

Groupe de travail Réseau
Request for Comments : 7667
 RFC rendue obsolète : 5117
 Catégorie : Information
 ISSN: 2070-1721

M. Westerlund, Ericsson
 S. Wenger, Vidyo
 novembre 2015

Traduction Claude Brière de L'Isle

Topologies de RTP

Résumé

Le présent document discute des topologies de points d'extrémité en point à point et multipoints utilisées dans les environnements fondés sur le protocole de transport en temps réel (RTP, *Real-time Transport Protocol*). En particulier, les topologies centralisées couramment employées dans l'industrie de la visioconférence sont transposées dans la terminologie de RTP.

Le présent document est mis à jour avec des topologies supplémentaires et remplace la RFC 5117.

Statut de ce mémoire

Le présent document n'est pas une spécification sur la voie de la normalisation de l'Internet ; il est publié à des fins d'information.

Le présent document a été produit par l'équipe d'ingénierie de l'Internet (IETF). Il représente le consensus de la communauté de l'IETF. Il a subi une révision publique et sa publication a été approuvée par le groupe de pilotage de l'ingénierie de l'Internet (IESG). Tous les documents approuvés par l'IESG ne sont pas candidats à devenir une norme de l'Internet ; voir la Section 2 de la RFC5741.

Les informations sur le statut actuel du présent document, tout errata, et comment fournir des réactions sur lui peuvent être obtenues à <http://www.rfc-editor.org/info/rfc7667>

Notice de droits de reproduction

Copyright (c) 2015 IETF Trust et les personnes identifiées comme auteurs du document. Tous droits réservés.

Le présent document est soumis au BCP 78 et aux dispositions légales de l'IETF Trust qui se rapportent aux documents de l'IETF (<http://trustee.ietf.org/license-info>) en vigueur à la date de publication de ce document. Prière de revoir ces documents avec attention, car ils décrivent vos droits et obligations par rapport à ce document. Les composants de code extraits du présent document doivent inclure le texte de licence simplifié de BSD comme décrit au paragraphe 4.e des dispositions légales du Trust et sont fournis sans garantie comme décrit dans la licence de BSD simplifiée.

Table des Matières

1. Introduction.....	2
2. Définitions.....	2
2.1 Glossaire.....	2
2.2 Définitions en rapport avec la taxonomie de groupage RTP.....	3
3. Topologies.....	3
3.1 Point à point.....	3
3.2 Point à point via un boîtier de médiation.....	4
3.3 Point à multipoints utilisant la diffusion groupée.....	7
3.4 Point à multipoints utilisant le maillage.....	10
3.5 Point à multipoints utilisant le traducteur de la RFC 3550.....	11
3.6 Point à multipoints utilisant le modèle de mixeur de la RFC 3550.....	13
3.7 Boîtier de médiation de transmission sélective.....	17
3.8 Point à multipoints utilisant des MCU de commutation de vidéo.....	19
3.9 Point à multipoints utilisant des MCU à terminaison RTCP.....	19
3.10 Terminal à composants séparés.....	20
3.11 Mixeur/traducteurs non symétriques.....	22
3.12 Topologies combinées.....	22
4. Propriétés des topologies.....	22
4.1 Transmission des supports de tous à tous.....	23
4.2 Interopérabilité de transport ou des supports.....	23

4.3 Adaptation du débit binaire par domaine.....	23
4.4 Agrégation de supports.....	24
4.5 Vue de tous les participants à la session	24
4.6 Détection de boucle.....	24
4.7 Cohérence entre extensions d'en-têtes et RTCP.....	24
5. Comparaison des topologies.....	25
6. Considérations sur la sécurité.....	25
7. Références.....	26
7.1 Références normatives.....	26
7.2 Références pour information.....	26
Remerciements.....	27
Adresse des auteurs.....	27

1. Introduction

Les topologies du protocole de transport en temps réel (RTP) [RFC3550] décrivent les méthodes pour interconnecter les entités RTP et leur comportement de traitement pour RTP et le protocole de contrôle de RTP (RTCP). Le présent document essaye de dissiper la confusion passée et existante, en particulier en ce qui concerne les termes non définis dans RTP mais d'utilisation courante dans l'industrie de la communication, comme l'unité de contrôle multipoints (MCU, *Multipoint Control Unit*).

Quand le profil audio-visuel avec rétroaction (AVPF, *Audio-Visual Profile with Feedback*) [RFC4585] a été développé, l'accent a été principalement mis sur la prise en charge efficace des scénarios de point à point et de petit multipoints sans contrôle de multipoints centralisé. En pratique, cependant, la plupart des conférences multipoints opèrent en utilisant des unités centralisées appelées des MCU. Les MCU peuvent mettre en œuvre une fonction de mixeur ou de traducteur (dans la terminologie de RTP [RFC3550]) et de support de signalisation. Elles peuvent aussi contenir des fonctions supplémentaires de couche d'application. Le présent document se concentre sur les aspects de transport de supports de MCU qui peuvent être réalisés en utilisant RTP, comme exposé ci-dessous. Sont aussi considérées les propriétés des mixeurs et traducteurs, et comment certains types de MCU déployés dévient de ces propriétés.

Le présent document codifie aussi de nouvelles architectures multipoints qui ont été récemment introduites et qui n'étaient pas prévues dans la RFC 5117 ; donc, le présent document remplace la [RFC5117]. Ces architectures utilisent le codage vidéo adaptable et la diffusion simultanée, et leurs unités centralisées associées sont appelées des boîtiers de médiation de transmission sélective (SFM, *Selective Forwarding Middlebox*). Cette codification donne une base d'informations communes pour les travaux futurs de discussion et de spécification.

Les nouvelles topologies sont le point à point via un boîtier de médiation (paragraphe 3.2), la diffusion groupée spécifique de source (SSM, *Source-Specific Multicast*) (paragraphe 3.3.2), SSM avec ressources locales en envoi individuel (paragraphe 3.3.3) le point à multipoints utilisant le maillage (paragraphe 3.4) le boîtier de transmission sélective (paragraphe 3.7), et le terminal à composants séparés (paragraphe 3.10). Le point à multipoints utilisant le modèle de mixeur de la RFC 3550 (paragraphe 3.6) a été significativement étendu pour couvrir deux versions différentes, à savoir le mixeur de mixage de supports (*Media-Mixing Mixer*) (paragraphe 3.6.1) et le mixeur à commutation de supports (*Media-Switching Mixer*) (paragraphe 3.6.2).

Le document tente de préciser et expliquer de façon informelle certaines sections de la spécification de RTP [RFC3550]. Il n'est pas destiné à mettre à jour ou changer ce qui est spécifié de façon normative dans la RFC 3550.

2. Définitions

2.1 Glossaire

ASM (*Any-Source Multicast*) : toute source en diffusion groupée

AVPF (*Audio-Visual Profile with Feedback*) : profil RTP étendu pour rétroactions fondées sur RTCP

CSRC (*Contributing Source*) : source contributive

Liaison : transport de données jusqu'au prochain bond IP

Boîtier de médiation (*middlebox*) : appareil sur le chemin que traversent les supports entre deux points d'extrémité

MCU (*Multipoint Control Unit*) : unité de contrôle multipoints

Chemin : enchaînement de plusieurs liaisons, résultant en un transfert de données de bout en bout.

PtM : point à multipoints

PtP : point à point

SFM (*Selective Forwarding Middlebox*) : boîtiers de médiation de transmission sélective

SSM (*Source-Specific Multicast*) : diffusion groupée spécifique de source

SSRC (*Synchronization Source*) : source de synchronisation

2.2. Définitions en rapport avec la taxonomie de groupage RTP

Les définitions suivantes sont tirées de la [RFC7656].

Session de communication : association entre deux ou plusieurs participants qui communiquent ensemble via une ou plusieurs sessions multimédia.

Point d'extrémité : Une seule entité adressable qui envoie ou reçoit des paquets RTP. Il peut être décomposé en plusieurs blocs fonctionnels, mais tant qu'il se comporte comme une seule entité de pile RTP, il est classé comme un seul "point d'extrémité".

Source de supports : c'est la source logique d'un flux de supports numérique qui progresse dans le temps synchronisé avec une horloge de référence. Ce flux est appelé un flux de source.

Session multimédia : association entre un groupe de participants engagés dans une communication via une ou plusieurs sessions RTP.

3. Topologies

Cette Section définit plusieurs topologies pertinentes pour le contrôle de codec mais aussi l'usage de RTP dans d'autres contextes. La section commence par les cas de point à point, avec ou sans boîtiers de médiation. Puis elle suit un certain nombre de méthodes différentes pour établir une communication de point à multipoints. Elles sont structurées autour des outils les plus fondamentaux, c'est-à-dire, la diffusion groupée, un maillage de connexions, des traducteurs, des mixeurs, et finalement des MCU et des SFM. La Section se termine par la discussion des terminaux décomposés, des comportements de boîtier de médiation asymétrique, et des topologies.

Les topologies peuvent être référencées dans d'autres documents par un nom abrégé, indiqué par le préfixe "Topo-".

Pour chaque topologie définie pour RTP, on discute comment RTP, RTCP, et les supports portés sont traités. Par rapport à RTCP, on discute aussi le traitement des messages de rétroaction RTCP comme défini dans les [RFC4585] et [RFC5104].

3.1 Point à point

Nom abrégé : Topo-point à point

La topologie point à point (PtP) (Figure 1) consiste en deux points d'extrémité, communiquant en utilisant l'envoi individuel. Les trafics RTP et RTCP sont portés de point d'extrémité à point d'extrémité, en utilisant seulement du trafic en envoi individuel (même si, dans des cas exotiques, ce trafic en envoi individuel se trouve être convoyé sur une adresse IP de diffusion groupée).

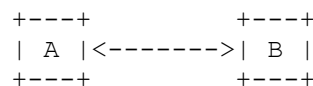


Figure 1 : Point à point

La principale propriété de cette topologie est que A envoie à B, et seulement B, tandis que B envoie à A, et seulement A. Cela évite toutes les complexités du traitement de plusieurs points d'extrémité et de combiner les exigences qui en découlent. Noter qu'un point d'extrémité peut quand même utiliser plusieurs sources de synchronisation RTP (SSRC) dans une session RTP. Le nombre de sessions RTP utilisées entre A et B peut aussi être quelconque, sous réserve seulement de limitations de niveau système comme la gamme du nombre d'accès.

Les messages de rétroaction RTCP pour la SSRC indiquée sont communiqués directement entre les points d'extrémité. Donc, cette topologie pose un minimum (si il en est) de problèmes pour tous les messages de rétroaction. Pour les sessions RTP qui utilisent plusieurs SSRC par point d'extrémité, il peut être pertinent de mettre en œuvre la prise en charge de la suppression des rapports croisés comme défini dans "Envoi de plusieurs flux de supports dans une seule session RTP" [RFC8108].

3.2 Point à point via un boîtier de médiation

Ce paragraphe discute des cas où deux points d'extrémité communiquent mais ont un ou plusieurs boîtiers de médiation impliqués dans la session RTP.

3.2.1 Traducteurs

Nom abrégé : Topo-PtP-Traducteur

Deux principales catégories de traducteurs peuvent être distinguées : traducteurs de transport et traducteurs de supports. Les deux types de traducteur partagent des attributs communs qui les séparent des mixeurs. Pour chaque flux RTP que reçoit le traducteur, il génère un flux RTP individuel dans l'autre domaine. Un traducteur conserve la SSRC pour un flux RTP à travers la traduction, tandis qu'un mixeur peut choisir un seul flux RTP parmi plusieurs reçus (dans des cas comme la commutation audio/vidéo) ou envoyer un flux RTP composé de plusieurs supports mélangés reçus dans plusieurs flux RTP (dans des cas comme le mixage audio ou l'empilement vidéo) mais toujours sous sa propre SSRC, éventuellement en utilisant le champ de CSRC pour indiquer la ou les sources du contenu. Les mixeurs sont plus courants dans les cas de point à multipoints que dans un PtP. La raison en est que dans les cas d'utilisation de PtP, un boîtier de médiation va principalement se concentrer sur permettre l'interopérabilité, entre des points d'extrémité autrement non interopérables, comme le transcodage à un codec que le receveur prend en charge, ce qui peut être fait par un traducteur de supports.

Comme spécifié au paragraphe 7.1 de la [RFC3550], l'espace de SSRC est commun pour tous les participants à la session RTP, indépendamment du côté de la session où le traducteur réside. Donc, il est de la responsabilité des points d'extrémité (comme participants à la session RTP) d'utiliser la détection de collision de SSRC, et la SSRC est donc un champ que le traducteur ne peut pas changer. Toutes les informations de description de source (SDS, *Source Description*) associées à une SSRC ou CSRC ont aussi besoin d'être transmises entre les domaines pour toute SSRC/CSRC utilisée dans les différents domaines.

Un traducteur n'utilise généralement pas de SSRC qui lui soit propre et n'est pas visible comme un participant actif à la session RTP. Une raison d'avoir sa propre SSRC est quand un traducteur agit comme surveillant de la qualité qui envoie des rapports RTCP et donc il est exigé qu'il ait une SSRC. Un autre exemple est le cas où un traducteur est prêt à utiliser des messages de rétroaction RTCP. Cela peut, par exemple, se produire dans un traducteur configuré à détecter les pertes de paquets d'une vidéo importante, et qu'il veut déclencher la réparation par le point d'extrémité qui envoie les supports, en envoyant des messages de rétroaction. Alors que ces rétroactions pourraient utiliser la SSRC de la cible pour le traducteur (le point d'extrémité receveur) cela exigerait à son tour la traduction des rapports du RTCP cible pour les rendre cohérents. Il peut être plus simple d'exposer une SSRC supplémentaire dans la session. Le seul souci est que les points d'extrémité qui ne prennent pas en charge la totalité de la spécification RTP peuvent avoir des problèmes avec plusieurs SSRC qui font des rapports sur les flux RTP envoyés par ce point d'extrémité, car ce cas d'utilisation peut être vu comme exotique par les mises en œuvre.

En général, une mise en œuvre de traducteur devrait considérer quels messages de rétroaction RTCP ou messages de contrôle de codec elle a besoin de comprendre en relation avec la fonction du traducteur lui-même. Ceci est complètement en ligne avec l'exigence de traduire aussi les messages RTCP entre les domaines.

3.2.1.1 Relais/ancrage de transport

Nom abrégé : Topo-PtP-relais

Il existe un certain nombre de types différents de boîtiers de médiation qui pourraient être insérés entre deux points d'extrémité au niveau transport, par exemple, pour effectuer des changements sur les en-têtes IP/UDP, et sont donc des traducteurs de transport de base. Ces boîtiers de médiation ont de nombreuses variations incluant des traversées de NAT [RFC3022] en étiquetant le chemin des supports avec un relais de domaine d'adresse publique et des topologies de réseau où le flux RTP est obligé de passer par un point particulier pour examen en employant un relais, ou pour préserver la confidentialité en cachant les adresses de transport de chaque homologue à l'autre partie. D'autres protocoles ou fonctionnalités qui fournissent ce comportement sont la traversée en utilisant des serveurs de relais autour des NAT (TURN) [RFC5766] des passerelles de bordure de session, et des nœuds de traitement de supports avec des fonctions d'ancrage des supports.

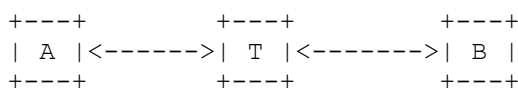


Figure 2: Point à point avec traducteur

Un élément commun de ces fonctions est qu'elles sont normalement transparentes au niveau RTP, c'est-à-dire, elles n'effectuent pas de changement sur des champs de paquet RTP ou RTCP et affectent seulement les couches inférieures. Elles peuvent cependant affecter le chemin car les paquets RTP et RTCP sont acheminés entre les points d'extrémité dans la session RTP, et par là, elles affectent indirectement la session RTP. Pour cette raison, on pourrait penser que les boîtiers de médiation de type traducteur de transport n'ont pas besoin d'être inclus dans le présent document. Cette topologie peut cependant poser des exigences supplémentaires pour la mise en œuvre RTP et ses interactions avec la solution de signalisation. Dans la signalisation et dans certains champs RTCP, des adresses réseau autres que celles du relais peuvent survenir car B a une adresse réseau différente de celle du relais (T). Les mises en œuvre qui ne peuvent pas prendre en charge cela ne vont pas non plus fonctionner correctement quand les points d'extrémité sont soumis à un NAT.

Les mises en œuvre de relais de transport ont aussi à tenir compte des considérations de sécurité. En particulier, le filtrage d'adresse de source des paquets entrants est généralement important dans les relais, pour empêcher des attaquants d'injecter du trafic dans une session, qu'un homologue peut, en l'absence d'une sécurité adéquate dans le relais, penser qu'il vient de l'autre homologue.

3.2.1.2 Traducteur de transport

Nom abrégé : Topo-Trn-traducteur

Les traducteurs de transport (Topo-Trn-traducteur) ne modifient pas le flux RTP lui-même mais sont concernés par les paramètres de transport. Les paramètres de transport, au sens de ce paragraphe, comprennent les adresses de transport (pour faire le pont entre différents domaines comme de l'envoi individuel à la diffusion groupée) et la mise en paquets des supports pour permettre que d'autres protocoles de transport soient interconnectés à une session (dans des passerelles).

Les traducteurs qui font le pont entre différents mondes de protocoles sont concernés par la transposition du concept de SSRC/CSRC (source contributive) en protocole non RTP. Quand on conçoit un traducteur en un protocole de transport non fondé sur RTP, une considération importante est comment traiter les différentes sources et leurs identités. Ce problème n'est pas discuté plus avant.

Dans les traducteurs de transport, le présent mémoire s'intéresse principalement à ceux qui utilisent RTP sur les deux côtés, et c'est ce qui est supposé à partir d'ici.

Les traducteurs de transport les plus basiques qui opèrent en dessous du niveau de RTP ont déjà été discutés au paragraphe 3.2.1.1.

3.2.1.3 Traducteur de supports

Nom abrégé : Topo-Media-traducteur

Les traducteurs de supports (Topo-Media-traducteur) modifient les supports dans le flux RTP. Ce processus est couramment appelé le transcodage. La modification des supports peut être aussi petite que de supprimer des parties du flux, et elle peut aller jusqu'à un décodage et recodage complet du flux (jusqu'au niveau de l'échantillon ou équivalent) en utilisant un codec de supports différent. Les traducteurs de supports sont couramment utilisés pour connecter les points d'extrémité sans un point commun d'interopérabilité dans le codage des supports.

Les traducteurs de supports autonomes sont rares. Le plus courant est une combinaison de traducteur de transport et de supports utilisée pour traduire les deux aspects de supports et de transport du flux RTP portant les supports entre deux domaines de transport.

Quand la traduction des supports se produit, la tâche du traducteur en ce qui concerne le traitement du trafic RTCP devient substantiellement plus complexe. Dans ce cas, le traducteur a besoin de réécrire le rapport de receveur RTCP du point d'extrémité B avant de le transmettre au point d'extrémité A. La réécriture est nécessaire parce que le flux RTP reçu par B n'est pas le même flux RTP que reçoivent les autres participants. Par exemple, le nombre de paquets transmis à B peut être inférieur à celui que A envoie, à cause des différences de format des supports et de débit des données. Donc, si les rapports de receveur étaient transmis sans changement, le plus haut numéro de séquence étendu indiquerait que B a été

substantiellement en dessous en réception, alors que ce n'est très probablement pas le cas. Donc, le traducteur doit traduire ce numéro en un numéro de séquence correspondant pour le flux que le traducteur a reçu. Des exigences similaires existent pour la plupart des autres champs dans les rapports de receveur RTCP.

Un traducteur de supports peut dans certains cas agir au nom de la source "réelle" (le point d'extrémité qui envoie à l'origine les supports au traducteur) et répondre aux messages de rétroaction RTCP. Cela peut arriver, par exemple, quand un point d'extrémité receveur demande une réduction de bande passante, et que le traducteur de supports n'a pas détecté d'encombrement ou d'autres raisons pour une réduction de bande passante entre le point d'extrémité envoyeur et lui-même. Dans ce cas, il est raisonnable que le traducteur de supports réagisse aux messages de contrôle de codec eux-mêmes, par exemple, en transcodant à un débit de supports inférieur.

Une variante de comportement de traducteur qui mérite d'être signalée est celle décrite à la Figure 3 d'un point d'extrémité A qui envoie à B un flux RTP contenant des supports (seulement). Sur le chemin, il y a un appareil T qui manipule le flux RTP au nom de A. Un exemple courant est que T ajoute un second flux RTP contenant des informations de correction d'erreur directe (FEC, *Forward Error Correction*) afin de protéger le flux RTP de A (non protégé par la FEC). Dans ce cas, T a besoin de lier sémantiquement le nouveau flux RTP de FEC au flux RTP de A qui porte les supports, par exemple, en utilisant le même CNAME que A.

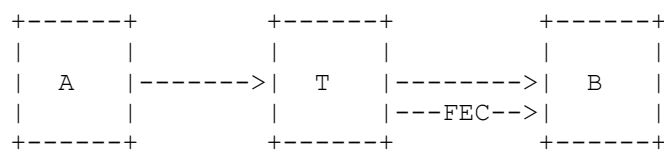


Figure 3: Traducteur de supports ajoutant la FEC

Il peut aussi y avoir des cas où l'information est ajoutée dans le flux RTP original, tout en laissant intacts la plupart ou tous les paquets RTP originaux (à l'exception de certains champs d'en-tête RTP, comme les numéros de séquence). Un exemple est l'injection de métadonnées dans le flux RTP, portées dans leurs propres paquets RTP.

De même, un traducteur de supports peut parfois retirer des informations d'un flux RTP, tout en laissant par ailleurs les paquets RTP restants inchangés (là encore à l'exception de certains champs d'en-tête RTP).

Tout type de fonctionnalité où T manipule le flux RTP, ou ajoute flux RTP un d'accompagnement, au nom de A est aussi couvert par la définition de traducteur de supports.

3.2.2. Sessions RTP dos à dos

Nom abrégé : Topo-Dos à dos

Il existe des boîtiers de médiation qui interconnectent deux points d'extrémité (A et B) à travers eux-mêmes (MB), mais qui ne font pas partie d'une session RTP commune. À la place, ils établissent deux sessions RTP différentes : une entre A et le boîtier de médiation et une autre entre le boîtier de médiation et B. Cette topologie est appelée Topo-Dos-à-dos.

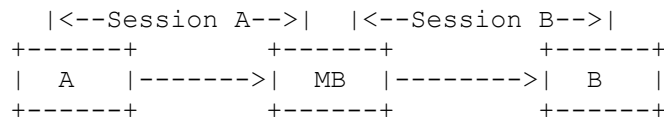


Figure 4 : Sessions RTP dos à dos à travers un boîtier de médiation

Le boîtier de médiation qui agit comme une passerelle de niveau application fait un pont entre les deux sessions RTP. Ce pontage peut être aussi basique que de transmettre les charges utiles RTP entre les sessions ou plus complexe en incluant le transcodage des supports. La différence de cette topologie par rapport au contexte d'une seule session RTP est le traitement des SSRC et des autres identifiants relatifs à la session, comme les CNAME. Avec deux sessions RTP différentes, ils peuvent être changés librement et il est de la responsabilité du boîtier de médiation de maintenir les relations correctes.

La signalisation ou d'autres fonctionnalités de niveau RTP ci-dessus qui font référence au flux RTP peuvent être ce qui est le plus impacté par l'utilisation de deux sessions RTP et du changement d'identifiants. La structure avec deux sessions RTP met aussi une exigence de contrôle d'encombrement sur le boîtier de médiation, parce qu'il devient pleinement responsable du flux de supports qu'il génère dans chacune des sessions.

L'adhérence au contrôle d'encombrement peut être résolue localement sur chacun des deux segments ou en pontant les statistiques provenant du point d'extrémité receveur à travers le boîtier de médiation au point d'extrémité envoyeur. Du point de vue d'une mise en œuvre, cependant, cette dernière exige de traiter un certain nombre d'incohérences. D'abord, la perte de paquet doit être détectée pour un flux RTP envoyé de A au boîtier de médiation, et cette perte doit être rapportée au moyen d'un numéro de séquence sauté dans le flux RTP du boîtier de médiation à B. Ce couplage et les incohérences résultantes sont conceptuellement plus faciles à traiter quand on considère les deux flux RTP comme appartenant à une seule session RTP.

3.3 Point à multipoints utilisant la diffusion groupée

La diffusion groupée est une fonctionnalité de couche IP qui est disponible dans certains réseaux. Deux nuances principales peuvent être distinguées : la diffusion groupée toutes sources (ASM, *Any-Source Multicast*) [RFC1112] où tout participant au groupe de diffusion groupée peut envoyer à l'adresse de groupe et s'attendre à ce que le paquet arrive à tous les participants au groupe, et la diffusion groupée spécifique de source (SSM, *Source-Specific Multicast*) [RFC3569], où seulement un hôte IP particulier envoie au groupe de diffusion groupée. Chacun de ces modèles est discuté dans les paragraphes suivants.

3.3.1 Diffusion groupée toutes sources (ASM)

Nom abrégé : Topo-ASM (était Topo-Multicast)

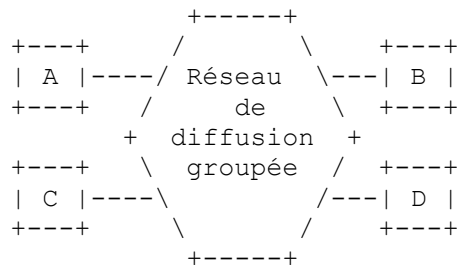


Figure 5 : Point à multipoints utilisant la diffusion groupée

Le point à multipoints (PtM) est défini ici comme utilisant une topologie de diffusion groupée comme modèle de transmission, dans lequel le trafic provenant de tout participant au groupe de diffusion groupée atteint tous les autres participants au groupe de diffusion groupée, excepté dans les cas de :

- o perte de paquet, ou
- o quand un participant au groupe de diffusion groupée ne souhaite pas recevoir le trafic pour un groupe de diffusion groupée spécifique et donc, n'a pas souscrit au groupe de diffusion groupée IP en question. Ce scénario peut se produire, par exemple, lorsque une session multimédia est distribuée en utilisant deux groupes de diffusion groupée ou plus, et un participant à un groupe de diffusion groupée est abonné seulement à un sous ensemble de ces sessions.

Dans le contexte ci-dessus, "trafic" englobe les deux trafics RTP et RTCP. Le nombre de participants au groupe de diffusion groupée peut varier entre un et beaucoup, car RTP et RTCP s'adapte à de très grands groupes de diffusion groupée (la limite théorique du nombre de participants dans une seule session RTP est dans la gamme des milliards). Cela peut être réalisé en utilisant ASM.

Pour l'usage de rétroactions, il est utile de définir un "petit groupe de diffusion groupée" comme un groupe où le nombre de participants au groupe de diffusion groupée est assez faible (et où les autres facteurs comme la connexité sont assez bons) pour permettre aux participants d'utiliser des rétroactions précoces ou immédiates, comme défini dans AVPF [RFC4585]. Même quand l'environnement permettrait l'utilisation d'un petit groupe de diffusion groupée, certaines applications peuvent quand même vouloir utiliser des options plus limitées pour les rétroactions RTCP disponibles aux grands groupes de diffusion groupée, par exemple, quand il est probable que le seuil du petit groupe de diffusion groupée (en termes de participants au groupe de diffusion groupée) peut être excédé durant la vie d'une session.

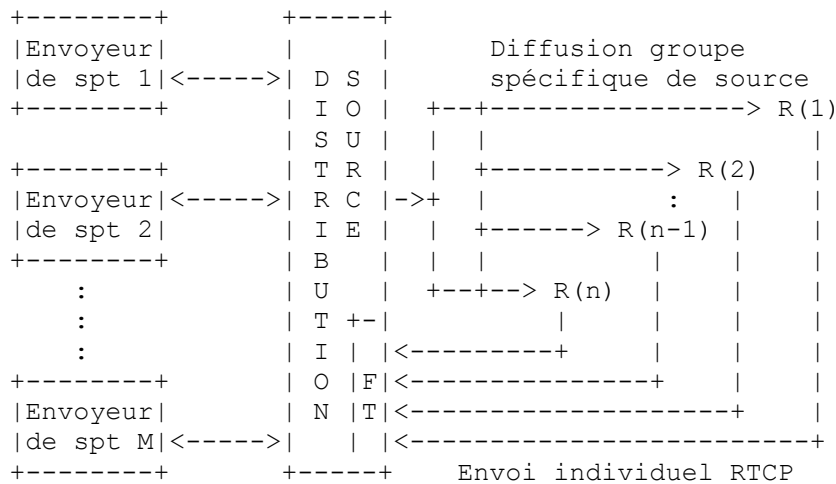
Les messages de rétroaction RTCP en diffusion groupée atteignent comme données de supports, chaque abonné (sous réserve des pertes de paquets et de l'abonnement au groupe de diffusion groupée). Donc, le mécanisme de suppression de rétroactions discuté dans la [RFC4585] est normalement exigé. Chaque point d'extrémité individuel qui est un participant au groupe de diffusion groupée a besoin de traiter chaque message de rétroaction qu'il reçoit, non seulement pour

déterminer si il est affecté ou si le message de rétroaction s'applique seulement à un autre point d'extrémité, mais aussi pour déduire les restrictions de rythme sur l'envoi de ses propres messages de rétroaction, si il en est.

3.3.2 Diffusion groupée spécifique de source (SSM)

Nom abrégé : Topo-SSM

Dans la diffusion groupée toutes sources, tout participant au groupe de diffusion groupée peut envoyer à tous les autres participants au groupe de diffusion groupée, en envoyant un paquet au groupe de diffusion groupée. À l'opposé, la diffusion groupée spécifique de source [RFC3569], [RFC4607] se réfère à des scénarios où seulement une source (source de distribution) peut envoyer au groupe de diffusion groupée, créant une topologie qui ressemble à celle ci-dessous :



FT (*Feedback Target*) cible de rétroaction : le transport de la cible de rétroaction à la source de distribution est via l'envoi individuel ou la diffusion groupée RTCP si elles ne sont pas colocalisées.

Figure 6 : Point à multipoints utilisant la diffusion groupée spécifique de source

Dans la topologie SSM (Figure 6), un certain nombre de points d'extrémité RTP envoyeurs (appelés sources RTP à partir d'ici) (1 à M) sont autorisés à envoyer des supports au groupe SSM. Ces sources envoient des supports à une source de distribution dédiée, qui transmet le flux RTP au groupe de diffusion groupée au nom des sources RTP originales. Le flux RTP atteint les points d'extrémité receveurs (appelés receveurs à partir d'ici) (R(1) à R(n)). Les messages RTCP des receveurs ne peuvent pas être envoyés au groupe de diffusion groupée, car le groupe de diffusion groupée SSM a par définition seulement un envoyeur IP. Pour prendre en charge RTCP, une extension RTP pour SSM [RFC5760] a été définie. Elle utilise la transmission en envoi individuel pour envoyer RTCP depuis chaque receveur à une ou plusieurs cibles de rétroaction (FT, *Feedback Target*). Les cibles de rétroaction relayent le RTCP non modifié, ou fournissent un sommaire des rapports RTCP des participants au groupe entier en transmettant le trafic RTCP à la source de distribution. La Figure 6 montre seulement une seule cible de rétroaction intégrée dans la source de distribution, mais pour l'adaptabilité, la FT peut être répartie et chaque instance peut avoir la responsabilité de sous groupes de receveurs. Pour les rapports sommaires, cependant, il doit normalement y avoir une seule cible de rétroaction qui agrège tous les sommaires en un message commun pour tout le groupe receveur.

L'extension RTP pour SSM spécifie comment les rétroactions (les informations de réception et les événements spécifiques de la rétroaction) sont traitées. Les problèmes plus généraux associés à l'utilisation de la diffusion groupée, où chacun reçoit ce qu'envoie la source de distribution, doivent être pris en compte.

La situation susmentionnée résulte en un comportement commun pour la diffusion groupée RTP :

1. Les applications de diffusion groupée utilisent souvent un groupe de sessions RTP, et non pas une seule. Chaque point d'extrémité a besoin d'être un membre de la plupart ou de toutes ces sessions RTP afin de bien fonctionner.
2. Au sein de chaque session RTP, le nombre de collecteurs de supports va probablement être bien plus grand que le nombre de sources RTP.
3. Les applications de diffusion groupée ont besoin de signaler les fonctions pour identifier les relations entre les sessions RTP.

- 4. Les applications de diffusion groupée ont besoin de signaler les fonctions pour identifier les relations entre les SSRC dans les différentes sessions RTP.

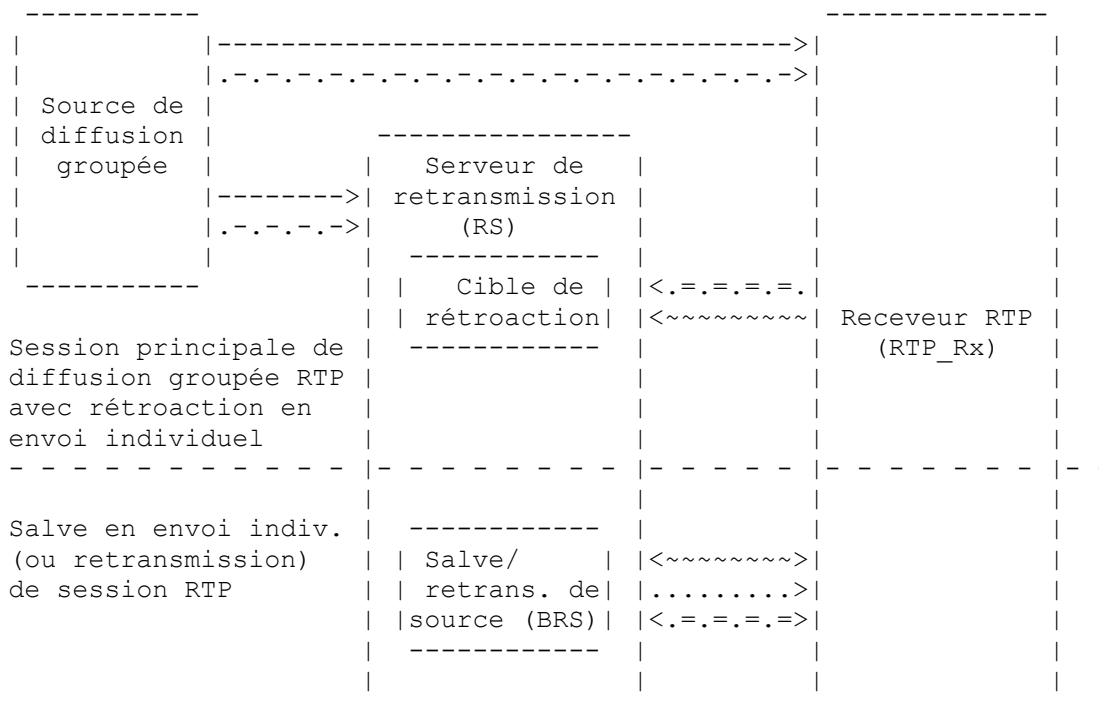
Toutes les configurations de diffusion groupée partagent une exigence de signalisation : tous les points d'extrémité ont besoin d'avoir le même RTP et la même configuration de type de charge utile. Autrement, le point d'extrémité A pourrait, par exemple, utiliser le type de charge utile 97 pour identifier le vidéo codec H.264, tandis que le point d'extrémité B l'identifierait comme MPEG-2, avec des résultats imprévisibles mais très certainement pas plaisants à voir.

Les solutions de sécurité pour ce type de communication de groupe sont aussi un défi. D'abord, la gestion de clés et le protocole de sécurité doivent prendre en charge la communication de groupe. L'authentification de la source devient plus difficile et exige des solutions spécialisées. Pour plus de discussion sur ce sujet, voir "Options pour sécuriser les sessions RTP" [RFC7201].

3.3.3 SSM avec ressources locale en diffusion individuelle

Nom abrégé : Topo-SSM-RAMS

L'acquisition rapide fondée sur l'envoi individuel de sessions RTP de diffusion groupée " [RFC6285] résulte en extensions supplémentaires à la topologie SSM.



-----> Flux RTP de diffusion groupée
 .-.-.-.-> Flux RTCP de diffusion groupée
 .=.=.=.==> Rapports RTCP en envoi individuel
 ~~~~~> Messages en envoi individuel de rétroaction RTCP  
 .....> Flux RTP en envoi individuel

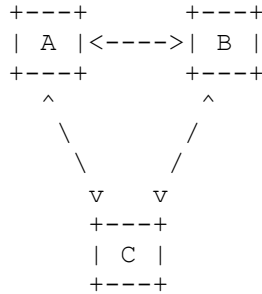
**Figure 7 : SSM avec ressources locales d'envoi individuel (RAMS)**

L'extension d'acquisition rapide permet à un point d'extrémité qui se joint à une session SSM de diffusion groupée de demander que les supports commençant au dernier point de synchronisation (à partir d'où les supports peuvent être décodés sans exiger de contexte établi par le décodage avant les paquets) soient envoyés à grande vitesse jusqu'au moment où, après le décodage de ces paquets de supports livrés par salves, le rythme correct de supports est rétabli, c'est-à-dire que les paquets de supports sont reçus dans les intervalles de mémoire tampon adéquats pour cette application. Ceci est réalisé en établissant d'abord une session RTP PtP en envoi individuel entre la source de salve/retransmission (BRS) (Figure 7) et le receveur RTP. La session en envoi individuel est utilisée pour transmettre les paquets en antémémoire provenant du groupe de diffusion groupée à une vitesse supérieure à la normale afin de synchroniser le receveur au flux RTP de diffusion

groupée en cours. Une fois que le receveur RTP et son décodeur ont accroché la livraison en cours de la session de diffusion groupée, le receveur passe à la réception directe du groupe de diffusion groupée. Dans de nombreuses applications déployées, la session RTP en point à point (qui existe toujours) est utilisée comme canal de réparation, c'est-à-dire, pour le trafic RTP de retransmission des paquets non reçus du groupe de diffusion groupée.

### 3.4 Point à multipoints utilisant le maillage

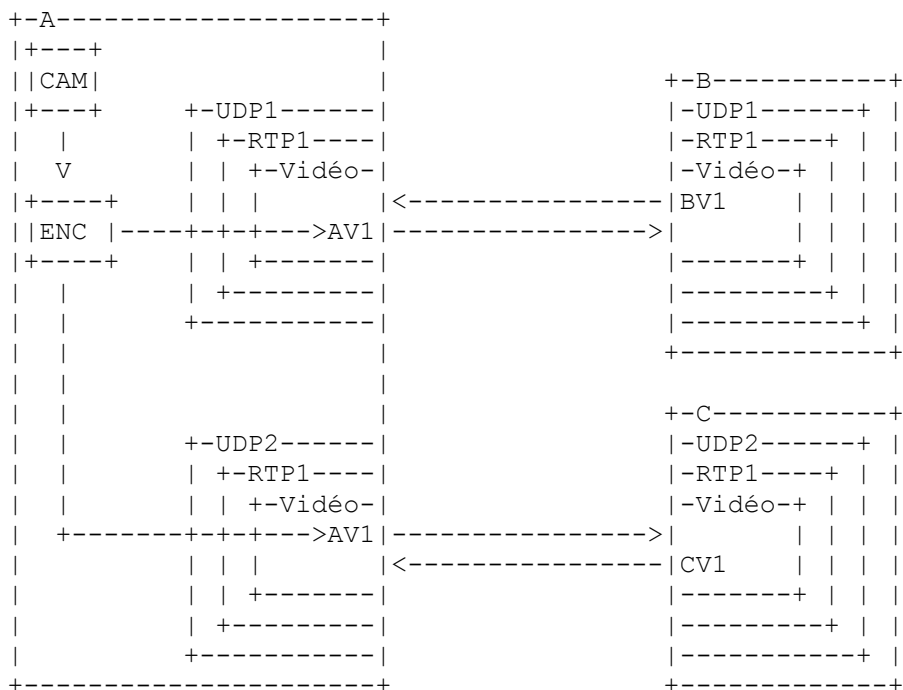
Nom abrégé : Topo-Maillage



**Figure 8 : Point à multipoints utilisant un maillage**

Sur la base de la définition de session RTP, il est clairement possible d'avoir une session RTP conjointe impliquant trois points d'extrémité ou plus sur plusieurs flux de transport en envoi individuel, comme la session à trois points d'extrémité joints décrite ci-dessus. Dans ce cas, A a besoin d'envoyer ses flux RTP et ses paquets RTCP aux deux B et C sur leurs flux de transport respectifs. Tant que tous les points d'extrémité font la même chose, chacun va avoir une vue conjointe de la session RTP.

Cette topologie ne crée aucune exigence supplémentaire au delà du besoin d'avoir plusieurs flux de transport associés à une seule session RTP. Noter qu'un point d'extrémité peut utiliser un seul accès local pour recevoir tous ces flux de transport (dans ce cas, l'accès d'envoi, l'adresse IP, ou la SSRC peut être utilisé pour le démultiplexage) ou il pourrait avoir des accès de réception locaux séparés pour chaque point d'extrémité.



**Figure 9 : Maillage multi envois individuels avec session RTP jointe**

La Figure 9 décrit la vue du point d'extrémité A en utilisant une session RTP commune quand il établit le maillage comme montré à la Figure 8. Il y a seulement une session RTP (RTP1) mais deux flux de transport (UDP1 et UDP2). La source des supports (CAM) est codée et transmise sur la SSRC (AV1) à travers les deux couches de transport. Cependant, comme c'est



### 3.5.1 Traducteur de relais - transport

Nom abrégé : Topo-PtM-Trn-traducteur

Ce paragraphe discute des usages seulement de traducteur de transport pour activer des sessions en multipoints.

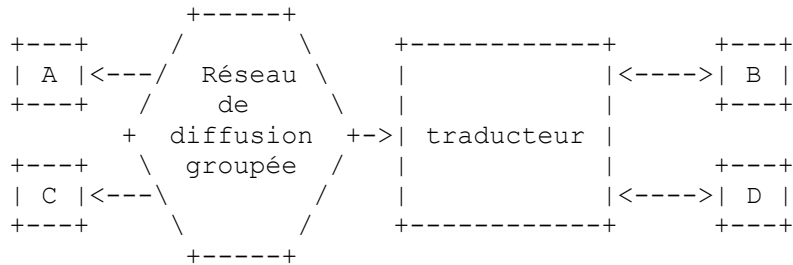


Figure 11 : Point à multipoints utilisant la diffusion groupée

La Figure 11 décrit un exemple de traducteur de transport qui effectue au moins la traduction d'adresse IP. Il permet aux points d'extrémité B et D (qui n'ont pas la capacité de diffusion groupée) de prendre part à une session de diffusion groupée toutes sources qui implique les points d'extrémité A et C, en ayant le traducteur qui transmet leur trafic en envoi individuel aux adresses de diffusion groupée utilisées, et vice versa. Il doit aussi transmettre le trafic de B pour D, et vice versa, pour fournir à B et D une vue complète de la session.

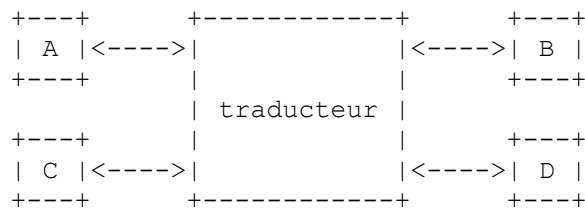


Figure 12 : traducteur (relais) RTP avec seulement des chemins d'envoi individuel

Un autre scénario de traducteur est décrit dans la Figure 12. Le traducteur dans ce cas connecte plusieurs points d'extrémité par envoi individuel. Cela peut être mis en œuvre en utilisant un très simple traducteur de transport qui, dans le présent document, est appelé un relais. Le relais transmet tout le trafic qu'il reçoit, RTP et RTCP, à tous les autres points d'extrémité. En faisant ainsi, un réseau de diffusion groupée est émulé sans s'appuyer sur une infrastructure de réseau à capacité de diffusion groupée.

Pour les rétroactions RTCP, il en résulte un ensemble de considérations similaires à celles décrites dans la topologie ASM de RTP. Il y a aussi des exigences de signalisation supplémentaires pour l'établissement de session ; par exemple, une configuration commune de types de charge utile RTP est exigée.

Les traducteurs de transport et les relais devraient toujours considérer de mettre en œuvre le filtrage d'adresse de source, pour empêcher des attaquants d'utiliser les accès d'écoute sur le traducteur pour injecter du trafic. Le traducteur peut, cependant, aller une étape plus loin, en particulier si la signalisation explicite de SSRC est utilisée, pour empêcher les points d'extrémité d'envoyer une SSRC autre que la leur propre (qui sont, par exemple, utilisées par les autres participants à la session). Cela peut améliorer les propriétés de sécurité de la session, en dépit de l'utilisation de clés de groupe qui au niveau cryptographique permettent à n'importe qui de se faire passer pour quelqu'un d'autre dans la même session RTP.

Un traducteur qui ne change pas le contenu du paquet RTP/RTCP peut fonctionner sans exiger d'avoir accès aux contextes de sécurité utilisés pour protéger le trafic RTP/RTCP entre les participants.

### 3.5.2 Traducteur de supports

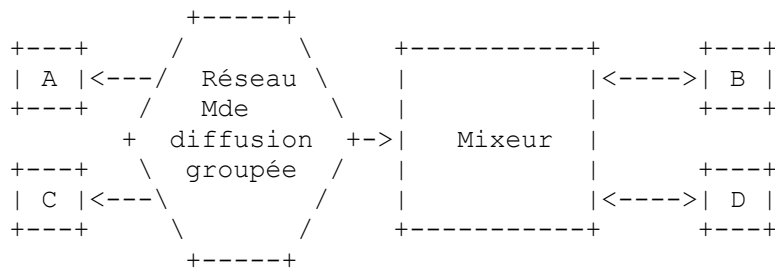
Dans le contexte de communications en multipoints, un traducteur de supports ne fournit pas de nouveau mécanisme pour établir une session multipoints. Il est plus un facilitateur qui assure qu'un certain point d'extrémité ou un ensemble défini de points d'extrémité peut participer à la session. Si le point d'extrémité B dans la Figure 11 était derrière un chemin de réseau limité, le traducteur pourrait effectuer un transcodage des supports pour permettre au trafic reçu des autres points

d'extrémité d'atteindre B sans surcharger le chemin. Ce transcodage peut aider les autres points d'extrémité dans la partie diffusion groupée de la session, en n'exigeant pas la qualité transmise par A et en l'abaissant aux débits binaires que B est en fait capable de recevoir (et vice versa).

### 3.6 Point à multipoints utilisant le modèle de mixeur de la RFC 3550

Nom abrégé : Topo-Mixeur

Un mixeur est un boîtier de médiation qui agrège plusieurs flux RTP qui font partie d'une session en générant un ou plusieurs nouveaux flux RTP et, dans la plupart des cas, en manipulant les données du support. Une application courante pour un mixeur est de permettre à un participant de recevoir une session avec une quantité réduite de ressources.



**Figure 13 : Point à multipoints utilisant le modèle de mixeur de la RFC 3550**

Un mixeur peut être vu comme un appareil qui termine le flux RTP reçu des autres points d'extrémité dans la même session RTP. En utilisant les données de supports portées dans le flux RTP reçu, un mixeur génère des flux RTP dérivés qui sont envoyés aux points d'extrémité receveurs.

Le contenu que fournit le mixeur est l'agrégat mélangé de ce que le mixeur reçoit sur les chemins PtP ou PtM, qui font partie de la même session de communication.

Le mixeur crée la source des supports et le flux RTP de source tout comme un point d'extrémité, car il mixe le contenu (souvent dans le domaine non compressé) et ensuite le code et le met en paquets pour sa transmission à un point d'extrémité receveur. Les champs Compte de CSRC (CC) et CSRC dans l'en-tête RTP peuvent être utilisés pour indiquer les contributeurs au nouveau flux RTP généré. Les SSRC des flux à mixer à l'entrée du mixeur apparaissent comme les CSRC à la sortie du mixeur. Ce flux de sortie utilise une unique SSRC qui identifie le flux du mixeur. La CSRC devrait être transmise entre les différents points d'extrémité pour permettre la détection de boucles et l'identification des sources qui font partie de la session de communication. Noter que le paragraphe 7.1 de la RFC 3550 exige que l'espace de SSRC soit partagé entre les domaines pour ces raisons. Cela implique aussi que toutes les informations de SDES ont normalement besoin d'être transmises à travers le mixeur.

Le mixeur est chargé de générer les paquets RTCP en accord avec son rôle. Il est un receveur RTP et devrait donc envoyer les rapports de receveur RTCP pour les flux RTP qu'il reçoit et termine. Dans son rôle d'envoyeur RTP, il devrait aussi générer des rapports d'envoyeur RTCP pour les flux RTP qu'il envoie. Comme spécifié au paragraphe 7.3 de la RFC 3550, un mixeur ne doit pas transmettre RTCP non altéré entre les deux domaines.

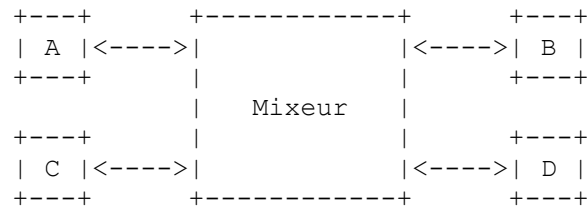
Le mixeur décrit à la Figure 13 est impliqué dans trois domaines qui doivent être séparés : le réseau de diffusion groupée toutes sources (incluant les points d'extrémité A et C) le point d'extrémité B, et le point d'extrémité D. En supposant que tous les quatre points d'extrémité dans la conférence soient intéressés à recevoir le contenu provenant de tous les autres points d'extrémité, le mixeur produit différents flux RTP mixés pour B et D, car celui pour B peut contenir du contenu reçu de D, et vice versa. Cependant, le mixeur peut seulement avoir besoin d'une SSRC par type de supports dans chaque domaine où il est l'entité receveuse et le transmetteur du contenu mixte.

Dans le domaine de diffusion groupée, un mixeur a encore besoin de fournir une vue mixte des autres domaines. Cela rend le mixeur plus simple à mettre en œuvre et évite tous les problèmes avec le traitement avancé de RTCP ou la détection de boucles, qui seraient problématiques si le mixeur avait un comportement non symétrique. Voir au paragraphe 3.11 des détails sur ce sujet. L'opération de mixage pourrait cependant être différente dans chaque domaine.

Un mixeur est chargé de recevoir les messages de rétroaction RTCP et de les traiter de façon appropriée. La définition de "approprié" dépend du message lui-même et du contexte. Dans certains cas, la réception d'un message de contrôle de codec par le mixeur peut résulter en la génération et la transmission de messages de rétroaction RTCP par le mixeur aux points

d'extrémité dans le ou les autres domaines. Dans d'autres cas, un message est traité en local par le mixeur et donc non transmis dans un autre domaine.

Quand on remplace le réseau de diffusion groupée de la Figure 13 (à la gauche du mixeur) par des chemins d'envoi individuel comme décrit à la Figure 14, le modèle de mixeur est très similaire à celui discuté au paragraphe 3.9. Voir la discussion du paragraphe 3.9 sur les différences entre ces deux modèles.



**Figure 14 : Mixeur RTP avec seulement des chemins en envoi individuel**

On discute maintenant en détails des différentes opérations de mixage qu'un mixeur peut effectuer et comment elles peuvent affecter le comportement de RTP et RTCP.

### 3.6.1 Mixeur de mixage de supports

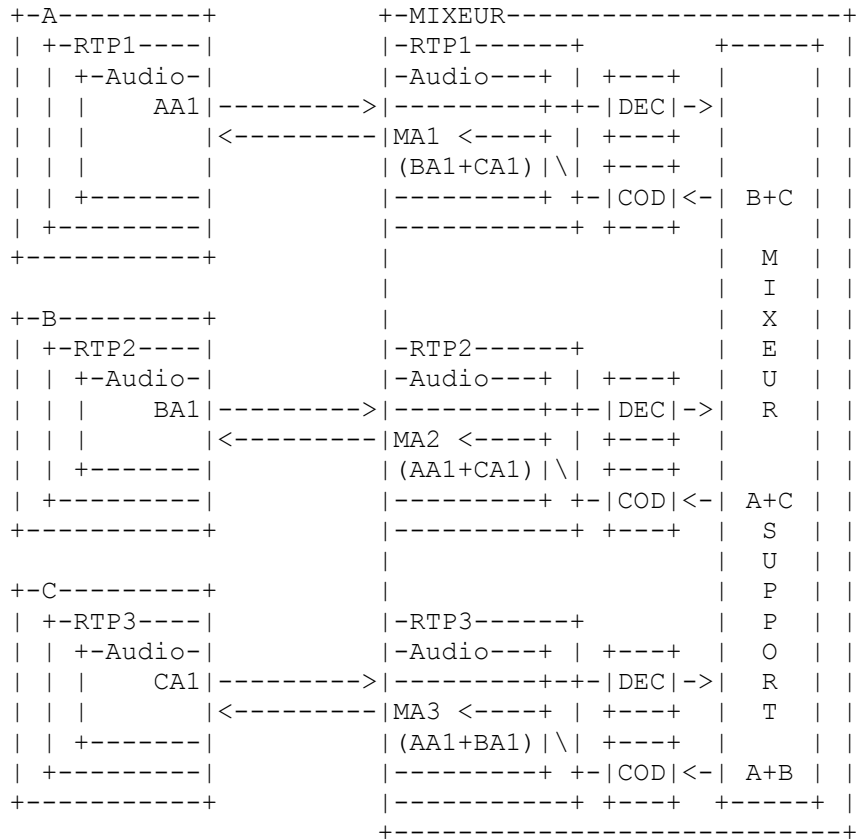
Le mixeur de mixage de supports est probablement celui auquel on pense le plus souvent quand on entend le terme "mixeur". Son mode de fonctionnement de base est qu'il reçoit un flux RTP de plusieurs points d'extrémité et choisit le ou les flux à inclure dans un mélange de domaines de supports. Le choix peut être par configuration statique ou dynamique, par des moyens qui dépendent du contenu, comme une activation vocale. Le mixeur crée alors un seul flux RTP sortant à partir de ce mélange.

Le mixeur de mixage de supports le plus couramment déployé est probablement le mixeur audio, utilisé dans les conférences vocales, où le résultat consiste en un mélange de tous les signaux audio d'entrée ; cela a besoin qu'une signalisation minimale soit établie. Du point de vue du traitement du signal, le mixage audio est relativement direct et couramment possible pour un nombre raisonnable de points d'extrémité. Supposons, par exemple, qu'on veuille mixer  $N$  flux provenant de  $N$  différents points d'extrémité. Le mixeur a besoin de décoder ces  $N$  flux, normalement dans le domaine d'échantillonnage, et ensuite de produire  $N$  ou  $N+1$  mélanges. Différents mélanges sont nécessaires afin que chaque point d'extrémité obtienne un mélange de toutes les autres sources sauf la sienne, car il en résulterait un écho. Quand  $N$  est inférieur au nombre de tous les points d'extrémité, on peut produire un mélange de tous le  $N$  flux pour le groupe qui ne sont pas actuellement inclus dans le mélange ; donc,  $N+1$  mélanges. Ces flux audio sont alors codés à nouveau, mis en paquets RTP, et envoyés. Dans de nombreux cas, la normalisation du niveau audio, la suppression de bruit, et des étapes similaires de traitement du signal sont aussi exigées ou désirables avant que commence le processus réel de mixage.

En vidéo, le terme "mixage" a une interprétation différente de celle de l'audio. Il est couramment utilisé pour se référer au processus de combinaison spatiale des flux vidéo contributeurs, qui est aussi appelé un "pavage". Les vidéos reconstruites, adaptées de façon appropriée, peuvent être arrangées dans l'espace comme un ensemble de tuiles, chaque tuile contenant la vidéo provenant d'un point d'extrémité (montrant normalement un participant humain). Les tuiles peuvent être de tailles différentes afin que, par exemple, un participant particulièrement important, ou l'orateur qui parle le plus fort, soit montré dans une tuile plus grande que les autres participants. Une image de soi-même peut être incluse dans le pavage, qui peut être produite en local ou comme rétroaction provenant d'un mixeur et une image vidéo reconstruite. Une telle boucle à distance permet une surveillance en toute confiance, c'est-à-dire, elle permet au participant de se voir lui-même avec la même qualité que les autres participants le voient. Le pavage fonctionne normalement sur la vidéo reconstruite dans le domaine d'échantillonnage. L'image pavée est codée, mise en paquets, et envoyée par le mixeur aux points d'extrémité receveurs. Il est possible qu'un boîtier de médiation avec des tâches de mixage de supports contienne seulement un mixeur du type susmentionné, et dans ce cas, tous les participants voient nécessairement la même vidéo pavée, même si elle est envoyée sur des flux RTP différents. Plus courant, cependant, sont les arrangements de mixage où un mixeur individuel est disponible pour chaque accès sortant du boîtier de médiation, permettant des compositions individuelles pour chaque point d'extrémité receveur (une caractéristique généralement appelée un affichage personnalisé).

Un problème avec le mixage des supports est qu'il consomme à la fois de grandes quantités de ressources de traitement des supports (pour le processus de décodage et de mixage dans le domaine non compressé) et de ressources de codage (pour le codage du signal mélangé). Un autre problème est la dégradation de qualité créée par le décodage et recodage des supports, qui est le résultat de la nature encline aux pertes de la plupart des codecs de supports couramment utilisés. Un troisième problème est la latence introduite par le mixage des supports, qui peut être substantielle et perçue de façon dérangementante

dans le cas de vidéo, ou en cas d'audio si l'audio mixé est synchronisé avec le mouvement des lèvres dans une vidéo à latence élevée. L'avantage du mixage de supports est qu'il est direct pour les points d'extrémité de traiter le seul flux de supports (qui inclut l'agrégation mélangée de nombreuses sources) car ils n'ont pas besoin de traiter plusieurs décodages, mixages locaux, et composition. En fait, les mixeurs ont été introduits dans les temps qui précèdent RTP de sorte que les points d'extrémité receveurs traditionnels à un seul flux (qui, dans certains environnements de protocole, n'ont en fait pas besoin de connaître la nature multipoints de la conférence) peuvent réussir à participer à ce qu'un utilisateur reconnaîtrait comme une visioconférence multiparties.



**Figure 15 : Détails de session et de SSRC pour mixeur de supports**

Du point de vue de RTP, le mixage de supports peut être un processus très simple, comme on peut être le voir à la Figure 15. Le mixeur présente une SSRC vers le point d'extrémité receveur, par exemple, MA1 à l'homologue A, où le flux associé est le mélange de supports des autres points d'extrémité. Comme chaque homologue, dans cet exemple, reçoit une version différente d'un mélange provenant du mixeur, il n'y a pas de relation réelle entre les différentes sessions RTP en termes d'informations réelles de supports ou de niveau transport. Il y a cependant des relations communes entre RTP1-RTP3, à savoir les informations d'espace de SSRC et d'identité. Quand A reçoit le flux MA1, qui est une combinaison des flux BA1 et CA1, le mixeur peut inclure les informations de CSRC dans le flux MA1 pour identifier les sources contributives BA1 et CA1, permettant au receveur d'identifier les sources contributives même si cela n'était pas possible à travers les supports eux-mêmes ou par d'autres moyens de signalisation.

La CSRC a, à son tour, une utilité dans les extensions RTP, comme l'extension d'en-tête RTP pour indication de niveau audio de mixeur à client [RFC6465]. Si les SSRC provenant des chemins de point d'extrémité à mixeur sont utilisées comme des CSRC dans une autre session RTP, alors RTP1, RTP2, et RTP3 deviennent une session conjointe car ils ont un espace de SSRC commun. À ce point, le mixeur a aussi besoin de considérer quelles informations RTCP il a besoin d'exposer dans les différents chemins. Dans le scénario ci-dessus, un mixeur va normalement n'exposer rien de plus que les informations de SDES et le BYE RTCP pour une CSRC qui quitte la session. Le but principal serait d'activer le lien correct avec la logique d'application et autres sources d'informations. Cela active aussi la détection de boucle dans la session RTP.

### 3.6.2 Mixeur de commutation de supports

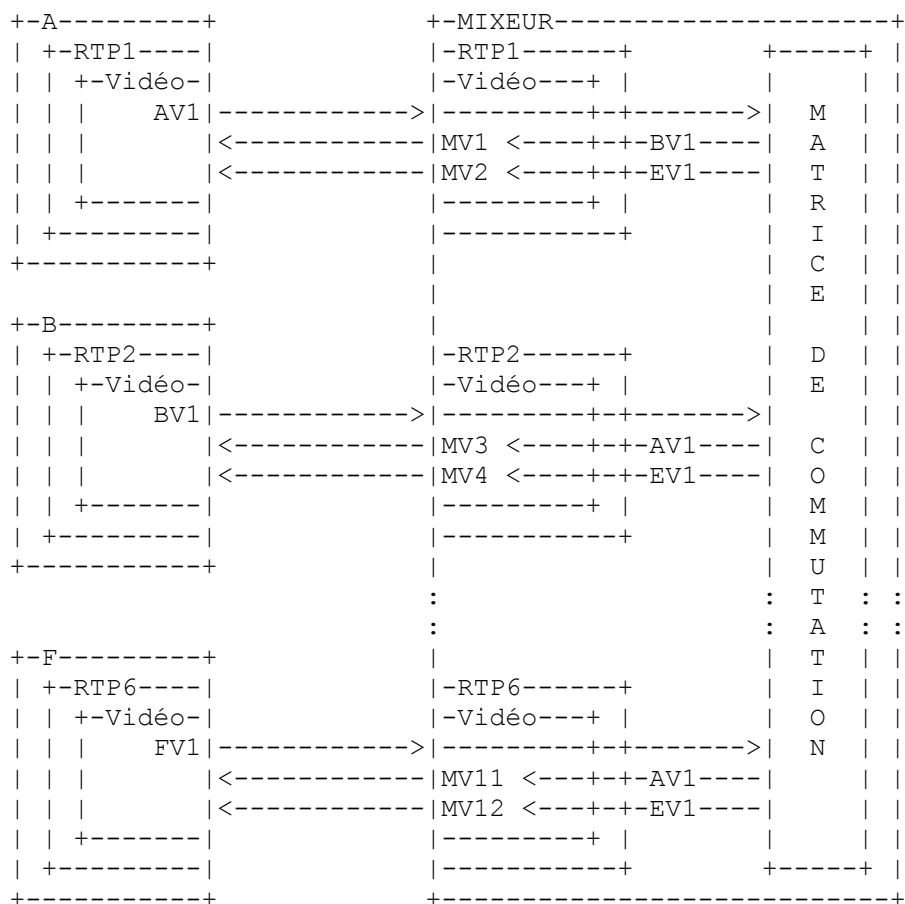
Les mixeurs de commutation de supports sont utilisés dans des scénarios de fonctionnalité limitée où pas, ou seulement très peu de présentation concurrente de plusieurs sources est exigé par l'application et aussi dans des usages plus complexes multi-flux avec le receveur qui mixe ou pave, incluant en combinaison avec la diffusion simultanée et/ou l'adaptabilité entre

source et mixeur. Un mixeur RTP fondé sur la commutation de supports évite les opérations de décodage et codage des supports dans le mixeur, car il transmet théoriquement le flux de supports codés qu'il envoyait au mixeur. Il n'évite cependant pas le cycle de déchiffrement et rechiffrement lorsque il réécrit les en-têtes RTP. Transmettre les supports (à la différence de reconstruire-mixer-coder les supports) réduit la quantité de ressources de calcul nécessaires dans le mixeur et augmente la qualité des supports (à la fois en termes de fidélité et de réduction de la latence).

Un mixeur de commutation de supports tient un réservoir de SSRC représentant les flux RTP conceptuels ou fonctionnels que le mixeur peut produire. Ces flux RTP sont créés en choisissant les supports d'un des flux RTP reçus par le mixeur et transmis à l'homologue en utilisant la propre SSRC du mixeur. Le mixeur peut commuter entre les sources disponibles si c'est exigé par le concept de la source, comme l'orateur actuellement actif. Noter que le mixeur, dans la plupart des cas, a quand même besoin d'effectuer une certaine quantité de traitement des supports, car de nombreux formats de supports ne permettent pas de "régler dans le flux" à des points arbitraires de leur flux binaire.

Pour réaliser un flux RTP cohérent à partir de la SSRC du mixeur, le mixeur a besoin de réécrire l'en-tête du paquet RTP entrant. D'abord, le champ SSRC doit être réglé à la valeur de la SSRC du mixeur. Ensuite, le numéro de séquence doit être le suivant dans la séquence des paquets sortants qu'il envoie. Troisièmement, la valeur de l'horodatage RTP doit être ajustée en utilisant un décalage qui change chaque fois qu'on commute la source des supports. Enfin, selon la négociation du type de charge utile RTP, la valeur qui représente cette configuration particulière de charge utile RTP peut devoir être changée si les différents chemins de point d'extrémité à mixeur ne sont pas arrivés sur le même numérotage pour une configuration donnée. Cela aussi exige que les différents points d'extrémité prennent en charge un ensemble commun de codecs, autrement le transcodage des supports pour la compatibilité de codec serait encore exigée.

On examine maintenant le fonctionnement d'un mixeur de commutation de supports qui prend en charge une visioconférence avec six points d'extrémité participants (A-F) où les deux plus récents orateurs dans la conférence sont montrés à chaque point d'extrémité receveur. Donc, le mixeur a deux SSRC qui envoient de la vidéo à chaque homologue, et chaque homologue est capable de traiter localement deux flux vidéo simultanément.



**Figure 16 : Mixeur RTP de commutation de supports**

Le mixeur de commutation de supports peut, comme le mixeur de mixage de supports, réduire le débit binaire exigé pour la transmission des supports vers les différents homologues en choisissant et transmettant seulement un sous ensemble des flux RTP qu'il reçoit des points d'extrémité envoyeurs. Dans le cas où le mixeur reçoit des transmissions en diffusion simultanée ou un codage adaptable de la source des supports, le mixeur a plus de degrés de liberté pour choisir des flux ou



sous ensembles de flux à transmettre à un point d'extrémité receveur, les deux fondés sur les restrictions de transport ou de point d'extrémité ainsi que sur la logique d'application.

Pour s'assurer qu'un receveur de supports dans un point d'extrémité peut correctement décoder les supports dans le flux RTP après une commutation, un codec qui utilise la prédiction temporelle a besoin de commencer son décodage à partir de points de rafraîchissement indépendants, ou de points dans le flux binaire qui offrent une fonction similaire (comme "des points de rafraîchissement sales"). Pour certains codecs, par exemple, les codecs audio et de parole fondés sur la trame, ceci est facilement réalisé en commençant le décodage aux limites de paquet RTP, car chaque limite de paquet donne un point de rafraîchissement (en supposant une mise en paquets appropriée du côté du codeur). Pour les autres codecs, en particulier dans la vidéo, les points de rafraîchissement sont moins courants dans le flux binaire ou peuvent n'être pas présents du tout sans une demande explicite au codeur concerné. Le message de contrôle de codec RTPC Demande intra complète [RFC5104] a été défini pour cela.

Dans ce type de mixeur, on pourrait considérer de terminer complètement les sessions RTP entre les différents chemins de point d'extrémité et de mixeur. Les mêmes arguments et considérations que discutés au paragraphe 3.9 doivent être pris en considération et s'appliquent ici.

### 3.7 Boîtier de médiation de transmission sélective

Une autre méthode pour traiter les supports dans le mixeur RTP est de "projeter", ou rendre disponible, toutes les sources RTP potentielles (SSRC) dans une session RTP indépendante par point d'extrémité. Le boîtier de médiation peut choisir laquelle des sources potentielles qui transmettent activement à ce moment des supports va être envoyée à chaque point d'extrémité. Ceci est similaire au mixeur de commutation de supports mais a quelques différences importantes dans les détails de RTP.

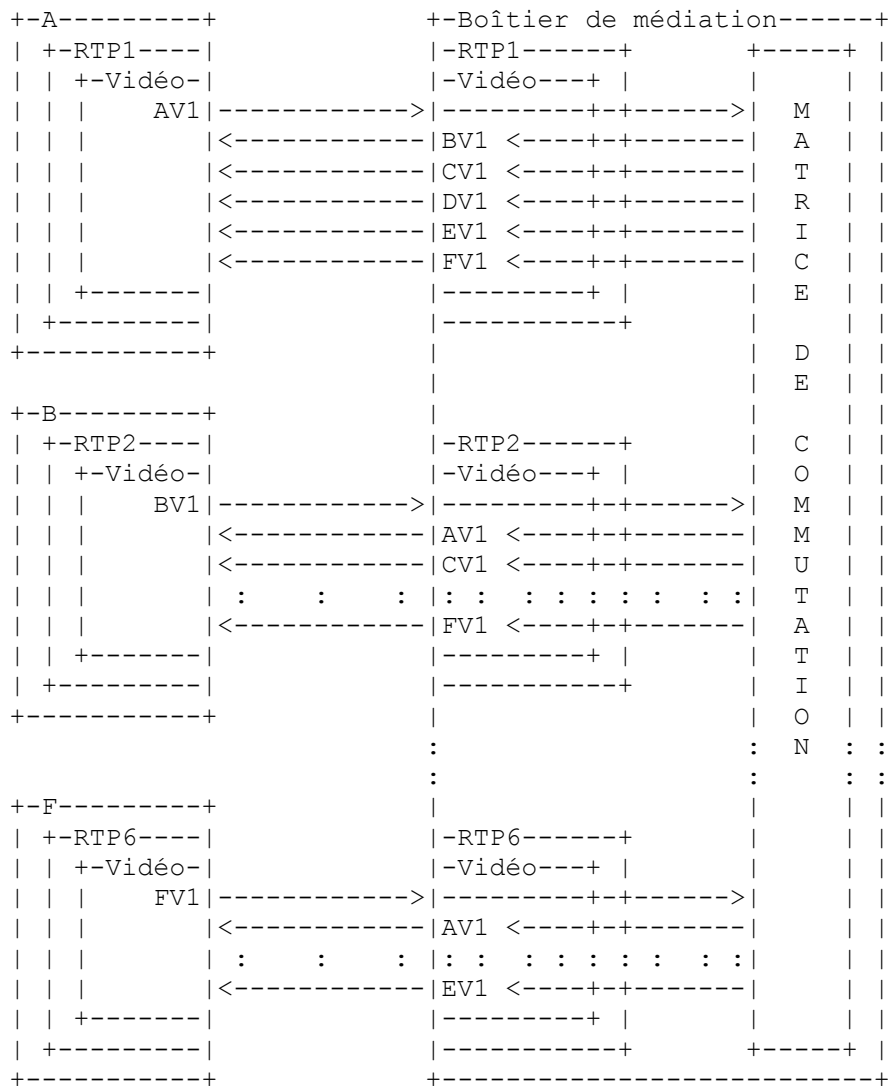


Figure 17 : Boîtier de médiation de transmission sélective

Dans la conférence à six points d'extrémité décrite ci-dessus (à la Figure 17) on peut voir que le point d'extrémité A a connaissance des cinq SSRC entrantes, BV1-FV1. Si ce boîtier de médiation a l'intention d'avoir un comportement similaire à celui du paragraphe 3.6.2 où le mixeur fournit aux points d'extrémité les deux derniers points d'extrémité qui ont pris la parole, alors seulement deux sur ces cinq SSRC ont besoin de transmettre concurremment des supports à A. Comme le boîtier de médiation choisit la source dans les différentes sessions RTP qui transmettent des supports aux points d'extrémité, chaque flux RTP exige de réécrire certains champs d'en-tête RTP quand ils sont projeté d'une session dans une autre. En particulier, le numéro de séquence a besoin d'être incrémenté de façon consécutive sur la base du paquet actuellement transmis dans chaque session RTP. Donc, le décalage de numéro de séquence RTP va changer chaque fois qu'une source est activée dans une session RTP. L'horodatage (éventuellement un décalage) reste le même.

Les sessions RTP peuvent être considérées comme indépendantes, d'où résulte que les numéros de SSRC utilisés peuvent aussi être traités indépendamment. Cela simplifie la détection et l'évitement de collision de SSRC mais exige des outils comme des tableaux de transposition entre les sessions RTP. Utiliser des sessions RTP indépendantes n'est pas exigé, car il est possible que le comportement de commutation s'effectue aussi avec un espace de SSRC commun. Cependant, dans ce cas, la détection et le traitement des collisions devient un problème différent. Il appartient à la mise en œuvre d'utiliser un seul espace de SSRC commun ou des espaces séparés.

Utiliser des espaces de SSRC séparés a des implications. Par exemple, le flux RTP qui est envoyé par le point d'extrémité B au boîtier de médiation (BV1) peut utiliser une valeur de SSRC de 12 345 678. Quand ce flux RTP est envoyé au point d'extrémité F par le boîtier de médiation, il peut utiliser toute valeur de SSRC, par exemple, 87 654 321. Par suite, chaque point d'extrémité peut avoir une vue différente de l'usage d'application d'une SSRC particulière. Toutes les informations d'identité de niveau RTP, comme les éléments de SDES, ont aussi besoin de mettre à jour la SSRC référencée, si les éléments de SDES inclus sont destinés à être mondiaux. Donc, l'application ne doit pas utiliser de SSRC comme référence au flux RTP quand elle communique directement avec d'autres homologues. Cela affecte aussi la détection de boucle, qui va échouer parce qu'il n'y a pas d'espace de noms et d'identités commun à travers les différentes branches de la session de communication au niveau RTP. À la place, cette responsabilité incombe aux couches supérieures.

Le boîtier de médiation est aussi responsable de la réception de toutes les demandes de contrôle de codec RTCP qui viennent d'un point d'extrémité et de décider si il peut agir sur la demande en local ou a besoin de traduire la demande dans la branche transport/session RTP qui contient la source des supports. Les points d'extrémité et le boîtier de médiation ont besoin de mettre en œuvre des fonctions de contrôle de codec en relation avec la conférence pour fournir une bonne expérience. La demande intra complète est couramment utilisée pour demander à la source des supports que des points de commutation soient fournis entre les sources et la demande de débit temporaire maximum de supports (TMMBR) pour permettre au boîtier de médiation d'agréger les réponses de contrôle d'encombrement vers la source des supports afin de lui permettre d'ajuster son débit binaire (évidemment, seulement dans le cas où la limitation n'est pas dans la liaison de la source au boîtier de médiation).

Le boîtier de médiation de transmission sélective a été introduit dans les systèmes de visioconférence récemment développés en conjonction avec, et pour s'appuyer sur le codage vidéo adaptable ainsi que la diffusion simultanée. Un exemple de codage vidéo adaptable est l'Annexe G de H.264, mais d'autres codecs, incluant H.264 AVC et VP8, présentent aussi une caractéristique d'adaptabilité, bien que seulement dans la dimension temporelle. Dans les deux cas du codage adaptable et de la diffusion simultanée, le signal vidéo est représenté par un ensemble de deux flux binaires ou plus, fournissant un nombre correspondant de points distincts de fidélité. Le boîtier de médiation choisit quelles parties d'un flux binaire adaptable (ou quel flux binaire, dans le cas de diffusion simultanée) transmettre à chacun des points d'extrémité receveurs. La décision peut s'appuyer sur un certain nombre de facteurs, comme le débit binaire disponible, la présentation désirée, etc. Au contraire des MCU de transcodage, les SFM ont un délai extrêmement faible et présentent des caractéristiques qui sont normalement associées à des systèmes d'extrémité élevée (présentation personnalisée, localisation d'erreur) sans aucun traitement du signal au boîtier de médiation. Ils sont aussi capables de s'adapter à un grand nombre d'utilisateurs concurrents, et du fait de leur très faible délai, peuvent aussi être mis en cascade.

Cette version du boîtier de médiation pose aussi des exigences différentes au point d'extrémité quand il arrive à des instances de décodeur et traite le flux RTP qui fournit les supports. Comme chaque SSRC projetée peut, à tout moment, fournir des supports, le point d'extrémité a besoin d'être capable de traiter autant d'instances de décodeur que le boîtier de médiation a reçues, ou d'avoir une commutation efficace des contextes de décodeur dans un ensemble plus limité d'instances de décodeur réelles pour traiter avec les commutateurs. L'application a aussi plus de responsabilité pour mettre à jour comment les supports fournis vont être présenté à l'utilisateur.

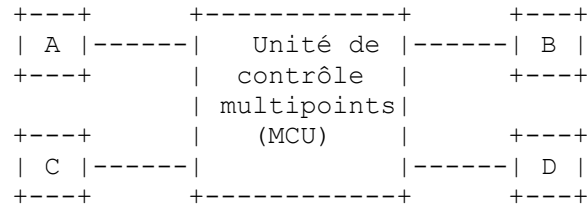
Noter que cette topologie pourrait être vue comme un traducteur de supports qui inclut une logique d'entrée/sortie au titre de la traduction des supports. La topologie a la propriété que toutes les SSRC présentes dans la session sont visibles à un point d'extrémité. Elle a aussi des aspects de mixeur, car les flux qu'elle fournit ne sont pas à la base des versions traduites, mais plutôt ils ont la propriété conceptuelle qui leur est allouée et peut être activée/désactivée, ainsi que livrés

complètement ou partiellement. Donc, cette topologie apparaît comme un hybride entre les modèles de traducteur et de mixeur.

Les différences entre un boîtier de médiation de transmission sélective et un mixeur de commutation de supports (paragraphe 3.6.2) sont mineures, et elles partagent beaucoup de propriétés. L'exigence d'avoir un grand nombre d'instances de décodage ou d'exiger une commutation efficace des contextes de décodeur, est un point de différence. L'autre est comment l'identification est effectuée, où le mixeur utilise la CSRC pour fournir les informations sur ce qui est inclus dans un flux RTP particulier qui représente un concept particulier. La transmission sélective obtient les informations de source de la SSRC et utilise à la place d'autres mécanismes pour indiquer l'usage auquel les flux sont destinés, si nécessaire.

### 3.8 Point à multipoints utilisant des MCU de commutation de vidéo

Nom abrégé : Topo-Video-switch-MCU



**Figure 18 : Point à multipoints en utilisant une MCU de commutation vidéo**

Cette topologie PtM était populaire dans les premières mises en œuvre de systèmes de visioconférence multipoints à cause de sa simplicité, et la conception de boîtier de médiation correspondante a été appelée "MCU de commutation vidéo". Les MCU plus complexes de terminaison de RTCP, discutées au paragraphe suivant, sont cependant devenues la norme, quand la technologie a permis des mises en œuvre à des coûts acceptables.

Une MCU de commutation vidéo transmet à un participant un seul flux de supports, choisi parmi les flux disponibles. Les critères du choix sont souvent fondés sur l'activité vocale dans la conférence audio-visuelle, mais d'autres mécanismes de gestion de conférence (comme le mode de présentation ou le contrôle explicite de la prise de parole) sont aussi connus.

La MCU de commutation vidéo peut aussi effectuer la traduction des supports pour modifier le débit binaire, le codage, ou la résolution du contenu. Cependant, elle peut encore indiquer l'expéditeur original du contenu par la SSRC. Dans ce cas, les valeurs des champs CC et CSRC sont conservées.

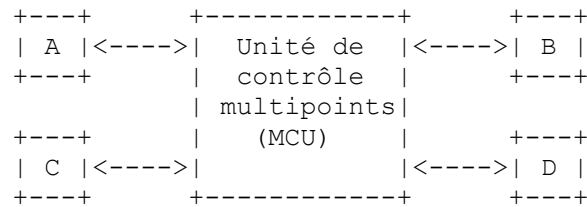
Si ils ne terminent pas RTP, les rapports d'expéditeur RTCP sont transmis pour l'expéditeur actuellement choisi. Tous les rapports de receveur RTCP sont librement transmis entre les points d'extrémité. De plus, la MCU peut aussi générer du trafic de contrôle RTCP afin de contrôler la session et/ou rapporter son état de son point de vue.

La MCU de commutation vidéo a la plupart des attributs d'un traducteur. Cependant, son choix de flux est un comportement de mixage. Des problèmes de RTP et RTCP sont associés à ce comportement. La suppression de tous les flux RTP sauf un résulte en ce que la plupart des participants voient seulement un sous ensemble des flux RTP envoyés à tout moment, souvent un seul flux RTP par conférence. Donc, les rapports de receveur RTCP rapportent seulement sur ces flux RTP. Par conséquent, les points d'extrémité émettant des flux RTP qui ne sont pas actuellement transmis reçoivent une vue de la session qui indique que leurs flux RTP ont disparu quelque part en chemin. Cela rend très problématique l'utilisation de RTCP pour le contrôle d'encombrement, ou pour tout type de rapport de qualité.

Pour éviter les problèmes susmentionnés, la MCU a besoin de mettre en œuvre deux caractéristiques. D'abord, elle a besoin d'agir comme un mixeur (voir le paragraphe 3.6) et transmettre le flux RTP choisi sous sa propre SSRC et avec les valeurs de CSRC appropriées. Ensuite, la MCU a besoin de modifier les RR RTCP qu'elle transmet entre les domaines. Par suite, il est recommandé de mettre en œuvre une conférence centralisée de commutation de vidéo en utilisant un mixeur conformément à la RFC 3550, au lieu de la mise en œuvre abrégée décrite ici.

### 3.9 Point à multipoints utilisant des MCU à terminaison RTCP

Nom abrégé : Topo-RTCP-terminating-MCU



**Figure 19 : Point à multipoints en utilisant des MCU de modification de contenu**

Dans ce scénario de PtM, chaque point d'extrémité fait fonctionner une session RTP en point à point entre lui-même et la MCU. C'est une topologie très couramment déployée dans la visioconférence multipoints. Le contenu que fournit la MCU à chaque participant est soit :

- a. un choix du contenu reçu des autres points d'extrémité ou
- b. l'agrégat mélangé de ce que la MCU reçoit des autres chemins PtP, qui font partie de la même session de communication.

Dans le cas (a), la MCU peut modifier le contenu en termes de débit binaire, de format de codage, ou de résolution. Aucun mécanisme RTP explicite n'est utilisé pour établir les relations entre le flux RTP original des supports envoyés et le flux RTP qu'envoie la MCU. En d'autres termes, le flux RTP sortant utilise normalement une SSRC différente, et peut bien utiliser un type de charge utile (PT, *payload type*) même si ce PT différent se trouve être transposé en le même type de supports. C'est un résultat de la négociation individuelle de session RTP par chaque point d'extrémité.

Dans le cas (b), la MCU est la source des supports et génère le flux RTP de source lorsque elle mélange le contenu reçu et ensuite le code et le met en paquets pour transmission à un point d'extrémité. Conformément à RTP [RFC3550], la SSRC des contributeurs est à signaler en utilisant le mécanisme CSRC/CC. En pratique aujourd'hui, la plupart des MCU déployées ne mettent pas en œuvre cette caractéristique. À la place, l'identification des points d'extrémité dont le contenu est inclus dans le résultat du mixeur n'est indiqué par aucun mécanisme RTP explicite. C'est-à-dire, la plupart des MCU déployées règlent le champ CC dans l'en-tête RTP à zéro, indiquant par là qu'il n'y a pas d'informations de CSRC disponibles, même si elles pourraient identifier les points d'extrémité envoyeurs originaux comme suggéré dans RTP.

La principale caractéristique qui met à part cette topologie de ce que décrit la RFC 3550 est la coupure de la session RTP courante à travers l'appareil centralisé, comme la MCU. Il en résulte la perte de l'indication explicite au niveau RTP de tous les participants. Si on utilisait les mécanismes disponibles dans RTP et RTCP pour signaler explicitement cela, la topologie suivrait l'approche d'un mixeur RTP. L'absence d'une indication explicite pose au moins les problèmes potentiels suivants :

1. La détection de boucle ne peut pas être effectuée au niveau RTP. Quand on connecte sans faire attention deux MCU mal configurées, une boucle pourrait être générée.
2. Il n'y a pas d'informations sur les envoyeurs de supports actifs disponibles dans le paquet RTP. Comme ces informations manquent, les receveurs ne peuvent pas les utiliser. Cela prive aussi le client des informations relatives aux envoyeurs actuellement actifs d'une façon utilisable par la machine, empêchant donc les clients d'indiquer les orateurs actuellement actifs dans les interfaces d'utilisateur, etc.

Noter que de nombreuses/la plupart des MCU déployées (et des points d'extrémité de visioconférence) s'appuient sur des mécanismes de couche de signalisation pour l'identification des sources contributives, par exemple, un paquetage SIP de conférence [RFC4575]. Cela allège, dans une certaine mesure, les problèmes susmentionnés résultant de l'ignorance du mécanisme de CSRC de RTP.

### 3.10 Terminal à composants séparés

Nom abrégé : Topo-Split-Terminal

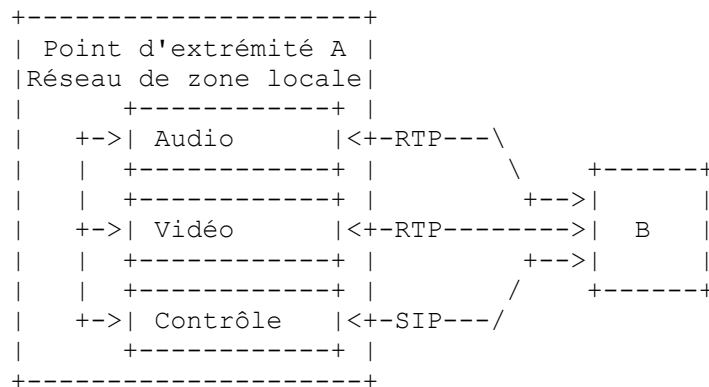
Dans certaines applications, par exemple, dans certains systèmes de téléprésence, les terminaux peuvent n'être pas intégrés dans une seule unité fonctionnelle mais composés de plus d'une sous unité. Par exemple, un terminal d'espace de téléprésence qui emploie plusieurs caméras et moniteurs peut consister en plusieurs sous unités de visioconférence, chacune capable de traiter une seule caméra et moniteur. Un autre exemple sera celui d'un terminal de visioconférence dans lequel l'audio est traité par une sous unité, et la vidéo par une autre. Chacune de ces sous unités utilise sa propre interface réseau physique (par exemple : un cordon Ethernet) et sa propre adresse réseau.

Les diverses sous unités (de traitement des supports) ont besoin d'être interconnectées (logiquement et physiquement) par une fonction de contrôle, mais leur fonction de plan des supports peut être étalée. Ces types de terminaux sont appelés des

terminaux à composants séparés. Historiquement, les premiers terminaux à composants séparés étaient peut-être les outils logiciels d'audio et visioconférence indépendants utilisés sur le MBONE à la fin des années 1990.

Un exemple d'un tel terminal à composants séparés est décrit à la Figure 20. Au sein du terminal à composants séparés A, au moins les sous unités audio et vidéo sont adressées par leur propre adresse réseau. Dans certains de ces systèmes, la sous unité de pile de contrôle peut aussi avoir sa propre adresse réseau.

Du point de vue de RTP, chacune des sous unités termine RTP et agit comme un point d'extrémité au sens où chaque sous unité inclut sa propre pile RTP indépendante. Cependant, comme les sous unités font sémantiquement partie du même terminal, il est approprié que cette relation sémantique soit exprimée dans les éléments de protocole RTCP, à savoir dans le CNAME.



**Figure 20 : Terminal à composants séparés**

Il est de plus raisonnable que les sous unités partagent une horloge commune à partir de laquelle les horloges RTP et RTCP sont déduites, pour faciliter la synchronisation et éviter une dérive d'horloge.

Pour indiquer que les flux de source audio et vidéo générés par des sous unités différentes partagent une horloge commune, et peuvent être synchronisés, le flux RTP généré à partir de ces flux de source doit inclure le même CNAME dans ses paquets SDES RTCP. L'utilisation d'un CNAME commun pour les flux RTP portés dans des flux de couche transport différents est entièrement normale pour les envoyeurs RTP et RTCP, et les points d'extrémité, les boîtiers de médiation, et autres outils pleinement conformes à RTP ne devraient pas avoir de problème avec cela.

Cependant, en dehors du scénario du terminal à composants séparés (et peut-être du scénario d'un point d'extrémité multi-rattachements, qu'on ne discute pas plus ici) l'utilisation d'un CNAME commun dans le flux RTP envoyé à partir de points d'extrémité séparés (par opposition à un CNAME commun pour des flux RTP envoyés sur des flux de couche de transport différente entre deux points d'extrémité) est rare. Il a été rapporté qu'au moins quelques outils tiers comme certains moniteurs de réseau ne traitent pas avec douceur les points d'extrémité qui utilisent un CNAME commun sur plusieurs flux de couche transport : ils rapportent une condition d'erreur dans laquelle deux points d'extrémité séparés utilisent le même CNAME. Selon la sophistication du personnel de soutien, de tels rapports erronés peuvent conduire à des problèmes de prise en charge.

Le problème de prise en charge susmentionné peut parfois être évité si chacune des sous unités d'un terminal à composants séparés est configurée à utiliser un CNAME différent, la synchronisation entre les flux RTP étant indiquée par un canal de signalisation non RTP plutôt que d'utiliser un CNAME commun envoyé dans RTCP. Cela complique la signalisation, en particulier dans les cas où il y a plusieurs SSRC utilisées avec des exigences de synchronisation complexes, comme c'est le cas dans de nombreux systèmes de téléprésence courants. Sauf si on utilise des topologies de terminaison RTCP comme dans Topo-RTCP-terminating-MCU, les sessions qui impliquent plus d'une sous unité vidéo avec un CNAME commun sont pratiquement inévitables.

Les différents flux RTP composant un système de terminal séparé peuvent former une seule session RTP ou ils peuvent former plusieurs sessions RTP, selon la visibilité de leurs valeurs de SSRC dans les rapports RTCP. Si le receveur des flux RTP envoyés par le terminal séparé envoie des rapports relatifs à tous les flux RTP (c'est-à-dire, à chaque SSRC) dans chaque rapport RTCP, alors une seule session RTP est formée. Autrement, si le receveur du flux RTP envoyé par le terminal séparé n'envoie pas de rapports croisés dans RTCP, l'audio et la vidéo forment des sessions RTP séparées.

Par exemple, dans la Figure 20, B va envoyer des rapports RTCP à chaque sous unité de A. Si les paquets RTCP que B envoie à la sous unité audio de A incluent des rapports sur la qualité de réception de la vidéo ainsi que de l'audio, et de

façon similaire, si les paquets RTCP que B envoie à la sous unité vidéo de A incluent des rapports sur la qualité de réception de l'audio ainsi que de la vidéo, alors une seule session RTP est formée. Cependant, si les paquets RTCP que B envoie à la sous unité audio de A rapportent seulement sur l'audio reçu, et si les paquets RTCP que B envoie à la sous unité vidéo de A rapportent seulement sur la vidéo reçue, il y a alors deux sessions RTP séparées.

Former une seule session RTP à travers les flux RTP envoyés des différentes sous unités d'un terminal séparé donne à chaque sous unité la visibilité sur la qualité de réception des flux RTP envoyés par les autres sous unités.

Ces informations peuvent aider à diagnostiquer les problèmes de qualité de réception, mais au prix d'une utilisation accrue de la bande passante de RTCP.

Les flux RTP envoyés par les sous unités d'un terminal séparé doivent utiliser le même CNAME dans leurs paquets RTCP si ils doivent être synchronisés, qu'une seule session RTP soit formée ou non.

### 3.11 Mixeur/traducteurs non symétriques

Nom abrégé : Topo-Asymétrique

Il est théoriquement possible de construire une MCU qui soit un mixeur dans une direction et un traducteur dans l'autre. La principale raison à considérer serait de permettre des topologies similaires à celles de la Figure 13, où le mixeur n'a pas besoin de mixer dans la direction de B ou D vers les domaines de diffusion groupée avec A et C. À la place, les flux RTP provenant de B et D sont transmis sans changement. Éviter ce mixage économiserait des ressources de traitement des supports qui effectueraient le mixage dans les cas où il n'est pas nécessaire. Cependant, il y aura encore le besoin de mixer les supports de B vers D. C'est seulement dans la direction B -> domaine de diffusion groupée ou D -> domaine de diffusion groupée qu'il va être possible de travailler comme traducteur. Dans toutes les autres directions, il va fonctionner comme mixeur.

Le mixeur/traducteur va quand même avoir besoin de traiter et changer le RTCP avant de le transmettre dans les directions de B ou D vers le domaine de diffusion groupée. Un problème est que A et C ne savent rien du flux de supports mixé que le mixeur envoie à B ou D. Donc, tous les rapports relatifs à ces flux doivent être supprimés. Aussi, les rapports de receveur relatifs aux flux RTP de A et C vont manquer. Pour éviter que A et C pensent que B et D ne reçoivent pas du tout A et C, le mixeur a besoin d'insérer des rapports générés en local qui reflètent la situation pour les flux provenant de A et C dans les rapports d'envoyeur de B et D. Dans la direction opposée, les rapports de receveur provenant de A et C sur les flux de B et D doivent aussi être agrégés dans les rapports de receveur du mixeur envoyés à B et D. Comme B et D ont seulement le mixeur comme source pour le flux, tous les RTCP provenant de A et C doivent être supprimés par le mixeur.

Cette topologie est donc problématique, et il est si facile que le traitement RTCP soit erroné qu'il n'est pas recommandé de la mettre en œuvre.

### 3.12 Topologies combinées

Des topologies peuvent être combinées et reliées à chaque autre en utilisant des mixeurs ou traducteurs. Cependant, il faut faire attention dans le traitement de l'espace de SSRC/CSRC. Un mixeur ne transmet pas RTCP à partir des sources dans d'autres domaines, mais génère plutôt ses propres paquets RTCP pour chaque domaine dans lequel il mixe, incluant les nécessaires informations de SDES pour les deux CSRC et SSRC. Donc, dans un domaine mixé, les seuls SSRC vus vont être présents dans le domaine, alors qu'il peut y avoir des CSRC provenant de tous les domaines connectés ensemble avec une combinaison de mixeurs et traducteurs. L'espace combiné de SSRC et CSRC est commun sur tout traducteur ou mixeur. Il est important de faciliter la détection de boucles, quelque chose qui est probablement encore plus important dans les topologies combinées à cause du comportement mélangé entre les domaines. Tout hybride, comme la Topo-Video-switch-MCU ou Topo-Asymétrique, exige une réflexion approfondie sur la façon dont RTCP est traité.

## 4. Propriétés des topologies

Les topologies discutées à la Section 3 ont des propriétés différentes. Cette section décrit ces propriétés. Noter que, même si une certaine propriété est prise en charge dans un concept de topologie particulier, la fonction nécessaire peut être de mise en œuvre facultative.

#### 4.1 Transmission des supports de tous à tous

Pour récapituler, la diffusion groupée, et en particulier ASM, fournit la fonctionnalité que tout le monde peut envoyer à, ou recevoir de, tout le monde au sein de la session. SSM peut fournir une fonction similaire en ayant la capacité que tous ceux qui ont l'intention de participer comme envoyeur aient celle d'envoyer leurs supports à la source de distribution SSM. La source de distribution SSM transmet les supports à tous les receveurs abonnés au groupe de diffusion groupée. Les maillages, MCU, mixeurs, boîtiers de transmission sélective (SFM, *Selective Forwarding Middlebox*) et traducteurs peuvent tous fournir cette fonction au moins à un niveau de base. Cependant, il y a quelques différences dans le type d'accessibilité qu'elles fournissent.

Les topologies qui se rapprochent le plus de l'émulation de la diffusion groupée toutes sources IP, avec des capacités de transmission de tous à tous, sont la fonction de traducteur de transport appelée "relais" au paragraphe 3.5, ainsi que le maillage avec sessions RTP jointes (paragraphe 3.4). Les traducteurs de supports, maillage avec sessions RTP indépendantes, les mixeurs, les SFU, et les variantes de MCU ne fournissent pas une transmission pleinement maillée au niveau du transport ; à la place, elles permettent seulement une transmission limitée du contenu provenant des autres participants à la session.

La "transmission des supports de tous à tous" exige que tout point d'extrémité qui transmet des supports considère les chemins vers le moins capable des points d'extrémité receveur. Autrement, les transmissions de supports peuvent surcharger ce chemin. Donc, un point d'extrémité envoyeur a besoin de surveiller le chemin de lui-même à tout point d'extrémité receveur, pour détecter le receveur actuellement le moins capable et d'adapter son taux d'envoi en conséquence. Comme plusieurs points d'extrémité peuvent envoyer simultanément, les ressources disponibles peuvent varier. Les rapports de receveur de RTCP aident à effectuer cette surveillance, au moins à moyen terme.

La consommation de ressources pour effectuer la transmission de tous à tous varie selon la topologie. ASM et SSM présentent tous deux l'avantage que seulement une copie de chaque paquet traverse une liaison particulière. Utiliser un relais cause la transmission d'une copie d'un paquet par chemin de point d'extrémité au relais et paquet transmis. Cependant, dans la plupart des cas, les liaisons qui portent les multiples copies vont être celles qui sont proches du relais (qui peut être supposé faire partie de l'infrastructure de réseau avec une bonne connexité au cœur de réseau) plutôt que des points d'extrémité (qui peuvent être derrière des liaisons d'accès plus lentes). Les topologies de maillage causent la traversée de N-1 flux de paquets transmis de la liaison de premier bond à partir du point d'extrémité, dans un maillage avec N points d'extrémité. Pendant combien de temps les différents chemins sont commun est très dépendant de la situation.

La transmission de RTCP s'adapte par conception à tous les changements du nombre de participants du fait de l'algorithme de transmission, défini dans la spécification RTP [RFC3550], et des extensions dans AVPF [RFC4585] (quand elles sont applicables). De cette façon, les ressources utilisées pour RTCP restent dans les limites configurées pour la session.

#### 4.2 Interopérabilité de transport ou des supports

Tous les traducteurs, mixeurs, MCU de terminaison RTCP, et maillages avec sessions RTP individuelles permettent de changer le codage des supports ou le transport en autres propriétés des autres domaines, fournissant par là une interopérabilité étendue dans les cas où les points d'extrémité n'ont pas un ensemble commun de codecs de supports et/ou de protocoles de transport. Les boîtiers de médiation de transmission sélective peuvent adopter le transport et (au moins) transmettre sélectivement les flux codés qui correspondent à la capacité d'un point d'extrémité receveur. Cela exige un traducteur supplémentaire pour changer le codage des supports si les flux codés ne correspondent pas aux capacités du point d'extrémité receveur.

#### 4.3 Adaptation du débit binaire par domaine

Les points d'extrémité sont souvent connectés les uns aux autres par un ensemble hétérogène de chemins. Cela rend problématique le contrôle d'encombrement dans un point à multipoints. Dans les scénarios d'ASM, SSM, maillage avec session RTP commune, et relais de transport, chaque point d'extrémité envoyeur individuel doit s'adapter au point d'extrémité receveur derrière le chemin le moins capable, donnant une qualité sous optimale pour les points d'extrémité derrière les chemins les plus capables. Ce n'est plus un problème quand des traducteurs de supports, mixeurs, SFM, ou MCU sont impliqués, car chaque point d'extrémité a seulement besoin de s'adapter au chemin le plus lent au sein de son propre domaine. Les topologies de traducteur, mixeur, SFM, ou MCU exigent toutes que leurs flux RTP sortants respectifs ajustent le débit binaire, le taux de paquets, etc., pour s'adapter au chemin le moins capable dans le domaine de chaque autre. De cette façon on peut éviter de diminuer la qualité au point d'extrémité le moins capable dans tous les domaines au prix (en complexité, délai, équipement) du mixeur, SFM, ou traducteur, et potentiellement des envoyeurs de supports (codage de diffusion groupée/mise en couches et envoi des différentes représentations).

#### 4.4 Agrégation de supports

Dans la propriété de supports de tous à tous mentionnée ci-dessus et fournie par ASM, SSM, maillage avec session RTP commune, et relais, toutes les transmissions de supports simultanées partagent le débit binaire disponible. Pour les points d'extrémité avec des capacités de réception limitées, il peut en résulter une situation où même une qualité minimale de supports acceptable ne peut pas être réalisée, parce que plusieurs flux RTP ont besoin de partager les mêmes ressources. Une solution à ce problème est d'utiliser un mixeur, ou une MCU, pour agréger les multiples flux RTP en un seul, où le seul flux RTP prend moins de ressources en termes de débit binaire. Cette agrégation peut être effectuée selon différentes méthodes. Le mixage ou la sélection sont deux méthodes courantes. La sélection est presque toujours possible et facile à mettre en œuvre. Le mixage exige des ressources dans le mixeur et peut être relativement facile et n'impacte pas trop la qualité (audio) ou assez difficile (pavage vidéo, qui n'est pas seulement complexe à calculer mais aussi réduit le compte de pixels par flux, avec la perte correspondante de qualité perçue).

#### 4.5 Vue de tous les participants à la session

Le protocole RTP inclut la fonction d'identification des participants à la session par l'utilisation des champs SSRC et CSRC. De plus, il est capable de porter d'autres informations d'identité sur ces participants en utilisant le SDES RTCP. Dans les topologies qui fournissent une pleine fonction de tous à tous, c'est-à-dire, ASM, maillage avec session RTP commune, et relais, une mise en œuvre RTP conforme offre la fonction directement comme spécifié dans RTP. Dans les topologies qui n'offrent pas la communication de tous à tous, il est nécessaire que RTCP soit traité correctement dans les fonctions de pontage de domaines. RTP inclut du texte de spécification explicite pour les traducteurs et mixeurs, et pour les SFM la fonction exigée peut être déduite de ce texte. Cependant, la MCU décrite au paragraphe 3.8 ne peut pas offrir la pleine fonction pour l'identification des participants à la session par les moyens de RTP. Les topologies qui créent des sessions RTP indépendantes par point d'extrémité ou paire de points d'extrémité, comme une session RTP dos à dos, un maillage avec des sessions RTP indépendantes, et la MCU de terminaison RTCP (paragraphe 3.9) à l'exception de SFM, ne prennent pas en charge l'identification fondée sur RTP des participants à la session. Dans tous ces cas, d'autres mécanismes non fondés sur RTP doivent être mis en œuvre si cette connaissance est exigée ou désirable. Quand on en vient à SFM, l'espace de noms de SSRC n'est pas nécessairement joint. À la place, l'identification va exiger la connaissance des transpositions de SSRC/CSRC que SFM a effectuées ; voir le paragraphe 3.7.

#### 4.6 Détection de boucle

Dans les topologies complexes avec de multiples domaines interconnectés, il est possible de former involontairement des boucles de supports. RTP et RTCP prennent en charge la détection de telles boucles, tant que les identifiants de SSRC et CSRC sont conservés et correctement réglés dans les paquets transmis. La détection de boucles va fonctionner dans ASM, SSM, maillage avec session RTP conjointe, et relais. Il est probable que la détection de boucle fonctionne pour la MCU de commutation de vidéo, paragraphe 3.8, au moins tant qu'elle transmet le RTCP entre les points d'extrémité. Cependant, les sessions RTP dos à dos, le maillage avec sessions RTP indépendantes, et les SFM vont définitivement casser le mécanisme de détection de boucle.

#### 4.7 Cohérence entre extensions d'en-têtes et RTCP

Certaines extensions d'en-tête RTP sont pertinentes non seulement de bout en bout mais aussi bond par bond, ce qui signifie au moins que certains des boîtiers de médiation dans le chemin sont informés de leur potentielle présence par la signalisation, interceptent et interprètent de telles extensions d'en-tête, et potentiellement aussi les réécrivent ou les génèrent. Les extensions d'en-tête modernes suivent généralement le "Mécanisme général pour les extensions d'en-tête RTP" [RFC5285], qui permet tout ce qui précède. Des exemples de ces extensions d'en-tête incluent l'identifiant de supports (MID, *Media ID*) de la [RFC8843]. Au moment de la rédaction du présent document, il y avait aussi une proposition sur comment inclure des SDES dans une extension d'en-tête RTP [RFC7941].

Quand de telles extensions d'en-tête sont utilisées, tout boîtier de médiation qui les comprend doit s'assurer de la cohérence entre les extensions qu'il voit et/ou génère et le RTCP qu'il reçoit et génère. Par exemple, le MID du faisceau est envoyé dans une extension d'en-tête RTP et aussi dans un messages SDES RTCP. Cette apparente redondance a été introduite parce que les boîtiers de médiation non avertis peuvent choisir d'éliminer les extensions d'en-tête RTP. Évidemment, l'incohérence entre le MID envoyé dans l'extension d'en-tête RTP et dans le message SDES RTCP pourrait conduire à des résultats indésirables, et donc, la cohérence est nécessaire. Les boîtiers de médiation non avertis de la nature d'une extension d'en-tête, comme spécifié dans la [RFC5285], sont libres de transmettre ou éliminer les extensions d'en-tête.



## 5. Comparaison des topologies

Le tableau ci-dessous tente de résumer les propriétés des différentes topologies. La légende des abréviations de topologies est : Topo-Point-à-point (PtP), Topo-ASM (ASM), Topo-SSM (SSM), Topo-Trn-traducteur (TT), Topo-Media-traducteur (incluant le traducteur de transport) (MT), Topo-Maillage avec session jointe (MJS), Topo-maillage avec sessions individuelles (MIS), Topo-Mixeur (Mix), Topo-Asymétrique (ASY), Topo-Video-switch-MCU (VSM), Topo-RTCP-terminating-MCU (RTM), et boîtier de transmission sélective (SFM). Dans le tableau, O indique Oui ou soutien complet, N indique Pas de soutien, (O) indique un soutien partiel, et N/A indique non applicable.

| Propriété               | PtP | ASM | SSM | TT | MT | MJS | MIS | Mix | ASY | VSM | RTM | SFM |
|-------------------------|-----|-----|-----|----|----|-----|-----|-----|-----|-----|-----|-----|
| Supports de tous à tous | N   | O   | (O) | O  | O  | O   | (O) | (O) | (O) | (O) | (O) | (O) |
| Interopérabilité        | N/A | N   | N   | O  | O  | O   | O   | O   | O   | N   | O   | O   |
| Adaptation par domaine  | N/A | N   | N   | N  | O  | N   | O   | O   | O   | N   | O   | O   |
| Agrégation des supports | N   | N   | N   | N  | N  | N   | N   | O   | (O) | O   | O   | N   |
| Pleine vue de session   | O   | O   | O   | O  | O  | O   | N   | O   | O   | (O) | N   | O   |
| Détection de boucle     | O   | O   | O   | O  | O  | O   | N   | O   | O   | (O) | N   | N   |

Noter que le traducteur de supports inclut aussi la fonction de traducteur de transport.

## 6. Considérations sur la sécurité

L'utilisation de mixeurs, SFM, et traducteurs a un impact sur la sécurité et sur les fonctions de sécurité utilisées. Le problème principal est que les mixeurs, SFM, et traducteurs modifient les paquets, empêchant donc l'utilisation de la protection d'intégrité et de l'authentification de la source, sauf si des appareils de confiance prennent part au contexte de sécurité, par exemple, l'appareil peut envoyer des paquets du protocole sécurisé de transport en temps réel (SRTP, *Secure Real-time Transport Protocol*) et du protocole sécurisé de contrôle de transport en temps réel (SRTCP, *Secure Real-time Transport Control Protocol*) [RFC3711] aux points d'extrémité dans la session de communication. Si le chiffrement est employé, le traducteur de supports, le SFM, et le mixeur doivent être capables de déchiffrer les supports pour effectuer leurs fonctions. Un traducteur de transport peut être utilisé sans accès à la charge utile chiffrée dans les cas où il traduit des parties qui ne sont pas incluses dans le chiffrement et la protection de l'intégrité, par exemple, les numéros d'adresse IP et d'accès UDP dans un flux de supports qui utilise SRTP [RFC3711]. Cependant, en général, le traducteur, SFM, ou mixeur a besoin de faire partie du contexte de signalisation et d'obtenir l'association de sécurité nécessaire (par exemple, les contextes de chiffrement SRTP) établis avec ses participants à la session RTP.

Inclure le mixeur, SFM, et traducteur dans le contexte de sécurité permet à l'entité, si elle est détournée ou se comporte mal, d'effectuer un certain nombre d'attaques très sérieuses comme si elle avait le plein accès. Elle peut effectuer toutes les attaques possibles (voir la RFC 3550 et tous les profils applicables) comme si la session de supports n'était pas protégée du tout, tout en donnant l'impression aux participants à la session qu'ils sont protégés.

Les traducteurs de transport n'ont pas d'interactions avec la cryptographie qui fonctionne au dessus de la couche de transport, comme SRTP, car cette sorte de traducteur laisse non altérés l'en-tête et la charge utile RTP. Les traducteurs de supports, par ailleurs, ont de fortes interactions avec la cryptographie, car ils altèrent la charge utile RTP. Un traducteur de supports dans une session qui utilise la protection cryptographique a besoin d'effectuer un traitement cryptographique sur les paquets entrants et sortants.

Un traducteur de supports peut avoir besoin d'utiliser des clés de chiffrement différentes pour le traitement entrant et sortant. Pour SRTP, des clés différentes sont exigées, parce que dans la RFC 3550 le traducteur de supports laisse la SSRC inchangée durant son traitement de paquets, et le partage de clés SRTP n'est permis que quand des SSRC distinctes peuvent être utilisées pour protéger des flux de paquets distincts.

Quand le traducteur de supports utilise des clés différentes pour traiter les paquets entrants et sortants, chaque participant à la session a besoin de recevoir la clé appropriée, selon qu'il écoute le traducteur ou la source originale. (Noter qu'il y a une différence architecturale entre la traduction de supports RTP, dans laquelle les participants peut s'appuyer sur le champ Type de charge utile RTP d'un paquet pour déterminer le traitement approprié, et la traduction de supports protégés cryptographiquement, dans laquelle les participants doivent utiliser des information qui ne sont pas portées dans le paquet.)

Quand on utilise des mécanismes de sécurité avec des traducteurs, SFM, et mixeurs, il est possible que le traducteur, SFM, ou mixeur puisse créer une association de sécurité différente pour les différents domaines dans lesquels ils travaillent. Le faire a des implications :

D'abord, cela peut affaiblir la sécurité si le mixeur/traducteur accepte un algorithme ou clé plus faible dans un domaine plutôt que dans un autre. Donc, il faut faire attention à ce que des paramètres de sécurité de force appropriée soient négociés dans tous les domaines. Dans de nombreux cas, "approprié" se traduit en "force similaire". Si un système de gestion de clés permet la négociation de paramètres de sécurité résultant en une force différente de la sécurité, alors ce système devrait le notifier aux participants dans les autres domaines.

Ensuite, le nombre de contextes de chiffrement (clés et état relatif à la sécurité) nécessaires (par exemple, dans SRTP [RFC3711]) peut varier entre mixeurs, SFM, et traducteurs. Un mixeur a normalement besoin de représenter seulement une seule SSRC par domaine et a donc besoin de créer seulement une association de sécurité (contexte de chiffrement SRTP) par domaine. À l'opposé, un traducteur a besoin d'une association de sécurité par participant vers lequel il traduit, dans le domaine opposé. Quand on examine la Figure 11, le traducteur a besoin de deux associations de sécurité vers le domaine de diffusion groupée : une pour B et une pour D. Il peut être forcé de maintenir un ensemble d'associations de sécurité totalement indépendantes entre lui-même et B et D, respectivement, afin d'éviter deux occurrences de bourrage. Ces contextes doivent aussi être capables de traiter toutes les sources présentes dans les autres domaines. Donc, utiliser des associations de sécurité complètement indépendantes (pour certains mécanismes de chiffrement) peut forcer un traducteur à traiter  $N \cdot DM$  clés et l'état qui s'y rapporte, où  $N$  est le nombre total de SSRC utilisées sur tous les domaines et  $DM$  est le nombre total de domaines.

Les topologies ASM, SSM, Relais, et Maillage (avec session RTP commune) ont chacune plusieurs points d'extrémité qui exigent une connaissance partagée des différents contextes de chiffrement pour les points d'extrémité. Ces topologies multiparties ont des exigences particulières sur la gestion de clés ainsi que sur les fonctions de sécurité. Spécifiquement, l'authentification de la source dans ces environnements a des exigences particulières.

Il existe un certain nombre de mécanismes différents pour fournir des clés aux différents participants. Un exemple est le choix entre des clés de groupe et des clés uniques par SSRC. Le modèle de gestion de clés approprié est impacté par les topologies qu'on a l'intention d'utiliser. Les propriétés de sécurité finales dépendent à la fois des topologies utilisées et des propriétés des mécanismes de chiffrement et elles doivent être considérées par l'application. Exactement quels mécanismes sont utilisés sort du domaine d'application du présent document. Voir les options de sécurité RTP [RFC7201] pour obtenir une meilleure compréhension de la plupart des options disponibles.

## 7. Références

### 7.1 Références normatives

- [RFC3550] H. Schulzrinne, S. Casner, R. Frederick et V. Jacobson, "[RTP : un protocole de transport pour les applications en temps réel](#)", STD 64, juillet 2003. DOI 10.17487/RFC3550 (*MàJ par RFC7164, RFC7160, RFC8083, RFC8108, RFC8860*)
- [RFC4585] J. Ott et autres, "[Profil RTP étendu pour rétroaction](#) fondée sur le protocole de contrôle de transport en temps réel (RTCP) (RTP/AVPF)", juillet 2006. DOI 10.17487/RFC4585 (*P.S., MàJ par RFC8108*)
- [RFC7656] J. Lennox, et autres, "Taxonomie de la sémantique et des mécanismes pour les sources de RTP", novembre 2015. DOI 10.17487/RFC7656 (*Info*)

### 7.2 Références pour information

- [RFC1112] S. Deering, "Extensions d'hôte pour [diffusion groupée sur IP](#)", STD 5, août 1989. (*Mise à jour par la RFC2236*)
- [RFC3022] P. Srisuresh, K. Egevang, "[Traducteur d'adresse réseau IP traditionnel](#)", janvier 2001. DOI 10.17487/RFC3022 (*Information*)
- [RFC3569] S. Bhattacharyya et autres, "Généralités sur la [diffusion groupée de source spécifique](#) (SSM)", juillet 2003. DOI 10.17487/RFC3569 (*Info.*)
- [RFC3711] M. Baugher et autres, "Protocole de [transport sécurisé en temps réel](#) (SRTP)", mars 2004. DOI 10.17487/RFC3711 (*P.S. ; MàJ par RFC9335*)

- [RFC4575] J. Rosenberg et autres, "[Paquetage d'événement](#) du protocole d'initialisation de session (SIP) pour l'état Conference", août 2006. DOI 10.17487/RFC4575 (P.S.)
- [RFC4607] H. Holbrook, B. Cain, "[Diffusion groupée spécifique de source pour IP](#)", août 2006. DOI 10.17487/RFC4607 (P.S.)
- [RFC5104] S. Wenger et autres, "[Messages de contrôle de codec](#) dans le profil audio-visuel RTP avec rétroaction (AVPF)", février 2008. DOI 10.17487/RFC5104 (P.S. ; MàJ par [RFC7728](#), [RFC8082](#))
- [RFC5117] M. Westerlund, S. Wenger "Topologies dans RTP", janvier 2008. DOI 10.17487/RFC5117 (*Info. , Remplacée par [RFC7667](#)*)
- [RFC5285] D. Singer, H. Desineni, "Mécanisme général pour les extension d'en-tête RTP", juillet 2008. DOI 10.17487/RFC5285 (P.S. ; remplacée par [RFC8285](#))
- [RFC5760] J. Ott, J. Chesterfield, E. Schooler, "Extensions au protocole de contrôle RTP (RTCP) pour les sessions de diffusion groupée à une seule source avec retour en envoi individuel", février 2010. DOI 10.17487/RFC5760 (P. S.)
- [RFC5766] R. Mahy, P. Matthews, J. Rosenberg, "Traversée de NAT au moyen d'un relais (TURN) : Extensions de relais aux utilitaires de traversée de session pour les NAT (STUN)", avril 2010. (DOI 10.17487/RFC5766) (P. S. ; MàJ par [RFC8155](#) ; Remplacée par [RFC8656](#))
- [RFC6285] B. Ver Steeg et autres, "Acquisition rapide fondée sur l'envoi individuel de sessions RTP en diffusion groupée", juin 2011. (DOI 10.17487/RFC6285) (P.S.)
- [RFC6465] E. Iovov, E. Marocco, J. Lennox, "Extension d'en-tête de protocole de transport en temps réel (RTP) pour les indications de niveau audio de mélangeur à client", décembre 2011. (DOI 10.17487/RFC6465) (P.S.)
- [[RFC7201](#)] M. Westerlund, C. Perkins, "Options pour sécuriser les sessions RTP", avril 2014. (DOI 10.17487/RFC7201) (*Information*)
- [[RFC7941](#)] M. Westerlund, et autres, "Extension d'en-tête RTP pour les éléments de description de source du protocole de contrôle de RTP (RTCP)", août 2016. (DOI 10.17487/RFC7941) (P.S. ; MàJ par [RFC8843](#), [9143](#))
- [[RFC8108](#)] J. Lennox, et autres, "Envoi de flux RTP multiples dans une seule session RTP", mars 2017. (DOI 10.17487/RFC8108) (P.S. ; MàJ 3550, 4585)
- [RFC8843] C. Holmberg, H. Alvestrand, C. Jennings, "Négociation de multiplexage de support avec le protocole de description de session (SDP)", janvier 2021. (DOI : 10.17487/RFC8843) (P.S. ; remplacée par [RFC9143](#))

## Remerciements

Les auteurs tiennent à remercier Mark Baugher, Bo Burman, Ben Campbell, Umesh Chandra, Alex Eleftheriadis, Roni Even, Ladan Gharai, Geoff Hunt, Suresh Krishnan, Keith Lantz, Jonathan Lennox, Scarlet Liuyan, Suhas Nandakumar, Colin Perkins, et Dan Wing de leur aide à la relecture et l'amélioration de ce document.

## Adresse des auteurs

Magnus Westerlund  
Ericsson  
Farogatan 2  
SE-164 80 Kista  
Sweden  
téléphone : +46 10 714 82 87  
mél : [magnus.westerlund@ericsson.com](mailto:magnus.westerlund@ericsson.com)

Stephan Wenger  
Vidyo  
433 Hackensack Ave  
Hackensack, NJ 07601  
USA  
mél : [stewe@stewe.org](mailto:stewe@stewe.org)