FFT Doc 09.002 v3.0 Draft (Novembre 2019)

Fédération Française des Télécommunications
Commission Innovation et Normalisation
Groupe de travail Interconnexion IP
Sous-groupe architecture

Architecture
Principes et recommandations

Fédération Française des Telecoms

Internet

http://www.fftelecoms.org

Table des matières

1. Contexte

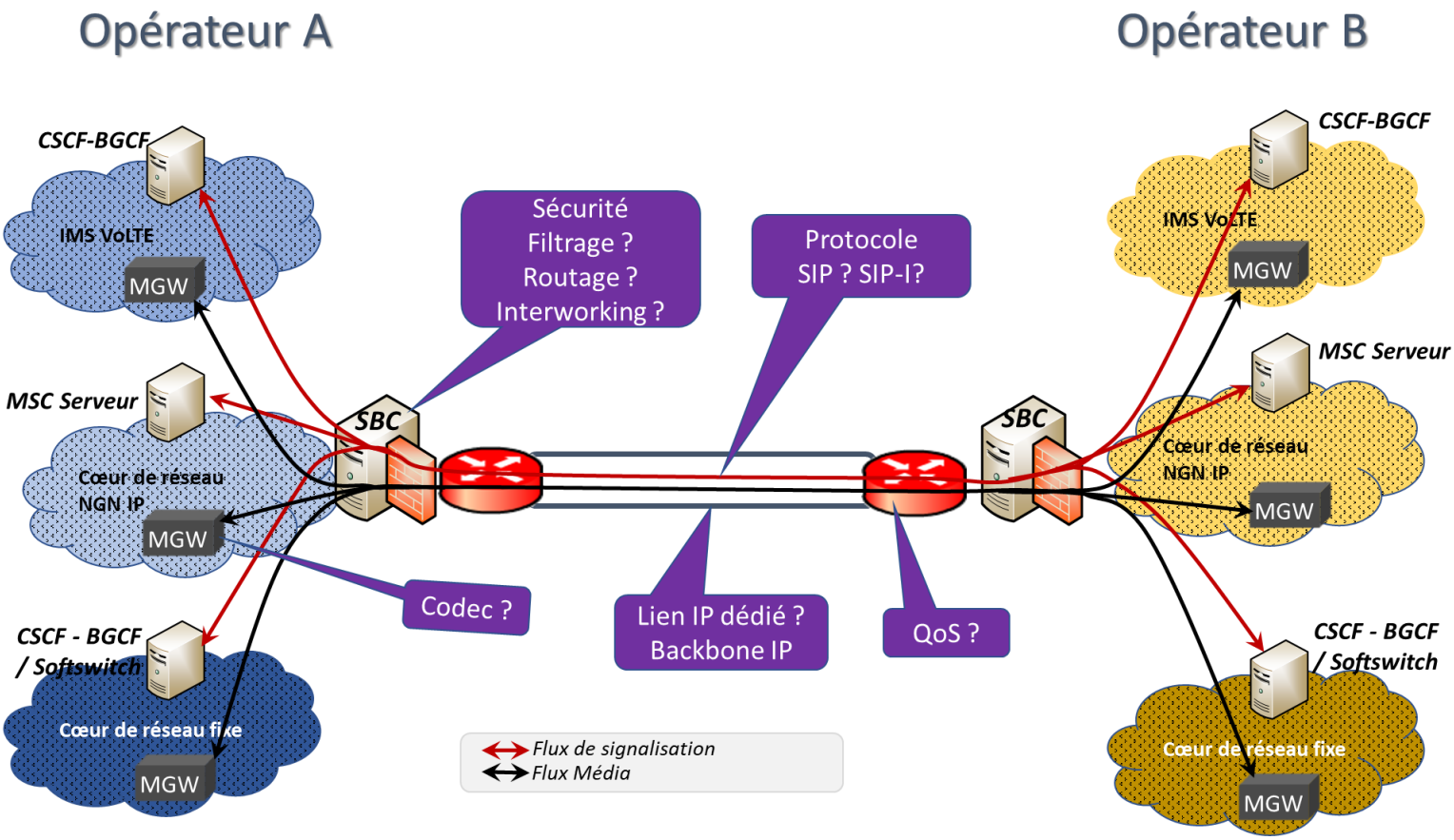
Au sein de la Fédération Française des Télécommunications, les opérateurs se sont réunis afin d'étudier les principes directeurs permettant de mettre en œuvre une architecture IP pour l'interconnexion entre opérateurs nationaux et répondant au cahier des charges services pour l'interconnexion de services de téléphonie et fonctionnalités associées (e.g. échanges de fax, connexion 64kb/s sans restriction).

L'objectif de ce document est donc de décrire l'architecture ainsi que les briques fonctionnelles à détailler pour construire une interconnexion en IP entre deux opérateurs nationaux. Le présent document a pour but également d'énoncer les principes structurants d'architecture et de faire des recommandations quant aux choix multiples qui se présentent dans le cadre de cette interconnexion.

Dans un premier temps, le périmètre de l'étude est le service voix pour une interconnexion entre deux opérateurs nationaux pour des destinations nationales et internationales.

Le groupe de travail architecture a réfléchi sur les fonctionnalités majeures de l'architecture devant être mises en place pour assurer l'interconnexion en IP entre opérateurs nationaux. Certains sujets seront approfondis de façon à dégager des recommandations.

Vue globale d'une architecture IP :



Les caractéristiques techniques qui sont abordées dans le document sont les suivantes :

- L'architecture de raccordement
- Les protocoles
- Les codecs
- La sécurité
- La sécurisation
- La qualité de service

2. Références

G.711	ITU-T recommendation “ Pulse code modulation (PCM) of voice frequencies“
G.729	ITU-T recommendation “Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear prediction (CS-ACELP)”
AMR set 7	3GPP TS 26.103 Version 11.0.0 “3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Speech codec list for GSM and UMTS”
WB-AMR	3GPP TS 26.103 Version 14.0.0 “3rd Generation Partnership Project; Technical Specification Group Services and System Aspects;Speech codec list for GSM and UMTS”
G.722	ITU-T recommendation “7 kHz audio-coding within 64 kbit/s" [Réf Dect-ND ETSI EN 300 175-8]
Clearmode	IETF RFC 4040 “RTP Payload Format for a 64 kbit/s Transparent”
Telephone event	IETF RFC 4733 "RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals"
Standards ETSI pour l’émission et la réception de DTMFs	ETSI ES 201 235-1 (généralités) ETSI ES 201 235-2 (émission de DTMFs) ETSI ES 201 235-3 (réception de DTMFs) ETSI ES 201 235-4 (prise en compte dans les terminaux des clients finaux)
Cahier des charges servIces	FFT Doc 09.001 (v1.0)
Livre blanc de la FFT sur la transition du RTC vers la voix sur IP	https://www.fftelecoms.org/app/uploads/2017/08/livre_blanc_fin_rtc_-2.pdf

3. Glossaire

ACL	Access Control List
ASR	Answer Seizure Ratio
BGP	Border Gateway Protocol
CDR	Charging Data Record
H2M	Human-to-Machine
IP	Internet Protocol
ISBC	Interconnect Session Border Controller
M2M	Machine-to-Machine
MGW	Media Gateway
MTU	Maximum Transmission Unit
NER	Network Efficiency Rate
POP	Point Of Presence
RTP	Real-time transport protocol
RTR	Routeur
SIP	Session Initiation Protocol
SBC	Session Border Controller
TCP	Transmission Control Protocol
TDM	Time Division Multiplexer
UDP	User Datagram Protocol
VAD	Voice Activity Detection
VLAN	Virtual Local Area Network
VOIP	Voix sur IP
VPN	Virtual Private Network

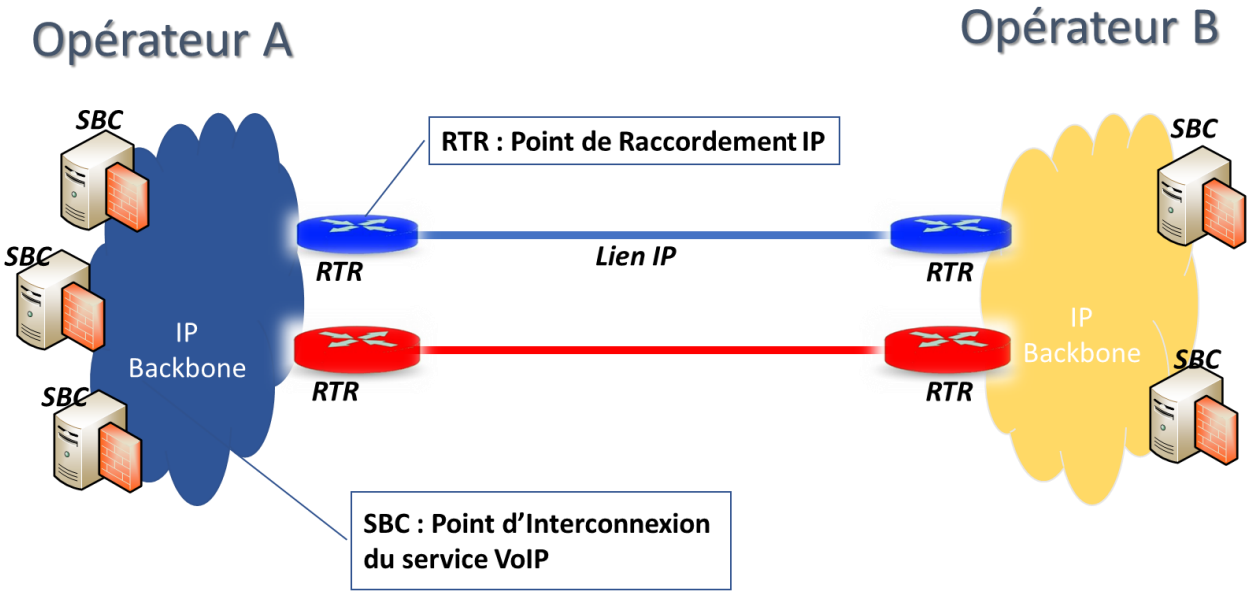
4. Architecture

La mise en place d'une interconnexion IP voix entre deux opérateurs nécessite la mise en place d'un équipement de bordure de type SBC. Les principales fonctionnalités de cet équipement sont :

- Gestion des protocoles de signalisation SIP ou SIP-I
- Sécurité (filtrage, contrôle de sessions, topology hiding)
- Interfonctionnement protocolaire voix (conversion SIP/SIP-I, gestion des préconditions)
- Transcodage
- Interfonctionnement IPv4/IPv6

4.1 Architecture de raccordement

<u>On distinguera les points de raccordement physique des points d'interconnexion logiques.</u>
On entend par point de raccordement physique (POP IP), les points de raccordement IP et par points d'interconnexion logiques, les points d'interconnexion du service lui-même, en l'occurrence ici la VOIP.



RTR = routeur
SBC = Equipement de bordure

4.1.1 Diminution du nombre de points de raccordement physique

La préconisation du groupe de travail est la suivante :
Le passage en IP de l'interconnexion va induire une baisse du nombre de points de raccordement dont le nombre cible optimal restera à définir en fonction des opérateurs et des conventions d'interconnexion (le minimum est fixé à deux points de raccordement)

4.1.2 Raccordement IP

Les préconisations du groupe de travail sont les suivantes

a) Pour des raisons de sécurisation, il faudra 2 points minimum de raccordement physique sur 2 liens physiques différents sur 2 équipements différents.

b) L'interface de raccordement est à minima le Giga Ethernet

c) Routeur distinct par lien ou à minima un port physique dédié

d) Le protocole IP est naturellement le protocole utilisé à l'interconnexion que ce soit pour les flux de signalisation ou flux média. L'interface devra être en mesure de supporter les deux versions du protocole IPv4 et IPv6 dans le but de s'adapter aux différents cas de figure possibles (voir focus sur le sujet au paragraphe § 4.1.2.1)

e) Le protocole de routage est BGP. Il supportera les deux protocoles IPv4 et IPv6.

f) Chaque opérateur devra assurer l'étanchéité des flux entre le point de raccordement IP et le point d'interconnexion du service VOIP (séparation du flux interconnexion voix IP (contrôle + média) des autres flux circulant sur le backbone de l'opérateur)

g) Le lien d'interconnexion entre les 2 routeurs sera dédié et assuré au travers d'un VLAN au minimum. Il est recommandé de dédier un VLAN pour la signalisation et un VLAN pour le média

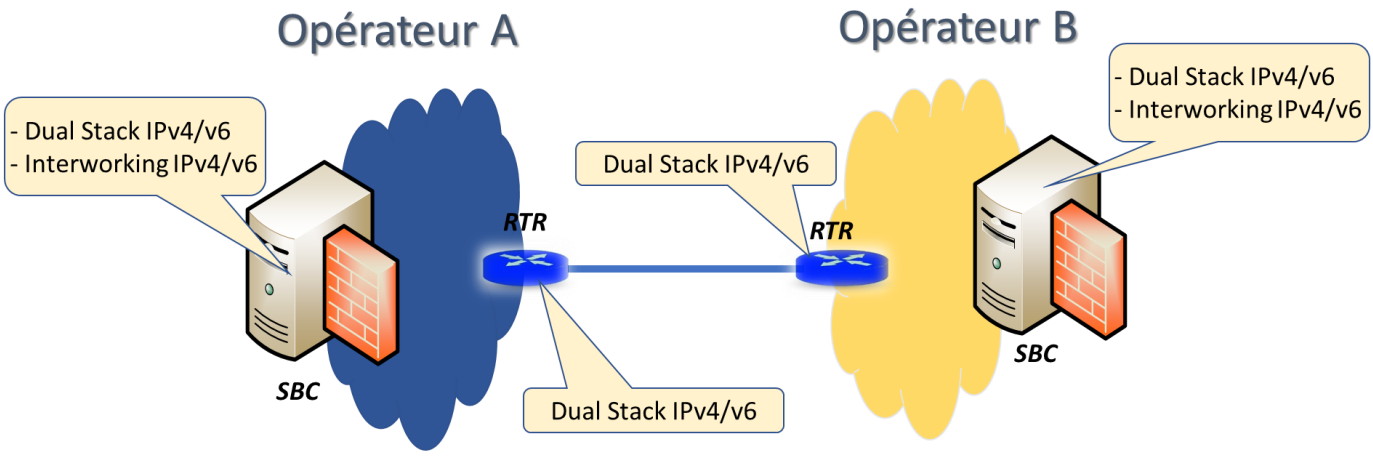
h) La possibilité de définir plusieurs VLAN à l'interconnexion pourra être envisagée selon les cas notamment avec l'arrivée de services autres que la voix.

4.1.2.1 Focus sur le support du protocole IP

Afin de palier à la pénurie d'adresses IPv4 et de s'adapter aux différentes architectures possibles notamment pour les opérateurs utilisant le protocole IPv6 dans leur cœur de réseau, il est nécessaire que les deux versions du protocole IP à savoir IPv4 et IPv6 soient supportés à l'interconnexion.
Dans ce but, les équipements de bordure I-SBC et les routeurs d'interconnexion devront pouvoir être configuré en mode « Dual Stack » pour permettre l'utilisation de l'un et/ou l'autre des versions du protocole IP

La nécessité d'une fonction « d'interworking IPv4⇔ IPv6 » :
En effet, la décision de passer en IPv6 à l'interconnexion dans un accord bilatéral entre deux opérateurs n'oblige pas forcément ces mêmes opérateurs à disposer d'un réseau cœur interne en IPv6. Ils pourront migrer à leur rythme voire même rester en IPv4
Il est alors nécessaire de supporter à minima une fonctionnalité « d'interworking IPv4⇔IPv6 » sur un équipement dans le réseau pour permettre l'ajustement et l'interfonctionnement des différentes versions du protocole IP entre les cœurs de réseau des opérateurs et la partie interconnexion/raccordement inter-opérateurs. Les deux types de flux pouvant être concernés : flux de signalisation et flux média.

Le schéma ci-dessous illustre un exemple de mise en place d'implémentation de « l'interworking IPv4/IPv6 » sur l'équipement I-SBC permettant ainsi le fonctionnement de bout en bout :



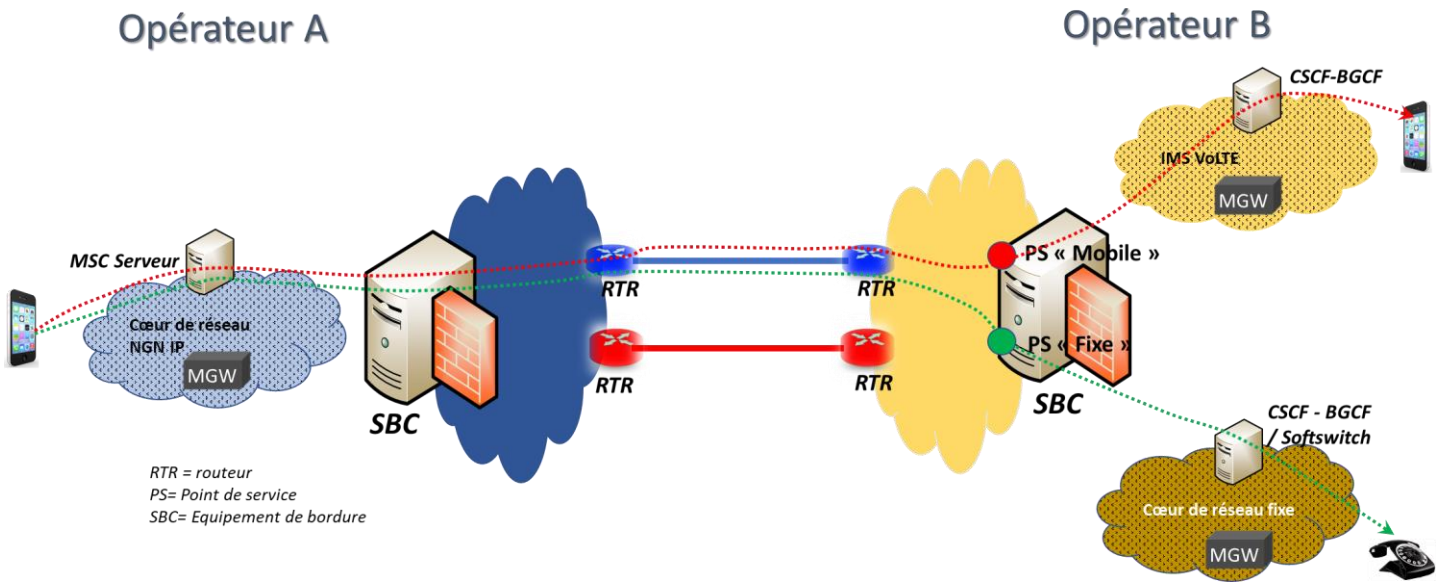
Le choix du protocole IPV6 sera fait sur accord bilatéral.

4.2 Architecture du service d'interconnexion

4.2.1 Les points d'interconnexion logiques du service voix

En interconnexion IP, afin de faciliter leur gestion et de diminuer les coûts, l'objectif est que les points d'interconnexion logiques traitant les flux de signalisation (resp. des flux media) soient en nombre limité.

Les architectures mises en place entre les opérateurs prennent comme hypothèse la mise place de deux points de service distincts pour les terminaisons fixe et mobile. Ceci permet entre autre de gérer plus facilement les niveaux fonctionnels entre les réseaux fixe et mobile (les préconditions par exemple)



Les points d'interconnexion logiques doivent implémenter au minimum les fonctions permettant de répondre aux besoins de sécurité de l'interconnexion (cf. § 4.2.5).
Les points d'interconnexion logiques doivent masquer la topologie des réseaux interconnectés, pour des raisons de sécurité et de gestion. A titre d'exemple, un SBC fonctionnant en mode « Back-to-Back User Agent » (B2BUA).

4.2.2 Routage des appels voix vers un numéro téléphonique national et interconnexion en mode IP

Avant de livrer un appel voix destiné à un numéro téléphonique français sur une interface d'interconnexion IP d'un opérateur national, il est recommandé :

- de traiter la portabilité du numéro demandé pour connaître l'opérateur de souscription de l'abonné appelé et acheminer l'appel d'interconnexion en prenant en compte cette information.
- de vérifier que l'appel en cours d'établissement doit bien être livré sur un point d'interconnexion IP (rappel : pour les besoins d'interopérabilité de bout en bout de certains usages spéciaux (ou de certains services résiduels), un appel voix peut devoir être acheminé de bout en bout en mode TDM, cf. travaux menés par l'APNF sur le sujet).

La cohabitation de plusieurs types de réseau (IMS, NGN, Softswitch) et plusieurs protocoles (SIP, SIP-I, ISUP) impose aux opérateurs de mettre en place une logique de routage pour livrer un appel sur le point de service et garantir ainsi une interopérabilité de bout en bout.

On distingue deux cas :

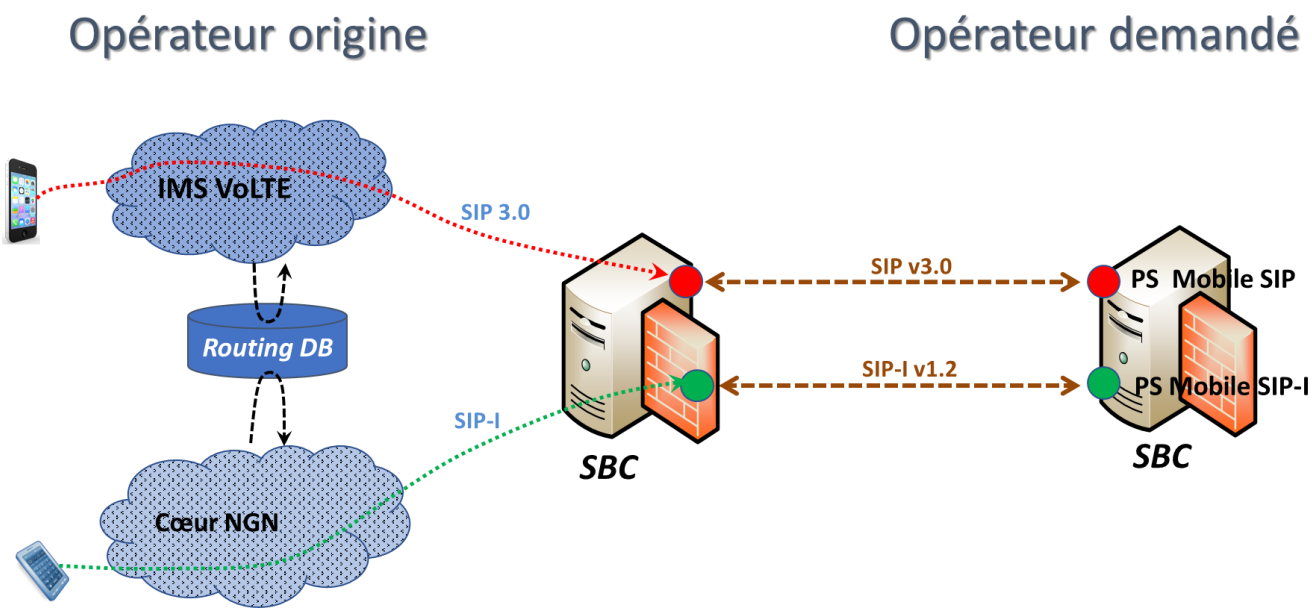
4.2.2.1 Routage de appels Mobile à Mobile

Afin de gérer les différences protocolaires et d'accompagner de manière graduelle la migration vers la VoLTE et vers le tout SIP, il est convenu de maintenir, dans un premier temps, deux Points de Service pour la livraison des appels à destination d'un mobile :

- Point de Service pour la livraison des appels en SIP-I,
- Point de Service pour la livraison des appels en SIP (profil FFTv3.0).

Ci-dessous un exemple d'architecture pour le routage des appels mobile où:

- Les appels Origine IMS VoLTE et à destination d'un mobile sont livrés sur le point de Service SIP de l'opérateur demandé
- Les autres appels départ mobile et à destination d'un mobile sont livrés sur le Point de Service SIP-I de l'opérateur demandé comme le montre le schéma ci-dessous :



La condition pour qu'un appel puisse être livré sur l'interface SIP est qu'on puisse satisfaire le niveau fonctionnel requis sur cette interface

Il est rappelé que le protocole cible pour les appels mobile-mobile est le SIP. Des études complémentaires sont nécessaires pour cadrer les éventuels cas d'appels non compatibles et identifier les solutions pour migrer ce trafic mobile vers le tout SIP.

4.2.2.2 Routage des appels Fixe vers Mobile

En fonction des accords bi-latéraux et des architectures déjà mises en place. Les appels Fixe vers Mobile (que ce soit IMS VoLTE ou legacy) peuvent continuer à être livrés, si c'est déjà le cas, sur le point Service SIP-I de l'opérateur mobile demandé. Toutefois, il est fortement recommandé, si l'opérateur fixe supporte le protocole SIP (sans préconditions) de livrer ce trafic sur le point de service SIP de l'opérateur mobile demandé. En effet, le protocole SIP est la cible également pour les réseaux de type fixe.

4.2.3 Les protocoles

4.2.3.1 Le choix des protocoles

Les protocoles retenus sont l'un et/ou l'autre des suivants :
- SIP-I (ISUP encapsulé compatible avec la spécification du SPIROU défini par l'ARCEP et utilisé pour l'interconnexion TDM en France, SIP-I : ITU Q.1912.5 Annexe C) et tel que défini par la FFT dans son profil SIP-I
- SIP (SIP 3GPP TS 24.229) et tel que défini par la FFT dans son profil SIP

SIP est la cible à l'interface de signalisation pour tous les services vocaux.

Le choix a été fait afin de traiter les cas suivants :
- mobile – mobile
- fixe – fixe
- fixe – mobile

4.2.3.2 Transport du protocole SIP

La préconisation du groupe de travail est de transporter sur UDP le protocole SIP utilisé à l'interface d'interconnexion voix entre opérateurs.

. Note 1 : dans le cas d'un paquet UDP dont la taille est supérieure au MTU, il est fortement recommandé d'utiliser la fragmentation UDP au lieu de la bascule en TCP. Il est à noter que dans le cas de l'utilisation du protocole IPv6 à l'interconnexion, le risque de fragmentation sur un réseau IPv6 est en principe limité car il existe le mécanisme de « Path MTU Discovery » pour adapter à la source la taille du MTU.
Dans le cas où une fragmentation serait nécessaire, celle-ci étant gérée sur les équipements d'extrémité, une adaptation manuelle de la MTU sur l'équipement source peut être nécessaire pour garantir le bon fonctionnement et éviter la perte de paquets

Note 2 : sur accord bilatéral, il est possible d'utiliser TCP à l'interconnexion.

4.2.3.3 Transport du flux média :

Le flux média RTP est transporté sur UDP sur IP v4 ou IPv6.

4.2.4 DTMF

D'un point de vue service, 2 types de DTMF sont à considérer :

- Les DTMF émises par un usager humain (depuis le clavier d'un terminal téléphonique) vers une machine (« DTMF Human-to-Machine (H2M) »)
    - Exemple 1 : DTMF émise par l'appelant lors d'un appel aboutissant sur la messagerie vocale de l'appelé.
    - Exemple 2 : DTMF émise par l'appelant vers un serveur vocal (e.g. appel vers un SVA qui utilise une interaction homme machine)

- Les DTMF émises par une machine vers une autre machine (« DTMF Machine-to-Machine (M2M) »)
    - Exemple : train de DTMF émis par un automate d'alarme vers un centre de télésurveillance.

Le transport de DTMF via une infrastructure d'interconnexion IP est abordé dans le § 4.2.5.

4.2.5 Les codecs

L'objectif de ce paragraphe est de définir la liste des codecs pouvant être supportés à l'interface d'interconnexion et leurs règles d'utilisation. L'utilisation de tout autre Codec est possible dans le cadre d'accord bilatéraux.

4.2.5.1 Codecs à bande étroite

- Toute offre SDP émise à l'interface d'interconnexion IP doit inclure par défaut le codec G711 loi A.

Par conséquent, les opérateurs dont les clients sont exclusivement en G729 devront être capables de transcoder en G711 les appels à destination (et en provenance) de leurs clients dès lors qu'ils sont interconnectés en full IP avec un autre opérateur national.

- L'interface d'interconnexion IP doit pouvoir faire passer en transparent des DTMF M2M « rapides » via des paquets G711 (cf. « Livre blanc de la FFT paru en 2017 sur la transition du RTC vers la voix sur IP »), par conséquent :
    - Si une offre SDP reçue à l'interface d'interconnexion IP d'un opérateur contient le codec G711, ce composant doit être passé en transparent dans le SDP émis vers l'aval par le SBC d'entrée de cet opérateur.

- Si une réponse SDP reçue à l'interface d'interconnexion IP d'un opérateur contient le codec G711, ce composant doit être passé en transparent dans le SDP émis vers l'amont par le SBC de sortie de cet opérateur.

Note : le transport des DTMFs via des paquets G711 banalisés ne doit être utilisé que pour certains usages spéciaux M2M comme décrits ci-dessus et n'est pas applicable au transport des DTMF H2M (cf. § 4.2.5.4).

- Il est admis que chaque opérateur assure la gestion de l'information Ptime dans SDP ; si un opérateur ne peut en assurer la gestion, il doit s'assurer que le temps de paquétisation est fixé à 20ms par configuration statique.

- Configuration de chaque codec bande étroite accepté :

- **AMR set 7** (12.2 kbps uniquement) ; Ptime=20 ms ; Payload Type = dynamic entre 96 et 127
  - octet-align = bandwidth-efficient operation; channels = 1
  - Media format specific parameters mode-set=7
  - Media format specific parameters max-red=0

- **G711 loi A ;** Ptime=20 ms sans VAD ; Payload Type=8

- **G.729** ; Ptime=20 ms ; avec ou sans annexe A, Payload Type=18 ; Annex b=no

- Règles d'utilisation

Pour les interconnexions directes mobile-mobile seulement, l'activation de TrFO est attendue des deux côtés de l'interface d'interconnexion, le groupe de travail préconise l'utilisation du codec AMR set 7.

Pour les autres cas, les codecs voix recommandés à l'interface de l'interconnexion IP sont le G711 loi A et le G729 avec ou sans annexe A avec la configuration décrite ci-dessus.

Dans le cas d'une offre SDP avec les codecs, G711 loi A et G729 avec ou sans annexe A, la position du G711 loi A est attendue avant le G729 avec ou sans annexe A. Dans le cadre d'un accord bilatéral, le G729 avec ou sans annexe A peut-être positionné en première place de l'offre SDP.

Si aucun accord bilatéral sur le codec voix à supporter à l'interface n'a pu être trouvé, le G711 loi A avec un temps de paquétisation de 20 ms est utilisé par défaut.

NB :
- Transcoder Free Operation (TrFO) : Notion spécifique aux réseaux mobiles et à leur interconnexion qui correspond à la configuration d'un appel voix ou multimédia pour lequel aucun élément de transcodage est présent dans le chemin media.
- Le TrFO implique l'activation de mécanismes de négociation de codec « out of band » entre les 2 extrémités (e.g. BICC vs SIP ou SIP-I sur G-MSC) afin que les mêmes codecs et « mode set » soient utilisés sur l'ensemble du chemin media.
- Cela doit contribuer d'une part à améliorer la qualité vocale en choisissant le meilleur codec disponible (e.g. AMR-WB) et d'autre part à préserver les ressources de transcodage et la bande passante en utilisant des codecs compressés.

4.2.5.2 Codecs à large bande

Il est admis que chaque opérateur assure la gestion de l'information Ptime dans SDP. Si un opérateur ne peut en assurer la gestion, il doit s'assurer que le temps de paquétisation est fixé à 20ms par configuration statique.

Configuration de chaque codec accepté :

- **G722** Ptime=20 ms**;** (Payload Type static =9)

- **WB AMR set 0** (6.6 kbps, 8.85 kbps, 12.65 kbps, 15.85kbps, 23.85kbps); Payload type = dynamic entre 96 et 127
  - octet-align = bandwidth-efficient operation ; channels = 1
  - Media format specific parameters mode-set=0,1,2
  - Media format specific parameters mode-change-period=2

- Media format specific parameters mode-change-capacity=2
- Media format specific parameters mode-change-neighbor=1
- Media format specific parameters max-red=0

Règles d'utilisation

Pour les interconnexions directes mobile-mobile, l'activation de TrFO est attendue des deux côtés de l'interface, le groupe de travail préconise l'utilisation du codec WB_AMR, avec la configuration décrite ci-dessus.

A l'interface d'interconnexion, lorsqu'un codec large bande est présenté dans l'offre SDP, il doit être présenté avec en plus un codec à bande étroite. Le codec à large bande est attendu avant le codec à bande étroite (le G711 est obligatoire dans l'offre SDP d'un INVITE mais d'autres codecs à bande étroite peuvent être ajoutés : cf. chapitre Codecs à bande étroite).

Pour les interconnexions fixe-fixe, le G722 avec la configuration décrite ci-dessus est recommandé.

Pour les interconnexions fixe-mobile, la voix large bande nécessite actuellement un transcodage entre WB_AMR et G722. Ce point devrait être traité en bilatéral.

Par défaut, si aucun accord n'a été trouvé entre les deux opérateurs interconnectés en IP, les codecs à bande étroite seront utilisés (cf chapitre Codecs à bande étroite).

4.2.5.3 Pseudo-codec Clearmode

Quand un appel transparent 64 kbit/s est demandé, le SDP doit alors contenir le pseudo-codec Clearmode [RFC4040].
Le pseudo-codec clearmode n'est prévu que dans le cadre du profil SIPI

4.2.5.4 Telephone event

Dans le cas des appels voix bande étroite ou large bande, l'indication du support de « telephone-event » durant l'échange offre/réponse SDP est obligatoire à l'interface d'interconnexion pour le transport de DTMFs de bout en bout. L'absence d'une telle indication signifiera le non support d'échanges de signaux DTMF sauf dans les cas suivants :

- appel 'data' établi en G711 pour certains usages spéciaux à base de DTMF M2M (cf. § 4.2.5.1)
- appel 'data' 64 kbit/s (pseudo-codec Clearmode) (voir note)
-

Note : dans ce cas de figure, le telephone-event ne doit pas être indiqué dans le corps de message SDP émis à l'interface d'interconnexion IP.

- Le passage à une autre phase d'appel nécessitant une modification du support des DTMF est autorisé et devra s'effectuer via un nouvel échange offre/réponse SDP. Par exemple, suppression de « telephone-event » pour le service FAX, ajout de « telephone-event » pour une reprise suite à mise en attente.

La fréquence d'échantillonnage (ou taux d'échantillonnage) doit être identique à celle associée au flux audio, /8000 pour les codecs à bande étroite ou G722 et /16000 pour AMR-WB (set 0).

L'encodage du codec SDP associé doit être réalisé suivant la [RFC4733], qui par ailleurs définit le format du RTP payload pour les digits DTMF, avec les précisions suivantes :

- L'attribut fmtp doit être utilisé pour déclarer la liste des évènements DTMF supportés
- Seuls les évènements de 0 à 15 sont supportés
- Les paquets RTP DTMF doivent utiliser la même séquence de numéros et les mêmes références d'horodatage utilisées pour les paquets audio RTP.

« Telephone event » peut être considéré comme un codec audio, ainsi il est traité de la même manière que les autres codecs audio. Les règles de négociation SDP de la RFC 3264 doivent être appliquées.

4.2.5.5 Nouveaux Codec

Suite à l'introduction de la VoLTE, de nouveaux Codec sont possibles à utiliser sur accord bilatéral :

- EVS (*Enhanced Voice Services)*
- Support des débits 15.85kbps et 23.85kbps du WB-AMR

4.2.6 La qualité de service-

4.2.6.1 Les objectifs

La qualité de service est définie par l'acheminement nominal des appels et la qualité de service de la voix de bout en bout.

Des indicateurs sont définis afin de mesurer ces deux critères.

Le bon acheminement des appels est mesuré par les indicateurs suivants :
- NER (1-Taux d'Echec Réseau)
- ASR (Taux d'Efficacité des Appels)

La qualité de service de la voix sera mesurée par les indicateurs suivants :
- Gigue
- Taux de perte de paquets

4.2.6.2 Les moyens

Chaque opérateur est garant du trafic envoyé. L'opérateur doit vérifier le trafic qu'il émet.
Chaque opérateur doit se donner les moyens de vérifier la qualité du trafic reçu.

Les moyens de mesures de la qualité de service peuvent être :

- L'utilisation des CDR ou des remontées de valeurs issus des équipements d'interconnexion du réseau de l'opérateur (routeur, SBC)

L'utilisation des sondes (ou des CDR issus de sondes)

4.2.7 La sécurité et la sécurisation

4.2.7.1 Le principe général de la sécurité

Contrairement au monde TDM, le réseau IP est par essence ouvert et nécessite la mise en place d'une brique de sécurité.

Il est donc important de mettre en place un équipement de sécurité et d'identifier les fonctionnalités permettant de se prémunir d'éventuelles attaques. Mais chaque opérateur a le choix de la solution pour rendre ce type de fonction.

L'architecture de service sécurisée doit garantir le service de bout en bout et les modalités pourront être précisées lors des accords bilatéraux entre les deux parties.

4.2.7.2 Les vulnérabilités :

Chaque opérateur est garant de l'étanchéité des flux d'interconnexion au sein de son réseau.

L'opérateur doit garantir la non propagation de flux parasites sur l'interconnexion, malgré cela il appartient à chaque opérateur de se protéger en cas de défaillance de l'opérateur tiers ou contre toute attaque d'un tiers.

Les constats et préconisations du groupe de travail sont les suivantes :

a) En mode de raccordement direct par des liens dédiés, le risque d'attaque est faible. Quant aux besoins de la confidentialité et à l'intégrité des communications, on aura un niveau équivalent au TDM. Il n'est donc à priori pas nécessaire de chiffrer les communications en liens dédiés.

b) Il faudrait être capable de donner une liste d'adresses, de ports et de protocoles autorisés, avec la possibilité de bloquer certains ports connus (à voir si en pratique cela est réalisable).

c) Les adresses IP V4 ou IPv6 utilisées au sein de chaque infrastructure d'interconnexion entre opérateurs seront publiques et ne devront pas être annoncées sur l'Internet.

d) Chaque opérateur choisit la façon d'étanchéifier les flux au sein de son réseau (VPN, …).

e) Des équipements d'interconnexion différents peuvent assurer la sécurité de la signalisation et du média

f) La mise en place de mécanisme de sécurité au niveau du routeur (ACL) : contrôle d'accès à une liste d'adresses sources bien identifiées permettrait d'assurer un premier niveau de filtrage.

4.2.7.3 Redondance et sécurisation

Chaque opérateur est garant de la disponibilité du service au sein de son réseau.

Le principe de la sécurisation est de s'assurer qu'entre deux opérateurs le trafic passera toujours, grâce à une sécurisation au niveau du raccordement et au niveau des équipements fournissant le service.

1. Le principe est donc de s'assurer qu'il y a toujours un second chemin pour écouler le trafic en cas de problème sur le chemin nominal.
Il faut que le chemin soit sécurisé (redondance des liens et chemins pouvant être différents) mais il faut aussi que les équipements d'extrémité (routeurs) soient redondés, sachant que les 2 chemins peuvent être différents.

2. Il faut que les équipements fournissant le service d'interconnexion soient redondés aussi bien sur la partie signalisation que sur la partie media.

Aussi, 2 modes de redondance peuvent être mis en place pour la sécurisation du trafic :

- Modèle du N+1 garantie de sécurisation de 100% du trafic par une méthode Normal / secours (N SBC nominaux / 1 SBC de backup)
- Partage de charge entre équipements I-SBC

La remarque suivante est à prendre en compte :

Malgré la sécurisation qui est mise en place, il est possible, lors de basculements, que l'utilisateur perde la session en cours. L'utilisateur devra alors réitérer son appel pour bénéficier de la sécurisation.

5. Historique

Historique du document		
V1.0.0	Avril 2009	Version approuvée par la commission normalisation
V.1.1	Janvier 2014	Mise à jour du chapitre « Codecs »
V1.1.1	Avril 2014	Mise à jour du chapitre « Codecs » avec la version V9
V1.1.2	Juin 2014	Prise en compte des remarques suite à la consultation
V1.1.2	Juillet 2014	Finalisation du document V1.1.2
V1.9	Mai 2018	Prise en compte du transport de DTMF M2M via l'architecture d'interconnexion IP, inclusion d'une section sur le routage des appels d'interconnexion et d'une annexe sur les mécanismes de protection du service d'interconnexion voix
2.0	Juin 2018	Finalisation du document V2.0
3.0	Novembre 2019	Prise en compte de la VoLTE. Ce document est associé au profil SIP FFT 3.0

6. Annexe : mécanismes de protection du service d'interconnexion voix

Il est conseillé aux opérateurs de mettre en place des mécanismes de protection contre les bouclages d'appels et les répétitions de tentatives d'appels afin de protéger leur service d'interconnexion d'une surcharge pouvant aller jusqu'à la perte complète du service de gros mis en œuvre entre opérateurs.
La fonctionnalité basée sur l'en-tête SIP Max-Forwards est un de ces mécanismes mais elle ne permet de se protéger que dans un monde SIP de bout en bout, elle n'est pas suffisante dans les autres cas. Il peut être nécessaire de compléter cette fonctionnalité par d'autres dispositifs.
Les dispositifs décrits ci-dessous sont à considérer comme faisant partie d'une boite à outils et la mise en œuvre de certains doivent faire l'objet d'accords bilatéraux.

1. Dispositif de protection contre les boucles d'appel

Il est préconisé de se protéger des boucles d'appel inter-opérateurs en les détectant sur les équipements mettant en œuvre l'interconnexion IP (en fonction de leurs capacités fonctionnelles) par l'utilisation d'un ou plusieurs mécanismes.

En premier lieu, il est préconisé de disposer d'une solution de supervision de trafic qui alerte sur détection d'un 'burst' d'appels anormal entre deux opérateurs (nombre de sessions qui augmente significativement sur un faible délai).

Pour limiter les boucles d'appels, les principes suivants sont à adopter :
- traiter la portabilité du numéro demandé au sein de son propre réseau avant d'envoyer un appel à l'interface d'interconnexion,
- traiter la supervision de l'interconnexion par d'autres dispositifs que le bouclage d'appel.

2. Dispositif de protection contre la répétition d'appels

Il est préconisé de se protéger contre la répétition automatique d'appels et 'burst' de tentatives d'appels par l'utilisation d'un ou plusieurs des mécanismes listés ci-dessous (liste non exhaustive) :
- limiter sur ses équipements d'interconnexion ISBC le nombre maximum de répétitions par appel de manière globale ou en fonction du code d'erreur (par exemple limiter au nombre de points de service de l'opérateur distant),
- limiter sur ses équipements d'interconnexion ISBC globalement toute répétition d'appel ou sur une majorité de codes d'erreur pendant une durée limitée pour des périodes de fort trafic (par exemple jour de l'an).

Pour faire face à des périodes à forts pics d'appels prévisibles (e.g. appels vers indicatifs spécifiques à fort trafic entrant), il est conseillé de mettre en place le mécanisme décrit ci-contre : remplacer, si reçus sur les équipements d'interconnexion du réseau appelé, les codes d'erreur autorisant la re-tentative d'appel par un code d'erreur équivalent qui ne la permet pas.
Par exemple, remplacer le code d'erreur SIP 480 par le code 603, solution qui est préconisée de façon permanente pour les appels vers les indicatifs supports d'événements médiatiques (jeux, télévote…) qui peuvent provoquer des 'bursts' de trafic importants, et en mode préventif pour pallier des risques de 'bursts' d'appels ponctuels, par exemple lors des pics de trafic de fin d'année.

3. Dispositif de protection contre les appels à fort pic de trafic

D'une manière générale, en fonction des capacités de ses équipements d'interconnexion ISBC, il peut être envisagé de limiter le seuil des CAPS en fonction du profil client qui s'appliquerait sur les 'bursts' de tentatives d'appels.