	Descriptif architecture réseau MEXIC	Réf : MEXIC_Descriptif_Architecture_Reseau.docx
		Page 1 sur 9

Rédaction		Vérification	
Par :	Date :	Par :	Date :
A. LOURMIERE N. BOUTEILLER	27/05/2010	D. MOREAU N. PLEY	16/06/2010

Approbation	
Par :	Date :
T. BEDOIN M. FASQUELLE	23/06/2010

Historique des modifications de la fiche		
N°version	Date	Objet de la modification
Référence	27/05/2010	Création du document

Niveau de confidentialité : Restreint aux Partenaires de la Banque de France

Documents de référence (en amont)	
Référence	Objet

Documents associés (en aval et connexes)	
Référence	Objet

Liste de diffusion

Sommaire

1. OBJET DU DOCUMENT.....	3
2. GLOSSAIRE	3
3. DESCRIPTION DE LA SOLUTION.....	4
3.1. SPÉCIFICATIONS TECHNIQUES.....	4
3.1.1. Boucle locale.....	4
3.1.2. Equipements d'accès au service	4
3.1.3. Bande passante	4
3.1.4. Sécurité	4
3.1.5. Adressage IP	4
3.1.6. Routage.....	5
3.1.7. Translation d'adresses.....	8
3.1.8. QoS.....	8
3.1.9. Niveau de service.....	8
3.2. CONTACTS OPÉRATEURS.....	8

1. Objet du document

La Banque de France a lancé un projet concernant le raccordement IP de ses partenaires. Dans cette optique, la Banque de France a agréé des opérateurs Télécoms, dont la liste est disponible au chapitre 2.2 ; chaque opérateur fournit un VPN IP MPLS dédié, sur lequel sont raccordés les deux sites centraux de la Banque de France. Par la suite, les partenaires ont la possibilité de commander un accès chez un (ou plusieurs) de ces opérateurs, créant ainsi un canal de communication avec le système d'information de la Banque de France.

Ce document décrit les principales caractéristiques de l'architecture réseau mise en place dans le cadre du projet.

2. Glossaire

Ce chapitre définit les termes clés utilisés dans les chapitres ci-dessous.

Termes	Définitions
MEXIC	Migration des Echanges X25 vers IP CFONB
IP	Protocole Réseau (Internet Protocol) permettant un service d'adressage unique pour l'ensemble des équipements connectés
MPLS	MultiProtocol Label Switching Protocole conçu pour fournir un service unifié de transport de données en utilisant une technique de commutation de paquets

3. Description de la solution

3.1. Spécifications techniques

Voici les principales caractéristiques techniques à connaître concernant l'implémentation des réseaux IP VPN MPLS dédiés au projet MEXIC.

3.1.1. Boucle locale

Les opérateurs présentent dans leur catalogue un grand choix de types d'accès télécoms auxquels peuvent souscrire les Partenaires. Les boucles locales reposeront sur des supports cuivre ou fibre optique. Les technologies d'accès peuvent notamment être de type (xDSL) à débit symétrique ou asymétrique en fonction des solutions dont dispose l'opérateur.

3.1.2. Equipements d'accès au service

Le raccordement des sites au réseau privé virtuel d'un opérateur agréé est réalisé à partir de routeurs CE appartenant à l'opérateur et hébergés dans les locaux des partenaires. Les partenaires donnent accès à leurs locaux pour que les opérateurs puissent installer les accès télécoms. Ils fournissent également l'énergie électrique nécessaire aux CE.

Les opérateurs présentent le service d'interconnexion IP sur les interfaces LAN des équipements CE.

L'opérateur est donc responsable du service d'interconnexion IP entre les interfaces de(s) CE constituant la liaison et les interfaces de CE situées sur les sites de collecte BdF. Sa responsabilité ne pourra pas être engagée en cas de défaut sur les réseaux locaux.

3.1.3. Bande passante

Chaque partenaire détermine la bande passante à souscrire auprès des opérateurs qu'il aura choisis en fonction de ses besoins. Ce dimensionnement devra prendre en compte l'ensemble des informations échangées, notamment dans le cas où la liaison supporte plusieurs applicatifs.

Le débit des accès centraux de la Banque de France est dimensionné par les opérateurs, en fonction des débits souscrits par les partenaires et de leurs utilisations réelles.

3.1.4. Sécurité

Les réseaux IP VPN MPLS utilisés sont des réseaux dédiés aux dialogues avec la Banque de France : un partenaire ne pourra pas utiliser son lien Télécom pour joindre d'autres partenaires. Des mécanismes de sécurité seront implémentés au niveau opérateur afin de s'en assurer. Le design de ces réseaux est de type Hub & Spoke, la Banque de France étant au centre de l'architecture.

De son côté, la Banque de France assure le cloisonnement entre les différents opérateurs agréés, tous raccordés à ses datacenters, afin de prévenir tout rebond.

Par ailleurs, les communications transitant sur ces réseaux ne seront pas chiffrées au niveau transport ; charge à l'applicatif utilisé de chiffrer les données si nécessaire.

3.1.5. Adressage IP

Le plan d'adressage IP est défini par la Banque de France, qui garde la maîtrise de la solution technique globale. Les dialogues au sein de ces réseaux seront effectués par l'intermédiaire de cet adressage.

Un sous-réseau privé (RFC 1918) avec un masque de sous-réseau en « /18 » est alloué à chaque opérateur qui redistribuera ces adresses IP aux machines des partenaires (par l'intermédiaire d'un découpage de la plage globale en subnets).

Un sous-réseau unique en « /24 » sera alloué aux machines Banque de France. En effet, les machines BdF auront les mêmes adresses IP quel que soit l'opérateur par lequel transite un flux. Voici les plages d'adresses par opérateurs :

- BT : 172.18.64.0/18
- COLT : 172.18.192.0/18
- COMPLETEL : 172.18.0.0/18
- OBS : 172.19.0.0/18
- SFR : 172.18.128.0/18

Les adresses IP des machines des partenaires dans le plan d'adressage MEXIC dépendent donc de l'opérateur choisi. Les opérateurs seront chargés de communiquer aux partenaires le subnet à utiliser, après estimation du nombre de machines partenaire devant dialoguer sur le VPN IP MPLS. La Banque de France adressera ses différentes machines dans le subnet 172.17.0.0/24.

3.1.6. Routage

La Banque de France assure de son côté le routage de l'architecture centrale. Pour un opérateur donné, les deux chaînes d'accès peuvent être vues comme un seul accès logique (utilisation de liens de niveau 2 entre les routeurs CE et sur le vlan d'interconnexion avec les routeurs BdF) ; le subnet 172.17.0.0/24 est annoncé depuis chacun de ses deux accès avec des poids différents selon le site, de sorte que tout le trafic d'un opérateur ne passe que par un seul site à un instant T. Ce mécanisme est répété pour chacun des opérateurs. Des bascules globales pourront être programmées, afin de valider le fonctionnement de la chaîne de secours. En cas de pannes sur une des chaînes Télécoms, ceci est transparent en termes de routage pour le partenaire : le même réseau sera à viser pour joindre la Banque de France.

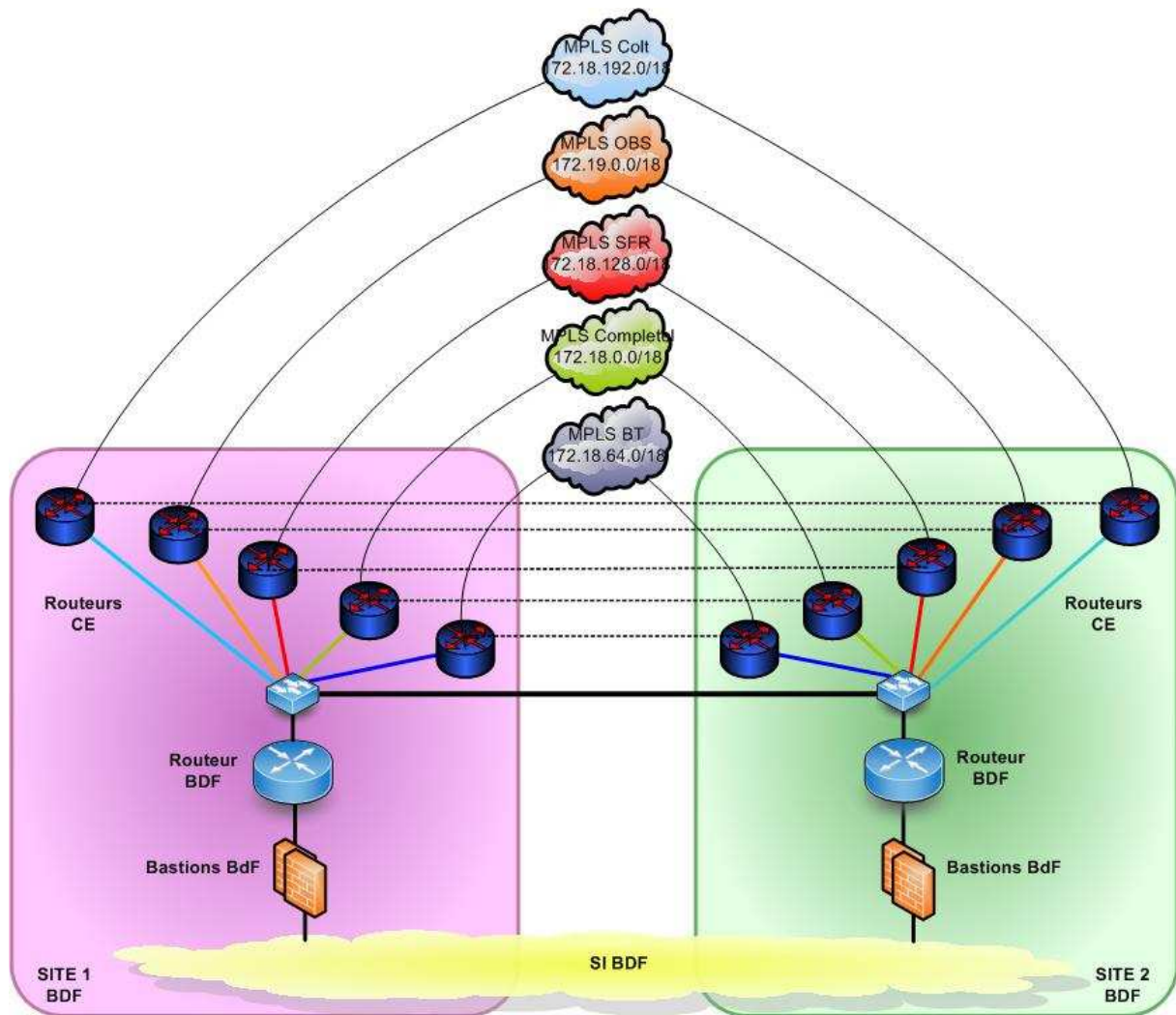


Schéma 1 : Architecture logique générale

Coté partenaire, l'architecture de routage devra être définie par ses soins, en collaboration avec le (ou les) opérateur(s). Un choix devra notamment être fait concernant le niveau de sécurisation souhaité : accès mono, accès Dual localisé sur un même site géographique, accès Dual sur site non co-localisé, deux accès distincts (chez le même opérateur ou non),...

Du routage statique ou dynamique pourra être configuré avec l'opérateur, suivant les possibilités et les propositions de chaque partie.

Les accès de type Dual (bénéficiant d'un lien de niveau 2 entre les deux routeurs, cf schémas 3 et 4) présentent l'avantage d'être vu comme un seul accès logique, et donc de disposer d'un adressage IP unique. Ceci peut notamment être utile dans l'optimisation des scénarios de bascule en cas de panne. Ils permettent également de faciliter le routage en sortie : en cas de panne de l'accès nominal, le routage sortant pourra se faire automatiquement par l'autre lien, via les interconnexions entre routeurs WAN. Dans le cas de deux accès distincts (cf schémas 5 et 6), le partenaire devra gérer en amont le routage, au sein de son réseau local, afin d'assurer correctement les bascules.

Les schémas ci-dessous présentent les différentes architectures potentiellement utilisables. Chaque opérateur confirmera les différentes offres qu'ils proposent sur ces différents modèles.

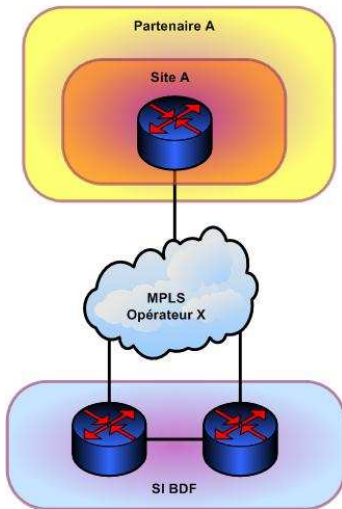


Schéma 2 : Architecture 1 site – 1 accès Mono

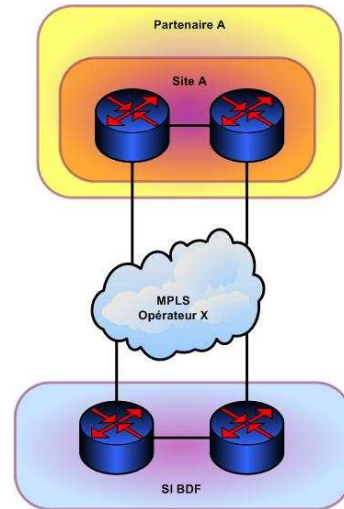


Schéma 3 : Architecture 1 site – 1 accès Dual

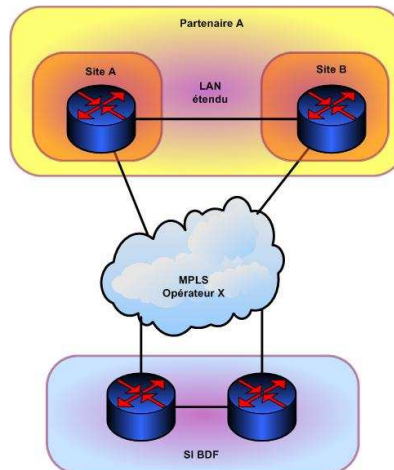


Schéma 4 : Architecture 2 sites – 1 accès Dual

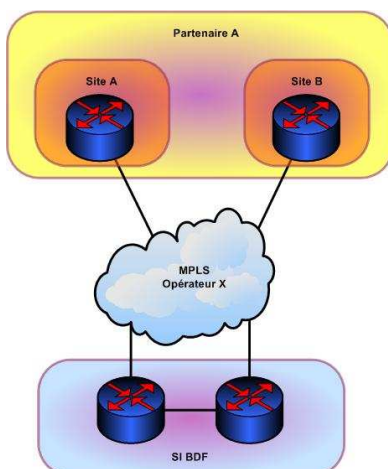


Schéma 5 : Architecture 2 sites – 2 accès Mono
Même opérateur

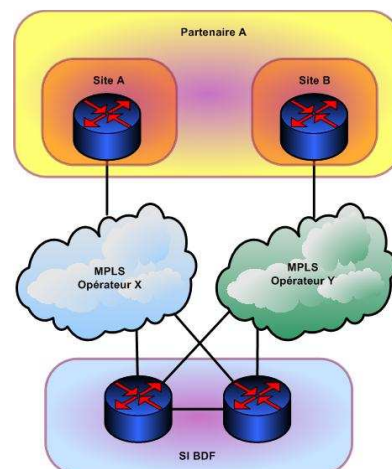


Schéma 6 : Architecture 2 sites – 2 accès Mono
2 opérateurs différents

3.1.7. Translation d'adresses

La règle générale est d'utiliser l'adressage IP MEXIC pour communiquer avec les CE. Les partenaires peuvent gérer eux-mêmes les translations d'adresse dont ils ont besoin entre leur réseau interne et les CE MEXIC.

Cependant, pour des besoins particuliers, des translations sur les CE permettront de faire correspondre l'adressage IP privé des partenaires avec l'adressage IP MEXIC. Ainsi, les problématiques d'adressage interne de chacun seront transparentes pour la Banque de France et ses Partenaires :

- si le partenaire ne souhaite pas utiliser la plage d'adresse MEXIC prédéfinie pour les machines Banque de France, l'opérateur pourra traduire une autre plage choisie par le partenaire vers cette plage MEXIC,
- de même si le partenaire ne souhaite pas utiliser la plage d'adresses MEXIC qui lui a été attribuée, l'opérateur pourra traduire une autre plage choisie par le partenaire vers cette plage MEXIC.

3.1.8. QoS

Les opérateurs implémentent des dispositifs de gestion de la QoS afin d'assurer sur chaque réseau MEXIC le transport de flux hétérogènes dans les meilleures conditions.

La Banque de France définit les classes de services (CoS) qui sont offertes par les réseaux MEXIC, en fonction des types de flux transitant sur ce réseau. L'opérateur garantira une part minimum de la bande passante à chaque classe de service en cas de congestion sur les boucles locales. Pour l'instant, deux classes de service sont prévues : une pour les flux de Télétransmission, et une pour les flux transactionnels (POBI).

Au moment des commandes Télécoms, il reviendra au partenaire de se rapprocher de l'opérateur afin d'étudier la mise en place de la QoS sur ses accès.

3.1.9. Niveau de service

Les engagements de service de l'opérateur envers l'accès Télécom du partenaire seront définis dans le contrat signé entre l'opérateur et le partenaire. Différents niveaux de service peuvent être proposés par les différents opérateurs ; charge au partenaire de contractualiser comme il le souhaite en fonction des offres des providers. Comme dans le cadre d'un abonnement MPLS classique, des pénalités pourront être réglées par l'opérateur en cas de non-respect des engagements contractuels.

La Banque de France ne pourra être tenue pour responsable de la défaillance d'un opérateur.

3.2. Contacts opérateurs

Les contacts commerciaux opérateurs à utiliser dans le cadre du projet sont les suivants :

- **BT :**

Christophe CAVAZZA

01 56 52 84 53

Christophe.cavazza@bt.com

- **Colt :**

Jean-Yves MONTABORD

01 70 99 55 39

Jean-yves.montabord@colt.net

- **Completel :**

Artur DULKO
01 72 75 53 37
a.dulko@completel.fr

- **OBS :**

Corinne Chantepie
01 56 66 11 63
corinne.chantepie@orange-ftgroup.com
Laurent Piedallu
01 56 66 03 73
laurent.piedallu@orange-ftgroup.com

- **SFR :**

Manuela BOISRAMÉ
01 70 18 23 87
Manuela.boisrame@sfr.com

Il revient au partenaire de prendre contact et de négocier directement avec les opérateurs ; la Banque de France ne dispose pas du catalogue, ni des tarifs des opérateurs.