Groupe de travail Réseau
**Request for Comments : 5239**
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

M. Barnes, Nortel
C. Boulton, Avaya
O. Levin, Microsoft Corporation

juin 2008

# Cadre pour conférence contralisée



**Résumé**
Le présent document définit le cadre pour les conférences centralisées. Ce cadre permet aux participants qui utilisent divers protocoles de signalisation d'appel, comme SIP, H.323, Jabber, Q.931 ou le sous-système Utilisateur RNIS (ISUP, *ISDN User Part*) d'échanger des supports dans une conférence en envoi individuel centralisée. Le cadre de conférence centralisée définit des entités logiques et des conventions de dénomination. Le cadre mentionne aussi un ensemble de protocoles de conférence, qui sont complémentaires des protocoles de signalisation d'appel, pour construire des applications de conférence évoluées. Le cadre lie ensemble tous les composants définis pour le bénéfice des constructeurs de systèmes de conférence.

## Table des matières

## 1. Introduction

Le présent document définit le cadre pour les conférences centralisées. Ce cadre permet aux participants qui utilisent divers protocoles de signalisation d'appel, comme SIP, H.323, Jabber, Q.931 ou ISUP, d'échanger des supports dans une conférence en envoi individuel centralisée. À part des références à des fonctions générales (par exemple, établissement et suppression) les détails de ces protocoles de signalisation d'appel sortent du domaine d'application du présent document.

Le cadre de conférence centralisée définit des entités logiques et des conventions de dénomination. Le cadre mentionne aussi un ensemble de protocoles de conférence, qui sont complémentaires des protocoles de signalisation d'appel, pour construire des applications de conférence évoluées.

Le cadre de conférence centralisée est compatible avec le modèle fonctionnel présenté dans le cadre de conférence SIP [RFC4353]. La Section 10 du présent document discute des relations entre le cadre de conférence centralisée et le cadre de conférence SIP, dans le contexte du modèle de conférence centralisée présenté dans ce document.

## 2. Conventions

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDÉ", "PEUT", et "FACULTATIF" dans le présent document sont à interpréter comme décrit dans le BCP 14, [RFC2119] et indiquent les niveaux d'exigence pour les mises en œuvre conformes.

## 3. Terminologie

Le présent document de cadre de conférence centralisée généralise, quand c'est approprié, la terminologie du cadre de conférence SIP [RFC4353] et introduit de nouveaux concepts, dont la liste est donnée ci-dessous. Plus de détails et de précisions sur les nouveaux termes et concepts sont fournis dans les Sections suivantes de ce document.

Conférence active : le terme de "conférence active" se réfère à un objet conférence qui a été créé et activé via l'allocation de ses identifiants (par exemple, identifiant d'objet conférence et identifiant de conférence) et le centre associé. Une conférence active est créée sur la base d'une ébauche de système de conférence par défaut ou d'une réservation de conférence spécifique.

Protocole de signalisation d'appel : il est utilisé entre un participant et un centre. Dans ce contexte, le terme "appel" signifie un canal ou une session utilisé pour les flux de supports.

Ébauche de conférence : c'est un objet conférence statique au sein d'un système de conférence, qui décrit un réglage typique de conférence pris en charge par le système. Une ébauche de conférence est la base de la création d'objets conférence dynamiques. Un système peut maintenir plusieurs ébauches. Chaque ébauche est composée des valeurs et gammes initiales pour les éléments dans l'objet, conformément aux schémas de données pour les informations de conférence.

Protocole de contrôle de conférence (CCP, *Conference Control Protocol*) : un protocole de contrôle de conférence fournit l'interface pour la manipulation des données et la restitution d'état pour les données de la conférence centralisée, représentée par l'objet conférence.

Fabrique de conférence : c'est une entité logique qui génère des URI uniques pour identifier et représenter un centre de conférence.

Identifiant de conférence (ID) : c'est un URI spécifique du protocole de signalisation d'appel qui identifie un centre de conférence et son instance de conférence associée.

Informations de conférence : elles incluent les définitions des caractéristiques de base de conférence, comme les identifiants de conférence, les membres, la signalisation, les capacités, et les types de supports applicables à une large gamme d'applications de conférence. Les informations de conférence incluent aussi les données de support et spécifiques d'application pour les caractéristiques ou capacités de conférence améliorées, comme des mixeurs de supports. Les informations de conférence sont le type de données (c'est-à-dire, le schéma XML) pour un objet conférence.

Instance de conférence : une instance de conférence se réfère à une mise en œuvre interne d'une conférence spécifique, représentée comme un ensemble d'objets conférence logiques et d'identifiants associés.

Objet conférence : un objet conférence représente une conférence à un certain stade (par exemple, description sur la création, réservation, activation, etc. de conférence) qu'un système de conférence maintient afin de décrire les capacités du système et de fournir l'accès aux services disponibles pour chaque objet indépendamment. Le schéma d'objet conférence se fonde sur les informations de conférence.

Identifiant d'objet conférence : un identifiant d'objet conférence est un URI qui identifie de façon univoque un objet conférence et est utilisé par un protocole de contrôle de conférence pour accéder aux, et modifier les informations de conférence.

Politiques de conférence : politiques de conférence se réfère collectivement à un ensemble de droits, permissions, et limitations relevant des opérations effectuées sur un certain objet conférence.

Réservation de conférence : une réservation de conférence est un objet conférence, qui est créé à partir d'un système par défaut ou d'une ébauche choisie par le client.

État de conférence : l'état de conférence reflète l'état d'une instance de conférence et est représenté en utilisant un schéma spécifique bien défini.

Système de conférence : un système de conférence se réfère à une solution de conférence fondée sur le modèle de données discuté dans ce document cadre et construit en utilisant les spécifications de protocole référencées dans ce document cadre.

Identifiant d'utilisateur de conférence : identifiant unique pour un utilisateur dans la portée d'un système de conférence. Un utilisateur peut avoir plusieurs identifiants d'utilisateur de conférence au sein d'un système de conférence (par exemple, pour représenter des rôles différents).

La parole : la parole se réfère à un ensemble de données ou ressources associées à une instance de conférence, pour lequel un accès temporaire est accordé à un participant, ou groupe de participants, à la conférence.

Gestion de la parole : la gestion de la parole *(floor chair)* est un client conforme au protocole de contrôle de la prise de parole, soit un participant humain, soit une entité automatique, qui est autorisé à gérer l'accès à la prise de parole et peut accorder, refuser, ou révoquer l'accès. La gestion de la parole n'est pas nécessairement un participant à l'instance de conférence.

Centre *(focus)* : un centre est une entité logique qui maintient l'interface de signalisation d'appel avec chaque client participant et l'objet conférence représentant l'état actif. À ce titre, le centre agit comme un point d'extrémité pour chacun des protocoles de signalisation pris en charge et est responsable de toutes les opérations principales de jonction à la conférence (par exemple, se joindre, quitter, mettre à jour l'instance de conférence) et de la négociation/maintenance des supports entre un participant à la conférence et le centre.

Graphe des supports : le graphe des supports est la représentation logique des flux de supports pour une conférence.

Mixeur de supports : un mixeur de supports est l'entité logique qui a la capacité de combiner les entrées de supports du même type, de transcoder les supports, et de distribuer le ou les résultats à une seule ou plusieurs sorties. Dans ce contexte, le terme "support" signifie tout type de données livrées sur le réseau en utilisant les moyens de transport

appropriés, comme le protocole de contrôle des données en temps (RTCP) (défini dans la [RFC3550]) ou le protocole de relais de session de message (défini dans la [RFC4975]).

Rôle : un rôle donne le contexte pour l'ensemble des opérations de conférence qu'un participant peut effectuer. Un rôle par défaut (par exemple, de participant standard à une conférence) va toujours exister, fournissant à un utilisateur un ensemble de base d'opérations de conférence. Sur la base de l'authentification et de l'autorisation spécifiques d'un système, un utilisateur peut prendre différents rôles, comme de modérateur de conférence, permettant l'accès à une plus large gamme d'opérations de conférence.

Session annexe *(sidebar)* : une session annexe est une instance de conférence séparée qui n'existe que dans le contexte d'une instance de conférence parente. L'objectif d'une session annexe est d'être capable de fournir des supports supplémentaires ou de remplacement à des participants spécifiques.

Chuchotement : un chuchotement *(whisper)* implique une entrées de support unique à un ou des participants spécifiques au sein d'une instance de conférence spécifique, accomplie en utilisant une session annexe. Un exemple de chuchotement serait une annonce injectée seulement au président de la conférence ou à un nouveau participant qui se joint à une conférence.

## 4. Vue générale

Une conférence centralisée est une association de points d'extrémité, appelés les participants à la conférence, avec un point d'extrémité central, appelé le centre de conférence. Le centre a des relations d'homologue directes avec les participants en maintenant une interface de signalisation d'appel séparée avec chacun. Par conséquent, dans ce modèle de conférence centralisée, le graphe de signalisation d'appel est toujours en étoile.

La plus basique prise en charge de conférence dans ce modèle serait une conférence ad hoc, non gérée, qui n'exigerait pas nécessairement les fonctions définies dans ce cadre. Par exemple, elle pourrait être prise en charge en utilisant la fonction de signalisation SIP de base avec un participant servant de centre ; les documents de cadre de conférence SIP [RFC4353] avec la commande d'appel de conférence SIP pour les agents d'utilisateur [RFC4579] traitent ce type de scénarios.

En plus des caractéristiques de base, un système de conférence qui prend en charge le modèle de la conférence centralisée proposé dans ce document cadre peut cependant offrir des fonctionnalités plus riches, en incluant des applications de conférence dédiées avec des capacités explicitement définies, des conférences récurrentes réservées, en fournissant les protocoles standard pour gérer et contrôler les différents attributs de ces conférences.

Les exigences principales pour les conférences centralisées sont mentionnées dans la [RFC4245]. Ces exigences sont applicables aux systèmes de conférence qui utilisent divers protocoles de signalisation d'appel, incluant SIP. Des exigences de conférence supplémentaires sont fournies dans les [RFC4376] et [RFC4597].

Le système de conférence centralisée proposé par ce cadre est construit autour du concept fondamental d'un objet conférence. Un objet conférence fournit la représentation des données d'une conférence durant chacune des diverses étapes d'une conférence (par exemple, création, réservation, active, terminée, etc.). On accède à un objet conférence via les éléments fonctionnels logiques avec lesquels s'interface un client de conférence en utilisant les divers protocoles identifiés à la Figure 1. Les éléments fonctionnels définis pour un système de conférence décrit par le cadre sont un serveur de contrôle de conférence, un serveur de contrôle de la prise de parole, un nombre quelconque de centres, et un service de notification. Un protocole de contrôle de conférence (CCP) fournit l'interface entre un client de contrôle de conférence et de supports et le serveur de contrôle de conférence. Un protocole de contrôle de la prise de parole (par exemple, le protocole de contrôle binaire de la prise de parole (BFCP, *Binary Floor Control Protocol*)) fournit l'interface entre un client de contrôle de la prise de parole et le serveur de contrôle de la prise de parole. Un protocole de signalisation d'appel (par exemple, SIP, H.323, Jabber, Q.931, ISUP, etc.) fournit l'interface entre un client de signalisation d'appel et un centre. Un protocole de notification (par exemple, SIP Notify [RFC3265]) fournit l'interface entre le client de conférence et le service de notification.

Un système de conférence peut prendre en charge un sous ensemble des fonctions de conférence décrites dans la décomposition logique de système de conférence de la Figure 1 et décrit dans ce document. Cependant, il y a des composants essentiels qui vont être normalement utilisés par la plupart des autres fonctions avancées, comme le service de notifications. Par exemple, le service de notifications est utilisé pour corréler des information, comme la liste des participants avec leurs flux de supports, entre les divers autres composants.

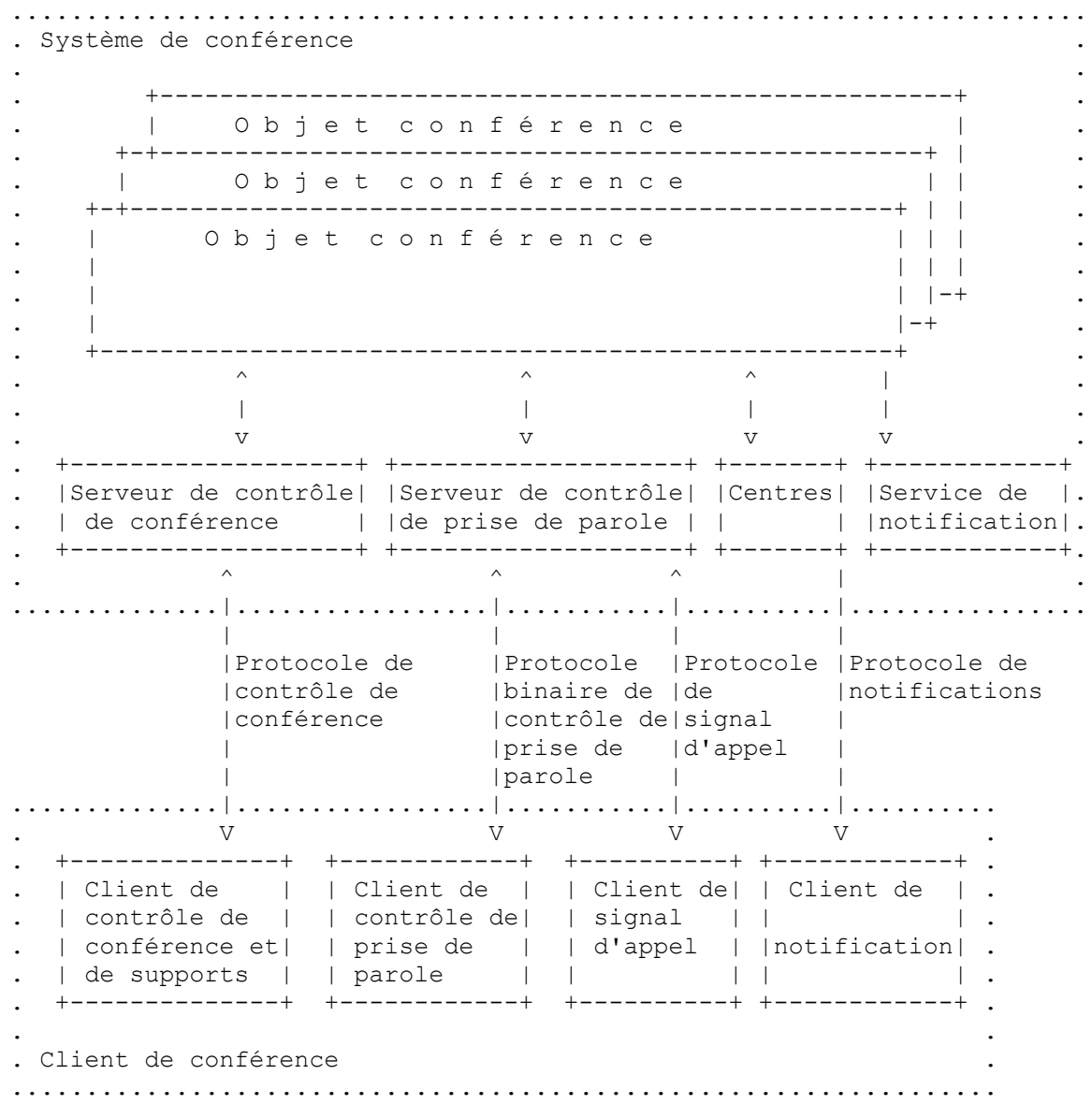



**Figure 1 : Décomposition logique du système de conférence**

Le graphe des supports d'une conférence peut être centralisé, décentralisé, ou de toute combinaison des deux et potentiellement différer par type de supports. Dans le cas centralisé, les sessions de supports sont établies entre un mixeur de supports contrôlé par le centre et chacun des participants. Dans le cas décentralisé (c'est-à-dire, réparti) le graphe des supports est un maillage en diffusion groupée ou multi envois individuels parmi les participants. Par conséquent, le traitement des supports (par exemple, le mixage) peut être contrôlé soit par le centre seul, soit par les participants. Les concepts dans ce document cadre portent clairement sur un modèle de supports centralisés. Les concepts peuvent aussi s'appliquer au cas de supports décentralisés ; cependant, les détails de ce cas sont laissés pour de futures études.

La Section 5 du présent document fournit plus de détails sur l'objet conférence. La Section 6 définit les constructions et les identifiants qui DOIVENT être mis en œuvre pour gérer les objets de conférence, leurs instances, et les utilisateurs associés à un système de conférence. La Section 7 du présent document décrit comment un système de conférence est construit logiquement en utilisant le modèle de données de haut niveau défini et comment les objets de conférence sont maintenus. La Section 8 décrit les mécanismes fondamentaux de conférence et fournit une vue d'ensemble générale des protocoles. La Section 9 fournit ensuite des réalisations de divers scénarios de conférence, détaillant les manipulations des objets de conférence en utilisant les protocoles définis. La Section 10 de ce document résume les relations entre ce cadre de conférence centralisée et le cadre de conférence SIP.

## 5. Données de conférence centralisée

Les données de conférence centralisée sont représentées de façon logique par l'objet conférence. Un objet conférence est du type "type d'informations de conférence", comme illustré à la Figure 2. Les informations de type de conférence sont extensibles.

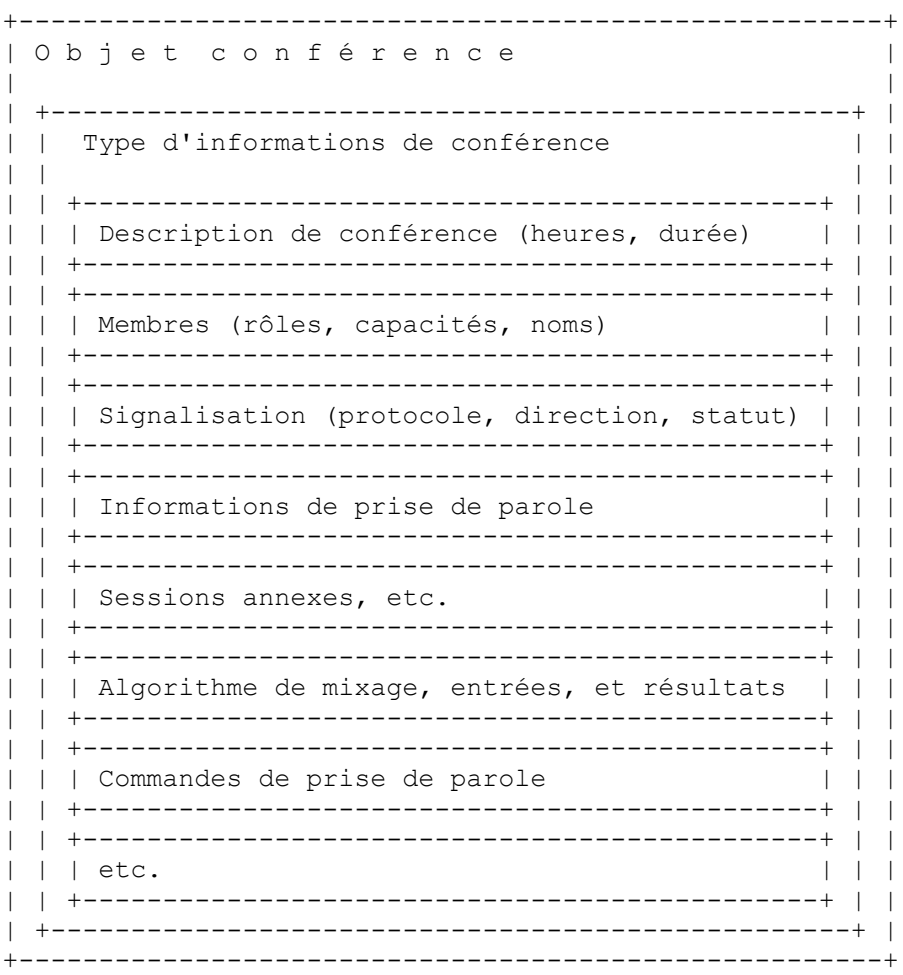



**Figure 2 : Décomposition du type d'objet Conférence**

Dans un système fondé sur ce cadre de conférence, le même type d'objet conférence est utilisé pour représenter une conférence durant les différentes étapes de la conférence, comme d'exprimer les capacités du système de conférence, de réserver les ressources de conférence, ou de refléter l'état des conférences en cours. La Section 7 décrit la sémantique de l'utilisation des objets de conférence. Le schéma XML exact de l'objet conférence, incluant l'organisation des informations de conférence est précisé dans un document distinct [RFC6501].

Avec le modèle de données de base, comme défini dans la [RFC6501], la réalisation de ce cadre exige une infrastructure de politique. Les politiques requises par ce cadre pour gérer et contrôler l'accès aux données incluent des limites locales au niveau du système associées à des éléments de données spécifiques, comme les membres, et les gammes de limitations des autres éléments de données. Des considérations de politique supplémentaires pour une réalisation de système fondée sur ce modèle de données sont discutées au paragraphe 5.2.

### 5.1 Informations de conférence

Il y a un ensemble central de données dans les informations de conférence qui est utilisé dans toute conférence, indépendamment de la nature spécifique du support de conférence (par exemple, les algorithmes de mixage effectués, le contrôle de la prise de parole appliqué, etc.). Cet ensemble central de données dans les informations de conférence contient les définitions qui représentent les capacités de l'objet conférence, les membres, les rôles, la signalisation d'appel, et l'état des supports pertinents aux différentes étapes du cycle de vie de la conférence. Cet ensemble central d'informations de

conférence peut être représenté en utilisant le type de conférence, comme défini dans le paquetage d'événement de conférence SIP [RFC4575]. Normalement, les participants avec un accès en lecture seule aux informations de conférence vont être intéressés seulement par cet ensemble central d'informations de conférence.

Afin de prendre en charge des manipulations de supports plus complexes et des caractéristiques de conférence améliorées, les informations de conférence, comme définies dans le modèle de données [RFC6501], contiennent des données supplémentaires au delà de celles définies dans le paquetage d'événements de conférence SIP [RFC4575]. Les informations définies dans le modèle de données [RFC6501] fournissent des détails spécifiques du mixage des supports, les contrôles de prise de parole disponibles, et autres données nécessaires pour prendre en charge des caractéristiques de conférence améliorées. Ces informations permettent aux clients autorisés de manipuler le comportement du mixeur via le centre, avec la distribution résultante des supports à tous les participants ou à des participants individuels. En faisant ainsi, un client peut changer son propre état et/ou l'état des autres participants à la conférence.

De nouvelles spécifications de conférence centralisée pourront étendre le type de base de conférence défini dans le modèle de données [RFC6501], et introduire des éléments de données supplémentaires à utiliser dans le type d'informations de conférence.

### 5.2 Politiques de conférence

Les politiques de conférence se réfèrent collectivement à un ensemble de droits, permissions et limitations relevant des opérations effectuées sur un certain objet conférence.

L'ensemble des droits décrit les privilèges d'accès en lecture/écriture pour l'objet conférence dans son ensemble. Cet accès va généralement être accordé et défini en termes de donner l'accès en lecture seule ou en lecture/écriture aux clients avec certains rôles dans la conférence. Gérer cet accès exigerait d'un système de conférence qu'il ait accès aux informations de politique de base pour prendre les décisions, mais n'exige pas nécessairement une représentation explicite dans le modèle de politique. À ce titre, pour le présent document cadre, les politiques représentées par l'ensemble de droits sont reflétées dans la réalisation du système (Section 7).

Les permissions et limites exigent des mécanismes de politique explicites et sortent du domaine d'application du modèle de données [RFC6501] et de ce document cadre. Cependant, il y a des considérations de politique importantes pour un système de conférence. Un système de conférence associe des politiques spécifiques sous forme de permissions et limitations à chaque utilisateur dans un système de conférence. Les permissions peuvent varier selon le rôle associé à un identifiant d'utilisateur de conférence spécifique. Un système de conférence devrait fournir un rôle d'utilisateur par défaut qui permette seulement la participation à une conférence par les moyens de signalisation par défaut.

L'identifiant d'objet conférence fournit l'accès aux données associées à une conférence spécifique. Il est important de s'assurer que les éléments dans les données ont des contrôles individuels de politique pour donner de la souplesse dans la définition des divers rôles et des éléments de données spécifiques qui peuvent être manipulés par des utilisateurs avec des rôles spécifiques.

De plus, l'interface de notification de conférence permet que des éléments de données spécifiques soient envoyés aux utilisateurs qui s'enregistrent pour de telles notifications. Il est important que le contrôle d'accès approprié soit fourni afin que seuls les utilisateurs autorisés à voir des éléments de données spécifiques reçoivent ces données dans les notifications.

## 6. Constructions et identifiants de conférence centralisée

Cette Section fournit les détails des identifiants associés aux constructions du cadre de conférence centralisée et des identifiants EXIGÉS pour s'adresser aux clients associés à un système de conférence et les gérer. Une vue d'ensemble de l'allocation, des caractéristiques, et du rôle fonctionnel des identifiants est fournie.

### 6.1 Identifiant de conférence

L'identifiant de conférence est un URI spécifique du protocole de signalisation d'appel qui identifie un centre de conférence spécifique et son instance de conférence associée. Une fabrique de conférence est une méthode pour générer un identifiant de conférence univoque, pour identifier et s'adresser à un centre de conférence, en utilisant une interface de signalisation d'appel. Les détails sur l'utilisation d'une fabrique de conférence pour la signalisation SIP se trouvent dans la [RFC4579]. L'identifiant de conférence peut aussi être obtenu en utilisant le protocole de contrôle de conférence ou autrement, y

compris par des mécanismes propriétaires, hors bande. Pour réaliser le cadre de conférence centralisé dans le présent document, un système de conférence est EXIGÉ pour prendre en charge SIP comme protocole de signalisation d'appel par défaut. Les autres protocoles de signalisation d'appel (par exemple, ISUP) sont FACULTATIFS.

### 6.2 Objet Conférence

Un objet conférence fournit la représentation logique d'une instance de conférence à une certaine étape, comme une ébauche de conférence représentant les capacités d'un système de conférence, les données représentant une réservation de conférence, et l'état de la conférence durant une conférence active. Chaque objet conférence est adressable de façon indépendante à travers l'interface de protocole de contrôle de conférence (voir au paragraphe 8.3). Un système de conférence DOIT fournit une ébauche par défaut représentant les capacités de base fournies par ce système de conférence spécifique.

La Figure 3 illustre les relations entre l'identifiant de conférence, le centre, et l'identifiant d'objet conférence dans le contexte d'une instance logique de conférence, avec l'objet conférence correspondant à une conférence active.

Un objet conférence représentant une conférence dans l'état actif peut avoir plusieurs signalements d'appel d'identifiants de conférence ; par exemple, un pour chaque protocole de signalisation d'appel pris en charge. Il y a une transposition biunivoque entre un objet conférence actif et un centre de conférence. Le centre est identifié en associant explicitement des identifiants de conférence univoques pour chaque protocole de signalisation pris en charge par l'objet conférence actif.

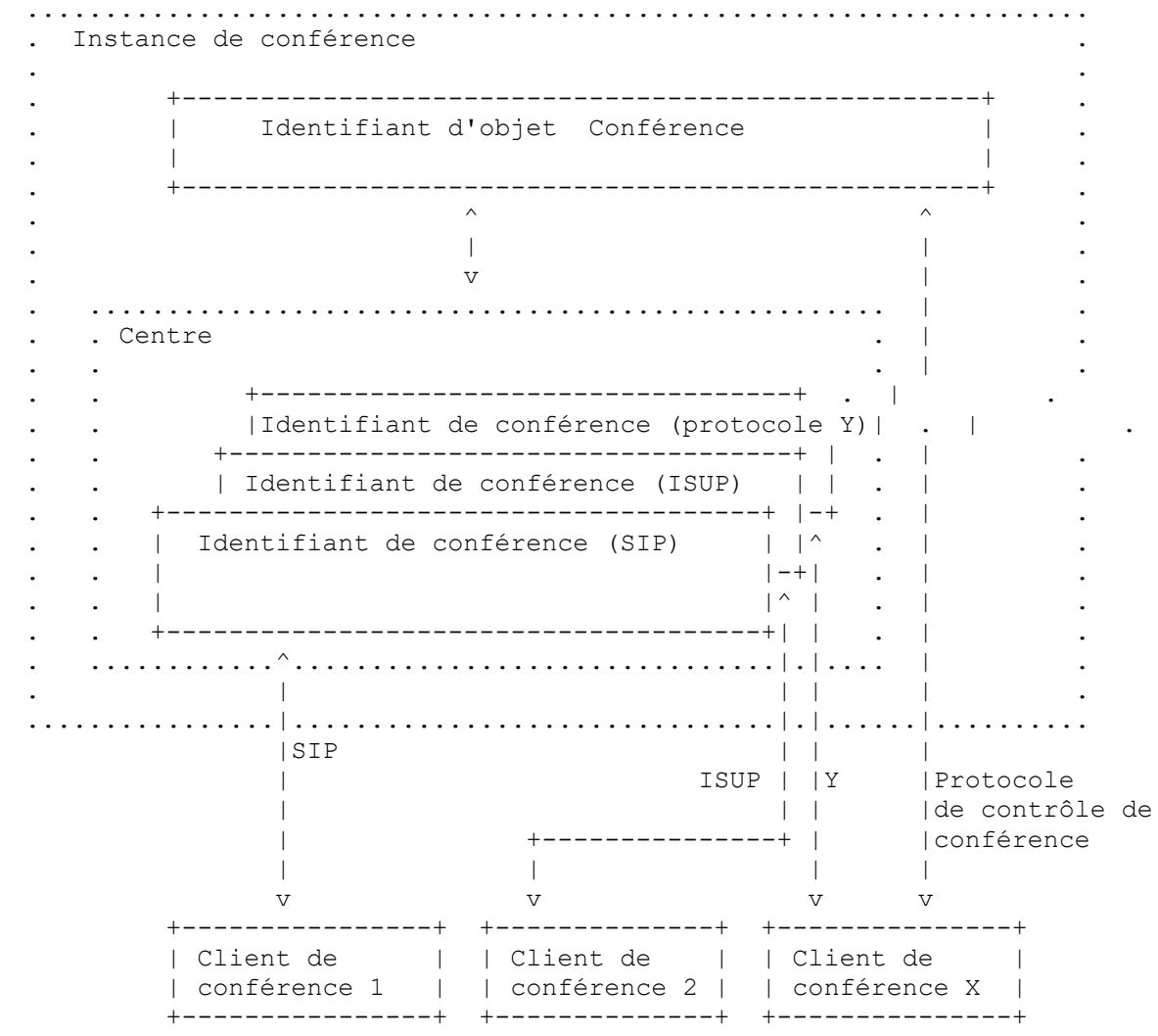



**Figure 3 : Relations d'identifiant pour une conférence active**

### 6.2.1 Identifiant d'objet Conférence

Afin de rendre chaque objet conférence accessible en externe, le système de conférence DOIT allouer un URI unique par objet conférence distinct dans le système. L'identifiant d'objet conférence est défini dans la [RFC6501]. Un système de conférence alloue un identifiant d'objet conférence pour chaque ébauche de conférence, pour chaque réservation de conférence, et pour chaque conférence active. La distribution de l'identifiant d'objet conférence dépend du cas d'utilisation spécifique et inclut divers mécanismes, comme le mécanisme du protocole de contrôle de conférence, le modèle de données et le paquetage de conférence, ou des mécanismes hors bande comme la messagerie électronique.

Quand un utilisateur souhaite créer ou se joindre à une conférence et qu'il n'a pas l'identifiant d'objet conférence pour cette conférence, des mécanismes de signalisation plus généraux s'appliquent. Un utilisateur peut avoir un identifiant d'objet conférence pré-configuré pour accéder au système de conférence ou d'autres protocoles de signalisation peuvent être utilisés et le système de conférence les transpose en un identifiant d'objet conférence spécifique. Une fois qu'une conférence est établie, un identifiant d'objet conférence est EXIGÉ pour que l'utilisateur manipule des données de la conférence ou tire parti de toute caractéristique évoluée de conférence. La même notion s'applique aux utilisateurs qui se joignent à une conférence en utilisant d'autres protocoles de signalisation. Ils sont capables de se joindre initialement à une conférence en utilisant tout autre protocole de signalisation pris en charge par le système de conférence spécifique, mais l'identifiant d'objet conférence DOIT être utilisé pour manipuler toutes données de conférence ou tirer parti d'une caractéristique de conférence évoluée. Comme mentionné précédemment, le mécanisme par lequel l'utilisateur apprend l'identifiant d'objet conférence varie et pourrait être via le protocole de contrôle de conférence, en utilisant le modèle de données et le paquetage de conférence ou des mécanismes entièrement hors bande comme la messagerie électronique ou une interface de la Toile.

L'identifiant d'objet conférence se transpose logiquement en autres identifiants spécifiques de protocole associés à l'instance de conférence, comme le BFCP "confid". La transposition de l'identifiant d'objet conférence peut être vue comme contenant des informations sensibles dans de nombreux systèmes de conférence. Le système de conférence doit s'assurer que les données sont protégées, que seuls des utilisateurs autorisés peuvent manipuler ces informations via le protocole de contrôle de conférence, et que seuls les utilisateurs appropriés reçoivent les informations par le protocole de notification. En général, ces informations ne sont pas supposées être distribuées au participant moyen à la conférence.

## 6.3 Identifiant d'utilisateur de conférence

Chaque utilisateur dans un système de conférence DOIT recevoir un unique identifiant d'utilisateur de conférence. L'identifiant d'utilisateur de conférence est défini dans la [RFC6501]. L'identifiant d'utilisateur de conférence est utilisé en association avec l'identifiant d'objet conférence pour identifier de façon univoque l'utilisateur dans la portée du système de conférence. Il y a aussi une exigence pour identifier les utilisateurs de système de conférence qui peuvent ne pas participer à une instance de conférence. Des exemples de ces utilisateurs seraient un président de contrôle de parole ou un contrôleur de politique de support non participant. L'identifiant d'utilisateur de conférence est EXIGÉ, dans les demandes de protocole de contrôle de conférence, pour déterminer de façon univoque qui produit les commandes, afin que les politiques appropriées puissent être appliquées à la commande demandée.

Un mode normal de distribution de l'identifiant d'utilisateur est hors bande durant la configuration du client de conférence ; donc, le mécanisme sort du domaine d'application du cadre et des protocoles de conférence centralisée. Cependant, un système de conférence DOIT aussi être capable d'allouer et distribuer un identifiant d'utilisateur durant la première interaction de signalisation avec le système de conférence, comme une demande initiale pour les ébauches ou l'ajout d'un nouvel utilisateur à une conférence existante en utilisant le protocole de contrôle de conférence. Quand un utilisateur rejoint une conférence en utilisant un protocole spécifique de la signalisation, comme SIP pour une conférence par appel numéroté, un identifiant d'utilisateur de conférence DOIT être alloué si un n'est pas déjà associé à cet utilisateur. Bien que cet identifiant d'utilisateur de conférence ne soit pas exigé pour que le participant se joigne à la conférence, il est EXIGÉ qu'il soit alloué et affecté par le système de conférence afin qu'il soit disponible pour être utilisé pour toute opération suivante de protocole de contrôle de conférence et/ou notifications associées à cette conférence. Par exemple, l'identifiant d'utilisateur de conférence va être envoyé dans toutes les notifications qui peuvent être envoyées aux participants existants, comme le modérateur, quand cet utilisateur rejoint la conférence.

L'identifiant d'utilisateur de conférence est logiquement associé aux autres identifiants d'utilisateur alloués au client de conférence pour d'autres interfaces de protocole, comme un utilisateur SIP authentifié. La transposition de l'identifiant d'utilisateur de conférence en identifiants d'utilisateur spécifiques de la signalisation exige que des méthodes pour protéger et sécuriser l'identité d'un utilisateur soient considérées. Le paragraphe 11.1 traite de l'authentification et l'autorisation de l'utilisateur et le paragraphe 11.2 traite de la sécurité et la confidentialité de l'identité de l'utilisateur. De plus, le système de conférence DOIT assurer le contrôle d'accès approprié autour de toute structure de données interne qui maintient ces

données persistantes. Ces informations ne vont normalement être disponibles qu'à un administrateur de système de conférence.

## 7. Réalisation d'un système de conférence

Les mises en œuvre fondées sur ce cadre de conférence centralisée peuvent aller de systèmes qui prennent en charge les conférences ad hoc, avec seulement le comportement par défaut, jusqu'aux systèmes sophistiqués avec la capacité de programmer des conférences récurrentes, ayant chacune des caractéristiques distinctes, intégrées avec des outils externes de réservation de ressources, et fournissant des photographies des informations de conférence à toutes les étapes du cycle de vie de la conférence.

Un objet conférence est la représentation logique d'une instance de conférence à une certaine étape, comme la description des capacités à la création, réservation, activation, etc. d'une conférence, qu'un système de conférence maintient afin de décrire les capacités du système et fournir l'accès aux services disponibles offerts par le système de conférence. Par conséquent, ce cadre de conférence centralisée ne rend pas obligatoire l'usage réel de l'objet conférence, mais définit plutôt le concept général d'arborescence de clonage et les mécanismes requis pour sa réalisation, comme décrit dans le détail au paragraphe 7.1.

Des exemples de conférence ad hoc et évoluée sont fournis aux paragraphes 7.2 et 7.3, ce dernier fournissant une description supplémentaire de l'objet conférence en termes d'étapes d'une conférence, pour prendre en charge les capacités de programmation et des autres capacités de conférence évoluée. La programmation d'une conférence sur la base de ces concepts et mécanismes est détaillée au paragraphe 7.4.

Comme exposé au paragraphe 5.2, la politique globale en termes de permissions et limitations sort du domaine d'application du présent document cadre. Les politiques applicables à l'objet conférence comme un tout en termes d'accès en lecture/écriture exigerait qu'un système de conférence ait accès aux informations de politique de base pour prendre les décisions. Dans les exemples de cette section, les politiques sont montrées logiquement associées aux objets conférence pour souligner l'exigence générale de la fonction de politique nécessaire pour la réalisation de ce cadre.

### 7.1 Arborescence de clonage

Le concept défini dans ce paragraphe est seulement une représentation logique, comme elle est reflétée à travers les mécanismes de la conférence centralisée : les URI et les protocoles. Bien sûr, la réalisation réelle du système peut différer du modèle présenté. L'intention est d'illustrer le rôle des éléments logiques dans la fourniture d'une interface aux données, sur la base du système de conférence et des actions du client de conférence, et de décrire les implications de protocole résultantes.

Tout objet conférence dans un système de conférence est créé soit en étant explicitement cloné à partir d'un objet parent existant, soit en étant implicitement cloné à partir d'une ébauche de conférence d'un système par défaut. Une ébauche de conférence est un objet conférence statique utilisé pour décrire la prise en charge normale d'un établissement de conférence par le système. Chaque système peut maintenir plusieurs ébauches, chacune décrivant normalement un type de conférence différent en utilisant le format des informations de conférence. Le présent document utilise la métaphore du "clonage" plutôt que celle de "héritage" parce qu'elle colle plus à l'idée de duplication d'objet, plutôt qu'à un concept de réutilisation et extension d'un type de données.

L'opération de clonage doit spécifier si la liaison entre parent et enfant doit ou non être maintenue dans le système. Si aucune liaison entre le parent et l'enfant n'existe, les objets deviennent indépendants et l'enfant n'est pas impacté par les opérations sur l'objet parent ni soumis aux limitations de l'objet parent.

Une fois le nouvel objet créé, on peut s'y adresser par un unique URI d'objet conférence alloué par le système, comme décrit au paragraphe 6.2.1. Par défaut, l'objet nouvellement créé contient toutes les données existantes de l'objet parent. L'objet nouvellement créé peut étendre les données qu'il contient, dans les types de schéma pris en charge par le parent. Il peut aussi restreindre l'accès en lecture/écriture à ses objets. Cependant, sauf si l'objet est indépendant, il ne peut pas modifier les restrictions d'accès imposées par l'objet parent.

On peut, dans l'objet fils, accéder indépendamment à tout élément de données et, par défaut, le modifier indépendamment, sans affecter les données parentes.

Sauf si l'objet est indépendant, l'objet parent peut appliquer une politique différente en marquant certains éléments de données comme "applicable par le parent". Les valeurs de ces éléments de données ne peuvent pas être changées par un accès direct de l'objet fils, ni ne peuvent être étendues dans le seul objet fils.

La Figure 4 illustre un exemple de conférence (Parent B) qui est créée indépendamment de son parent (Parent A). Parent B crée deux objets fils, Fils 1 et Fils 2. Tous les éléments de données de Parent B peuvent être modifiés (c'est-à-dire, ils ne sont pas des éléments de données "applicable par le parent") et selon l'élément, les changements vont être reflétés dans Fils 1 et Fils 2, tandis que les changements à Parent A ne vont pas impacter les éléments de données de Parent B. Aucun élément de données "applicable par le parent", comme défini par Parent B, ne peut être modifié dans les objets fils.

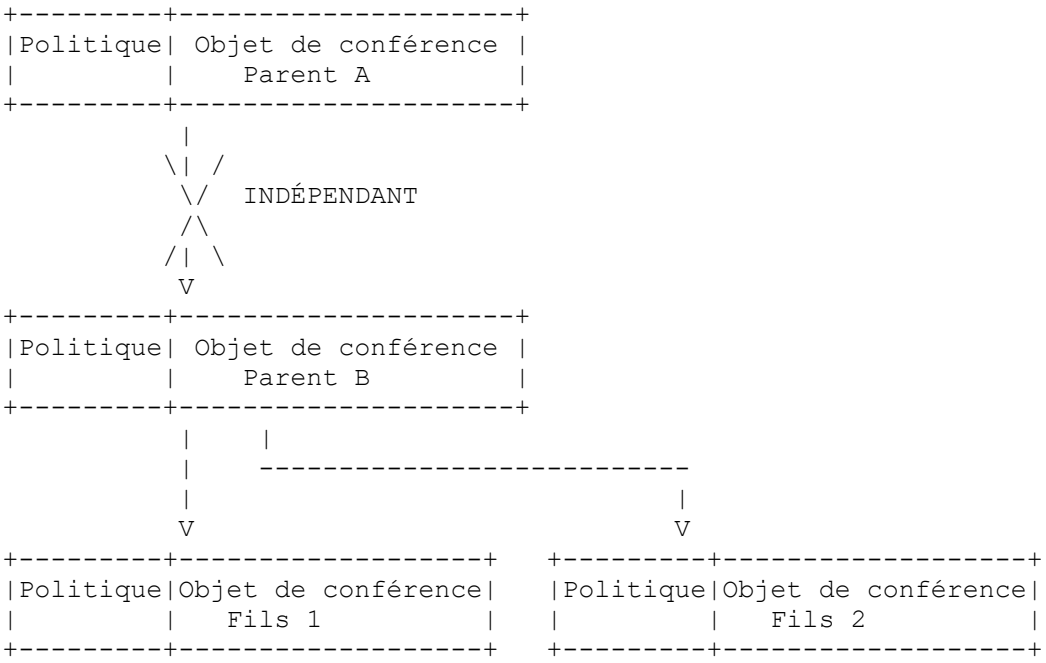



**Figure 4 : Arborescence de clonage**

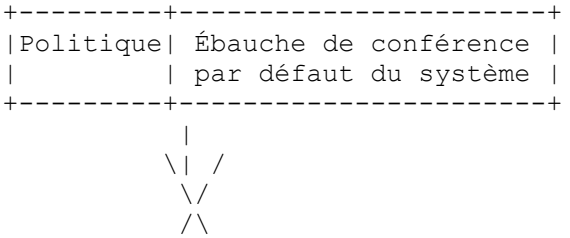
En utilisant le modèle de clonage défini et ses outils, les paragraphes qui suivent montrent des exemples de la façon dont les différents systèmes fondés sur ce cadre peuvent être réalisés.

### 7.2. Exemple ad hoc

La Figure 5 illustre comment une conférence ad hoc peut être créée et gérée dans un système de conférence. Un client peut créer une conférence en établissant un canal de signalisation d'appel avec une fabrique de conférences, comme spécifié au paragraphe 6.1. La fabrique de conférences peut choisir en interne une des ébauches de conférence que le système prend en charge sur la base des privilèges du client demandeur et des lignes de support incluses dans le corps du protocole de description de session (SDP, *Session Description Protocol*).

L'ébauche choisie avec ses valeurs par défaut est copiée par le serveur dans un nouvel objet conférence créé, appelé une "conférence active". À ce point, l'objet conférence devient indépendant de son ébauche. Un nouvel identifiant d'objet conférence, un nouvel identifiant de conférence, et un nouveau centre sont alloués par le serveur.

Pendant la durée de vie de la conférence, un client autorisé peut manipuler l'objet conférence, en effectuant des opérations comme l'ajout de participants, en utilisant le protocole de contrôle de conférence.



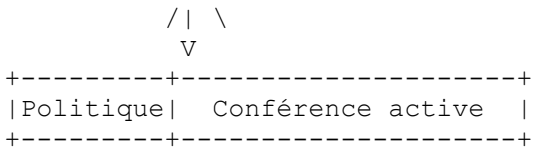



**Figure 5 : Création et durée de vie de conférence ad-hoc**

### 7.3 Exemple évolué

La Figure 6 illustre comment une conférence récurrente peut être spécifiée, programmée, réservée, et gérée selon les capacités d'un système dans un système de conférence. Un client va d'abord interroger un système de conférence sur ses capacités. Cela peut être fait en demandant une liste des ébauches de conférence que le système prend en charge. Chaque ébauche contient une combinaison spécifique de capacités et limitations du serveur de conférence en termes de types de supports pris en charge (par exemple, audio, vidéo, texte, ou leurs combinaisons) de rôles de participants, de nombre maximum de participants de chaque rôle, de disponibilité du contrôle de la prise de parole, de commandes disponibles pour les participants, de disponibilité et de type de conférences annexes, de définitions et noms des flux de supports, etc.

L'ébauche choisie avec ses valeurs par défaut est clonée par le client en un nouvel objet conférence créé, appelé une réservation de conférence, qui spécifie les ressources nécessaire dans le système pour cette instance de conférence. À ce point, la réservation de conférence devient indépendante de son ébauche. Le client peut aussi changer les valeurs par défaut, dans les gammes du système, et ajouter des informations supplémentaires, telles que la liste des participants et l'heure de début de la conférence, à la réservation de conférence.

À ce point, le client peut demander au serveur de conférence de créer de nouvelles réservations de conférence en attachant la réservation de conférence à la demande. Par suite, le serveur peut allouer les ressources nécessaires, créer des objets de conférence supplémentaires pour réservations de conférence filles, et allouer des identifiants d'objet conférence pour toutes, la réservation de conférence originale et chaque réservation de conférence fille.

À partir de ce moment, tout client autorisé est capable d'accéder et modifier chaque objet conférence indépendamment. Par défaut, les changements à une réservation de conférence fille individuelle ne va affecter ni la réservation de conférence parente, à partir de laquelle elle a été créée, ni ses apparentées.

Par ailleurs, certains des sous objets de la conférence, comme le nombre maximum de participants et la liste des participants, peuvent être définis par le système comme applicables par le parent. Par suite, ces objets ne peuvent être modifiés qu'en accédant à la réservation de conférence parente. Le changement de ces objets peut être appliqué automatiquement à chacune des réservations filles, selon la politique locale.

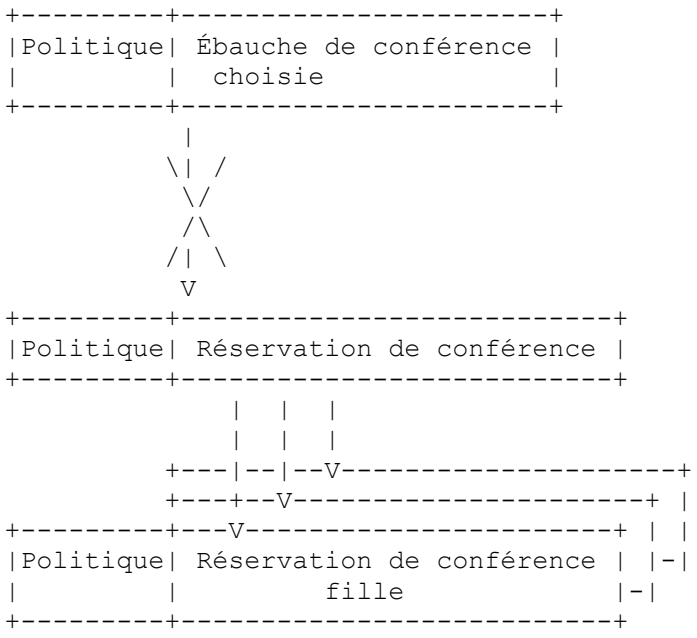



**Figure 6 : Définition, création, et durée de vie de conférence évoluée**

Quand vient le moment de programmer la réservation de conférence, soit via la détermination par le système que l'heure de début a été atteinte, soit via l'invocation du client, une conférence active est clonée sur la base de la réservation de conférence. Comme dans l'exemple ad hoc, la conférence active est indépendante de la parente, et les changements à la réservation de conférence ne vont pas impacter la conférence active. Tous les changements désirés doivent être ciblés sur la conférence active. Un exemple de cette interaction est montré au paragraphe 9.1.

### 7.4 Programmation d'une conférence

La capacité de programmer des conférences forme une partie importante de la solution du système de conférence. Une réservation de conférence individuelle a normalement une heure de début et une heure de fin spécifiées, les heures étant spécifiées par rapport à une seule heure fixe spécifiée (par exemple, "début" = 09.00 GMT, "fin" = "début" +2) selon les particularités du système. Dans la plupart des solutions de conférence évoluées, il est possible de non seulement programmer une occurrence individuelle d'une réservation de conférence, mais aussi de programmer une série de conférences en rapport les unes avec les autres (par exemple, une réunion hebdomadaire débutant le jeudi à 09.00 GMT).

Pour être capable de réaliser une telle fonctionnalité, un système de conférence a besoin d'être capable de programmer et maintenir de façon appropriée les réservations de conférence qui font partie d'une conférence récurrente. Le mécanisme proposé dans ce document utilise la spécification d'objet central de calendrier et de programmation de l'Internet définie dans la [RFC2445] en conjonction avec les concepts introduits à la Section 5 pour réaliser une capacité de programmation de conférence évoluée.

La Figure 7 illustre une vue simplifiée d'un client qui interagit avec un système de conférence. Le client utilise le protocole de contrôle de conférence (CCP) pour ajouter une nouvelle réservation de conférence au système de conférence en faisant l'interface avec le serveur de contrôle de conférence. Une demande CCP contient une réservation de conférence valide et une référence par valeur à un objet "iCal" qui contient les informations de programmation sur la conférence (par exemple, heure de début, heure de fin).

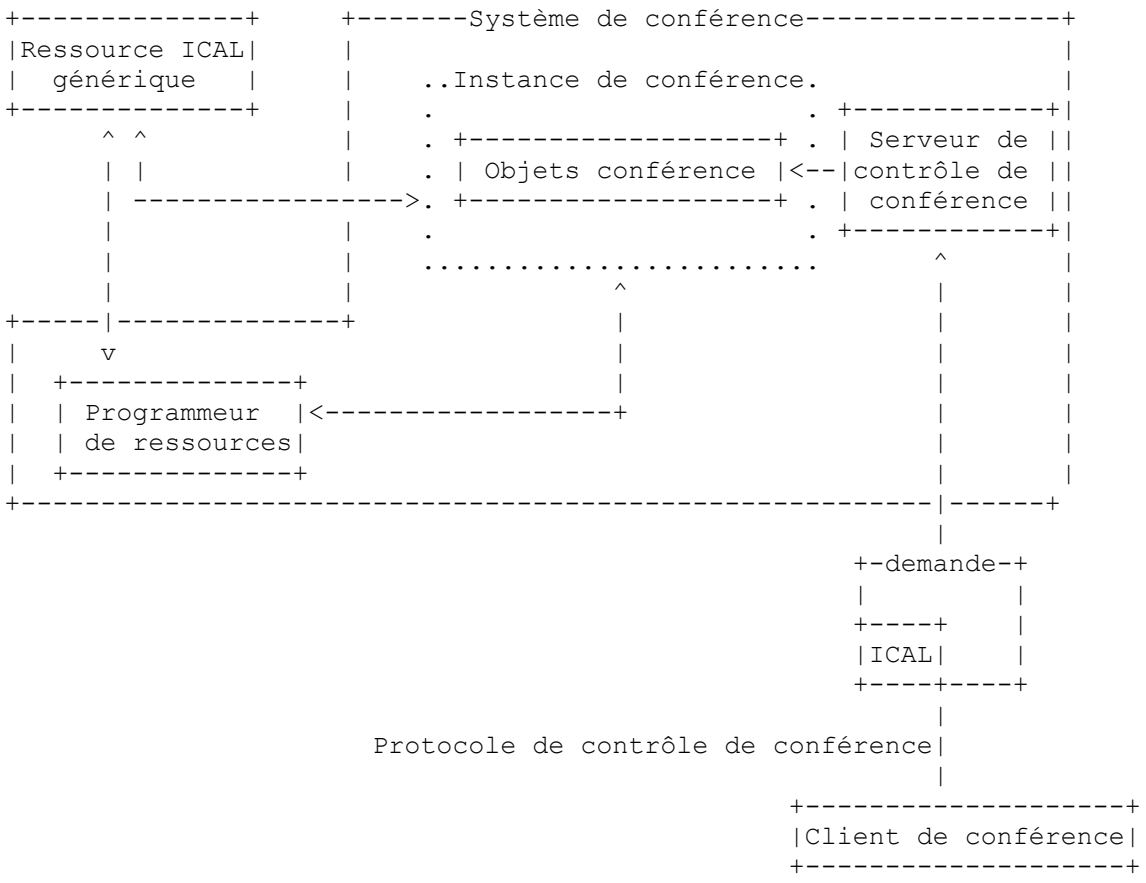



**Figure 7 : Programmation des ressources**

Une demande CCP de créer une nouvelle réservation de conférence est validée, y compris l'objet associé iCal, et la réservation de conférence résultante est créée. La réservation de conférence est représentée de façon univoque dans le système de conférence par un identifiant d'objet conférence (par exemple, xcon:hd87928374) comme introduit au paragraphe 6.2.1 et défini dans la [RFC6501]. Cet URI unique est retourné au client et peut être utilisé pour faire référence à la réservation de conférence, si des manipulations ultérieures sont requises (par exemple, modifier l'heure de début) en utilisant une demande CCP.

L'exemple précédent explique comment un client crée une réservation de conférence de base en utilisant une référence iCal en association avec un protocole de contrôle de conférence. La Figure 7 peut aussi être appliquée pour expliquer comment une série de conférences est programmée dans le système. La description est presque identique, à l'exception de la définition de iCal qui est incluse dans une demande CCP qui représente une série d'instances récurrentes de conférence (par exemple, heure de début/fin de conférence, chaque semaine). Le système de conférence va traiter cette demande de la même façon que dans le premier exemple. La demande CCP va être validée, ainsi que l'objet iCal associé, et la réservation de conférence est créée. La réservation de conférence et son identifiant d'objet conférence, créés pour cet exemple, représentent la série entière d'instances récurrentes de conférence plutôt qu'une seule conférence. Si le client utilise l'identifiant d'objet conférence fourni et une demande CCP d'ajuster la réservation de conférence, chaque instance de conférence dans la série va être altérée. Cela inclut toutes les futures occurrences, telles qu'une conférence programmée comme une série infinie, sous réserve des limitations de l'interface de calendrier disponible.

Un système de conférence qui prend en charge la programmation d'une série d'instances de conférence devrait aussi être capable de prendre en charge la manipulation dans une gamme spécifique de la série. Un bon exemple est une réservation de conférence programmée pour survenir chaque lundi à 09.00 GMT. Pour les trois prochaines semaines seulement, la réunion a été changée pour se tenir à 10.00 GMT dans un autre lieu. En se référant à la Figure 7, le client va construire une demande CCP dont l'objet est de modifier la réservation de conférence existante pour l'instance de conférence récurrente. Le client va inclure l'identifiant d'objet conférence fourni par le système de conférence pour faire explicitement référence à la réservation de conférence dans le système de conférence. Une demande CCP va contenir tous les changements requis à la réservation de conférence (par exemple, changement de lieu).

Le système de conférence confronte la demande CCP entrante à la réservation de conférence existante mais identifie que l'objet iCal associé se réfère seulement à une gamme de la série existante. Le système de conférence crée un enfant en clonant la réservation de conférence originale, pour représenter les instances de conférence altérées au sein de la série. L'objet fils cloné n'est pas indépendant de l'objet parent original, empêchant donc tout conflit potentiel de programmation (par exemple, un changement de l'heure de début de toute la série). La réservation de conférence clonée, représentant la série altérée des instances de conférence, a son propre identifiant d'objet conférence associé qui est retourné au client en utilisant une réponse CCP. Cet identifiant d'objet conférence est alors utilisé par le client pour faire toutes les futures altérations sur la nouvelle sous série définie. Ce procès peut être répété un nombre quelconque de fois parce que le nouvel identifiant d'objet conférence retourné qui représente une série altérée (clonée) d'instances de conférence, peut lui-même être manipulé en utilisant une demande CCP pour le nouvel identifiant d'objet conférence créé. Cela donne une approche flexible à la programmation d'instances de conférence récurrentes.

## 8. Mécanismes de conférence

### 8.1 Signalisation d'appel

Le centre est le composant central de la conférence. Les participants s'interfacent avec le centre en utilisant un protocole de signalisation d'appel (CSP) approprié. Les participants demandent à établir ou à se joindre à une conférence en utilisant le CSP. Après vérification des politiques applicables, un centre accepte alors la demande, envoie une indication de progrès relative à l'état de la demande (par exemple, pour un appel mis en attente en attendant que le modérateur approuve l'adhésion) ou la rejette en utilisant l'interface de signalisation d'appel.

Durant une conférence active, un protocole de contrôle de conférence peut être utilisé pour affecter l'état de la conférence. Par exemple, les demandes CCP d'ajout et suppression de participants sont communiquées au centre et confrontées à la politique de la conférence. Si elles sont approuvées, les participants sont ajoutés ou supprimés en utilisant la signalisation d'appel de et vers le centre.

### 8.2 Notifications

Un système de conférence est chargé de mettre en œuvre un service de notifications de conférence. Le service de notifications de conférence fournit des mises à jour sur l'état de l'instance de conférence aux parties autorisées, incluant les

participants. Un modèle pour les notifications qui utilisent SIP est défini dans la [RFC3265] avec les spécificités de la prise en charge des conférences définies dans la [RFC4575].

L'identifiant d'utilisateur de conférence et le rôle associé sont utilisés par le système de conférence pour filtrer les notifications afin qu'elles ne contiennent que les informations dont l'envoi à cet utilisateur est permis.

### 8.3 Protocole de contrôle de conférence

Le protocole de contrôle de conférence assure la manipulation des données et la restitution d'état pour les données de la conférence centralisée, représentées par l'objet conférence. Les détails du protocole de contrôle de conférence sont fournis dans des documents séparés.

### 8.4 Contrôle de la prise de parole

Un protocole de contrôle de la prise de parole permet à un client autorisé de gérer l'accès à un forum spécifique et d'accorder, refuser, ou révoquer l'accès aux autres utilisateurs de la conférence à ce forum. Le contrôle de la prise de parole n'est pas un mécanisme obligatoire d'une mise en œuvre de système de conférence, mais il fournit des caractéristiques évoluées de contrôle des entrées de supports pour les utilisateurs de conférence. Un mécanisme pour le contrôle de la prise de parole au sein d'un système de conférence est défini dans la spécification du protocole de contrôle à codage binaire de la prise de parole (BFCP, *Binary Floor Control Protocol*) [RFC4582].

Dans ce cadre, un client qui prend en charge le contrôle de la prise de parole a besoin d'obtenir des informations pour se connecter à un serveur de contrôle de la prise de parole pour lui permettre de produire des demandes de prise de parole. Ces informations de connexion peuvent être restituées en utilisant des informations fournies par des mécanismes comme la négociation utilisant l'échange SDP [RFC4566] d'offre/réponse [RFC3264] sur l'interface de signalisation avec le centre. Le paragraphe 11.3 fournit une discussion de l'authentification d'un client auprès d'un serveur de contrôle de la prise de parole.

Comme avec les informations de connexion du client au serveur de contrôle de la prise de parole, un client qui souhaite interagir avec un serveur de contrôle de la prise de parole a besoin d'accéder à des informations supplémentaires. Ces informations associent les interactions de contrôle de la prise de parole avec l'instance appropriée du forum. Une fois qu'une connexion a été établie et authentifiée (voir dans la [RFC4582] les détails de l'authentification) un message spécifique de contrôle de la prise de parole exige des informations détaillées pour identifier sans équivoque une conférence, un utilisateur, et un forum.

La conférence est identifiée sans équivoque par l'identifiant d'objet conférence, conformément au paragraphe 6.2.1. Cet identifiant d'objet conférence doit être inclus dans tous les messages de contrôle de la prise de parole. Quand le modèle SDP est utilisé comme décrit dans la [RFC4583], cet identifiant se transpose en l'attribut "confid" SDP.

Chaque utilisateur autorisé associé à un objet conférence est représenté de façon univoque par un identifiant d'utilisateur de conférence conformément au paragraphe 6.3. Cet identifiant d'utilisateur de conférence doit être inclus dans tous les messages de contrôle de la prise de parole. Quand on utilise l'échange SDP d'offre/réponse pour négocier une connexion de contrôle de la prise de parole avec le centre en utilisant le protocole de signalisation d'appel, l'identifiant d'utilisateur de conférence univoque est contenu dans l'attribut "userid" SDP, comme défini dans la [RFC4583].

Une session de supports au sein d'un système de conférence peut avoir un nombre quelconque de forums (0, un ou plus) qui sont représentés par l'identifiant de conférence. Quand on utilise l'échange SDP d'offre/réponse pour négocier une connexion de contrôle de la prise de parole avec le centre en utilisant l'interface de signalisation d'appel, l'identifiant de conférence univoque est contenu dans l'attribut "floorid" SDP, comme défini dans la [RFC4583], par exemple, a=floorid:1 m-stream:10. Chaque attribut "floorid", représentant un forum unique, a une étiquette "m-stream" qui contient un ou plusieurs identifiants. Les identifiants représentent des sessions individuelles de supports SDP (comme défini en utilisant "m=" de SDP) en utilisant l'attribut SDP "Label", comme défini dans la [RFC4574].

## 9. Réalisations de scénario de conférence

Cette section traite de la façon dont les scénarios de conférence évolués, dont beaucoup ont été décrits dans la [RFC4597], sont réalisé en utilisant ce cadre de conférence centralisée. L'objectif de cette section est de mieux illustrer le modèle, les mécanismes, et les protocoles présentés dans les sections précédentes et aussi servir à valider que le modèle, les mécanismes, et les protocoles sont suffisants pour prendre en charge les scénarios de conférence évolués.

Les scénarios donnent une vue générale des opérations et flux logiques généraux nécessaires. Les détails montrés dans les scénarios sont seulement à des fins d'illustration et ne reflètent pas nécessairement la structure réelle des messages de protocole de contrôle de conférence ni les données détaillées, incluant les états, qui sont définis dans des documents distincts. On devrait noter que toutes les entités impactées par la demande ne sont pas montrées dans le diagramme (par exemple, le centre) mais que l'accent est plutôt mis sur les nouvelles entités introduites par ce cadre de conférence centralisée.

### 9.1 Création de conférence

Il y a différentes façons de créer une conférence. Un participant peut créer une conférence en utilisant seulement des moyens de signalisation d'appel, comme SIP détaillé dans la [RFC4579]. Pour qu'un client de conférence ait plus de souplesse pour définir les caractéristiques et capacités d'une conférence, un client de conférence va mettre en œuvre un client de protocole de contrôle de conférence. En utilisant un protocole de contrôle de conférence, le client peut déterminer les capacités d'un système de conférence et ses diverses ressources.

La Figure 8 fournit un exemple d'un client "Alice"qui détermine les ébauches de conférence disponibles pour un système de conférence particulier et crée une conférence sur la base de l'ébauche désirée.

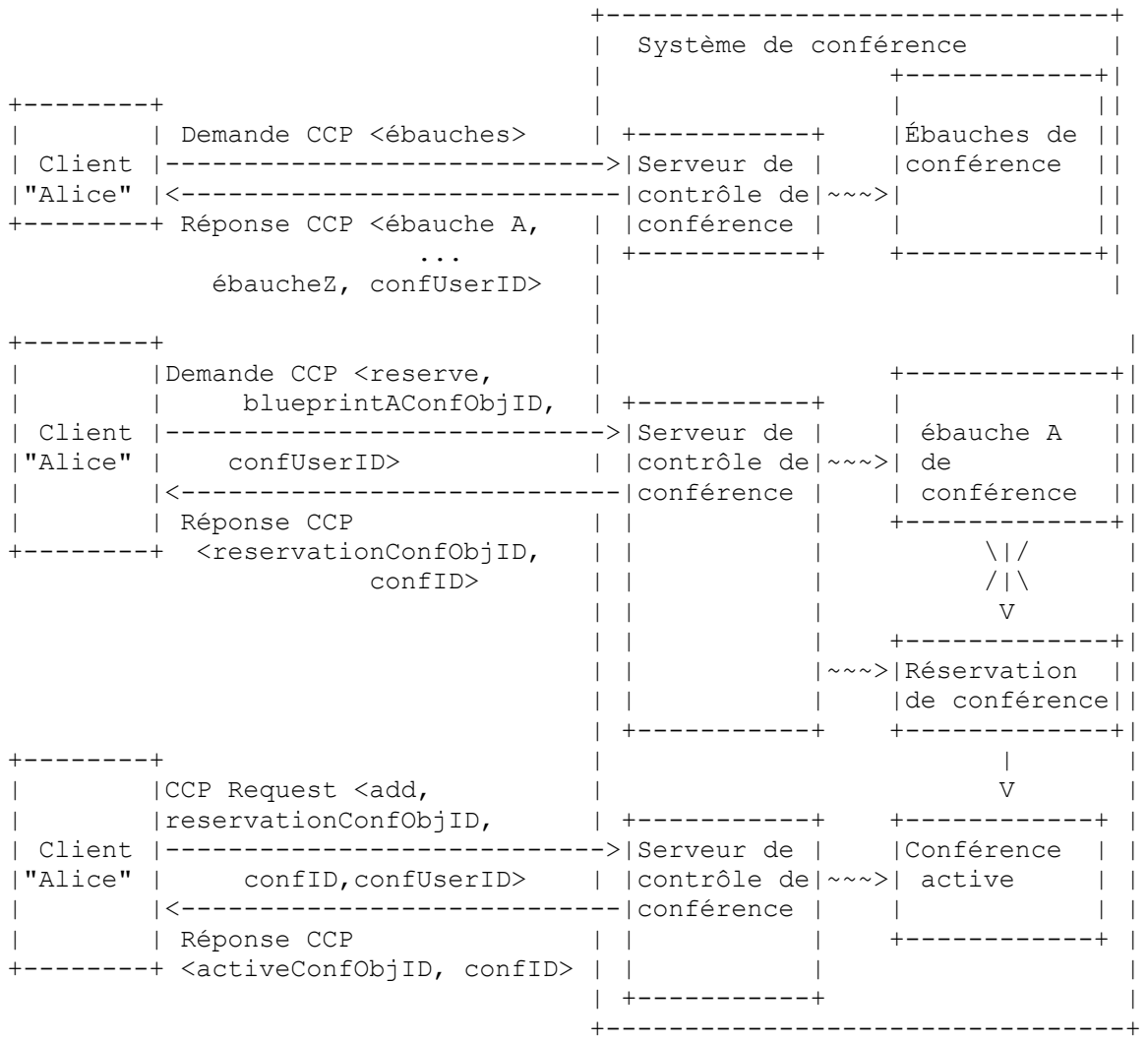



**Figure 8 : Création par le client d'une conférence avec des ébauches**

À réception de la demande du protocole de contrôle de conférence pour des ébauches, le système de conférence va d'abord authentifier "Alice" (et allouer un identifiant d'utilisateur de conférence, si nécessaire) et ensuite s'assurer que "Alice" a l'autorité appropriée selon les politiques du système pour recevoir toutes les ébauches prises en charge par ce système.

Toutes les ébauches que "Alice" est autorisée à utiliser sont retournées dans une réponse, avec l'identifiant d'utilisateur de conférence.

À réception de la réponse de protocole de contrôle de conférence contenant les ébauches, "Alice" détermine quelle ébauche utiliser pour la conférence à créer. "Alice" crée un objet conférence sur la base de l'ébauche (c'est-à-dire, la clone) et modifie les champs applicables, comme la liste des membres et l'heure de début. "Alice" envoie ensuite une demande au système de conférence pour créer une réservation de conférence sur la base de l'ébauche mise à jour.
À réception de la demande du protocole de contrôle de conférence de "réserver" une conférence fondée sur l'ébauche dans la demande, le système de conférence s'assure que l'ébauche reçue est une ébauche valide (c'est-à-dire, que les valeurs des divers champs sont dans les gammes admises). Le système de conférence détermine les droits d'accès appropriés en lecture/écriture de tous les utilisateurs à ajouter à une conférence sur la base de cette ébauche (en utilisant les membres, les rôles, etc.). Le système de conférence utilise l'ébauche reçue pour cloner une réservation de conférence. Le système de conférence réserve ou alloue aussi un identifiant de conférence à utiliser pour toutes les demandes de protocole suivantes provenant de tout membre de la conférence. Le système de conférence maintient la transposition entre cet identifiant de conférence et l'identifiant d'objet conférence associé à la réservation par l'instance de conférence.
À réception de la réponse de protocole de contrôle de conférence de réserver la conférence, "Alice" peut maintenant créer une conférence active en utilisant cette réservation ou créer des réservations supplémentaires sur la base des réservations existantes. Dans cet exemple, "Alice" a réservé un pont de conférence rendez-vous. Donc, "Alice" fournit les informations de conférence, incluant l'identifiant de conférence nécessaire, aux participants désirés. Quand le premier participant, y compris "Alice", demande à être ajouté à la conférence, une conférence active et un centre sont créés. Le centre est associé à l'identifiant de conférence reçu dans la demande. Tous les participants qui ont l'autorité pour manipuler la conférence vont recevoir l'identifiant d'objet conférence de l'objet conférence actif dans la réponse.

### 9.2 Manipulations de participant

Il y a différentes façons d'affecter l'état d'un participant dans une conférence. Un participant peut se joindre et quitter la conférence en utilisant seulement des moyens de signalisation d'appel, comme SIP. Cette sorte d'opération est appelée "signalement de première partie" et n'affecte pas l'état des autres participants à la conférence.
Des opérations limitées pour contrôler les autres participants à la conférence (ce qu'on appelle un "contrôle de tiers") à travers le centre, en utilisant seulement la signalisation d'appel, peuvent aussi être disponibles pour certains protocoles de signalisation. Par exemple, "Conférence pour agents d'utilisateur SIP" [RFC4579] montre comment SIP avec REFER peut être utilisé pour réaliser cette fonction.
Afin d'avoir un contrôle de conférence plus riche, un client d'utilisateur a besoin de mettre en œuvre un client de protocole de contrôle de conférence. En utilisant un protocole de contrôle de conférence, le client peut affecter son propre état, l'état des autres participants, et l'état des diverses ressources (comme les mixeurs de supports) qui peuvent indirectement affecter l'état de n'importe quel participant à la conférence.
La Figure 9 fournit un exemple d'un client, "Alice" qui impacte l'état d'un autre client, "Bob". Cet exemple suppose une conférence établie. Dans cet exemple, "Alice" veut ajouter "Bob" à la conférence.

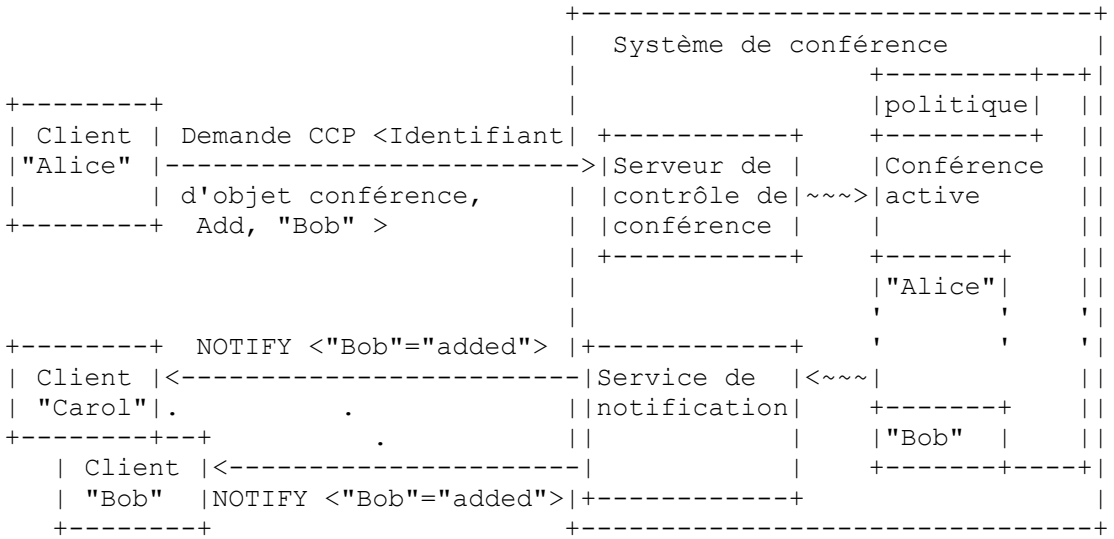



**Figure 9 : Manipulation de la conférence par le client – ajout d'une partie**

À réception de la demande du protocole de contrôle de conférence "d'ajouter" une partie ("Bob") dans la conférence spécifique identifiée par l'identifiant d'objet conférence, le système de conférence s'assure que "Alice" a l'autorité appropriée sur la base de la politique associée à cet objet conférence spécifique pour effectuer l'opération. Le système de conférence doit aussi déterminer si "Bob" est déjà un utilisateur de ce système de conférence ou si il est un nouvel utilisateur.

Si "Bob" est un nouvel utilisateur pour ce système de conférence, un identifiant d'utilisateur de conférence est créé pour Bob. Sur la base des informations d'adressage fournies pour "Bob" par "Alice", la signalisation d'appel pour ajouter "Bob" à la conférence est à l'instigation du centre.

Une fois que la signalisation d'appel indique que "Bob" a bien été ajouté à la conférence spécifiée, conformément aux mises à jour de l'état, et selon la politique, les autres participants (y compris "Bob") peuvent avoir notification de l'ajout de "Bob" à la conférence via le service de notifications de conférence.

### 9.3 Manipulations de supports

Il y a différentes façons de manipuler les supports dans une conférence. Un participant peut changer ses propres flux de supports en envoyant, par exemple, un re-INVITE avec un nouveau contenu SDP en utilisant seulement SIP. Cette sorte d'opération est appelée "signalement de première partie" et n'affecte pas l'état des autres participants à la conférence.

Afin d'effectuer un plus riche contrôle de conférence, un client d'utilisateur a besoin de mettre en œuvre un client de protocole de contrôle de conférence. En utilisant un protocole de contrôle de conférence, le client peut manipuler l'état des diverses ressources, comme les mixeurs de supports, ce qui peut indirectement affecter l'état de tout participant à la conférence.

La Figure 10 fournit l'exemple d'un client, "Alice", qui impacte l'état des supports d'un autre client, "Bob". Cet exemple suppose une conférence établie. Dans cet exemple, le client "Alice" dont le rôle est "modérateur" de la conférence, veut assourdir "Bob" sur une conférence multi parties de taille moyenne, car son appareil n'est pas muni d'un assourdisseur (et que manifestement il n'écoute pas l'appel) et que le bruit de fond dans son environnement de bureau perturbe la conférence.

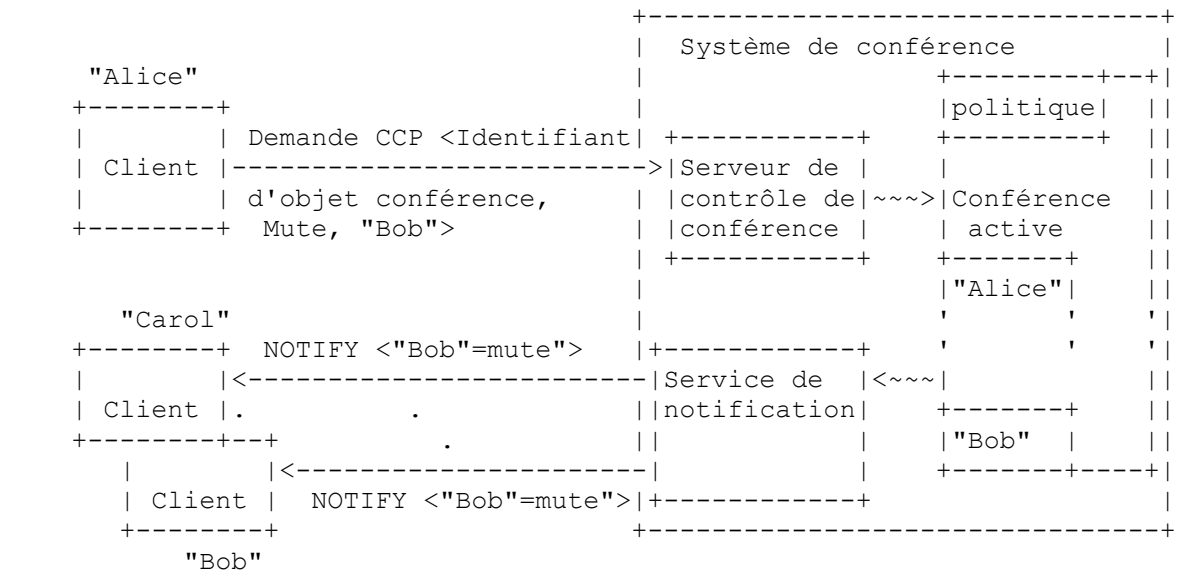



**Figure 10 : Manipulation de conférence par le client – changement à une partie**

À réception de la demande du protocole de contrôle de conférence "d'assourdir" une partie ("Bob") dans la conférence spécifique identifiée par l'identifiant d'objet conférence, le serveur de conférence s'assure que "Alice" a l'autorité appropriée sur la base de la politique associée à cet objet conférence spécifique pour effectuer l'opération. L'état de "Bob" est marqué comme "recvonly" *(réception seule)* et l'objet conférence est mis à jour pour refléter que le support de "Bob" n'est pas à "mixer" avec le support de conférence.

Selon la politique, d'autres participants (y compris "Bob") peuvent avoir notification de ce changement via le service de notifications de la conférence.

### 9.4 Manipulations de session annexe

Une session annexe peut être vue comme une instance de conférence séparée qui n'existe que dans le contexte d'une instance de conférence parente. Bien que vue comme une instance de conférence indépendante, elle ne peut pas exister sans une parente. Une session annexe est créée en utilisant les mêmes mécanismes qu'employés pour une conférence standard, comme décrit au paragraphe 7.1.

Un objet conférence qui représente une session annexe est créé en clonant le parent associé à la conférence existante et en mettant à jour toutes les informations spécifiques de la session annexe. Un objet conférence de session annexe est implicitement lié à l'objet conférence parent (c'est-à-dire, il n'est pas un objet indépendant) et est associé à l'identifiant d'objet conférence parent, comme le montre la Figure 11. Un système de conférence gère et applique les restrictions du parent et les restrictions localisées appropriées à l'objet conférence de session annexe (par exemple, aucun membre de l'extérieur de l'instance de conférence parente ne peut se joindre, la conférence de session annexe ne peut pas exister si la conférence parente est terminée, etc.).

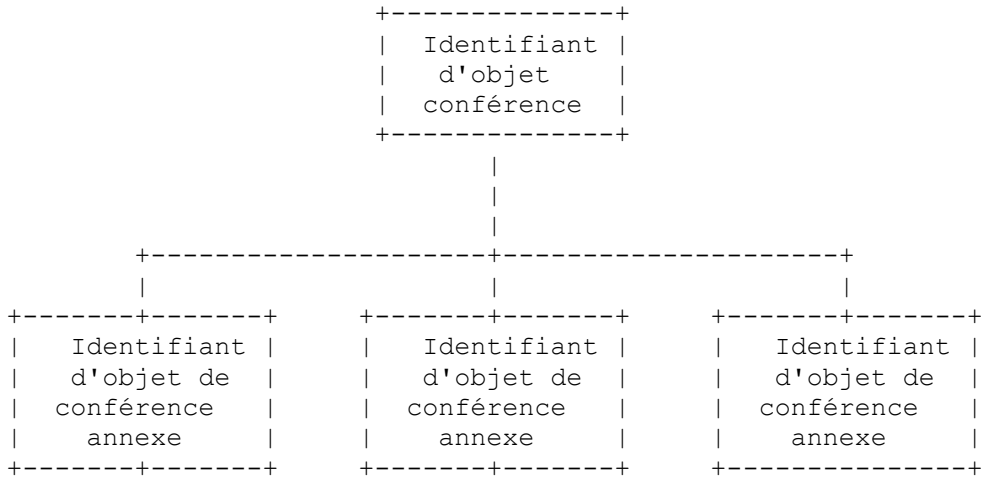



**Figure 11 : Transposition d'objet Conférence**

La Figure 11 illustre les relations entre un objet conférence et des objets de conférence annexes associés au sein d'un système de conférence. Chaque objet conférence annexe a un unique identifiant d'objet conférence, comme décrit au paragraphe 6.2.1. Le principal identifiant d'objet conférence agit comme identifiant de niveau supérieur pour les sessions annexes associées.

Un identifiant d'objet conférence annexe suit beaucoup des concepts mentionnés dans le modèle d'arborescence de clonage décrit au paragraphe 7.1. Un objet conférence annexe contient un sous ensemble des membres de l'objet conférence original. Les propriétés de l'objet conférence annexe peuvent être manipulées par un protocole de contrôle de conférence en utilisant l'identifiant d'objet conférence unique pour la session annexe. Il est aussi possible à l'objet conférence de niveau supérieur d'appliquer la politique sur l'objet conférence annexe (similaire à "applicable par le parent", comme discuté au paragraphe 7.1).

#### 9.4.1 Session annexe interne

La Figure 12 fournit un exemple d'un client, "Alice", impliqué dans une conférence active avec "Bob" et "Carol". "Alice" veut créer une session annexe pour avoir une discussion en aparté avec "Bob" tout en continuant de voir la vidéo associée à la conférence principale. Autrement, l'audio provenant de la conférence principale pourrait être maintenu à un volume réduit. "Alice" initie la session annexe en envoyant une demande au système de conférence pour créer une réservation de conférence fondée sur l'objet conférence actif. "Alice" et "Bob" vont rester sur la liste des participants à la conférence principale, de façon à ce que les autres participants pourraient être conscients de leur participation à la conférence principale, pendant qu'une conférence annexe interne se produit.

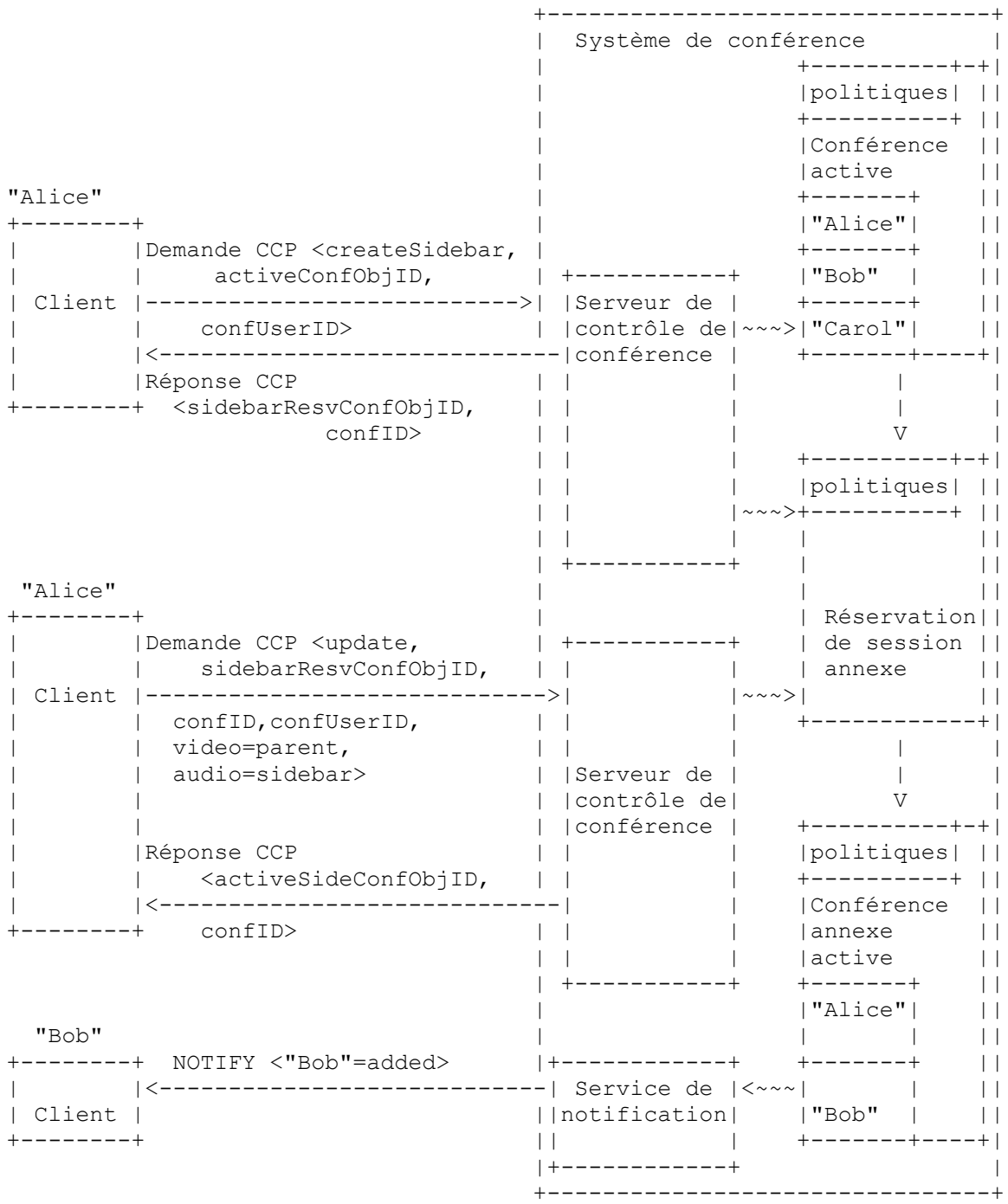



**Figure 12 : Création par le client d'une conférence annexe**

À réception de la demande du protocole de contrôle de conférence de "réserver" une nouvelle conférence annexe, fondée sur la conférence active reçue dans la demande, le système de conférence utilise la conférence active reçue pour cloner une réservation de conférence pour la session annexe. Comme mentionnée précédemment, la réservation de session annexe n'est PAS indépendante de la conférence active (c'est-à-dire, parente). Le système de conférence réserve aussi ou alloue un identifiant de conférence à utiliser pour toutes les demandes de protocole suivantes provenant de tout membre de la conférence. Le système de conférence maintient la transposition entre cet identifiant de conférence et l'identifiant d'objet conférence associé à la réservation de session annexe à travers l'instance de conférence.

À réception de la réponse de protocole de contrôle de conférence de réserver la conférence, "Alice" peut maintenant créer une conférence active utilisant cette réservation ou créer des réservations supplémentaires fondées sur les réservations existantes. Dans cet exemple, "Alice" veut seulement que "Bob" soit impliqué dans la session annexe, donc elle manipule les membres. "Alice" veut aussi seulement la vidéo provenant de la conférence originale et veut que l'audio soit restreint

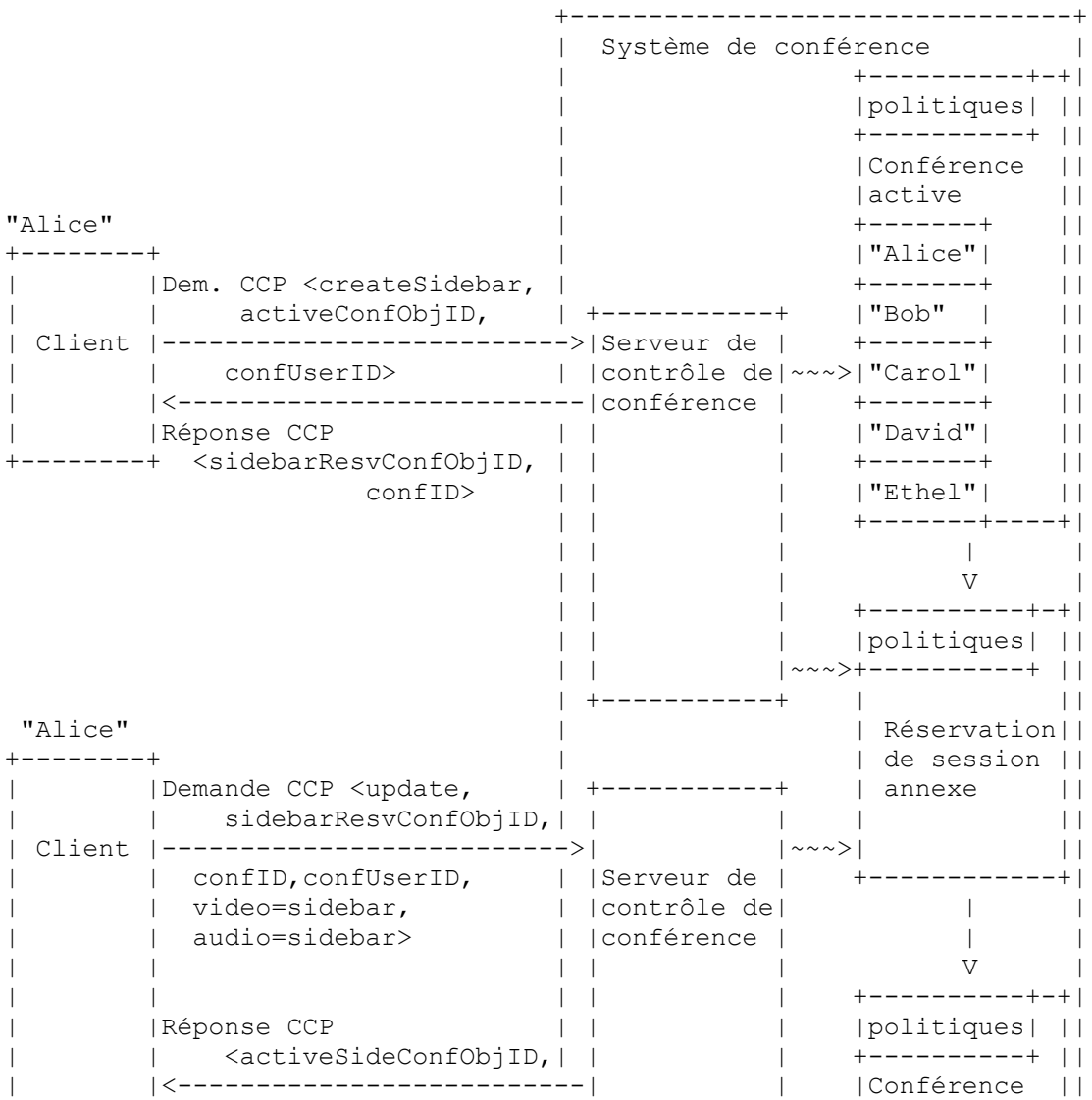
aux participants à la session annexe. Autrement, "Alice" pourrait manipuler les valeurs de supports pour recevoir l'audio de la conférence principale à un volume réduit. "Alice" envoie au protocole de contrôle de conférence une demande de mise à jour des informations dans la réservation et de création d'une conférence active.

À réception de la demande du protocole de contrôle de conférence de mettre à jour la réservation et de créer une conférence active pour la session annexe, comme identifié par l'identifiant d'objet conférence, le système de conférence s'assure que "Alice" a l'autorité appropriée sur la base des politiques associées à cet objet conférence spécifique pour effectuer l'opération. Le système de conférence doit aussi valider la mise à jour des informations dans la réservation, s'assurant qu'un membre comme "Bob" est déjà un utilisateur de ce système de conférence.

Selon les politiques, l'initiateur de la demande (c'est-à-dire, "Alice") et les participants à la session annexe (c'est-à-dire, "Bob") peuvent voir la notification de l'ajout à la session annexe via le service de notifications de conférence.

### 9.4.2 Session annexe externe

La Figure 13 fournit l'exemple d'un client, "Alice", impliqué dans une conférence active avec "Bob", "Carol", "David", et "Ethel". "Alice" reçoit un important message de texte via un chuchotement de "Bob" disant qu'un consommateur critique a besoin de parler à "Alice", "Bob", et "Ethel". "Alice" crée une session annexe pour avoir une discussion en aparté avec le consommateur "Fred" incluant les participants à la conférence actuelle à l'exception de "Carol" et "David", qui restent dans la conférence active. "Alice" initie la session annexe en envoyant au système de conférence une demande de création de réservation de conférence sur la base de l'objet conférence actif. "Alice", "Bob", et "Ethel" vont rester sur la liste des participants à la conférence principale en état de garde. Que l'état de garde de ces participants soit ou non visible aux autres participants dépend de la politique individuelle et locale.



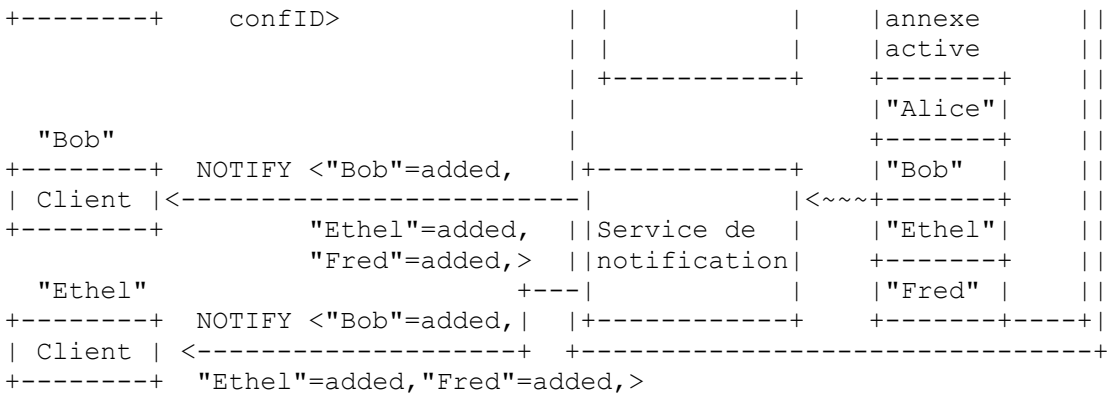



**Figure 13 : Création par le client d'une session annexe externe**

À réception de la demande du protocole de contrôle de conférence de "réserver" une nouvelle conférence annexe, sur la base de la conférence active reçue dans la demande, le système de conférence utilise la conférence active reçue pour cloner une réservation de conférence pour la session annexe. Comme exposé précédemment, la réservation de la session annexe n'est PAS indépendante de la conférence active (c'est-à-dire, parente). Le système de conférence réserve aussi ou alloue un identifiant de conférence à utiliser pour toutes les demandes de protocole suivantes provenant de tout membre de la conférence. Le système de conférence maintient la transposition entre cet identifiant de conférence et l'identifiant d'objet conférence associé à la réservation de session annexe par l'instance de conférence.

À réception de la réponse de protocole de contrôle de conférence de réserver la conférence, "Alice" peut maintenant créer une conférence active en utilisant cette réservation ou créer des réservations supplémentaires sur la base des réservations existantes. Dans cet exemple, "Alice" veut seulement que "Bob" et "Ethel", avec le nouveau participant "Fred" soient impliqués dans la session annexe ; donc, elle manipule les membres. "Alice" règle les supports de telle façon que les participants à la session annexe ne reçoivent aucun support provenant de la conférence principale. "Alice" envoie une demande du protocole de contrôle de conférence pour mettre à jour les informations dans la réservation et pour créer une conférence active.

À réception de la demande du protocole de contrôle de conférence de mettre à jour la réservation et de créer une conférence active pour la session annexe, comme identifié par l'identifiant d'objet conférence, le système de conférence s'assure que "Alice" a l'autorité appropriée sur la base des politiques associées à cet objet conférence spécifique pour effectuer l'opération. Le système de conférence doit aussi valider les informations mises à jour dans la réservation, en s'assurant que des membres comme "Fred" sont déjà utilisateurs de ce système de conférence ou si il sont de nouveaux utilisateurs. Comme "Fred" est un nouvel utilisateur de ce système de conférence, un identifiant d'utilisateur de conférence est créé pour "Fred". Sur la base des informations d'adressage fournies pour "Fred" par "Alice", la signalisation d'appel pour ajouter "Fred" à la conférence est à l'instigation du centre.

Selon les politiques, l'initiateur de la demande (c'est-à-dire, "Alice") et les participants à la session annexe (c'est-à-dire, "Bob" et "Ethel") peuvent avoir notification de son ajout à la session annexe via le service de notifications de conférence.

### 9.5 Contrôle de la prise de parole en utilisant des sessions annexes

Le contrôle de la prise de parole avec des sessions annexes peut être utilisé pour réaliser des scénarios de conférence comme des discussions d'analystes. Dans ce scénario, l'appel de conférence a un éventail d'orateurs à qui il est permis de parler dans la conférence principale. Les autres participants sont les analystes, à qui il n'est pas permis de parler tant que la parole ne leur est pas donnée. Pour demander l'accès à la parole, il doivent se joindre à une nouvelle session annexe avec le modérateur et poser leur question. Le modérateur peut aussi chuchoter avec chaque analyste quelle que soit leur statut/position dans la file d'attente de contrôle de la prise de parole, comme dans l'exemple de la Figure 15.

La Figure 14 fournit un exemple de la configuration impliquée par ce type de conférence. Comme dans les précédents exemples de session annexe, il y a la conférence principale avec une session annexe. "Alice" et "Bob" sont les principaux participants à la conférence, avec "A1", "A2", et "A3" représentant les analystes. La session annexe reste active pendant toute la conférence, avec le modérateur, "Carol", qui sert de présidente. Comme indiqué précédemment, la conférence annexe n'est PAS indépendante de la conférence active (c'est-à-dire, parente). Les analystes reçoivent l'identifiant d'objet conférence associé à la session annexe active quand ils se joignent à la conférence principale. Le système de conférence alloue aussi un identifiant de conférence à utiliser pour toutes les manipulations suivantes de la conférence annexe. Le

système de conférence maintient la transposition entre cet identifiant de conférence et l'identifiant d'objet conférence associé à la conférence annexe active par l'instance de conférence. Les analystes sont assourdis en permanence pendant la conférence principale. Les analystes sont passés dans la session annexe quand ils souhaitent parler. Un seul analyste a la parole à la fois. Tous les participants à la conférence principale reçoivent l'audio de la conférence annexe, ainsi que l'audio fourni par les orateurs de la conférence principale.

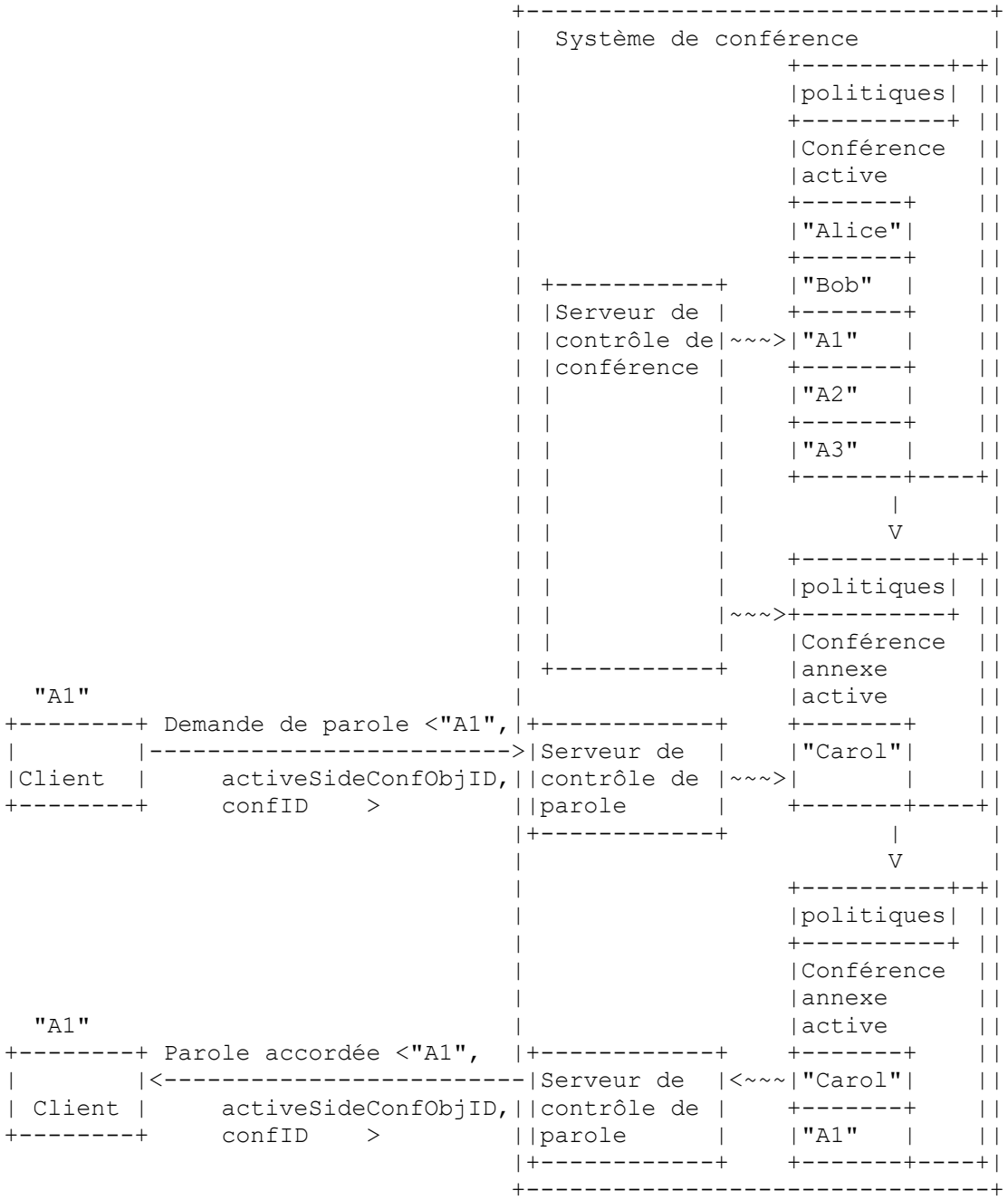



**Figure 14 : Contrôle de la prise de parole avec des sessions annexes**

Quand "A1" souhaite poser une question, il envoie un message Demande de parole au serveur de contrôle de la prise de parole. À réception de la demande, le serveur de contrôle de la prise de parole le notifie au modérateur, "Carol" de la conférence annexe active, qui sert de présidente. Noter que ce flux de signalisation n'est pas montré dans le diagramme. Comme aucun autre analyste n'a encore demandé la parole, "Carol" indique au serveur de contrôle de la prise de parole que la parole peut être accordée à "A1".

### 9.6 Chuchotement ou messages privés

Le cas des messages privés peut être traité comme une session annexe avec juste deux participants, similaire à l'exemple du paragraphe 9.4.1, mais plutôt que d'utiliser l'audio dans la session annexe, "Alice" pourrait ajouter un flux de supports fondé sur le texte à la session annexe. L'autre contexte, appelé chuchotement dans ce document se réfère à des situations impliquant un support à usage unique ciblé sur un ou des utilisateurs spécifiques. Un exemple de chuchotement serait une annonce injectée seulement au président de la conférence ou à un nouveau participant qui se joint à une conférence.

La Figure 15 fournit un exemple d'un utilisateur "Alice" qui préside une conférence de durée fixée avec "Bob" et "Carol". La configuration est telle que seule la présidence fournit un avertissement quand il reste seulement 10 minutes à la conférence. À ce moment, "Alice" est placée dans une session annexe créée par le système de conférence et seule "Alice" reçoit l'annonce.

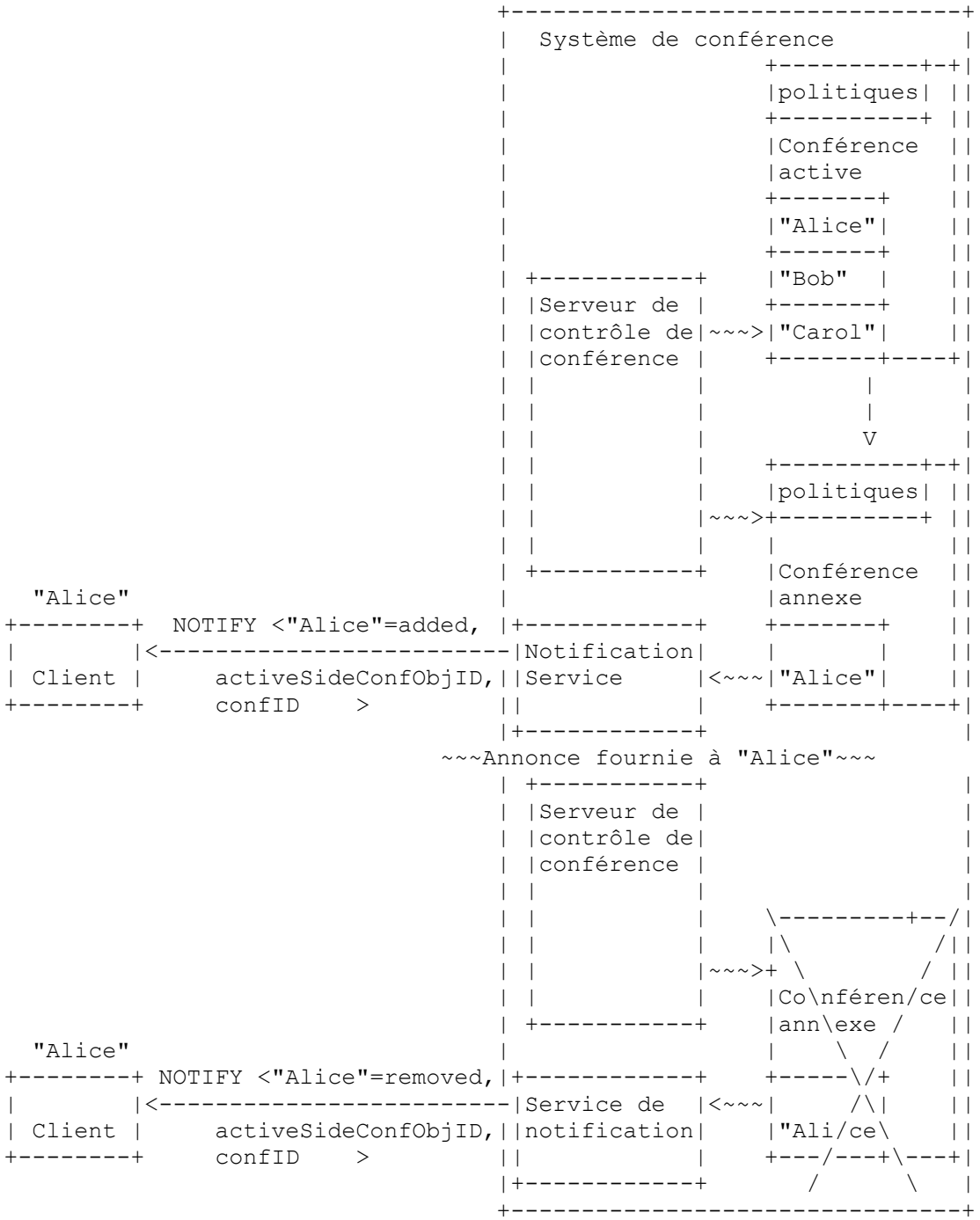



**Figure 15 : Chuchotement**

Quand le système de conférence détermine qu'il reste seulement 10 minutes dans la conférence que préside "Alice", plutôt que de créer une réservation comme on a fait pour la session annexe au paragraphe 9.4.1, le système de conférence crée directement une conférence annexe active, sur la base de la conférence active associée à "Alice". Comme exposé précédemment, la conférence annexe n'est PAS indépendante de la conférence active (c'est-à-dire, parente). Le système de conférence alloue aussi un identifiant de conférence à utiliser pour toutes les manipulations suivantes de la conférence annexe. Le système de conférence maintient la transposition entre cet identifiant de conférence et l'identifiant d'objet conférence associé à la conférence annexe active au moyen de l'instance de conférence.

Immédiatement après la création de la conférence annexe active, le support d'annonce est fourni à "Alice". Selon les politiques, "Alice" peut avoir la notification de son ajout à la session annexe via le service de notifications de la conférence. "Alice" continue de recevoir les supports provenant de la conférence principale.

L'annonce achevée, "Alice" est retirée de la session annexe, et la conférence annexe est supprimée. Selon les politiques, "Alice" peut avoir notification de sa suppression de la session annexe via le service de notifications de la conférence.

### 9.7 Annonces et enregistrements de conférences

Chaque participant peut exiger un différent type d'annonce et/ou de service d'enregistrement de la part du système. Par exemple, "Alice", la présidente de la conférence, pourrait faire l'appel pendant que "Bob" pourrait utiliser une interface d'utilisateur téléphonique pour créer une session annexe. Certaines annonces vont s'appliquer à tous les participants comme "Cette conférence va se terminer dans 10 minutes". L'enregistrement est souvent nécessaire pour prendre les noms des participants lorsque ils se joignent à une conférence, normalement après que le participant ait entré un code d'accès, comme exposé au paragraphe 9.8. Ces noms enregistrés sont alors annoncés à tous les participants lorsque le nouveau participant est ajouté à la conférence active.

Un exemple d'enregistrement et annonce de conférence, avec collecte de bi-tonalités multi fréquences (DTMF, *dual tone multi-frequency*) dans le contexte de ce cadre, est montré à la Figure 16.

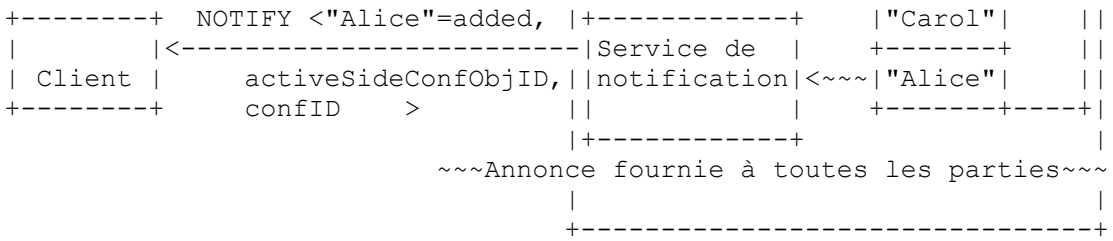



**Figure 16 : Enregistrement et annonces**

À réception de la demande du protocole de contrôle de conférence de "Alice" de joindre "Bob" à la conférence, le système de conférence transpose l'identifiant reçu dans la demande en l'objet conférence représentant la conférence active de "Bob". Le système de conférence détermine qu'un mot de passe est exigé pour cette conférence spécifique ; donc, une annonce demandant à "Alice" d'entrer le mot de passe est fournie à "Alice". Une fois que "Alice" a entré le mot de passe, il est validé à l'égard des politiques associées à la conférence active de "Bob". Le système de conférence se connecte alors à un serveur qui appelle et enregistre le nom de "Alice". Le système de conférence doit aussi déterminer si "Alice" est déjà un utilisateur de ce système de conférence ou si elle est un nouvel utilisateur.

Si "Alice" est un nouvel utilisateur de ce système de conférence, un identifiant d'utilisateur de conférence est créé pour "Alice". Sur la base des informations d'adressage fournies par "Alice", la signalisation d'appel pour ajouter "Alice" à la conférence est à l'instigation du centre.

Une fois que la signalisation d'appel indique que "Alice" a bien été ajoutée à la conférence spécifiée, selon les mises à jour de l'état, et selon les politiques, les autres participants (par exemple, "Bob") ont la notification de l'ajout de "Alice" à la conférence via le service de notifications de conférence, et une annonce est fournie à tous les participants indiquant que "Alice" s'est jointe à la conférence.

### 9.8 Surveillance de DTMF

Le système de conférence a aussi besoin de la capacité de surveiller les DTMF provenant de chaque participant individuel. Cela va normalement être utilisé pour entrer l'identifiant et/ou code d'accès pour se joindre à une conférence spécifique.

Un exemple de surveillance des DTMF, dans le contexte des éléments du cadre, est montré à la Figure 16.

### 9.9 Observation et guidage

La capacité d'observer une conférence permet à un participant avec l'autorité appropriée d'écouter la conférence, normalement sans être un participant actif et souvent comme un participant caché. Quand une telle capacité est disponible sur un système de conférence, il y a souvent une annonce fournie à chaque participant lorsque il se joint à la conférence indiquant que l'appel peut être surveillé. Cette capacité est utile dans le contexte de conférences qui pourraient rencontrer des difficultés techniques, permettant donc à un technicien d'écouter pour évaluer le type de problème.

Cette capacité pourrait aussi s'appliquer à des applications de centre d'appel car elle fournit un mécanisme pour qu'un superviseur observe comment l'agent traite un appel particulier avec un consommateur. Ce scénario peut être traité par un superviseur qui s'ajoute à la conférence active existante, avec un chemin de support audio en écoute seule. Si l'agent est informé de quand le superviseur se joint à l'appel devrait être configurable.

En poussant plus loin la capacité de superviseur, on introduit un scénario par lequel l'agent peut écouter le superviseur, ainsi que le consommateur. Le consommateur peut seulement écouter l'agent. Ce scénario impliquerait la création d'une session annexe avec l'agent et le superviseur. L'agent et le superviseur reçoivent tous deux l'audio provenant de la conférence principale. Quand l'agent parle, il est entendu par le consommateur dans la conférence principale. Quand le superviseur parle, il est entendu seulement par l'agent dans la conférence annexe.

Un exemple d'observation et de guidage est montré à la Figure 17. Dans cet exemple, l'agent de centre d'appel "Bob" est impliqué dans une conférence avec le consommateur "Carol". Comme "Bob" est un nouvel agent et que "Alice" voit qu'il a été sur l'appel avec "Carol" pendant plus longtemps que la durée normale, elle décide d'observer l'appel et de donner à "Bob" les directives nécessaires.

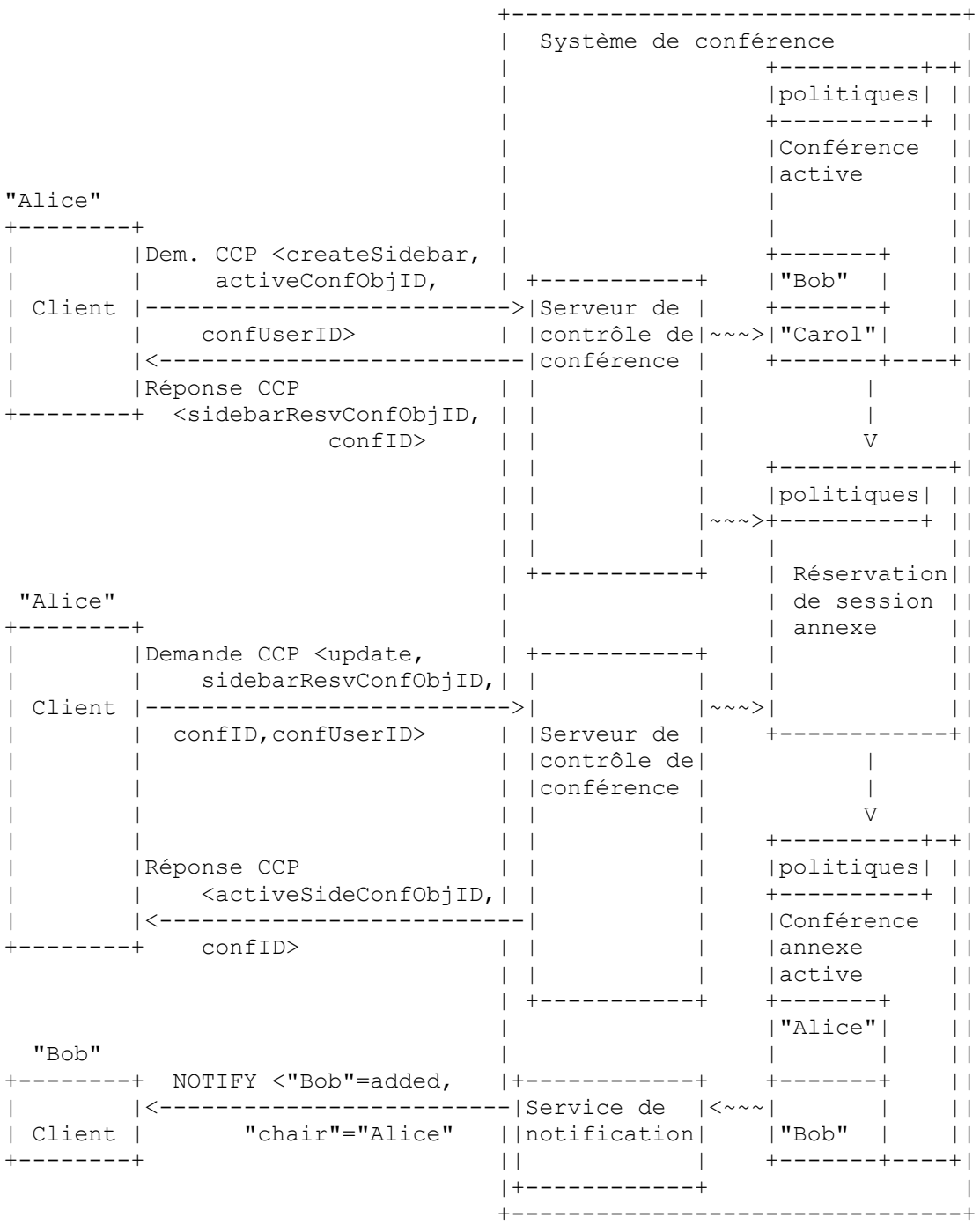



**Figure 17 : Superviseur créant une session annexe pour l'observation/guidage**

À réception de la demande du protocole de contrôle de conférence provenant de "Alice" de "réserver" une nouvelle conférence annexe, sur la base de la conférence active reçue dans la demande, le système de conférence utilise la conférence active reçue pour cloner une réservation de conférence pour la session annexe. Le système de conférence réserve aussi ou alloue un identifiant de conférence à utiliser pour toute demande de protocole suivante provenant de tout membre de la conférence. Le système de conférence maintient la transposition entre cet identifiant de conférence et l'identifiant d'objet conférence associé à la réservation de session annexe à travers l'instance de conférence.

À réception de la réponse de protocole de contrôle de conférence de réserver la conférence, "Alice" peut maintenant créer une conférence active en utilisant cette réservation ou créer des réservations supplémentaires sur la seule base des réservations existantes. Dans cet exemple, "Alice" veut seulement que "Bob" soit impliqué dans la session annexe ; donc, elle manipule les membres. "Alice" veut aussi que l'audio soit reçu par elle et "Bob" depuis la conférence originale, mais que tout l'audio sortant d'elle soit restreint aux participants à la session annexe, tandis que l'audio sortant de "Bob" devrait

aller à la conférence principale, de sorte que "Alice" et le consommateur "Carol" entendent tous deux le même audio provenant de "Bob". "Alice" envoie une demande du protocole de contrôle de conférence pour mettre à jour les informations dans la réservation et pour créer une conférence active.

À réception de la demande du protocole de contrôle de conférence de mettre à jour la réservation et de créer une conférence active pour la session annexe, comme identifiée par l'identifiant d'objet conférence, le système de conférence s'assure que "Alice" a l'autorité appropriée sur la base des politiques associées à cet objet conférence spécifique pour effectuer l'opération. Sur la base des informations d'adressage fournies pour "Bob" par "Alice", la signalisation d'appel pour ajouter "Bob" à la session annexe avec les caractéristiques de supports appropriées est à l'instigation du centre.

"Bob" a la notification de son ajout à la session annexe via le service de notifications de conférence ; donc, il sait que "Alice", le superviseur, est disponible pour le guider à travers cet appel.

## 10. Relations entre SIP et les cadres de conférence centralisées

Le cadre de conférence SIP [RFC4353] fournit une vue générale d'une large gamme de solutions de conférence centralisée connues aujourd'hui dans l'industrie de la conférence. Le document introduit une terminologie et des entités logiques afin de systématiser la vue d'ensemble et montrer le cœur commun de beaucoup de ces systèmes. Les entités logiques et les scénarios qui figurent dans le cadre de conférence SIP sont utilisés pour illustrer comment SIP [RFC3261] peut être utilisé comme moyen de signalisation dans ces systèmes de conférence. Le cadre de conférence SIP ne définit pas de nouveaux protocoles de contrôle de conférence à utiliser par le système général de conférence. Il utilise seulement le SIP de base [RFC3261], la conférence SIP pour agents d'utilisateur [RFC4579], et le paquetage de conférence SIP [RFC4575] pour les réalisations de conférence SIP.

Ce document de cadre de conférence centralisée définit un système particulier de conférence centralisée et les entités logiques qui le mettent en œuvre. Il définit aussi un modèle de données particulier et se réfère à l'ensemble de protocoles (au delà des moyens de signalisation d'appel) à utiliser parmi les entités logiques pour mettre en œuvre des caractéristiques de conférence évoluées. L'objet du groupe de travail XCON et de ce cadre est de réaliser l'interopérabilité entre les entités logiques provenant de différents fabricants pour le contrôle des différents aspects des applications de conférence évoluées.

Les entités logiques définies dans les deux cadres ne sont pas destinées à être transposées une à une. Les deux cadres diffèrent dans l'interprétation de la décomposition interne du système de conférence et des opérations correspondantes. Néanmoins, le SIP de base [RFC3261], la conférence SIP pour les agents d'utilisateur [RFC4579], et le paquetage de conférence SIP [RFC4575] sont pleinement compatibles avec les deux documents cadres. La base pour la compatibilité est fournie en incluant les éléments de données de base définis dans la [RFC4575] dans le modèle de données d'informations de conférence pour les conférences centralisées (XCON) [RFC6501]. Les agents d'utilisateur qui prennent seulement en charge la [RFC4579] et ne prennent pas en charge le protocole de contrôle de conférence fournissent quand même la conférence SIP de base, mais ne peuvent pas tirer parti des caractéristiques évoluées.

## 11. Considérations pour la sécurité

Il y a un grand nombre d'attaques potentielles relatives aux conférences, du fait de l'implication naturelle de nombreux points d'extrémité et des nombreuses capacités, souvent invoquées par l'utilisateur, fournies par le système de conférence. Des exemples d'attaques incluent un point d'extrémité qui tente d'écouter des conférences auxquelles il n'est pas autorisé à participer, un point d'extrémité qui tente de déconnecter ou assourdir d'autres utilisateurs, et le vol de service par un point d'extrémité qui tente de créer des conférences qu'il n'est pas autorisé à créer.

Plusieurs problèmes entourent la sécurité de ce cadre de conférence. Un ensemble de problèmes impliquent la sécurisation des protocoles actuels et les mécanismes d'autorisation associés. Ce premier ensemble de problèmes devrait être traité dans les spécifications des protocoles décrits à la Section 8 et de contrôle de politique. Les protocoles utilisés pour la manipulation et la restitution d'informations confidentielles doivent prendre en charge les mécanismes de confidentialité et d'intégrité. Des exigences similaires s'appliquent pour les protocoles de contrôle de la prise de parole. Le paragraphe 11.3 discute d'une approche de l'authentification de client d'un serveur de contrôle de la prise de parole. Il est RECOMMANDÉ que tous les protocoles qui s'interfacent avec le système de conférence mettent en œuvre la sécurité de la couche transport (TLS, *Transport Layer Security*).

Il y a aussi des problèmes de sécurité associés à l'autorisation d'effectuer des actions sur le système de conférence pour invoquer des capacités spécifiques. Le paragraphe 5.2 discute des politiques associées à l'objet conférence pour assurer que seules les entités autorisées sont capables de manipuler les données pour accéder aux capacités. Un autre ensemble de problèmes implique la confidentialité et la sécurité de l'identité d'un utilisateur dans la conférence, qui est discutée au paragraphe 11.2.

Un dernier problème se rapporte aux attaques de déni de service (DoS) sur le système de conférence lui-même. Afin de minimiser les potentielles attaques de DoS, il est recommandé que les systèmes de conférence exigent l'authentification de l'utilisateur et l'autorisation de tout client participant à une conférence. Il est recommandé que la signalisation et les protocoles de supports spécifiques incluent des mécanismes pour minimiser le potentiel de DoS.

### 11.1 Authentification et autorisation de l'utilisateur

De nombreuses décisions d'autorisation de politique se fondent sur l'identité de l'utilisateur ou sur le rôle que peut avoir un utilisateur. Les systèmes de conférence exigent normalement l'authentification des utilisateurs pour valider leur identité. Il y a plusieurs moyens pour qu'un utilisateur puisse authentifier son identité auprès du système. Pour les utilisateurs qui se joignent à une conférence en utilisant un des protocoles de signalisation d'appel, les mécanismes d'authentification d"utilisateur pour le protocole spécifique suffisent souvent. Pour le cas d'utilisateurs qui se joignent à la conférence via la signalisation SIP ou en utilisant le protocole de contrôle de conférence, TLS est RECOMMANDÉ.

Le système de conférence peut aussi connaître (par exemple, par des mécanismes hors bande) des utilisateurs spécifiques et allouer des mots de passe pour permettre que ces utilisateurs soient autorisés. Dans certains cas (par exemple, les utilisateurs du réseau téléphonique public commuté (RTPC)) des autorisation supplémentaires peuvent être exigées pour permettre à l'utilisateur de participer à la conférence. Cela peut être sous la forme d'un système de réponse vocale interactive (IVR, *Interactive Voice Response*) ou d'autres moyens. Les utilisateurs peuvent aussi être autorisés par la connaissance d'un identifiant de conférence particulier et d'un identifiant personnel (PIN, *Personal Identification*) pour lui. Parfois, un PIN n'est pas exigé et l'identifiant de conférence est utilisé comme un secret partagé.

Dans les cas où un utilisateur est autorisé via plusieurs mécanismes, il appartient au système de conférence de corréler (si il le désire) l'autorisation de l'interface de signalisation d'appel avec d'autres mécanismes d'autorisation. Un système de conférence peut éviter le problème des mécanismes multiples en restreignant les méthodes par lesquelles on peut se joindre à une conférence. Par exemple, de nombreux systèmes de conférence qui fournissent une interface à la Toile pour les conférences se corrèlent à la signalisation d'appel du RTPC en forçant un mode de numérotation pour se joindre à la conférence. Donc, il y a seulement besoin d'un seul PIN ou mot de passe pour se joindre à la conférence.

Quand un système de conférence présente l'identité des utilisateurs autorisés, il peut choisir de fournir les informations sur la façon dont l'identité a été prouvée ou vérifiée par le système. Un utilisateur peut aussi venir comme un utilisateur complètement non authentifié dans le système -- ce fait doit aussi être communiqué aux parties intéressées.

Quand des utilisateurs invités interagissent avec le système, c'est souvent dans le contexte d'une conférence particulière. Dans ce cas, l'utilisateur peut fournir un PIN ou mot de passe spécifique des conférences et qui autorise l'utilisateur à prendre un certain rôle dans cette conférence. L'utilisateur invité peut alors effectuer des actions qui sont permises à tout utilisateur tenant ce rôle.

Le terme "mot de passe" se réfère au secret partagé usuel, de taille raisonnable et difficilement prévisible. Aujourd'hui, les utilisateurs ont souvent des mots de passe contenant jusqu'à 30 bits (8 à 16 caractères) d'entropie. Un PIN est un cas particulier de mot de passe -- un secret partagé qui est seulement numérique et contient souvent un très petit nombre de bits (souvent pas plus de 10 bits ou 3 chiffres). Quand des systèmes de conférence sont utilisés pour de l'audio sur le RTPC, il est souvent besoin de s'authentifier en utilisant un PIN. Normalement, si l'utilisateur manque à produire le PIN correct plusieurs fois à la suite, l'appel du RTPC est déconnecté. Le taux de passages des appels et d'arriver au point d'entrer un PIN rend très difficile de faire une recherche exhaustive dans l'espace de PIN même pour des PIN de quatre chiffres. Quand on utilise une interface à haut débit pour se connecter à un système de conférence, il est souvent possible de faire des milliers de tentatives par seconde et l'espace de PIN pourrait faire l'objet d'une recherche rapide. À cause de cela, il n'est pas approprié d'utiliser des PIN pour l'autorisation d'interfaces qui permettent des interrogations rapides ou simultanées.

Une fois qu'un utilisateur est authentifié et autorisé à travers les divers mécanismes disponibles sur le système de conférence, un identifiant d'utilisateur de conférence est associé à tous les identifiants de signalisation spécifiques de l'utilisateur qui peuvent avoir été utilisés pour l'authentification et l'autorisation. Cet identifiant d'utilisateur de conférence peut être fourni à un utilisateur spécifique à travers l'interface de notification de conférence et va être fourni aux utilisateurs

qui interagissent avec le système de conférence en utilisant le protocole de contrôle de conférence. Cet identifiant d'utilisateur de conférence est exigé pour toutes les opérations suivantes sur l'objet conférence.

### 11.2 Sécurité et confidentialité de l'identité

Ce système de conférence a une idée de l'identité d'un utilisateur, mais cela ne signifie pas qu'il peut révéler cette identité aux autres utilisateurs, du fait de considérations de confidentialité. Les utilisateurs peuvent choisir diverses options pour révéler leur identité aux autres utilisateurs. Un utilisateur peut être "caché" de telle façon que les autres utilisateurs ne puissent pas voir qu'ils sont des participants à la conférence, "anonyme" de telle sorte que les utilisateurs puissent voir qu'un autre utilisateur est là, mais ne pas voir l'identité de l'utilisateur, ou il peut être "public" où les autres utilisateurs peuvent voir son identité. Si il y a plusieurs utilisateurs "anonymes", les autres parties vont être capables de les voir comme des parties "anonymes" indépendantes et vont être capables de dire combien de parties "anonymes" sont dans la conférence. Noter que la visibilité aux autres participants dépend de leurs rôles. Par exemple, l'identité des utilisateurs (y compris "anonymes" et "cachés") peut être affichée au modérateur ou administrateur, selon les politiques locales d'un système de conférence. L'état "caché" est souvent utilisé par des automates ou machines participant à une conférence (par exemple, enregistrement d'appel) et est aussi utilisé dans de nombreuses situations de centre d'appel.

Comme un système de conférence fondé sur ce cadre alloue un identifiant d'utilisateur de conférence unique pour chaque utilisateur du système de conférence, il n'est pas nécessaire de distribuer d'identifiant d'utilisateur spécifique de la signalisation aux autres utilisateurs ou participants. L'accès aux identifiants d'utilisateur spécifique de la signalisation peut être contrôlé en appliquant le contrôle d'accès approprié aux identifiants d'utilisateur spécifique de la signalisation dans le schéma des données.

### 11.3 Authentification du serveur de contrôle de la prise de parole

Le protocole de contrôle de la prise de parole contient des mécanismes que les clients peuvent utiliser pour authentifier les serveurs, et que les serveurs peuvent utiliser pour authentifier les clients, comme décrit dans la Section 9 de la RFC4582]. Les mécanismes précis utilisés pour de telles authentifications peuvent varier selon le protocole de contrôle d'appel utilisé. Les clients utilisant des protocoles de contrôle d'appel qui emploient un modèle SDP d'offre/réponse, comme SIP, utilisent le mécanisme décrit à la Section 8 de la [RFC4583]. Les clients qui utilisent d'autres protocoles de contrôle d'appel utilisent les mécanismes décrits dans le document sur l'établissement de connexion BFCP [RFC5018].

## 12. Remerciements

Le présent document résulte des discussions sur l'architecture au sein du groupe de travail XCON de l'IETF. Les auteurs tiennent à remercier Henning Schulzrinne pour sa proposition d'une "arborescence d'objet de conférence" et ses commentaires généraux, Cullen Jennings pour la fourniture d'éléments pour la section des "Considérations sur la sécurité", et Keith Lantz, Dave Morgan, Oscar Novo, Roni Even, Umesh Chandra, Avshalom Houri, Sean Olson, Rohan Mahy, Brian Rosen, Pierre Tane, Bob Braudes, Gregory Sperounes, et Gonzalo Camarillo pour leur relecture et leurs apports constructifs. De plus, les auteurs tiennent à remercier Scott Brim de ses commentaires sur gen-art et Kurt Zeilenga pour ses commentaires sur secdir.

## 13. Références

### 13.1 Référence normative

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. *(MàJ par* RFC8174)

### 13.2 Références pour information

[RFC2445] F. Dawson et D. Stenerson, "Spécification centrale des objets de calendrier et de programmation de l'Internet (iCalendar)", novembre 1998. *(P.S., Obsolète, voir* RFC5545*)*

[RFC3261] J. Rosenberg et autres, "SIP : Protocole d'initialisation de session", juin 2002. (*Mise à jour par* 3265, 3853, 4320, 4916, 5393, 6665, 8217, 8760)

[RFC3264] J. Rosenberg et H. Schulzrinne, "Modèle d'offre/réponse avec le protocole de description de session (SDP)", juin 2002. *(P.S. ; MàJ par* RFC8843, 9143)

[RFC3265] A.B. Roach, "Notification d'événement spécifique du protocole d'initialisation de session (SIP)", juin 2002. (*MàJ par* RFC6446) (*Remplacée par la* RFC6665)

[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. *(MàJ par* RFC7164, RFC7160, RFC8083, RFC8108, RFC8860)

[RFC4245] O. Levin, R. Even, "Exigences de haut niveau pour la conférence SIP à couplage étroit", novembre 2005. *(Information)*

[RFC4353] J. Rosenberg, "Cadre pour les conférences avec le protocole d'initialisation de session (SIP)", février 2006. *(Information)*

[RFC4376] P. Koskelainen et autres, "Exigences pour les protocoles de contrôle de l'orateur", février 2006. *(Information)*

[RFC4566] M. Handley, V. Jacobson et C. Perkins, "SDP : Protocole de description de session", juillet 2006. *(P.S. ; remplacée par RFC8866)*

[RFC4574] O. Levin, G. Camarillo, "Attribut Label du protocole de description de session (SDP)", août 2006. *(P.S.)*

[RFC4575] J. Rosenberg et autres, "Paquetage d'événement du protocole d'initialisation de session (SIP) pour l'état Conference", août 2006. *(P.S.)*

[RFC4579] A. Johnston, O. Levin, "Commande d'appel du protocole d'initialisation de session (SIP) – Conférence pour agents d'utilisateur", août 2006. (BCP0119)

[RFC4582] G. Camarillo et autres, "Protocole de contrôle à codage binaire de la prise de parole (BFCP)", novembre 2006. *(P.S. ; remplacée par RFC8855)*

[RFC4583] G. Camarillo, "Format de protocole de description de session (SDP) pour les flux du protocole de contrôle à codage binaire de la prise de parole (BFCP)", novembre 2006. *(P.S. ; remplacée par RFC8856)*

[RFC4597] R. Even, N. Ismail, "Scénarios de conférence", août 2006. *(Information)*

[RFC4975] B. Campbell, R. Mahy, et C. Jennings, "Protocole de relais de session de message (MSRP)", septembre 2007. *(P.S ; MàJ par* RFC7977, RFC8873)

[RFC5018] G. Camarillo, "Établissement de connexion dans le protocole de contrôle à codage binaire de la prise de parole (BFCP)", septembre 2007. *(P.S.)*

[RFC6501] O. Novo et autres, "Modèle de données d'informations de conférence pour conférence centralisée (XCON)", mars 2012. *(P.S.)*

## Adresse des auteurs

Chris Boulton
Avaya
Building 3
Wern Fawr Lane
St Mellons
Cardiff, South Wales CF3 5EA
mél : cboulton@avaya.com

Mary Barnes
Nortel
2201 Lakeside Blvd
Richardson, TX
USA
mél : mary.barnes@nortel.com

Orit Levin
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
USA
mél : oritl@microsoft.com

## Déclaration complète de droits de reproduction



### Propriété intellectuelle

L'IETF ne prend pas position sur la validité et la portée de tout droit de propriété intellectuelle ou autres droits qui pourrait être revendiqués au titre de la mise en œuvre ou l'utilisation de la technologie décrite dans le présent document ou sur la mesure dans laquelle toute licence sur de tels droits pourrait être ou n'être pas disponible ; pas plus qu'elle ne prétend avoir accompli aucun effort pour identifier de tels droits. Les informations sur les procédures de l'ISOC au sujet des droits dans les documents de l'ISOC figurent dans les BCP 78 et BCP 79.

Des copies des dépôts d'IPR faites au secrétariat de l'IETF et toutes assurances de disponibilité de licences, ou le résultat de tentatives faites pour obtenir une licence ou permission générale d'utilisation de tels droits de propriété par ceux qui mettent en œuvre ou utilisent la présente spécification peuvent être obtenues sur répertoire en ligne des IPR de l'IETF à http://www.ietf.org/ipr.

L'IETF invite toute partie intéressée à porter son attention sur tous copyrights, licences ou applications de licence, ou autres droits de propriété qui pourraient couvrir les technologies qui peuvent être nécessaires pour mettre en œuvre la présente norme. Prière d'adresser les informations à l'IETF à ietf-ipr@ietf.org.