CONTRAT OPERA Office
CONDITIONS PARTICULIERES 24.01

Annexe 2A – STAS OPERA Office Basic

OPERA
OFFICE

axione
animons le monde

Table des matières

Liste des Figures

Liste des Tableaux

1. PRESENTATION DU DOCUMENT

Ce document décrit les conditions techniques d'accès au service OPERA Office Basic.

Il se compose des parties suivantes :

- Présentation du Service ;
- Description de l'infrastructure de collecte ;
- Description des interfaces de livraison (abonné et collecte) ;
- Gestion des abonnés ;
- Echanges RADIUS entre le Client et le Fournisseur ;
- Règles de Quality Of Service (QoS).

Le respect des conditions décrites dans le présent document est fondamental pour la garantie de fourniture du service par le Fournisseur. Le Fournisseur ne pourrait pas garantir la fourniture du service dans le cas de non-respect de ces conditions.

Dans ce document les termes « Client », « Abonné » et « ONT » ont la signification suivante :

- Client : fait référence au Client ou l'usager utilisant les infrastructures de collecte et transport du Fournisseur afin de délivrer un service à ses utilisateurs ;
- Abonné : fait référence à un utilisateur final de type professionnel ayant souscrit un service auprès du Client ;
- ONT : Optical Network Terminal, fait référence à l'équipement de terminaison PON installé chez l'abonné.

2. DESCRIPTION DU SERVICE

2.1 Description générale du service

Le service OPERA Office Basic est une offre de collecte de trafic depuis des Locaux FTTH permettant à un opérateur de services, client du Fournisseur, d'assurer le raccordement et la collecte de ses abonnés professionnels à travers les infrastructures fibres optiques.

L'offre comprend le transport du trafic IP unicast Abonné jusqu'au site de livraison défini conjointement par le Client et le Fournisseur.

Le trafic IP unicast Abonné est acheminé, selon les règles de transport et d'authentification énoncées ci-dessous :

Service	Accès Abonné	Transport / Livraison	Identification Client	Authentification Abonné (à faire par le Client)
Data	PPPoE	L2TP sur Ethernet	Basée sur le Realm	RADIUS : Identifiant / mot de passe

Tableau 1 - Liste des flux transportés

Les caractéristiques du service sont les suivantes :

- Livraison du service chez l'Abonné sur une interface Ethernet ;
- Débit d'accès de la OPERA Office Basic permet au Client, selon les caractéristiques des infrastructures optiques, de proposer des services Data avec des débits asymétriques et non garantis jusqu'à 1 Gbits/s dans le sens descendant, et jusqu'à 500 Mbits/s dans le sens montant. Cependant AXIONE garanti 20Mbits/s dans les deux sens ;
- Identification de l'Abonné basée sur le Realm de l'identifiant PPP ;
- Collecte PPPoE et livraison en L2TP ;
- Adressage Abonné IPv4, IPv6 ou dual stack IPv4/IPv6 géré par l'opérateur Client ;

- Ségrégation du trafic dans un contexte MPLS/VPN dans le réseau du Fournisseur ;
- Point d'interconnexion avec le réseau du Client :
    - Porte de livraison Nationale, située dans un POP Fournisseur ou dans un POP opérateur Tiers éligible au service ;
    - Redondance possible avec une seconde porte de même catégorie.

L'accès Abonné est basé sur un modèle Point-Multipoint avec une technologie PON.

2.2 Schémas de principe

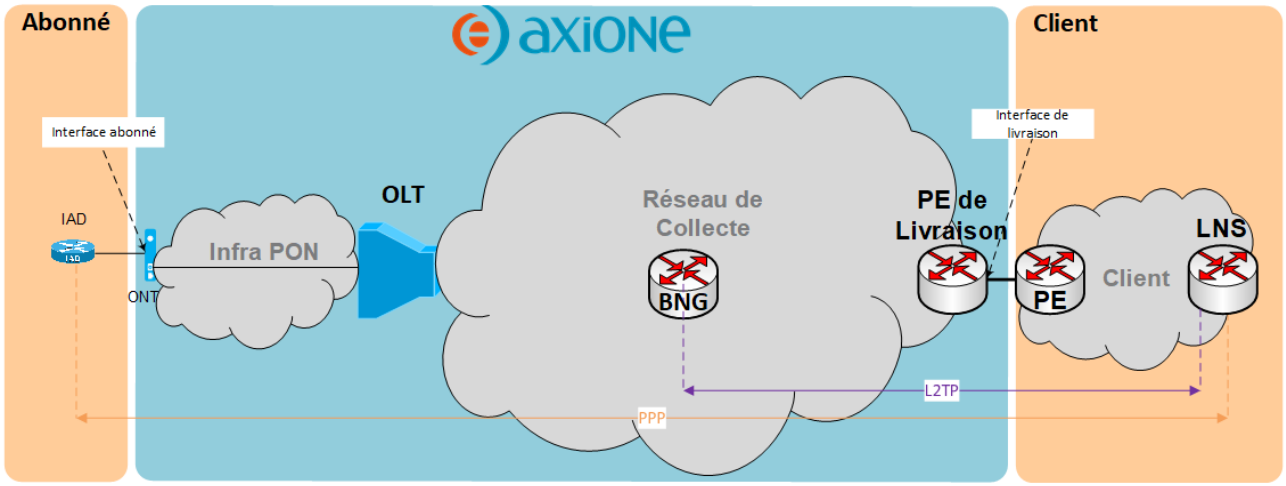


Figure 1 - Schéma de principe

Les infrastructures d'accès Point-Multipoint sont en liaison avec un réseau de collecte Ethernet (Eth/MPLS) pour joindre les BNGs du Fournisseur. Elles s'appuient d'une part sur des équipements de commutation Ethernet, tels que ONT/OLT pour l'accès, et d'autre part sur des équipements de commutation de labels MPLS pour la collecte.

Dans ces réseaux de collecte Ethernet, le cloisonnement des flux Client est assuré par l'implémentation d'une instance de commutation dont une des spécificités est d'interdire l'échange de trafic entre Abonnés.

Les équipements de commutation Ethernet ainsi que ceux du domaine Eth/MPLS apprennent les adresses MAC tel que décrit dans les standards IEEE 802.1D et RFC 4762.

Les BNGs ont pour rôle d'appliquer la limitation de débit des abonnés et d'établir un tunnel L2TP (rôle LAC) jusqu'au LNS Client.

Les collectes d'abonné sont gérées par 2 BNGs nationaux redondants en mode active/active.

2.3 Classes de service réseau

L'offre OPERA Office Basic, ne comprend qu'une seule classe de service Best Effort. Le réseau du Fournisseur ne prend pas en compte le marquage Client. Tous les flux sont transportés en Best Effort dans le réseau du Fournisseur.

3. INFRASTRUCTURE DE COLLECTE

3.1 Collecte Point-Multipoint

3.1.1 Synoptique

Les arbres PON peuvent adresser de 16 à 128 abonnés au maximum. Certains arbres PON peuvent être restreints à 16 abonnés afin de servir les Points de Mutualisation les plus éloignés de leur NRO et préserver le budget optique total des lignes des abonnés. Le schéma ci-après modélise quelques exemples de solutions de raccordement possibles des abonnés sans en dresser la liste exhaustive :

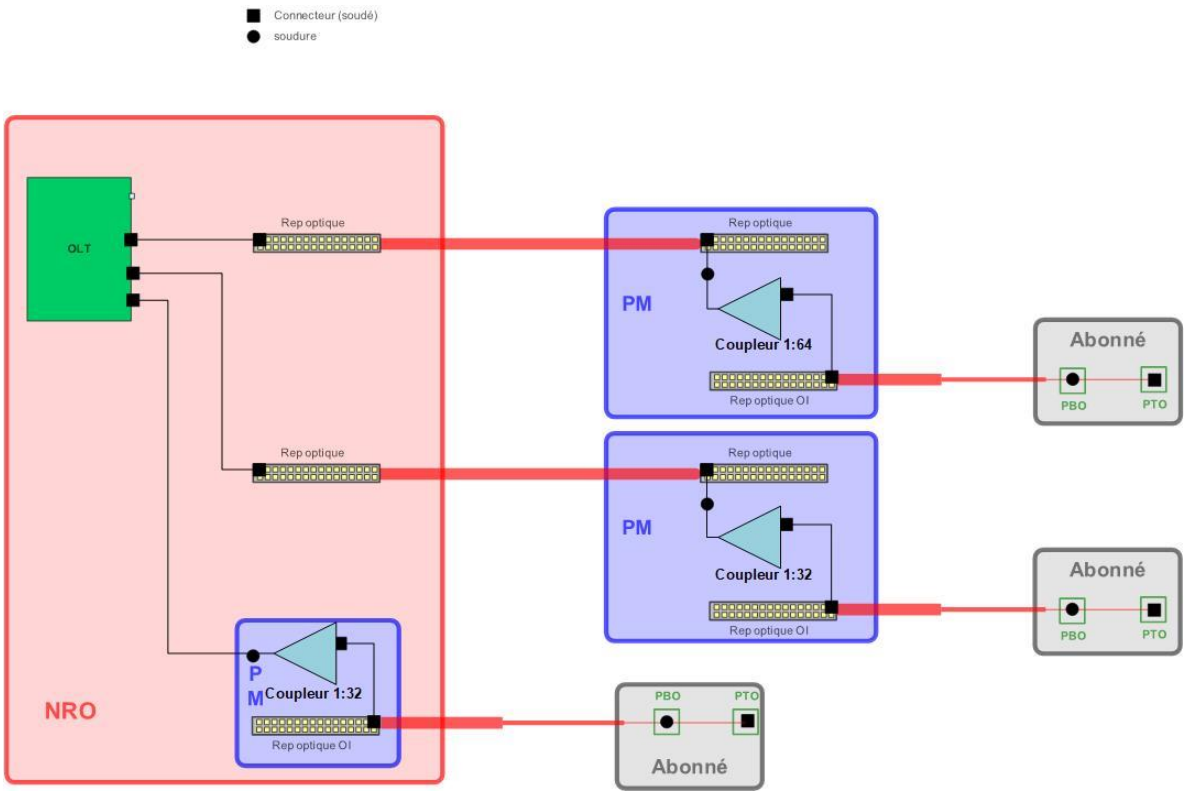


Figure 2 - Modélisation ODN

Les NRO peuvent prendre le rôle de PM afin de raccorder des abonnés.

L'utilisation de coupleurs 1:8, 1:16, 1:32 ou 1:64 dans les points de mutualisation est fonction de la distance PM / NRO.

3.1.2 Caractéristiques des éléments actifs

3.1.2.1 ONT

L'ONT est un équipement d'intérieur pourvu d'une alimentation externe en 220v AC. L'Abonné doit fournir une prise électrique permettant son alimentation.

C'est un modèle Bridge Ethernet dont les ports ont les caractéristiques suivantes :

- Port optique avec connecteur SC-APC ;
- Port cuivre gigabit-Ethernet par interface Abonné.

3.1.2.2 OLT

L'OLT est une plate-forme multiservices de haute capacité dont l'architecture du châssis permet de satisfaire aux besoins actuels et futurs. De fait, elle est adaptée au marché des services résidentiels ou entreprises hauts débits (FTTH, FTTB, FTTO) tout en permettant de déployer simultanément plusieurs technologies d'accès basée sur la fibre optique.

L'OLT supporte les types d'accès listés ci-après :

- GPON ;
- EPON ;
- NG-PON (XG-PON, XGS-PON...) ;
- P2P Fast-Ethernet/Gigabit-Ethernet/TenGigabit-Ethernet.

4. INTERFACE D'ACCES AU SERVICE

Le service OPERA Office Basic définit deux interfaces permettant, d'une part, le raccordement de l'installation Abonné (interface Abonné), et d'autre part, l'interconnexion entre le Client Opérateur de services et celui du Fournisseur (interface de Livraison).

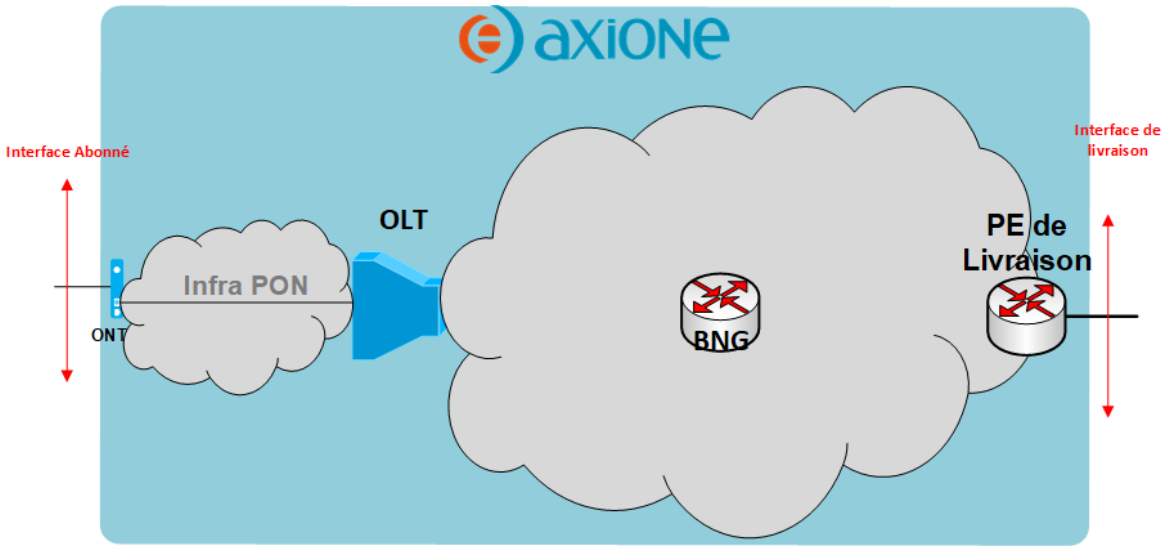


Figure 3 - Interfaces de service

4.1 L'interface Abonné

L'interface Abonné est de type cuivre, son débit peut prendre les valeurs 10 Mbps, 100 Mbps ou 1000 Mbits/s.

Les types d'interfaces d'accès supportées sont listés dans le tableau ci-dessous :

Topologie	Type Interface	Debit interface	Média	Portée (mètres)	Connecteur	Normes
Point-Multipoint GPON	1000-BaseT	1000 Mbit/s	4 paires de cuivre Impédance 100 Ohms Câble UTP 6	100m		IEEE 802.3ab ISO/IEC 8802.3
Point-Multipoint GPON	100-BaseT	100 Mbit/s	2 paires de cuivre Impédance 100 Ohms Câble UTP 5 minimum	100m	RJ-45 ISO 8877	IEEE 802.3u ISO/IEC 8802.3

Point-Multipoint GPON	10-BaseT	10 Mbit/s	2 paires de cuivre Impédance 100 Ohms Câble UTP 5	100m	(support for automatic inversion MDI / MDIX)	IEEE 802.3i ISO/IEC 8802.3

Tableau 2 - Caractéristiques de l'interface de service Abonné

Remarque :

L'indication de portée est conforme au standard ISO/IEC 8802.3. Il conviendra de tenir compte des pertes inhérentes aux divers points de coupure (répartiteurs, catégorie des câbles et des jarretières utilisées) et de recalculer la longueur maximale admissible.

Le connecteur est de type ISO 8877 (RJ 45) femelle, il est présenté par la figure suivante :

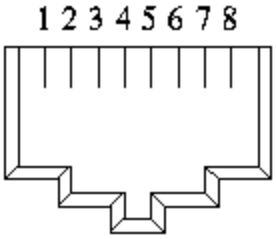


Figure 4 - Connecteur femelle RJ45

4.1.1 Spécifications du port Ethernet de l'ONT

Les caractéristiques physiques de l'interface Ethernet sont :

- Interface Cuivre ;
- Connecteur RJ-45 femelle ;
- Vitesse auto : 10/100/1000 Mbit/s ;
- Port MDI / MDI-X avec détection automatique du câble droit ou croisé.

4.1.2 Raccordement Abonné sur interface 10-BaseT ou 100-BaseT

Appairage des paires de cuivre et le brochage du connecteur sont présentés dans les tableaux ci-dessous :

Media	Paires utilisées
2 paires	(1 ; 2) et (3 ; 6)

Pin	Signal	Direction	Description
1	TxD +	→	Transmission de données vers l'équipement terminal (+)
2	TxD -	→	Transmission de données vers l'équipement terminal (-)
3	RxD +	←	Réception de données provenant de l'Equipement Terminal (+)
4	NC		Non utilisé
5	NC		Non utilisé
6	RxD -	←	Réception de données provenant de l'Equipement Terminal (-)
7	NC		Non utilisé
8	NC		Non utilisé

Tableau 3 - Appairage et Brochage du connecteur pour interface 10 Base-T ou 100 Base-T

Le raccordement de l'équipement Abonné doit être réalisé avec un câble dont les caractéristiques sont au moins équivalentes à la catégorie 5.

L'interface Ethernet de l'équipement Abonné doit être conforme à la norme IEEE 802.3u (100-BaseT) ou IEEE 802.3i (10-BaseT).

4.1.3 Raccordement Abonné sur interface 1000-BaseT

Appairage des paires de cuivre et le brochage du connecteur sont présentés dans les tableaux ci-dessous :

Media	Paires utilisées
4 paires	(1 ; 2) (3 ; 6) (4 ; 5) et (7 ; 8)

Pin	Signal	Direction	Description
1	BI_DA+	⟷	paire Bi-directionnelle A +
2	BI_DA-	⟷	paire Bi-directionnelle A -
3	BI_DB+	⟷	paire Bi-directionnelle B +
4	BI_DC+	⟷	paire Bi-directionnelle C +
5	BI_DC-	⟷	paire Bi-directionnelle C -
6	BI_DB-	⟷	paire Bi-directionnelle B -
7	BI_DD+	⟷	paire Bi-directionnelle D +
8	BI_DD-	⟷	paire Bi-directionnelle D -

Tableau 4 - Appairage et Brochage du connecteur pour interface 1000 Base-T

Le raccordement de l'équipement Abonné doit être réalisé avec un câble dont les caractéristiques sont équivalentes à la catégorie 6.

L'interface Ethernet de l'équipement Abonné doit être conforme à la norme IEEE 802.3ab (1000-BaseT) et configurée en mode auto-négociation avec une vitesse de transmission de 1000 Mbits/s.

4.1.4 Spécifications IP

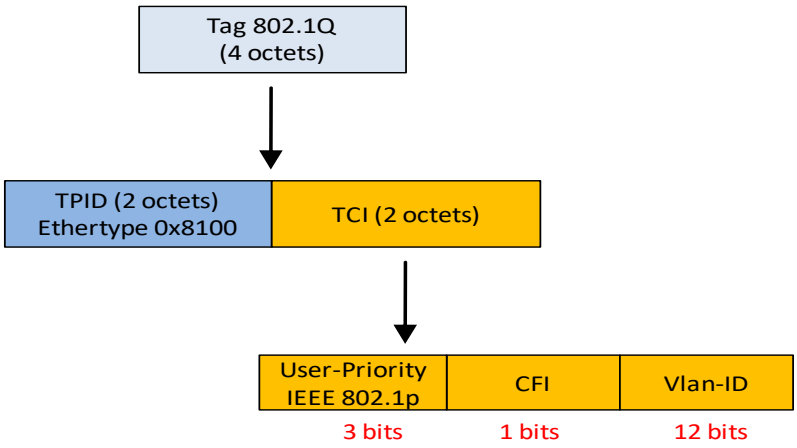
L'IAD Client ne doit pas envoyer vers le réseau des paquets IP avec une taille supérieure à 1500 octets.

4.1.5 Format des trames prises en charge

Les trames envoyées par l'IAD Client doivent correspondre à la norme IEEE 802.1Q et doivent avoir le format suivant :

DA (6 octets)	SA (6 octets)	Tag 802.1Q (4 octets)	Type/ Length (2 octets)	Data (46 à 1 500 octets)	FCS (4 octets)

La taille du tag 802.1Q est de 4 octets et se décompose de la façon suivante :



- TPID est un champ de contrôle définissant le type de tag. **La valeur de ce champ doit être fixée à 0x8100** ;
- TCI est constitué de 3 éléments :
  - 3 bits User-Priority définis par l'IEEE 802.1P. **Ces 3 bits doivent être fixés à 0** ;
  - 1 bit CFI (Canonical Format Indicator) qui détermine si le tag s'applique à une trame de type ethernet ou token-ring. **Ce bit doit être à 0** ;
  - 12 bits VID (VLAN Identifier) pour identifier le numéro du VLAN auquel la trame appartient, soit au total 4 096 VLANs. **Le VID doit être à 4001**.

4.2 L'interface de Livraison

L'interface de Livraison livre l'ensemble du trafic montant et descendant des abonnés sur le réseau de l'opérateur Client.

Elle est matérialisée par une ou plusieurs portes de livraison situées dans des points de présence du Fournisseur.

Le Client a la possibilité de souscrire au maximum deux portes. Lorsque le trafic est livré sur deux portes, il n'y a pas de partage de charge : une porte nominale et une porte de secours. La porte de secours peut avoir un débit inférieur à la porte nominale.

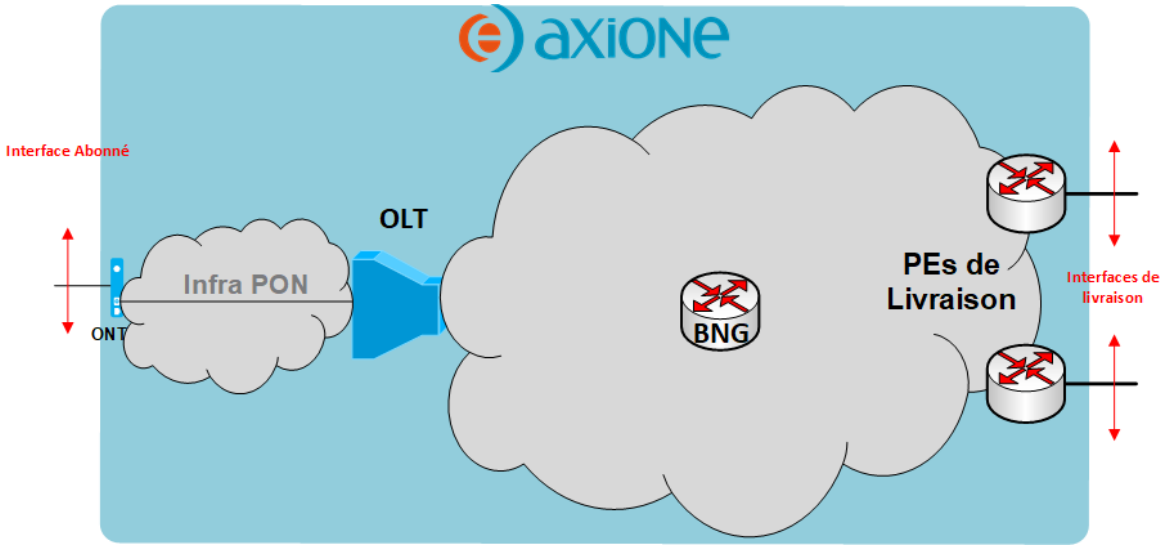


Figure 5 - Sécurisation de l'interface de Collecte

Afin d'autoriser la cohabitation des flux Unicast Abonné et les échanges RADIUS, des interfaces logiques (VLAN) distinctes sont définies sur l'interface de collecte :

- Un VLAN **Data** ;
- Un VLAN **RADIUS**.

L'interface de livraison peut être composée de plusieurs ports physiques, dans ce cas le protocole LACP devra être configuré par le Client.

4.2.1 Spécification des interfaces physiques

Seul l'accès fibre optique est disponible, les caractéristiques de l'interface sont les suivantes :

Type Interface	Debit interface	Média	Portée (mètres)	Type Fibre	Connecteur	Normes
1000Base-LX	1 Gbit/s	Fibre Optique Monomode	10Kms	Duplex	LC/PC	IEEE 802.3z ISO/IEC 8802.3
10GBase-LR	10 Gbits/s	Fibre Optique Monomode	10Kms	Duplex	LC/PC	IEEE 802.3ae

Tableau 5 - Caractéristiques de l'interface de Livraison

Remarque :

- L'indication de portée est conforme au standard ISO/IEC 8802.3. Il conviendra de tenir compte des pertes inhérentes aux divers points de coupure (répartiteurs optiques, pertes liées aux connecteurs des jarretières) et de recalculer la longueur maximale admissible.
- Sur ces interfaces, le client ne doit pas activer de mécanismes de spanning-tree. Il ne doit pas envoyer de paquets BPDU sur le port d'interconnexion.

4.2.2 Interconnexion IP

Comme spécifié au paragraphe 4.2, deux VLANs sont définis sur les interfaces de Livraison afin de séparer les échanges RADIUS des flux Data :

- Un VLAN **Data** pour le transport des flux data des abonnés ;
- Un VLAN **RADIUS** pour les échanges RADIUS.

Les numéros de VLAN sont spécifiés dans la fiche d'interconnexion.

Deux réseaux IP d'interconnexions sont nécessaires pour acheminer les échanges RADIUS et les flux Data :

- Un réseau en adressage ip **publique** IPv4 de type /30 ou /31 pour l'interconnexion **RADIUS** ;
- Un réseau en adressage ip **publique ou privée** IPv4 de type /30 ou /31 pour le VLAN **Data** Unicast.

Pour les adressages IP publiques, le Client doit disposer d'un numéro d'AS public.

Une session eBGP est établie entre le Fournisseur et le client ISP au niveau de chaque VLAN de l'interface de Livraison.

4.2.2.1 Caractéristiques de la session eBGP data

- Adressage IP fourni par le client ISP ;
- La fonctionnalité GTSM (RFC 5082) peut être activée pour sécuriser à minima la session eBGP en contrôlant qu'elle est établie avec le premier équipement IP joignable par cette interconnexion ;
- La fonctionnalité BFD peut être activée pour optimiser la durée de détection de la perte de la session eBGP ;
- Le Fournisseur annonce les préfixes BGP contenant les adresses IPv4 de ses LAC ;
- Le Client annonce les préfixes BGP contenant les adresses IPv4 de ses LNS ;

- Le Fournisseur appliquera un filtre sur les annonces BGP-4 du Client pour autoriser uniquement les adresses faisant partie des blocs d'adresses LNS préalablement déclarés par le Client ;
- Les communautés utilisées par le client seront ignorées sur le réseau du Fournisseur.

4.2.2.2 Caractéristiques de la session eBGP RADIUS

- Adressage IP fourni par le client ISP ;
- La fonctionnalité GTSM (RFC 5082) peut être activée pour sécuriser à minima la session eBGP en contrôlant qu'elle est établie avec le premier équipement IP joignable par cette interconnexion ;
- La fonctionnalité BFD peut être activée pour optimiser la durée de détection de la perte de la session eBGP ;
- Le Fournisseur annonce les adresses IPv4 de ses Proxy RADIUS ;
- Le Client annonce les adresses IPv4 de ses serveurs RADIUS ;
- Le Fournisseur appliquera un filtre sur les annonces BGP-4 du Client pour autoriser uniquement les adresses faisant partie des blocs d'adresses des serveurs RADIUS préalablement déclarés par le Client ;
- Les communautés utilisées par le client seront ignorées sur le réseau du Fournisseur ;

4.2.2.3 Attributs BGP

Les routes annoncées en BGP par le Client auront l'attribut local-preference positionné de la manière suivante sur les interfaces de livraison :

Type de livraison	Valeur attribut Local-Pref
Nominale	200
Secours	100

Tableau 6 - Attributs BGP des préfixes échangés

De la même façon, le Client devra marquer avec une locale préférence plus grande les routes apprises sur les interfaces de livraison nominale.

5. ARCHITECTURE DE SERVICE

5.1 Principe et modélisation de la livraison L2TP

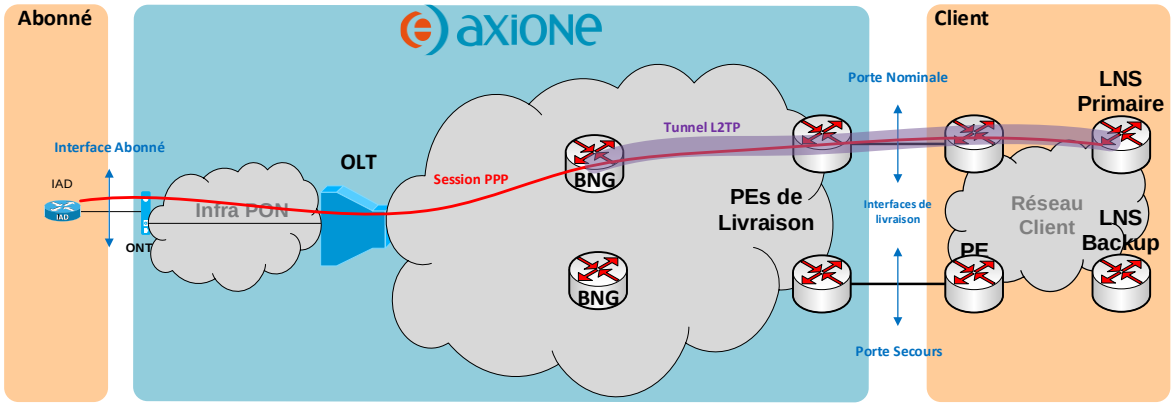


Figure 6 - Architecture PPP livrée en L2TP

Le Fournisseur transporte les sessions PPP initialisées par les IAD jusqu'à l'interface de livraison. Les sessions sont ainsi prolongées et livrées à travers des tunnels L2TP (Layer 2 Tunnelling Protocol - RFC-2661) jusqu'au réseau du client.

Le Fournisseur dispose de BNGs redondants qui jouent le rôle de LAC. Les tunnels L2TP sont établis en IPv4 entre les BNGs et un ou plusieurs LNS client.

En préalable à l'établissement des tunnels L2TP et des sessions PPP, une vérification du Realm de l'identifiant PPP de l'abonné est faite par le Fournisseur pour lui permettre d'identifier le Client. Un dialogue RADIUS est nécessaire entre le Fournisseur et le Client permettant d'échanger les informations nécessaires à l'établissement des tunnels L2TP. Il incombe au Client de gérer l'authentification et la configuration des IAD Abonné.

Ces deux mécanismes permettent un partage des responsabilités entre le Fournisseur et le client :

- Le Fournisseur a la charge du transport des sessions PPP depuis les sites Abonné jusqu'à l'interface de livraison ;
- Le Client est responsable de l'authentification des IAD, la terminaison des sessions PPP des abonnés et leur configuration (assignation d'adresse IP, ...).

Le schéma ci-après modélise les couches protocolaires mises en œuvre :

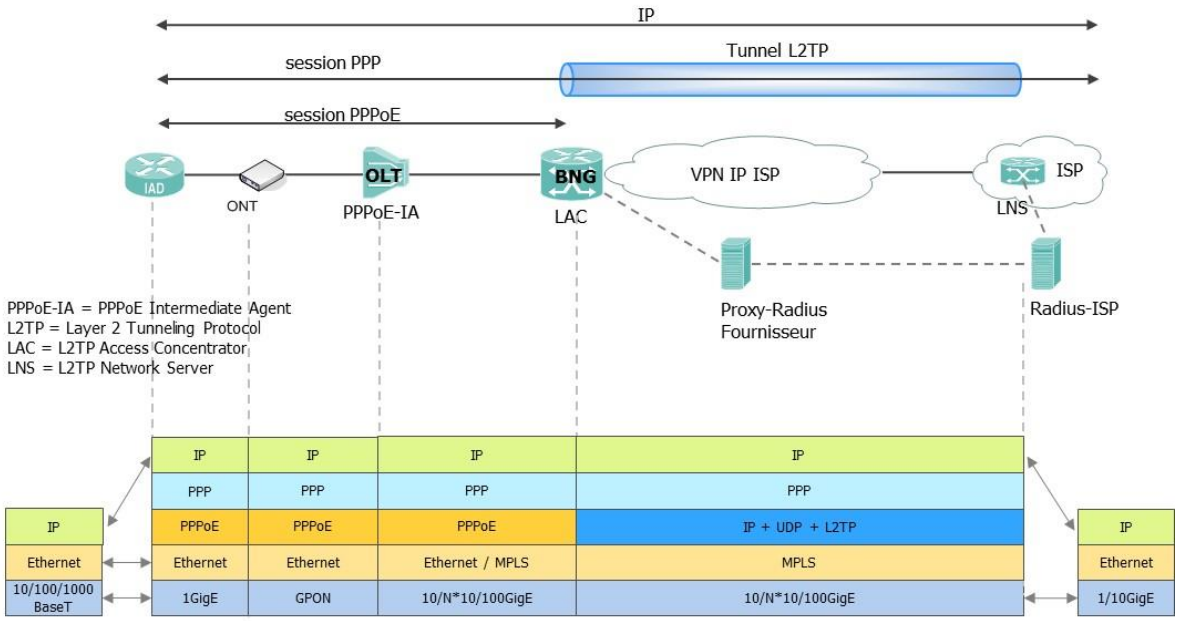


Figure 7 - Transport session PPP dans tunnel L2TP

Pour chaque abonné, une session L2TP est créée à l'intérieur du tunnel. Cette session est négociée au moment de prolonger la session PPP jusqu'au LNS du Client (i.e. une fois que le BNG a autorisé l'abonné).

Une fois le tunnel et la session établis, la session PPP entre l'Abonné et le Client peut être initialisée de façon complètement transparente pour le Fournisseur.

L'initialisation de la session PPP se déroule comme suit :

1. L'IAD initie une session PPPoE pour découvrir les BNG susceptibles de le prendre en charge ;
2. L'IAD initie une session PPP qui est interceptée par le BNG ;
3. Le BNG demande à l'IAD de s'authentifier ;
4. L'IAD envoie les paramètres d'authentification (identifiant / mot de passe) au BNG ;
5. Le BNG envoie une requête RADIUS d'autorisation au Proxy RADIUS Fournisseur ;
6. Le Proxy RADIUS Fournisseur transmet la requête au serveur RADIUS du Client ;
7. Le serveur RADIUS du client authentifie l'IAD et envoie un message d'autorisation au BNG (relayé par le Proxy RADIUS Fournisseur) ;
8. Le BNG prolonge la session PPP jusqu'au LNS du Client à travers un tunnel L2TP ;
9. L'IAD s'authentifie auprès du Client et récupère ses paramètres réseaux.

5.2 Tunnel L2TP

Le tunnel L2TP est créé entre deux équipements : le LAC (L2TP Access Concentrator) et le LNS (L2TP Network Server).

La fonction de LAC est assurée par un équipement Fournisseur identifié par une adresse IP publique ou privée que le Client aura fournie dans la fiche d'interconnexion.

La fonction de LNS doit être assurée par un équipement sous la responsabilité du Client. Le LNS est identifié par une adresse IP publique ou privée que le client aura fournie dans la fiche d'interconnexion.

La méthode de Tunnel L2TP implique plusieurs protocoles (PPP/L2TP/UDP/IP) pour transporter les paquets IP des abonnés à travers les réseaux Fournisseur et Client. La décomposition de cette surcouche est précisée ci-après :

- Entête PPP = 4 voire 8 octets max ;
- Entête L2TP = 16 octets max ;
- Entête UDP (port 1701) = 8 octets ;
- Entête IP = 20 octets.

La surcouche protocolaire entraine par conséquent un overhead de 52 octets maximums pour le trafic IP des abonnés et 44 octets en considérant uniquement le transport des sessions PPP pour le présent service.

Aussi, afin de se prémunir de problème MTU, l'interface du LNS ainsi que celle du LAC sur laquelle est monté le tunnel L2TP doit avoir une MTU égale à 2000. Les équipements intermédiaires (entre le LAC et le LNS) doivent avoir aussi une MTU supérieure ou égale à 2000.

Le tunnel L2TP doit être établi dynamiquement : le serveur RADIUS du Client communique les informations nécessaires à son établissement. L'établissement du tunnel suit le processus suivant :

- Un IAD abonné lance une demande de connexion via une requête PPP ;
- Sur réception de cette requête, le Fournisseur envoie un message RADIUS access_request au serveur RADIUS du Client ;
- Le serveur RADIUS du Client répond par un message access_accept précisant le tunnel L2TP dans lequel transporter la session PPP de l'abonné ;
- Dans le cas où le tunnel n'est pas encore créé, le LAC Fournisseur négocie l'établissement du tunnel L2TP avec le LNS du client.

Une sécurisation du LNS peut être mise en place. Pour cela, le client doit disposer d'un LNS primaire et d'un LNS de backup. Les attributs L2TP du message RADIUS « access-accept » doivent, dans ce cas, être tagués. Le Fournisseur prendra en compte l'attribut « tunnel-preference » pour identifier le LNS primaire. En cas d'échec lors de la tentative de création du tunnel sur le LNS primaire, le tunnel.

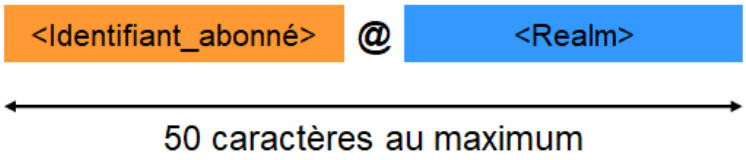
5.3 Format de l'identifiant et du mot de passe abonné

Le Client doit identifier ses abonnés sur la base de leur identifiant PPP.

Lors de la phase d'authentification, l'abonné se présente à travers le couple « identifiant / mot de passe » attribué par le Client. Le protocole d'authentification CHAP devra être utilisé pour l'authentification des abonnés.

Le format de l'identifiant devra être composé d'un maximum de 50 caractères et avoir le format <identifiant_abonné>@<Realm> :

- <identifiant_abonné> est une valeur alphanumérique. La chaîne de caractère doit contenir au moins un caractère ;
- <Realm> est une valeur alphanumérique qui identifie le Client. Le Client indique au moment de la commande le « Realm » à utiliser. Le Realm doit respecter les règles suivantes :
    - Le Client ne doit pas utiliser un identifiant correspondant à un terme déposé à l'ICANN (Internet Corporation for Assigned Names and Numbers) ;
    - Le Client ne pourra pas utiliser un Realm s'il est déjà utilisé par un autre Client ;
    - Il doit terminer par le suffixe « <fai>.ohb.axione.fr » (où <fai> est le nom du Client).



Le « mot_de_passe » utilisé par le client pour identifier un abonné devra être une valeur en alphanumérique.

Le Fournisseur définit un caractère alphanumérique comme tout caractère alphabétique de A à Z ou chiffre de 0 à 9. Un même caractère en majuscule et minuscule représente deux caractères alphabétiques différents.

5.4 Adressage IP des abonnés

Les IAD peuvent être adressés en IPv4, IPv6 ou dual stack IPv4/IPv6.

Le choix des adresses des IAD Abonné est de la responsabilité du Client. Le Fournisseur ne participe pas au routage des adresses du Client.

5.5 Profil de QoS Abonné PPP

Un seul profil QoS est disponible pour cette offre. Ce profil QoS ne comprend qu'une seule classe de service Best Effort. Un PIR global est défini pour l'abonné pour l'ensemble des files d'attentes. Tout le trafic Abonné doit être transporté en Best Effort.

Les valeurs de ce profil sont données dans le tableau ci-dessous :

Service	CIR Up	PIR Up	CIR Down	PIR Down
DATA	0M	500M	0M	1G

Le débit pour un abonné est : 1Gbps / 500Mbps.

5.5.1 Trafic descendant

Dans le sens Client vers l'Abonné, afin de respecter le marquage, le Client devra placer la valeur des 3 bits de poids fort du champ DSCP (ou IP Precedence) de l'entête IP des paquets de l'Abonné dans l'entête IP ajoutée et utilisée pour la session L2TP à **0**.

5.5.2 Trafic montant

Dans le sens Abonné vers Client, afin de respecter le marquage, le CPE abonné devra marquer la valeur des 3 bits de poids fort du champ DSCP (ou IP Precedence) à **0**.

5.6 RADIUS

5.6.1 Proxys RADIUS Fournisseur et serveur RADIUS Client

Le Fournisseur dispose d'un proxy RADIUS qui relaye les flux RADIUS (authentification et accounting) des abonnés jusqu'aux serveurs RADIUS du client. Le Client est responsable de l'authentification et du comptage.

Le Client peut installer un ou plusieurs serveurs RADIUS pour l'authentification des abonnés et un ou plusieurs serveurs pour le comptage. Le partage de charge entre les différents serveurs est possible sur le proxy RADIUS Fournisseur. L'algorithme Round Robin permet de distribuer uniformément les requêtes sur les différents serveurs RADIUS.

Le Client peut regrouper la fonction d'authentification et comptage sur les mêmes serveurs RADIUS.

Lors de la souscription au service, le client communiquera au Fournisseur :

- L'adresse IP publique du ou des serveurs RADIUS d'authentification ;
- L'adresse IP publique du ou des serveurs RADIUS de comptage ;
- Le secret RADIUS (mot de passe partagé entre le Serveur RADIUS et le Proxy RADIUS).

Le Client et le Fournisseur devront convenir d'un numéro de port UDP à utiliser pour les communications RADIUS entre le Proxy RADIUS et le serveur RADIUS. Le Fournisseur propose l'utilisation du port standard UDP 1812 pour l'authentification et 1813 pour le comptage.

Mécanisme Status-Server :

La fonctionnalité Status-Server (RFC 5997) doit être activée sur les serveurs Radius Client. Cette fonctionnalité est une extension du protocole RADIUS permettant à un client radius (ici les proxys RADIUS Fournisseur) de vérifier l'état opérationnel d'un serveur radius (ici les serveurs RADIUS Client). Il faut noter que ce mécanisme n'est pas équivalent à un "Keep Alive" permanent et transmis à travers un Access-Requets (RFC2865), mais est déclenché par le client radius lorsque le serveur radius est soupçonné d'être indisponible.

Sur l'absence de réponse à un Access-Request, le client radius envoie immédiatement un message status-server et détermine ensuite l'état opérationnel ou l'accessibilité du serveur par la réception ou l'absence de réponse de ce dernier au message status-server.

Dans le cas d'un radius client disposant de serveurs redondants, un tel mécanisme permet de détecter l'inaccessibilité d'un serveur et solliciter immédiatement un autre serveur sans attendre plusieurs requêtes et l'expiration d'un timeout.

Les messages status-server sont transmis au serveur radius à travers un Access-Request ou un Accounting-Request.

Le radius serveur répond par un message de type Access-Accept (authentication port) ou Accounting-Response (accounting port) aux sollicitations de type request Authenticator.

Sonde Radius :

Le Fournisseur dispose d'un serveur sonde RADIUS pour effectuer des statistiques de joignabilité RADIUS avec le serveur RADIUS client.

Lors de la souscription au service, le client communiquera au Fournisseur :

- Un couple « User-name » / « User-password » dédié à la sonde RADIUS ;
- Le secret RADIUS (par défaut il sera identique à celui partagé entre le Serveur RADIUS et le Proxy RADIUS).

Le Client devra, au même titre que pour les proxys RADIUS du Fournisseur, autoriser la sonde RADIUS à interroger son ou ses serveurs RADIUS.

5.6.2 Attributs RADIUS échangés

Les échanges entre le Proxy RADIUS Fournisseur et les serveurs RADIUS du client sont détaillés ci-dessous. Les attributs RADIUS mentionnés sont définis dans les RFC 2865 et 2868 pour l'authentification et RFC 2866 et 2867 pour le comptage.

Remarque : La liste des attributs radius spécifiés dans les messages ci-après n'est pas exhaustive et peut présenter des différences avec la réalité.

5.6.2.1 Access-Request

Ce message est émis par le Proxy RADIUS Fournisseur vers le serveur RADIUS Client.

Nom de l'attribut	Numéro attribut	Description	Syntaxe
User-name	1	Nom de l'abonné	Voir paragraphe 5.3
NAS-IP-Address	4	Adresse IP du BNG Fournisseur	XXX.XXX.XXX.XXX
NAS-Port-ID	87	NAS port ID	Interface logique de collecte du BNG associée à l'abonné
Service-Type	6	Type du service	Framed
Framed-Protocol	7	Indique la trame à utiliser pour l'accès par trame.	PPP
Acct-Session-Id	44	Identifiant de la session	Session ID
CHAP-Password	3	Mot de Passe CHAP de l'abonné	Password
CHAP-Challenge	60	Challenge CHAP	Challenge

5.6.2.2 Access-Accept

Dans le mode dynamique, le serveur RADIUS du client envoie au BNG les paramètres nécessaires à la création ou à l'identification du tunnel L2TP. Le tableau ci-dessous liste les attributs RADIUS spécifiant le tunnel L2TP à utiliser. Ces attributs sont ajoutés au message « access_accept » envoyé par le serveur RADIUS du client.

Nom de l'attribut	Numéro de l'Attribut	Description
Tunnel-Type	64	Type de tunnel à établir : valeur fixée à 3 pour L2TP
Tunnel-Medium-Type	65	Type de protocole de transport : valeur fixée à 1 pour IPv4
Tunnel-Server-Endpoint	67	Adresse IP du LNS terminant le tunnel L2TP
Tunnel-Assignment-ID	82	Cet attribut détermine l'identificateur du tunnel L2TP qui sera ultérieurement utilisé par le BNG pour déterminer le tunnel à utiliser pour le transport de chacun des paquets des abonnés. Ce champ doit contenir l'adresse IP du LNS.

Le Client peut envoyer la description de 2 tunnels. Les attributs doivent dans ce cas être tagués conformément à la RFC 2868. Pour chaque tunnel, le client doit renseigner l'attribut « tunnel-préférence ». Le BNG Fournisseur prend en compte cet attribut pour identifier le tunnel L2TP primaire et le tunnel L2TP de Backup (le tunnel primaire est celui ayant la préférence la plus faible).

Caractéristiques de l'attribut « Tunnel-Preference » :

Nom de l'attribut	Numéro de l'Attribut	Description
Tunnel-Preference	83	Préférence permettant de définir le tunnel L2TP primaire (celui qui a la préférence la plus faible)

Remarques : Les attributs RADIUS permettant de caractériser les tunnels L2TP sont spécifiés dans la RFC 2868.

Le Client peut demander que le LAC Fournisseur (BNG) envoie une valeur spécifique de l'Attribute Value Pairs (AVPs) Host Name (Attribute Type 7, RFC 3931) lors de l'établissement du tunnel L2TP. Le Client déclara cette valeur au Fournisseur, à travers la fiche d'interconnexion.

5.7 Synthèse des échanges pour l'établissement d'une session

Le schéma ci-dessous synthétise les messages PPP, L2TP et RADIUS échangés lors de l'ouverture d'une session PPP.

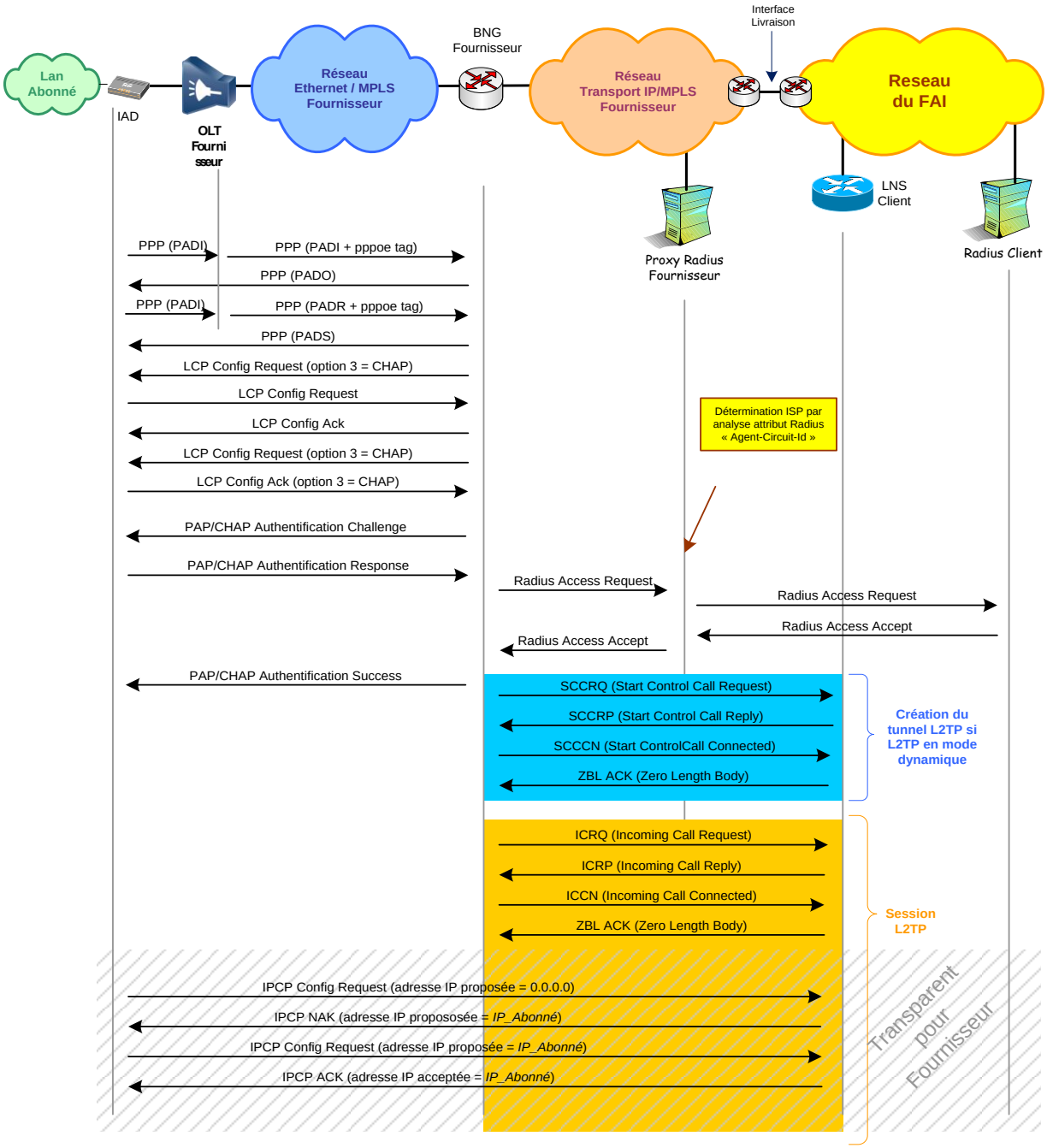


Figure 8 – Synthèse des échanges pour la création d'une session PPP-L2TP

ANNEXE 1 : GLOSSAIRE

BGP	Border Gateway Protocol
BNG	Broadband Network Gateway
CIR	Committed Information Rate
DSCP	Differenciated Service Code Point
EPON	Ethernet Passive Optical Network
FTTB	Fiber to the Building
FTTO	Fiber to the office
FTTH	Fiber to the Office
GPON	Gigabit Passive Optical Network
IAD	Integrated Access Device
L2TP	Layer Two Tunneling Protocol
LAC	L2TP Access Concentrator
LNS	L2TP Network Server
NG-PON	Next Generation Passive Optical Networks
NRO	Nœud de Raccordement Optique
OLT	Optical Line Terminal
ONT	Optical Network Terminal
P2P	Point to Point
PIR	Peak Information Rate
PPP	Point-to-Point Protocol
PPPOE	Point-to-Point Protocol over Ethernet
RFC	Request For Comment
VLAN	Virtual LAN
VPN	Virtual Private Network
XG-PON	10 Gigabit Passive Optical Network
XGS-PON	10 Gigabit Symmetrical Passive Optical Network