i>IP packet loss ratio</i>)
RIB	base d'informations de routage (IP) (<i>IP routing information base</i>)
SDL	langage de spécification et de description (<i>specification and description language</i>)
VoRTP	téléphonie RTP (<i>voice over RTP</i>)

I.3 Hypothèses

Du point de vue du support RTP:

- le protocole RTCP est activé;
- l'intervalle de transmission RTCP minimal est de 5 s (voir le § A.7/IETF RFC 3550);
- les extrémités homologues RTP continuent à envoyer des paquets RTCP pendant les "phases de silence" (inactivité vocale détectée ou microphone coupé).

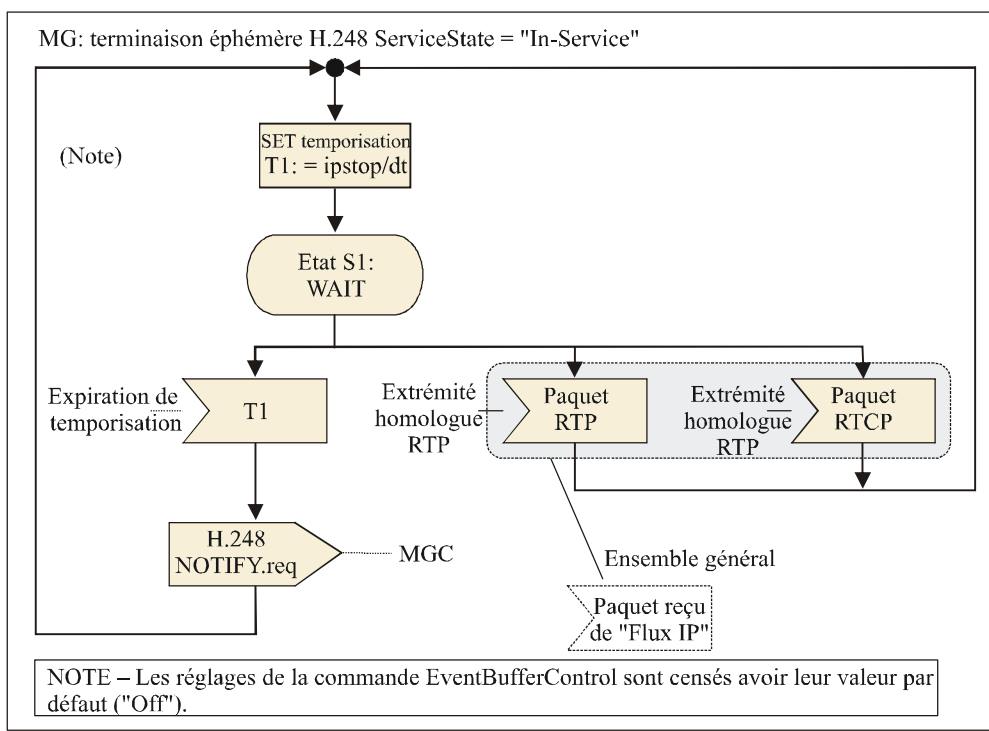
Du point de vue du paquetage H.248:

- le contrôleur MGC tient compte du réglage de mode de train (en cas de notification d'événement).

I.4 Exemple de logique de détection

La Figure I.1 décrit un exemple de logique de détection. L'événement est supposé être uniformément activé (réglage par défaut: EventBufferControl).

Il convient de remarquer que l'événement reste actif jusqu'à ce qu'il soit désactivé par le contrôleur MGC.



H.248.40(01-07)_F1.01

Figure I.1 – Exemple de logique SDL pour VoRTP

I.5 Recommandations relatives aux réglages des temporisations

Quelques Recommandations qualitatives; les réglages spécifiques peuvent dépendre des variables indiquées.

I.5.1 Objectif: "Détection une route IP interrompue"

Les réglages du temporisateur "ipstop/dt" peuvent être fondés sur l'intervalle de transmission RTP ("longueur maximale estimée de l'intervalle").

En cas de "détection rapide" comme ci-dessous, l'intervalle minimal de signalisation RTCP est requis.

NOTE – Des mécanismes de reroutage au niveau IP pourraient être envisagés (p. ex. intervalles de mise à jour des bases RIB/FIB en raison du(des) protocole(s) de routage IP appliqué(s)).

I.5.2 Objectif: "Détection la libération d'une extrémité RTP"

Les réglages du temporisateur "ipstop/dt" peuvent être fondés sur une combinaison de ce qui suit:

- intervalle de transmission RTCP ("longueur maximale estimée de l'intervalle"); et
- état du taux IPLR ("perte estimée de paquets RTCP").

S'il faut une "détection rapide" ou une "détection plus pessimiste", on calcule un temps de maintien de session RTP (p. ex. le "temps estimé de maintien du contexte" (C₀HT) pour le service VoRTP).

Appendice II

Exemple d'un cas de figure relatif à la détection d'un interblocage dans des scénarios de verrouillage IP

(Cet appendice ne fait pas partie intégrante de la présente Recommandation)

II.1 Introduction

La présente Recommandation peut être appliquée dans le contexte des applications conformes à la référence [b-UIT-T H.248.37]. La Figure II.1 montre une configuration de réseau possible.

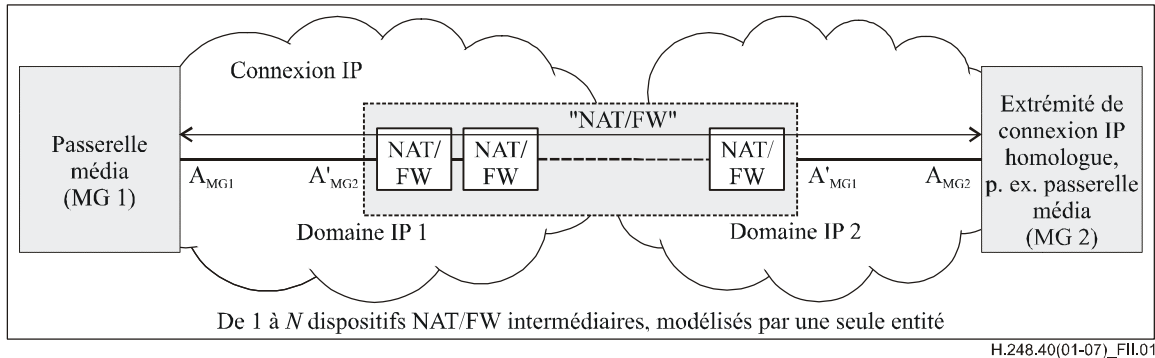


Figure II.1 – Configuration de réseau possible

Les applications [b-UIT-T H.248.37] prennent en charge les adaptations dynamiques d'adresse IP dans le plan d'utilisateur (strate de transport de réseau NGN en mode IP).

Cet appendice décrit la détection d'une situation d'interblocage dans le cadre d'un verrouillage.

II.1.1 Situation d'interblocage

Des paquets IP émis peuvent ne pas atteindre l'extrémité homologue en raison d'informations d'adressage incorrectes (en l'occurrence: tétraplets en cas de dispositifs de conversion NAPT). La Figure II.2 décrit un scénario possible.

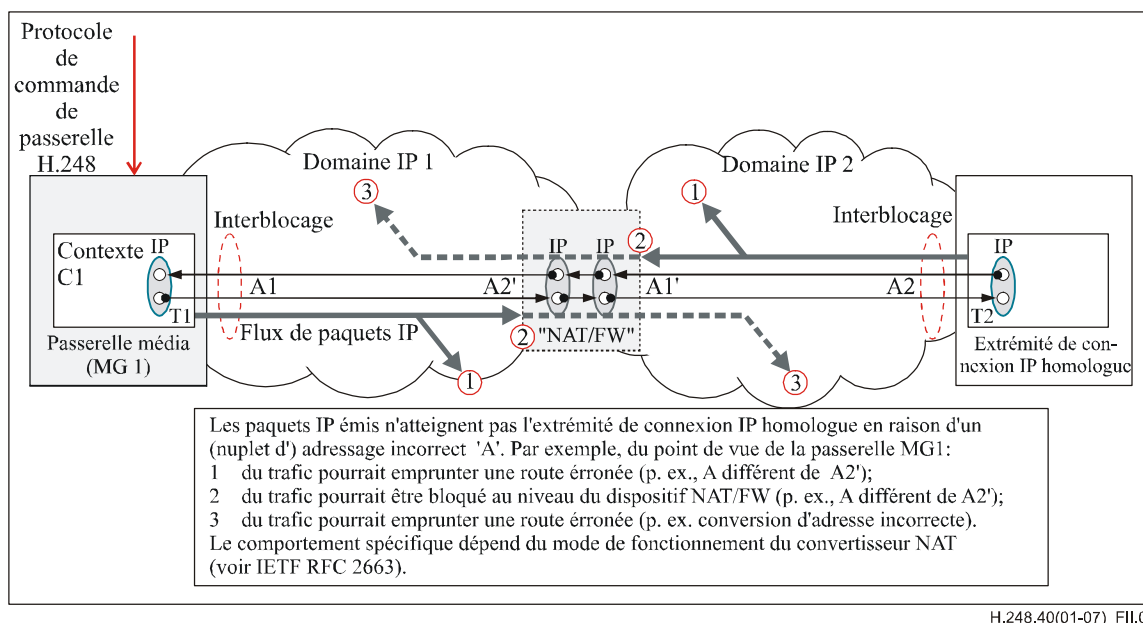


Figure II.2 – Situations d'interblocage possibles

Le nuplet d'adresse initialement incorrect a besoin d'un flux de paquets IP entrants afin de s'adapter à une adresse correcte (cette fonction est également appelée "verrouillage"; voir la référence [b-UIT-T H.248.37]).

Situation d'interblocage:

"Aucune mise à jour d'adresse en cas d'absence de flux entrant, assortie d'une impossibilité de livraison de paquet dans le sens sortant en raison d'informations d'adressage incorrectes, ..."

II.2 Hypothèses

La façon de résoudre finalement de telles situations d'interblocage est hors du domaine d'application de la présente Recommandation. L'hypothèse de base est que de telles actions pourront être enclenchées par des contrôleurs MGC sur la base d'Événements de notifications H.248.40.

Du point de vue d'une terminaison de support IP:

- néant.

Du point de vue H.248:

- le contrôleur MGC tient compte du réglage de mode de train (en cas de notification d'événement).

II.3 Exemple de logique de détection

Une activité dans le sens sortant n'est pas applicable. L'exemple de logique de détection conformément à la Figure I.1 est donc applicable également. Les Événements d'arrivée de paquet IP valide sont définis par les informations relatives au nuplet d'adressage disponibles, conformément au descripteur local (LD) H.248.

II.4 Recommandations relatives aux réglages des temporisations

Quelques Recommandations qualitatives; les réglages spécifiques peuvent dépendre des variables indiquées.

II.4.1 Objectif: "Détecter un interblocage dans des applications de verrouillage IP"

Les réglages du temporisateur "ipstop/dt" peuvent être fondés sur des valeurs "typiques du délai d'ouverture de session de bout en bout" si une "détection rapide" est requise.

NOTE – L'on part de l'hypothèse de "réglages de configuration de dispositif" stables après l'accomplissement d'un scénario de signalisation d'ouverture de session.

Appendice III

Exemple d'un cas de figure relatif à la détection d'une session en attente de téléphonie RTP

(Cet appendice ne fait pas partie intégrante de la présente Recommandation)

III.1 Introduction

La présente Recommandation peut servir à détecter et à éviter des sessions RTP en attente. Une session RTP est caractérisée par une (ou deux en cas de RTCP) connexions de transport IP en mode UDP entre deux systèmes d'extrémité RTP (voir IETF RFC 3550). Par exemple, dans la Figure III.1, les deux extrémités RTP homologues sont situées dans des passerelles MG de téléphonie VoRTP, c'est-à-dire dans les passerelles MG qui jouent le rôle de système d'extrémité RTP. L'extrémité de session RTP est donc associée à une terminaison éphémère.

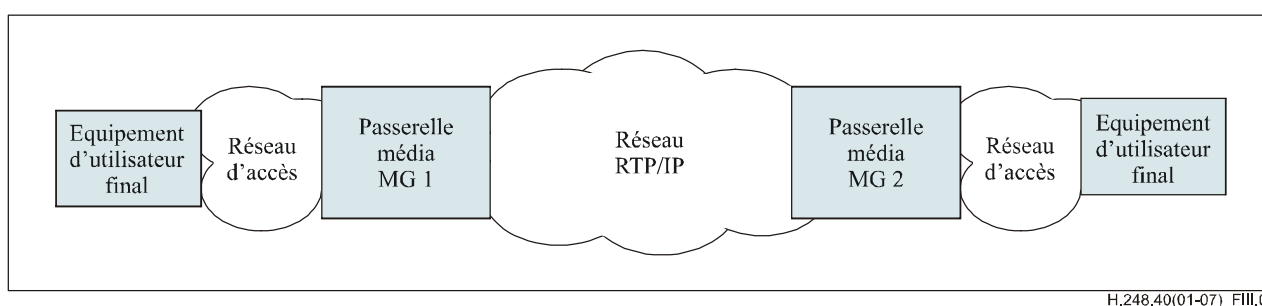


Figure III.1 – Configuration de réseau au cours d'une session de téléphonie RTP

Le "réseau d'accès" de la Figure III.1 n'est pas nécessairement "en mode RTP".

III.2 Abréviations

Cet appendice utilise l'abréviation suivante:

VoIP téléphonie IP (*voice over IP*)

III.3 Terminaison incorrecte d'une session de téléphonie RTP

La Figure III.1 montre deux équipements d'utilisateur engagés dans une connexion de téléphonie IP.

Si un des (ou les) deux côtés de la session (session RTP et/ou association de commande de communication/session) n'est (ne sont) pas bouclé(s) correctement, cela peut se traduire dans certains cas par la mise en attente de ressources ou par le maintien en survie de sessions pendant une durée inutilement longue. L'opérateur peut se protéger de cette situation par l'utilisation du présent paquetage H.248.40.

Normalement, dans ce cas, une situation d'attente ne peut pas n'être présumée qu'en raison d'une absence d'activité de données dans un seul sens. Il est nécessaire d'observer qu'aucun train RTP n'est reçu dans un sens ou dans l'autre avant de supposer l'existence d'une situation d'attente. Le contrôleur MGC devrait donc armer l'événement *ipstop* en donnant au paramètre *direction* une valeur égale à "both".

III.4 Relation entre "session RTP en attente" et "terminaison H.248 en attente"

Le scénario de session en attente décrit dans le § III.3 peut impliquer la suspension de ressources au niveau de la commande d'appel, c'est-à-dire que non seulement les ressources supports n'ont pas été libérées dans la passerelle MG, mais que les ressources de commande correspondantes n'ont pas été libérées non plus dans le contrôleur MGC. Cette sorte de scénario ne peut pas être résolue par le paquetage de détection de terminaison en attente H.248.36, car ce scénario n'implique pas de terminaison en attente.

Les paquetages H.248.40 et H.248.36 sont donc généralement découplés et complémentaires car ils s'adressent chacun à des conditions d'inactivité différentes, respectivement dans le plan d'utilisateur et dans le plan commande.

Bibliographie

[b-UIT-T H.248.37] Recommandation UIT-T H.248.37 (2005), *Protocole de commande de passerelle: paquetage de traversée de dispositif NAPT IP.*

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