

STAS

Ligne OPERA Office

Version 20.01 – Juillet 2020



Sommaire

1. Présentation du Document	5
2. Description du service Ligne OPERA Office	6
2.1. Description générale du service.....	6
2.2. Schémas de principe	7
2.3. Classes de service réseau.....	9
3. Infrastructures de Collecte.....	10
3.1. Collecte Point-Multipoint	10
3.1.1. Synoptique.....	10
3.1.2. Caractéristiques des éléments actifs.....	11
3.1.2.1. ONT.....	11
3.1.2.2. OLT	12
3.2. Format du Circuit-Id	12
3.2.1. Circuit-Id	12
3.2.2. DHCPv4.....	13
3.2.2.1. Agent Circuit-ID.....	13
3.2.2.2. Agent Remote-ID	13
3.2.3. DHCPv6.....	13
3.2.3.1. Interface-ID	13
3.2.3.2. Relay Agent remote-ID	13
3.2.4. PPPoE Tag.....	13
3.2.4.1. Agent Circuit-ID.....	13
3.2.4.2. Agent Remote-ID	14
3.2.5. Sysname.....	14
3.2.6. Format du Circuit-ID spécifique aux OLTs	14
4. Interfaces d'accès au service	16
4.1. L'interface Abonné.....	16
4.1.1. Spécifications du port Ethernet de l'ONT	17
4.1.2. Raccordement Abonné.....	17
4.1.3. Spécifications IP	18
4.2. L'interface de Collecte	18
4.2.1. Spécification des interfaces physiques	20
4.2.2. Interconnexion IP.....	20

5. Mode d'accès et livraison IPoE.....	23
5.1. Gestion IP/DHCP Abonné	23
5.2. Gestion profil de QoS Abonné.....	23
5.3. Paramétrage IP et DHCP	23
5.3.1. Durée de vie des adresses IPv6	23
5.3.2. Compteurs DHCP	24
5.4. Mode DHCP et RADIUS.....	25
5.4.1. Authentification et adressage IP de l'abonné	25
5.4.2. Détail des échanges RADIUS et DHCPv4.....	26
5.4.2.1. DHCPv4-Discover	26
5.4.2.2. DHCPv4-Renew	28
5.4.3. Détail des échanges RADIUS et DHCPv6.....	29
5.4.3.1. DHCPv6-Solicit.....	29
5.4.3.2. DHCPv6-Renew	31
5.5. Mode Full RADIUS.....	32
5.5.1. Authentification et adressage IP de l'abonné	32
5.5.2. Détail des échanges RADIUS et DHCP.....	33
5.5.2.1. DHCPv4-Discover	33
5.5.2.2. DHCPv4-Renew	35
5.5.3. Détail des échanges RADIUS et DHCPv6.....	36
5.5.3.1. DHCPv6-Solicit.....	36
5.5.3.2. DHCPv6-Renew	38
5.5.4. Limitation connue	39
5.6. Adressage IP des abonnés	40
5.6.1. Type d'adressage.....	40
5.6.2. Gestion des pools IP des abonnés	40
5.6.2.1. Mutualisation des pools IP	40
5.6.2.2. Gestion des pools IP par zone dans le réseau du Fournisseur	41
5.6.3. Adresses IP réservées	41
5.7. Profils de QoS Abonné IPoE	41
6. Mode d'accès PPP et livraison L2TP	43
6.1. Principe et modélisation de la livraison L2TP	43
6.2. Tunnel L2TP	45
6.3. Identification Abonné.....	46
6.3.1. Identification sur la base du « User-Name »	46

6.3.2. Identification sur la base du «Agent-Circuit-Id ».....	46
6.4. Adressage IP des abonnés.....	47
6.5. Profils de QoS Abonné PPP	47
6.5.1. Trafic descendant	47
6.5.2. Trafic montant.....	48
7. Echanges RADIUS	49
7.1. Serveurs RADIUS Fournisseur et ISP.....	49
7.2. Echanges RADIUS en mode IPoE.....	50
7.2.1. Access-Request envoyé au client	51
7.2.2. Access-Accept du client	51
7.3. Echanges RADIUS en mode PPPoE	52
7.3.1. Etablissement des tunnels L2TP	52
7.3.2. Synthèse des échanges lors de l'établissement d'une session PPP-L2TP	54
7.3.3. Attributs Radius échangés.....	55
Annexe 1 : Dictionnaire RADIUS.....	57
Annexe 2 : Glossaire	58

Liste des Figures

Figure 1 - Schéma de principe : mode d'accès IPoE	7
Figure 2 - Schéma de principe : mode d'accès PPPoE	8
Figure 3 - Réseau de collecte GPON du service Ligne OPERA Office	10
Figure 4 - Modélisation ODN	11
Figure 5 - Interfaces de service	16
Figure 6 - Connecteur femelle RJ45.....	17
Figure 7 - Sécurisation de l'interface de Collecte	18
Figure 8 - Etats successifs d'une adresse IPv6 sur une interface.....	24
Figure 9 - Mode DHCP et RADIUS (transaction DHCPv4-Discover)	26
Figure 10 - Mode DHCP et RADIUS (renouvellement du Bail DHCPv4)	28
Figure 11 - Mode DHCP et RADIUS (transaction DHCPv6-Solicit)	29
Figure 12 - Mode DHCP et RADIUS (renouvellement du Preferred-Lifetime DHCPv6)	31
Figure 13 - Mode FULL RADIUS (transaction DHCPv4-Discover)	33
Figure 14 - Mode FULL RADIUS (renouvellement du Bail DHCPv4).....	35
Figure 15 - Mode FULL RADIUS (transaction DHCPv6-Solicit).....	36
Figure 16 - Mode FULL RADIUS (renouvellement du Preferred-Lifetime DHCPv6).....	38
Figure 17 - Profil de QoS Abonné OPERA Office en mode IPoE	42
Figure 18 - Architecture collecte PPP livrée en L2TP	43
Figure 19 - Transport session PPP dans tunnel L2TP	44
Figure 20 - Détails des Echanges Radius	50
Figure 21 - Synthèse des échanges pour la création d'une session PPP-L2TP.....	54

Liste des Tableaux

Tableau 1 - Liste des flux transportés	6
Tableau 2 - Correspondance Trafic et CoS Fournisseur.....	9
Tableau 3 - Caractéristiques de l'interface de service Abonné	16
Tableau 4 - Appairage et Brochage du connecteur pour interface 10 Base-T ou 100 Base-T Erreur ! Signet non défini.	
Tableau 5 - Appairage et Brochage du connecteur pour interface 1000 Base-T	17
Tableau 6 - Caractéristiques de l'interface de Collecte	20
Tableau 7 - Attributs BGP des préfixes échangés	22

1. Présentation du Document

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

Il se compose des parties suivantes :

- Présentation du Service OPERA Office ;
- Description de l'infrastructure de collecte ;
- Description des interfaces de livraison (abonné et collecte) ;
- Gestion des abonnés (IP/DHCP, PPP/L2TP) ;
- Echanges RADIUS entre l'ISP et le Fournisseur ;
- Profils de QoS client sur les BNG Fournisseur.

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 tous les cas, la compatibilité des échanges entre le Fournisseur et le client sera validée lors d'une phase de tests préalables au démarrage du service. Des modifications seront étudiées en cas d'incompatibilité.

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

- Client : fait référence au Client ou l'utilisateur utilisant les infrastructures de collecte et transport du Fournisseur afin de délivrer un ou plusieurs services 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 GPON installé chez l'abonné.
- Fournisseur : Fait référence à Nouvelle-Aquitaine THD et à son concessionnaire fournisseur du présent service.

2. Description du service Ligne OPERA Office

2.1. Description générale du service

Le service « Ligne OPERA Office » 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 déployées dans les plaques opérées par le Fournisseur.

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, au choix du client ISP, selon les règles de transport et d'authentification énoncées ci-dessous :

Service	Accès Abonné	Transport / Livraison	Authentification	Identification Abonné
Data/Business/VoIP	IPoE	IP sur Ethernet	RADIUS + DHCP	RADIUS : attribut Agent-Circuit-id DHCPv4/v6 : option 82/18
Data/Business/VoIP	PPPoE	L2TP sur Ethernet	RADIUS	RADIUS : login/password + Agent-Circuit-id

Tableau 1 - Liste des flux transportés

Remarque :

- Dans le mode d'accès IPoE, la ligne est transparente à l'option DHCP 60 ;

Les caractéristiques du service sont les suivantes :

- Livraison du service chez l'abonné sur une interface Ethernet ;
- Débit d'accès de la « Ligne OPERA Office Activée » permet au Client, selon les caractéristiques des infrastructures optiques, de proposer des services Data jusqu'à 1 Gbits/s dans le sens descendant, et jusqu'à 300 Mbits/s dans le sens montant ;
- Authentification Abonné par RADIUS de l'opérateur Client ;
- Collecte et livraison trafic abonné selon 2 modes au choix du client :
 - Collecte IP/DHCP et livraison en IPoE ;
 - Collecte PPPoE et livraison en L2TP ;
- Adressage IP Abonné géré par l'opérateur Client :
 - IPv4 et / ou IPv6 pour le mode d'accès IPoE ;
 - Uniquement IPv4 pour le mode d'accès PPPoE ;
- Dans le mode d'accès IPoE, allocation des IP abonnés par le protocole DHCP (serveur DHCP Client ou Fournisseur suivant le mode retenu « DHCP et RADIUS » ou « Full-RADIUS ») ;
- Gestion dynamique des profils abonnés depuis le serveur RADIUS de l'opérateur Client ;

- Type de service : 3-Play (3 classes de services disponibles) ;
- Contrôle de la bande passante par classe de service (3 bits IP precedence du champ TOS - soit les 3 bits de poids forts du champ DSCP) et global par abonné ;
- Trois classes de services sont disponibles :
 - Data (débit asymétrique de 1 Gbits/s en descendant et 300 Mbits/s en montant)
 - Business (débit symétrique garanti de 10 Mbits/s ou 100 Mbits/s selon souscription)
 - Voix (débit symétrique garanti de 500Kbit/s maximum)
- Dépassement des classes Voix et Business non autorisé ;
- Ségrégation du trafic dans un contexte MPLS/VPN pour chacun des modes d'accès dans le réseau du Fournisseur ;
- Point d'interconnexion avec le réseau du Client :
 - Porte de collecte Locale ou 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 la technologie GPON.

2.2. Schémas de principe

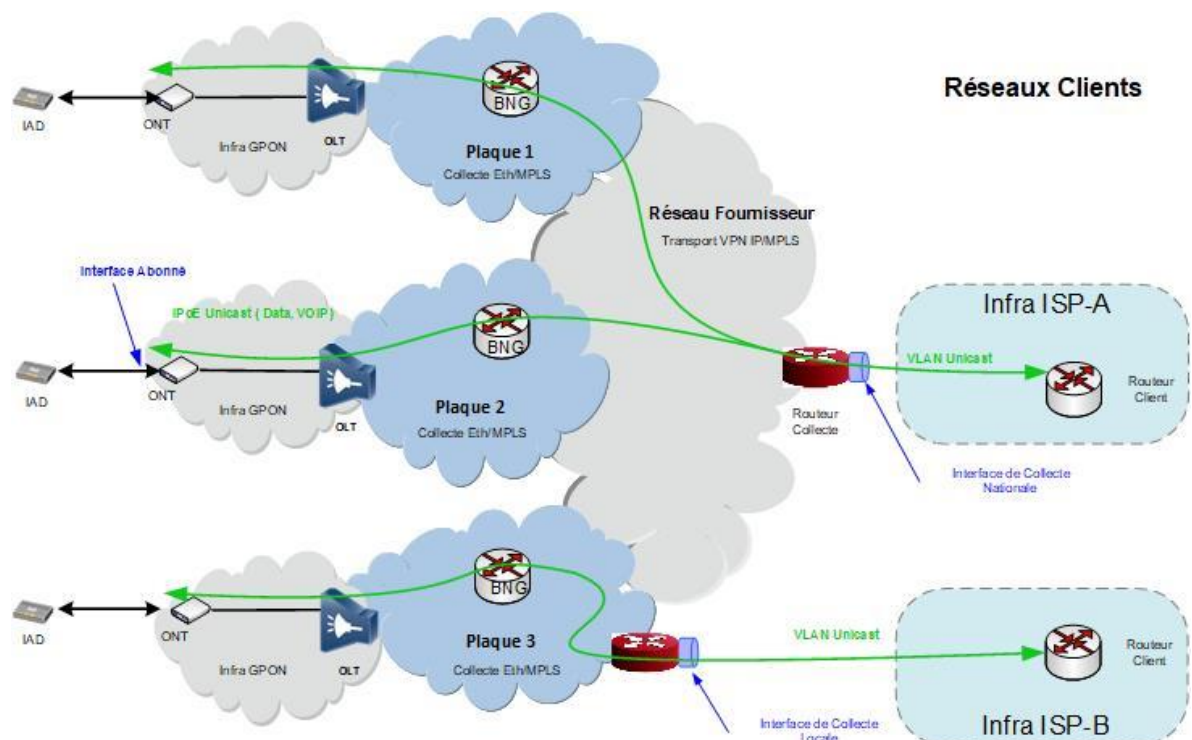


Figure 1 - Schéma de principe : mode d'accès IPoE

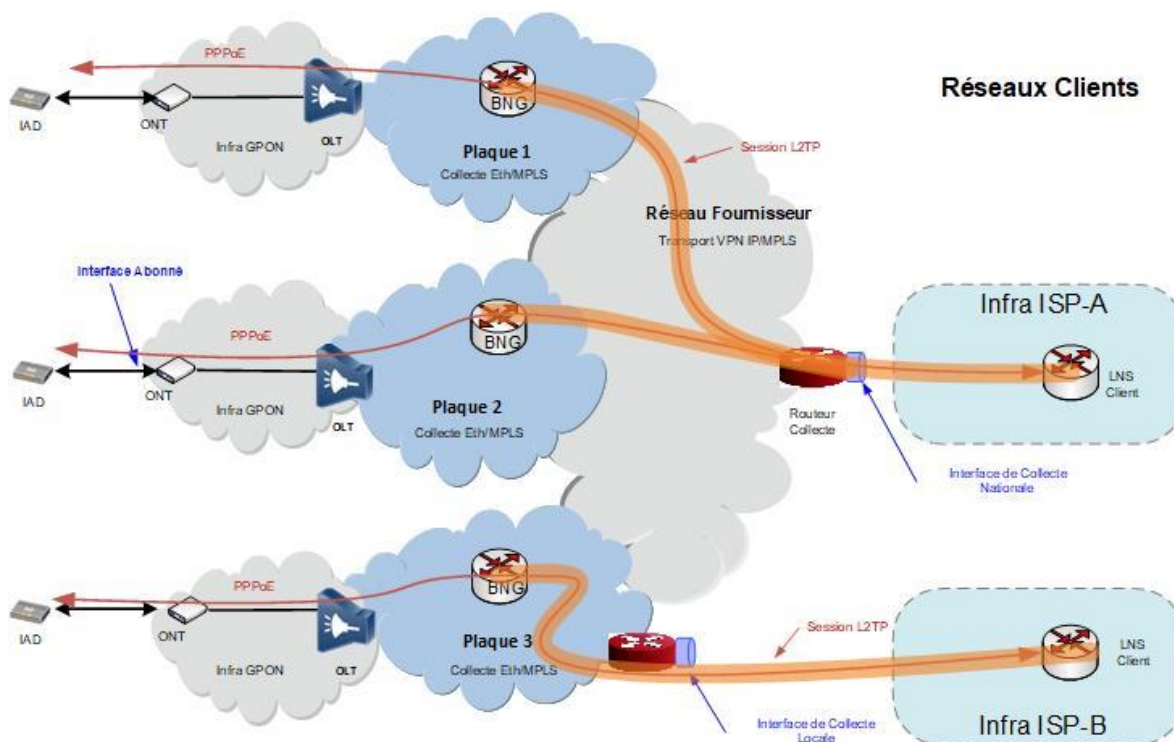


Figure 2 - Schéma de principe : mode d'accès PPPoE

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, tels que les OLTs et des routeurs multiservice 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 standard IEEE 802.1D et RFC 4762.

Le nombre d'adresses MAC par abonné est limité à 5 et leur « aging-time » est fixé, dans la chaîne de collecte niveau 2, à 2 heures. La durée des baux DHCP (ou preferred-lifetime en DHCPv6) et des timers ARP doit y être inférieure (avec timer ARP \geq Bail DHCP / 2) pour assurer un service sans discontinuité et éviter la diffusion de trafic de type « Unknown » ou « Broadcast » à travers les infrastructures du Fournisseur.

Les BNGs ont pour rôle d'appliquer le profil de service des abonnés et les mettre en relation avec l'infrastructure de transport de niveau 3 (VPN IP / MPLS) pour être accessibles depuis la porte de collecte. L'infrastructure globale assure une pleine transparence vis-à-vis du trafic échangé entre les Abonnés et le réseau de l'opérateur Client.

Les zones de collecte d'abonné sont gérées par 2 BNGs redondants en mode active/standby.

Les BNGs affectés à une zone de collecte sont choisis pour être au plus proche de celle-ci.

A noter qu'à travers les infrastructures d'accès Point-Multipoint, l'opérateur Client est en mesure d'adresser ses abonnés en IPv4 et / ou IPv6 pour le mode d'accès IPoE et uniquement en IPv4 pour le mode d'accès PPPoE.

La combinaison des 2 modes de collecte IPoE et PPPoE, est permise, mais ne l'est pas au niveau Abonné.

2.3. Classes de service réseau

La correspondance entre les classes de service du réseau du Fournisseur et les différents types de trafic associés est basée sur la valeur présentée par les 3 bits de l'IP Precedence du champ TOS contenu dans l'entête des paquets IP. La liste de ces correspondances est présentée dans le tableau ci-dessous :

Fournisseur	Client Opérateur de Services	
Classe de Service	Type de trafic	IP Precedence
Real Time	VOIP	5, 6, 7
Business	Business	3
Best Effort	Data	0, 1, 2, 4

Tableau 2 - Correspondance Trafic et CoS Fournisseur

3. Infrastructures de Collecte

3.1. Collecte Point-Multipoint

3.1.1. Synoptique

Le réseau de collecte dépeint ci-après est basé sur une infrastructure GPON et reprend le schéma de principe de la Figure 1.

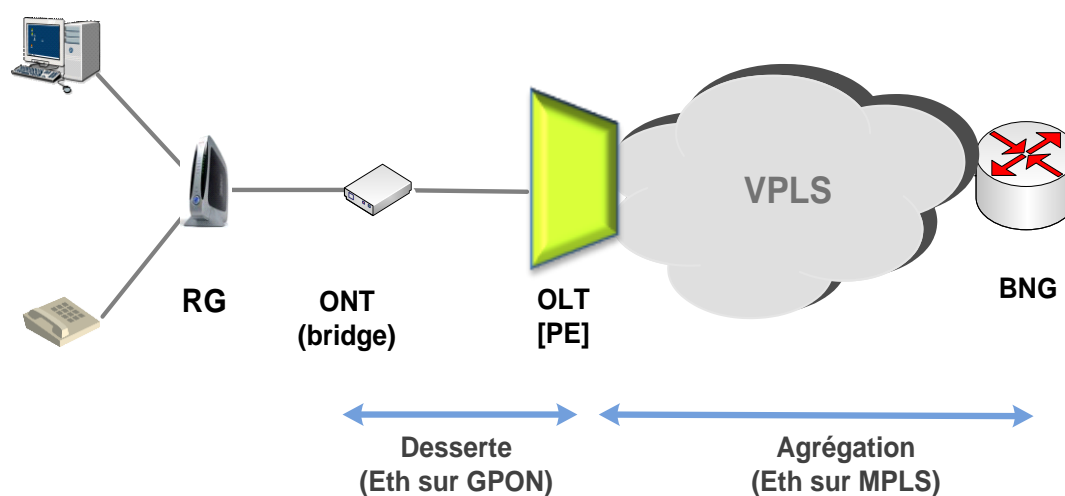


Figure 3 - Réseau de collecte GPON du service Ligne OPERA Office

Les arbres PON adressent 32 voire 64 Abonnés au maximum. Toutefois, 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 Abonnés. Le schéma ci-après modélise différentes solutions de raccordement des abonnés sans en faire la liste exhaustive :

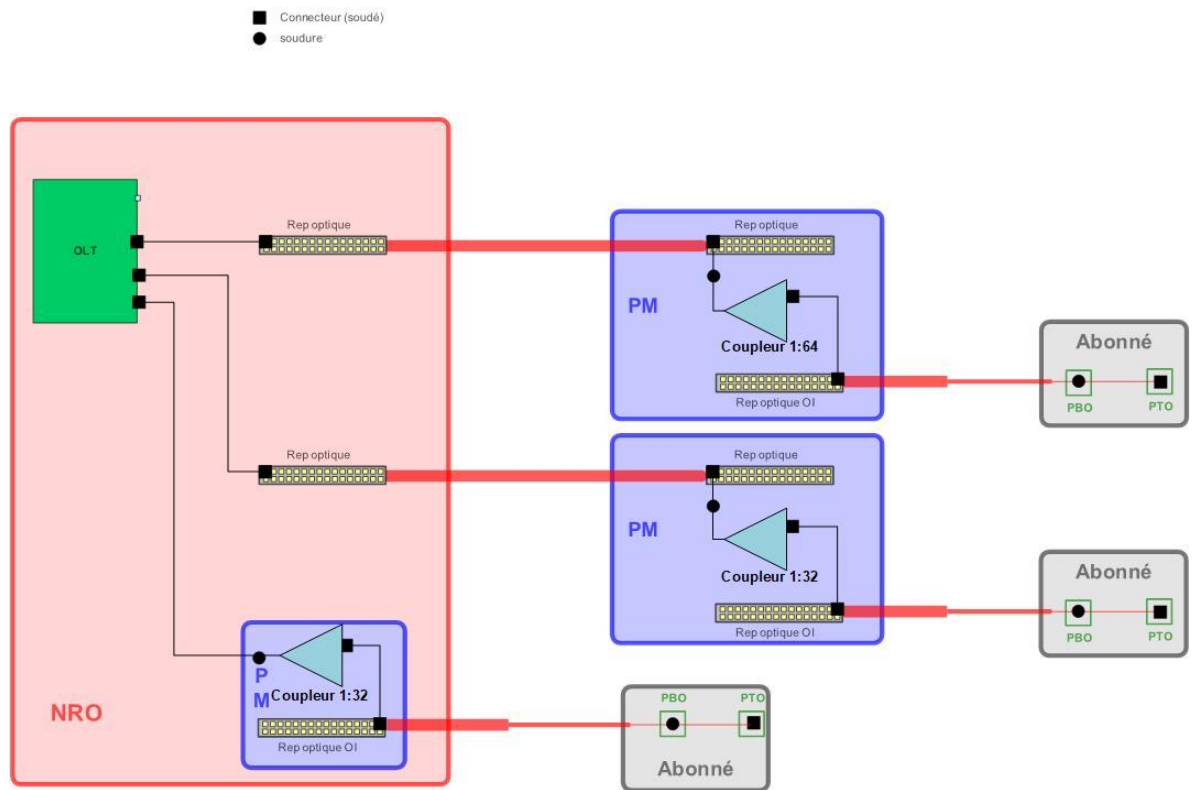


Figure 4 - Modélisation ODN

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

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

Avec le niveau de couplage 1:32, la distance optique maximale entre l'OLT et l'ONT avoisine 18 kms avec des modules optiques GPON de classe C+ au niveau de l'OLT.

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 Class B+ avec connecteur SC-APC ;
- Port cuivre gigabit-Ethernet par interface Abonné.

L'implémentation de la technologie GPON respecte les recommandations G.984.x de l'ITU-T :

- Nombre de T-CONT = 4 minimum ;

- Nombre de files d'attente associées à une interface Abonné = 8 ;
- Ordonnanceur des files d'attente supporte les modes « strict-priority », Weighted Fair Queuing » ainsi que la combinaison des deux dans le sens montant. Dans la voie descendante, seul le mode « strict-priority » est supporté.

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 puisqu'elle met à disposition de chaque carte de service une double connexion à 100 Gbits/s. De fait, elle est adaptée au marché des services résidentiels ou entreprises hauts débits tout en permettant de déployer simultanément plusieurs technologies d'accès basées sur la fibre optique.

En plus du mode d'accès GPON, retenu pour l'infrastructure de collecte point-multipoint, l'OLT supporte les types d'accès listés ci-après :

- EPON ;
- NG-PON (10G XG-PON1, XGS-PON ; NG-PON2) ;
- P2P Fast-Ethernet/Gigabit-Ethernet/TenGigabit-Ethernet.

3.2. Format du Circuit-Id

3.2.1. Circuit-Id

La notion de « Circuit ID » est communément employée dans les réseaux d'accès pour identifier de façon unique un Abonné en transmettant une information relative à l'équipement d'agrégation et au port d'accès, qu'il soit physique ou logique, auquel le client DHCP ou le client PPPoE est rattaché.

Mode IPoE :

Dans les transactions DHCPv4 le « Circuit-Id » est transmis par l'intermédiaire de l'option n°82 insérée par l'équipement d'agrégation des infrastructures de collecte Point-Multipoint. Elle est de taille variable et peut-être constituée d'une suite de sous options. Les codes des sous options Agent Circuit ID et Agent Remote ID sont respectivement 1 et 2.

Dans les transactions DHCPv6 le « Circuit-Id » est transmis par l'intermédiaire de l'option n°18 (Interface-ID) qui peut être complétée par l'option 37 (Relay Agent Remote-ID). L'équipement d'agrégation se comporte en relai DHCP de niveau 2 aussi appelé Lightweight DHCPv6 Relay Agent (LDRA), les options 18 et 37 sont définies respectivement par les RFC3315 et RFC4649.

Par analogie avec DHCPv4, l'option DHCPv6 n°18 correspond à la sous-option 1 de l'option 82 et l'option DHCPv6 n°37 correspond à la sous-option 2 de l'option 82.

Mode PPPoE :

Durant les échanges PPPoE, le « Circuit-Id » est transmis par l'intermédiaire d'un PPPoE Tag inséré par l'équipement d'agrégation des infrastructures de collecte Point-Multipoint en suivant les recommandations du Broadband Forum TR-156 (Architecture de collecte Ethernet pour services Broadband sur accès GPON – Using GPON access in the context of TR-101).

Dans ce contexte, les OLT sont appelés PPPoE Relay, ou PPPoE-Intermediate Agent. Ils insèrent les PPPoE Tag dans les messages PPPoE montants (émis par les IAD vers le réseau), c'est-à-dire durant la phases découverte et terminaison PPPoE en utilisant les messages PADI, PADR et PADT.

Le format du PPPoE Tag est défini dans le document BBF TR-101 § 3.9.2. Il se compose de plusieurs champs dont le TAG_ID (0x0105 = Vendor-Specific) et le TAG_VALUE (vendor id= 0x000DE9 = BBF) suivis d'une suite de sous options selon les besoins. Par analogie à l'option 82 DHCPv4, les codes des sous options Agent Circuit ID et Agent Remote ID sont respectivement 1 et 2.

3.2.2. DHCPv4

3.2.2.1. Agent Circuit-ID

Cette sous-option de l'option 82 contient la totalité des informations d'identification du circuit d'accès des Abonnés sur l'équipement d'agrégation. Elle est par conséquent systématiquement délivrée.

3.2.2.2. Agent Remote-ID

Cette sous-option de l'option 82 contient uniquement l'information du Sysname de l'équipement d'agrégation. Cette information est redondante avec celles contenues dans l'Agent Circuit-ID.

3.2.3. DHCPv6

3.2.3.1. Interface-ID

Cette option 18 a la même signification et reprend le format de l'Agent Circuit ID de l'option 82 de DHCPv4.

3.2.3.2. Relay Agent remote-ID

L'information transportée par l'option 37 est spécifique à l'équipement d'agrégation, elle peut être utilisée par exemple pour transmettre un numéro de VLAN, une description de port, ...

Dans le cas du présent service, l'option 37 n'est pas ajoutée.

3.2.4. PPPoE Tag

3.2.4.1. Agent Circuit-ID

La sous-option n°1 contient la totalité des informations d'identification du circuit d'accès des Abonnés sur l'équipement d'agrégation. Elle est par conséquent systématiquement délivrée.

Elle a la même signification et reprend le format de l'Agent Circuit ID de l'option 82 de DHCPv4.

3.2.4.2. Agent Remote-ID

Cette sous-option n°2 permet d'identifier l'abonné. C'est une chaîne de 63 caractères au maximum. Dans le cas du présent service, cette sous option n'est pas ajoutée.

3.2.5. Sysname

Le Sysname correspond au nom de l'équipement auquel est raccordé l'abonné.

Il est contenu dans les champs circuit-id / remote-id de l'option 82 DHCPv4, dans l'option 18 DHCPv6 et dans le Tag PPPoE.

Le format du sysname des OLT pour la collecte Point-MultiPoint en GPON est le suivant :

Valable pour tous OLT	olt-xxxdd-yy Avec : <ul style="list-style-type: none"> - xxx = le trigramme NRO (en minuscule) - dd = le numéro du département - yy = l'identifiant OLT rattachés à un même NRO
-----------------------	--

La chaîne de caractères xxxdd identifie le NRO.

3.2.6. Format du Circuit-ID spécifique aux OLTs

Dans les réseaux d'accès GPON, les options DHCP (82 ou 18) ou les PPPoE Tag sont insérés par l'OLT dans les messages DHCPv4, DHCPv6 ou PPPoE des transactions initiées par l'équipement Abonné.

Pour les OLTs, le format du « Circuit-ID » pourra prendre deux formes en fonction du modèle d'OLT sur lequel l'Abonné est raccordé :

■ Access_Node_ID PON Rack/Frame/Slot/PON/ONU/OnuSlt/UNI/I-VID

- Access_Node_ID = Le sysname de l'équipement ;
- PON = Indiquant la technologie de collecte ;
- Rack = Identifiant de baie de l'OLT toujours à la valeur 1 ;
- Frame = Identifiant de châssis OLT toujours à la valeur 1 ;
- Slot = Identifiant du Slot de l'OLT, de 01 à 16 ;
- PON = Identifiant de port de la carte GPON, de 01 à 16. Par défaut des cartes 8 ports PON mais dans les NRO denses des cartes 16 ports PON pourront être utilisées ;
- ONU = Identifiant ONT par arbre PON, de 1 à 128 (infra Fournisseur = 64 maximum) ;
- OnuSlt = slot de l'ONT, toujours à 1 ;
- UNI = Identifiant de port sur l'ONT représentant l'interface Abonné, toujours à 1 ;
- I-VID = Identifiant VLAN utilisé par l'équipement Abonné raccordé à l'UNI :
 - Celui-ci est vide si le trafic Abonné n'est pas marqué par une étiquette VLAN.

■ Access_Node_ID XPON Frame/Slot/Subslot/PON:ONU.gem.vlanid

- Access_Node_ID = Le sysname de l'équipement ;
- XPON = Indiquant la technologie de collecte ;
- Frame = Identifiant de châssis OLT toujours à la valeur 0 ;
- Slot = Identifiant du Slot de l'OLT, de 1 à 5 ;
- Subslot = Identifiant de la carte fille toujours à 0 ;
- PON = Identifiant de port de la carte GPON, de 0 à 15 ;
- ONU = Identifiant ONT par arbre PON, de 0 à 127 (infra Fournisseur = 64 maximum) ;
- Gem = Identifiant du gemport de l'ONT portant l'identification de l'Abonné, toujours à 1 ;
- Vlanid = Identifiant VLAN utilisé entre l'ONT et l'OLT, toujours à 1 ;

Pour le présent service, le « Circuit-ID » qui permet d'identifier de façon unique l'Abonné dans le réseau, pourra donc prendre les formes :

■ « sysname pon 1/1/Slot/**PON/ONU/1/Uni** »

- Exemple :
 - dans son format ascii : olt-bsn42-01 pon 1/1/01/01/4/1/1/
 - dans son format hexadécimal correspondant aux codes ascii :
6f6c742d62736e34322d303120706f6e20312f312f30312f30312f342f312f312f

■ « sysname xpon 0/Slot/0/**PON:ONU.1.1** »

- Exemple :
 - dans son format ascii : olt-bsn42-01 xpon 0/1/0/0:4.1.1
 - dans son format hexadécimal correspondant aux codes ascii :
6f6c742d62736e34322d30312078706f6e20302f312f302f303a342e312e31

4. Interfaces d'accès au service

Le service Ligne OPERA Office 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 Collecte).

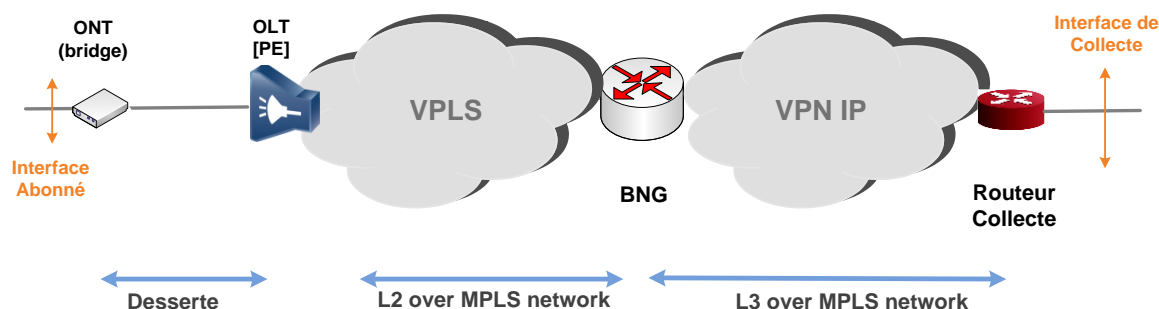


Figure 5 - Interfaces de service

4.1. L'interface Abonné

L'interface Abonné est de type cuivre, son débit est de 1 Gbits/s.

Topologie	Type Interface	Debit interface	Média	Portée (mètres)	Connecteur	Normes
Point-Multipoint GPON	1000-BaseT	1 Gbit/s	4 paires de cuivre Impédance 100 Ohms Câble UTP 6	100m	RJ-45 ISO 8877 (support for automatic inversion MDI / MDIX)	IEEE 802.3ab ISO/IEC 8802.3

Tableau 3 - 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 :

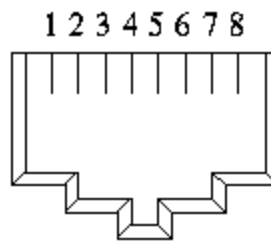


Figure 6 - Connecteur femelle RJ45

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 : 1 Gbit/s ;
- Port MDI / MDI-X avec détection automatique du câble droit ou croisé.

4.1.2. Raccordement Abonné

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 1 Gbits/s.

4.1.3. Spécifications IP

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

Le contenu du champ DSCP des paquets IP n'est pas modifié et peut-être utilisé par le client ISP pour faire correspondre ses flux avec les classes de services du réseau Fournisseur.

La valeur des 3 bits de poids fort du champ DSCP (ou IP Precedence) doit respecter les règles suivantes :

- Precedence = 5, 6, 7 pour le trafic associé à la classe de service VoIP ;
- Precedence = 3 pour le trafic associé à la classe de service Business ;
- Precedence = 0, 1, 2, 4 pour le trafic associé à la classe de service Data.

L'IAD installé chez l'abonné doit fonctionner en Ethernet « natif ». Le trafic ne doit pas être tagué avec un numéro de VLAN.

4.2. L'interface de Collecte

L'interface de Collecte 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 :

- Une porte Locale collecte uniquement les flux unicast issus d'une même DSP ;
- Une porte Nationale collecte les flux unicast de l'ensemble des réseaux opérés par le Fournisseur (accès issus de n'importe quel réseau de Délégation de Service).

Le client a la possibilité de souscrire au maximum 2 portes qui doivent être du même niveau (Locale ou Nationale). Lorsque le trafic est livré sur 2 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.

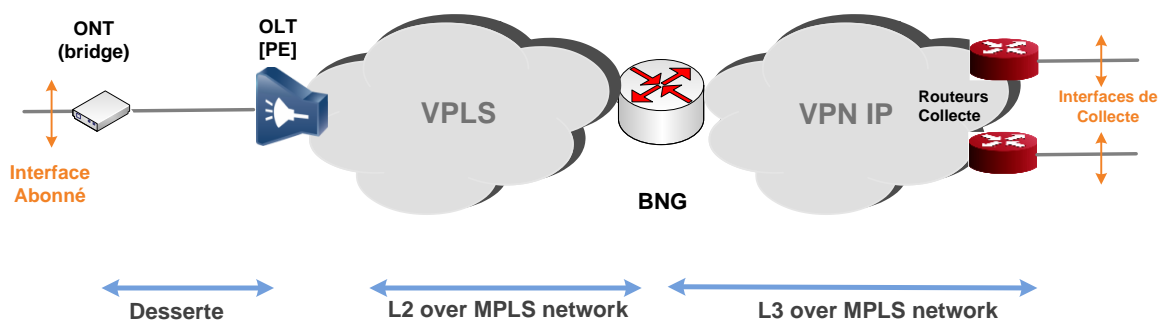


Figure 7 - Sécurisation de l'interface de Collecte

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 collecte 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 Collecte

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

Deux VLANs sont définis sur les interfaces de collecte. Un VLAN pour le transport des flux data (IPoE et/ou L2TP) des abonnés, le second pour les échanges RADIUS.

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

Les réseaux IP d'interconnexions sont en adressage publique IPv4 de type /31, voire IPv6 de type /127 pour le VLAN Data Unicast.

Le Client ISP 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 collecte.

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 IP des IADs en mode IPoE ainsi que les préfixes BGP contenant les adresses IP de ses LAC pour le mode PPPoE :

- Mode IPoE : A la convenance du Client ISP, les pools IP ou les préfixes spécifiques /32 pour IPv4 ou les préfixes spécifiques IA_NA en /64 et IA_PD, de /32 à /64, pour IPv6 par IAD ;
- Mode PPPoE : Les adresses de ses LAC

- sur une porte nationale, le Fournisseur annonce les adresses IP des LAC des réseaux d'initiative public pour lesquels le client a opté pour une livraison nationale ;
- sur une porte locale, le Fournisseur annonce uniquement les adresses IP des LAC locaux.

Le client annonce :

- Mode IPoE : Une route par défaut ;
- Mode PPPoE : Les adresses de ses LNS.

Le Fournisseur appliquera un filtre sur les annonces BGP-4 du client pour autoriser :

- Mode IPoE : Route par défaut uniquement ;
- Mode PPPoE :
 - Limitation du nombre total de routes annoncées par le client sur une interface de collecte à 300 ;
 - Seules les adresses faisant partie des blocs d'adresses LNS préalablement déclarés par le client sont redistribués dans le réseau du Fournisseur.

Les communautés utilisées par le client seront ignorées sur le réseau du Fournisseur.

Caractéristiques de la session eBGP RADIUS

- Adressage IP fourni par le Fournisseur ;
- 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 IP de ses Proxy RADIUS

Le client annonce :

- les adresses IP de ses serveurs RADIUS

Le Fournisseur appliquera les filtres suivants sur les annonces BGP-4 du client :

- Limitation du nombre total de routes annoncées par le client sur une interface de collecte au nombre de serveurs RADIUS du client ;
- Seules ces adresses sont redistribuées dans le réseau du Fournisseur.

Les communautés utilisées par le client seront ignorées sur le réseau du Fournisseur.

Attributs BGP et gestion du mode de redondance

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
Locale nominale	220
Locale secours	210
Nationale nominale	200
Nationale 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. Mode d'accès et livraison IPoE

5.1. Gestion IP/DHCP Abonné

Le présent service permet d'établir des sessions IP DHCP entre IAD et BNG, sans « switching » inter-abonné, routables jusqu'au réseau de l'opérateur client. Celui-ci est en mesure d'attribuer, à chacun de ses abonnés, au plus une adresse parmi les types suivants :

- IPv4 : une adresse /32 par IAD ;
- IA_NA (IPv6) sur infrastructure Point-Multipoint uniquement : une adresse /128 par IAD issu d'un range /64 dédié. Soit 1 range /64 par IAD ;
- IA_PD (IPv6) sur infrastructure Point-Multipoint uniquement : un préfixe de taille /32 à /64 par IAD.

L'opérateur client a le choix de gérer ses abonnés selon 2 méthodes ; « DHCP et RADIUS » ou « FULL RADIUS ».

Dans le mode « DHCP et RADIUS », le BNG du Fournisseur se comporte en relai DHCP entre les IAD abonnés et le serveur DHCP du client opérateur.

Dans le mode « FULL RADIUS », le BNG du Fournisseur se comporte en serveur DHCP vis-à-vis des IAD abonnés et leurs paramètres IP sont transmis par le serveur Radius du client opérateur.

Les échanges DHCP et RADIUS des 2 méthodes sont détaillées ci-après dans cette même section du document.

5.2. Gestion profil de QoS Abonné

La gestion du profil de QoS de l'abonné se fait dynamiquement à chaque nouvel échange DHCP entre l'abonné et le serveur DHCP (DHCPv4-Discover / DHCPv4-Renew ou DHCPv6-Solicit / DHCPv6-Renew). Les échanges DHCP doivent avoir un marquage IP precedence à 0.

Quel que soit le mode de gestion des abonnés, le BNG initie une transaction Radius lui permettant de récupérer le profil de l'abonné.

Pour cela l'opérateur client renvoie dans un message RADIUS Access-Accept l'attribut Class précisant le profil de l'abonné. Ce dernier est ensuite interprété par le réseau du Fournisseur et le profil de QoS associé est automatiquement activé au niveau du BNG.

5.3. Paramétrage IP et DHCP

5.3.1. Durée de vie des adresses IPv6

L'attribution d'une adresse IPv6 à une interface est temporaire et les différents états de sa durée de vie sont présentés par la figure suivante :

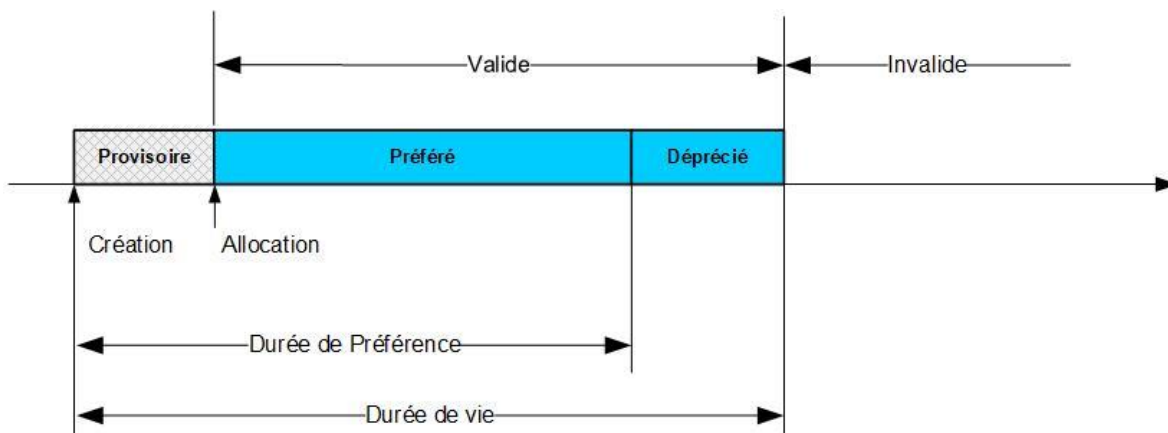


Figure 8 - Etats successifs d'une adresse IPv6 sur une interface

Les compteurs « Durée de vie » et « Durée de Préférence » contrôlent le cycle de vie des adresses IP sur une interface. Selon le mode d'auto-configuration, le compte à rebours démarre dès réception du message d'annonce d'un routeur ou d'un message DHCPv6 Reply.

La durée de vie (valid lifetime) indique la durée pendant laquelle l'adresse IP est associée à une interface.

La durée de préférence (preferred lifetime) est la durée pendant laquelle l'adresse IP est utilisable sans restriction dès lors que son unicité a été vérifiée. Cette durée est assimilable à la durée du bail DHCPv4.

Le cycle de vie d'une adresse IPv6 est régi par les états suivants :

- Etat Provisoire (tentative) : L'adresse a été attribuée par le mécanisme d'auto-configuration mais son unicité sur le lien n'a pas encore été vérifiée par le processus de Détection d'Adresse Dupliquée (DAD). Une adresse provisoire ne peut servir dans une communication ;
- Etat valide (valid) : L'unicité a été contrôlée, l'adresse est active sur une interface ;
 - Préféré (preferred) : L'adresse peut être utilisée sans restriction ;
 - Déprécié (deprecated) : L'adresse ne peut plus être utilisée pour de nouvelles communications mais reste active pour les connexions existantes ;
- Invalide (invalid) : L'adresse ne peut plus du tout être utilisée. Elle n'est plus active sur l'interface.

5.3.2. Compteurs DHCP

En supplément de la durée du bail pour IPv4 ou de la durée à l'état préféré pour IPv6, les clients DHCP gèrent 2 compteurs définis par T1 et T2 dans les RFC2131 pour DHCPv4 et RFC3315 pour DHCPv6. Ces compteurs sont à leur valeur par défaut telle que définie dans les RFC ou configurables par les serveurs sous formes d'options.

Le premier, T1, stipule la durée à partir de laquelle le client demande à son serveur un renouvellement de la durée d'utilisation de son adresse IP. Le second, T2, entre en action lorsque la demande de renouvellement a échoué en renégociant une nouvelle adresse IP en s'adressant à tous les serveurs susceptibles de répondre.

T2 doit être compris entre T1 et l'expiration du bail DHCPv4 ou de l'état préféré en DHCPv6.

Pour DHCPv4, T1 et T2 ne sont pas transmis au client DHCP. Lorsque le client DHCP utilise les valeurs par défaut, les compteurs sont :

- Bail = 7200 secondes (2 heures) ;
- T1 = Renew = $0,5 \times \text{Bail}$ (valeur par défaut selon RFC2131) = 3600 secondes ;
- T2 = Rebind = $0,875 \times \text{Bail}$ (valeur par défaut selon RFC2131) = 6300 secondes.

Pour DHCPv6, à la différence de DHCPv4, T1 et T2 sont toujours transmis au client DHCP. Les valeurs imposées par le Fournisseur sont les suivantes :

- Preferred lifetime = 7200 secondes (2 heures) ;
- Valid lifetime = 10800 secondes (3 heures) ;
- T1 = Renew = $0,5 \times \text{Bail}$ = 3600 secondes ;
- T2 = Rebind = $1,5 \times T1$ = 5400 secondes.

5.4. Mode DHCP et RADIUS

5.4.1. Authentification et adressage IP de l'abonné

A chaque nouvel échange IP/DHCP (DHCPv4-Discover / DHCPv4-Renew ou DHCPv6-Solicit / DHCPv6-Renew), une demande d'authentification RADIUS (RADIUS Access-Request) est envoyée au serveur RADIUS Client au travers d'un Proxy-RADIUS du Fournisseur.

Une fois la demande d'authentification validée par le serveur RADIUS client (RADIUS Access-Accept), le BNG du Fournisseur relaye la demande DHCP de l'abonné aux serveurs DHCP de l'opérateur client.

Une fois la phase d'authentification passée, le dialogue IP/DHCP client/serveur se déroule de façon standard.

L'opérateur client attribuera des adresses IP pour une durée de 2 heures (**bail DHCPv4 / preferred-lifetime pour DHCPv6 = 2 heures**).

5.4.2. Détail des échanges RADIUS et DHCPv4

5.4.2.1. DHCPv4-Discover

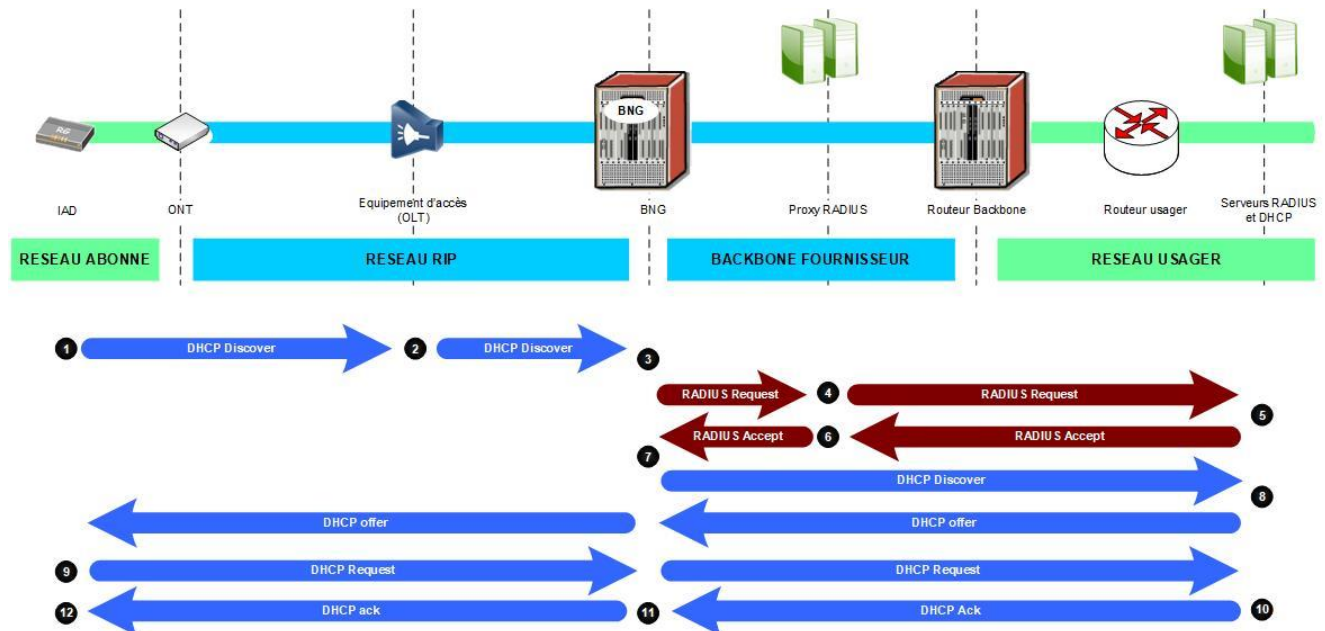


Figure 9 - Mode DHCP et RADIUS (transaction DHCPv4-Discover)

IAD

(1) L'IAD envoie un DHCP-Discover sur son port réseau.

OLT d'accès

(2) Celui-ci insère l'option 82 dans le DHCP-Discover du client en y renseignant les informations suivantes :

- Slot de l'équipement d'accès ;
- Port abonné ;
- Hostname de l'équipement d'accès.

BNG

A réception du DHCP-Discover le BNG Nominal bloquera le DHCP-Discover de l'IAD Abonné. Il générera un RADIUS Access-Request à destination du Proxy RADIUS Fournisseur (3) afin d'identifier l'abonné en recopiant certains champs du DHCP-Discover dans sa requête (circuit-id, remote-id et vendor-dhcp).

Proxy-RADIUS Fournisseur

Le Proxy-RADIUS Fournisseur identifie l'opérateur client de l'abonné sur la base de son circuit-id et proxifie l'Access-Request au RADIUS de l'opérateur client (4).

Le proxy-RADIUS peut si nécessaire en fonction du client opérateur rajouter et/ou supprimer des attributs de l'access-request initiale du BNG Fournisseur avant de le transmettre au RADIUS du client (cf chapitre suivant).

L'Access-Request transmis au client après traitement par le proxy-RADIUS contiendra à minima les informations suivantes :

- User-Name=<adresse_mac_IAD> ;
- User-Password = <mot-de-passe> ;
- NAS-IP-Address = <adresse IP du BNG auquel l'abonné est attaché > ;
- ADSL-Agent-Circuit-id=<circuit-id-access>;
- ADSL-Agent-Remote-id=<remote-id>.

Les attributs radius suivants seront transmis sur demande du client :

- Alc-DHCP-Vendor-Class-Id = <DHCP Option 60 (Vendor-ID)> ;
- Calling-Station-Id :
 - Pour un accès Point Multipoint = <nom-Fournisseur>#OLT#

RADIUS Client

Le RADIUS client authentifie l'abonné et renvoie un RADIUS Access-Accept (5) au proxy-RADIUS Fournisseur contenant les informations suivantes :

- Class = OPERA-Office-DL<hsiD>m<voipD>k-UL<hsiU>m<voipU>k-Bus<bus>m
 - <hsiD> : La valeur du débit HSI down max en Mbit/s
 - <hsiU> : La valeur du débit HSI up max en Mbit/s
 - <voipD> : La valeur du débit VoIP down max en Mbit/s
 - <voipU> : La valeur du débit VoIP up max en Mbit/s
 - <bus> : La valeur du débit Business up/down 10 Mbits/s ou 100 Mbits/s.

L'attribut Class permet de distinguer le profil de débit à appliquer à l'abonné. Il est construit en se référant aux valeurs maximales des débits descendants DATA/VOIP/BUSINESS et des débits montants DATA/VOIP/BUSINESS.

Exemple :

- Ligne OPERA Office avec débit symétrique Data 100Mbps, Business 10Mbps et voix de 500Kbps.

Class = **OPERA-Office-DL100m500k-UL100m500k-Bus10m**

Le proxy-Radius Fournisseur transmet le Radius Access-Accept au BNG Fournisseur en ajoutant les attributs propriétaires nécessaires à l'activation de l'abonné (6) :

- Identifiant Service du client ;
- Identifiant de l'abonné ;
- Profile de QoS (attribut Class renvoyé par le Radius Client).

A réception de l'Access-Accept, l'abonné est instancié, au sein du BNG, dans le VPN du client avec son profil de QoS.

A ce stade l'abonné n'a toujours pas obtenu d'IP. Le BNG relaie alors le DHCP-Discover (7) de l'abonné vers le serveur DHCP du client.

S'ensuit alors un dialogue DHCP standard, DHCP-Offer(8), DHCP-Request(9) et DHCP-Ack(10) entre l'IAD de l'abonné et le serveur DHCP du client.

Le DHCP-Ack permet au BNG Fournisseur de connaître l'adresse IP de l'abonné et la durée du bail DHCP.

5.4.2.2. DHCPv4-Renew

Chaque DHCP-Renew entraîne une nouvelle authentification de l'abonné. Si le profil de l'abonné a changé dans les bases RADIUS client la procédure de renouvellement de bail entrainera la mise à jour du profil de l'abonné.

Le schéma ci-dessous présente les échanges DHCP et RADIUS relatifs à un renouvellement de bail :

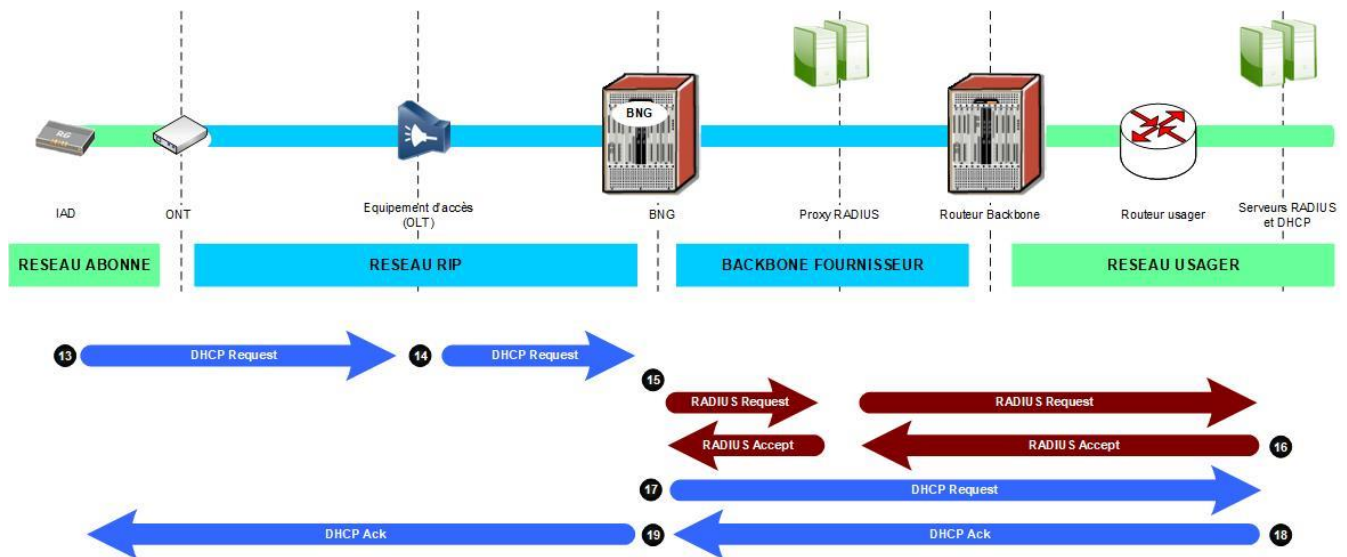


Figure 10 - Mode DHCP et RADIUS (renouvellement du Bail DHCPv4)

(13) L'IAD de l'abonné envoie un message unicast de type DHCP-Request pour renouveler le bail dhcp en conservant la même adresse IP.

(14) Le DHCP- Request est intercepté et l'option 82 de l'équipement d'accès est insérée.

(15) Le DHCP- Request est bloqué au niveau du BNG qui envoie un RADIUS Access-Request.

(16) En retour, le RADIUS Client répond avec un RADIUS Access-Accept. Le BNG met à jour le profil de l'abonné sur la base des informations descendues par le serveur RADIUS.

(17) Le DHCP- Request est alors retransmis par le BNG jusqu'au serveur DHCP du client.

(18) Le serveur DHCP répond alors par un DHCP-Ack à l'abonné.

(19) Le BNG enregistre l'adresse IP de l'abonné en analysant le DHCP-Ack pour mettre à jour sa table DHCP. Celle-ci faisant correspondre l'adresse mac et l'adresse IP de l'abonné.

5.4.3. Détail des échanges RADIUS et DHCPv6

5.4.3.1. DHCPv6-Solicit

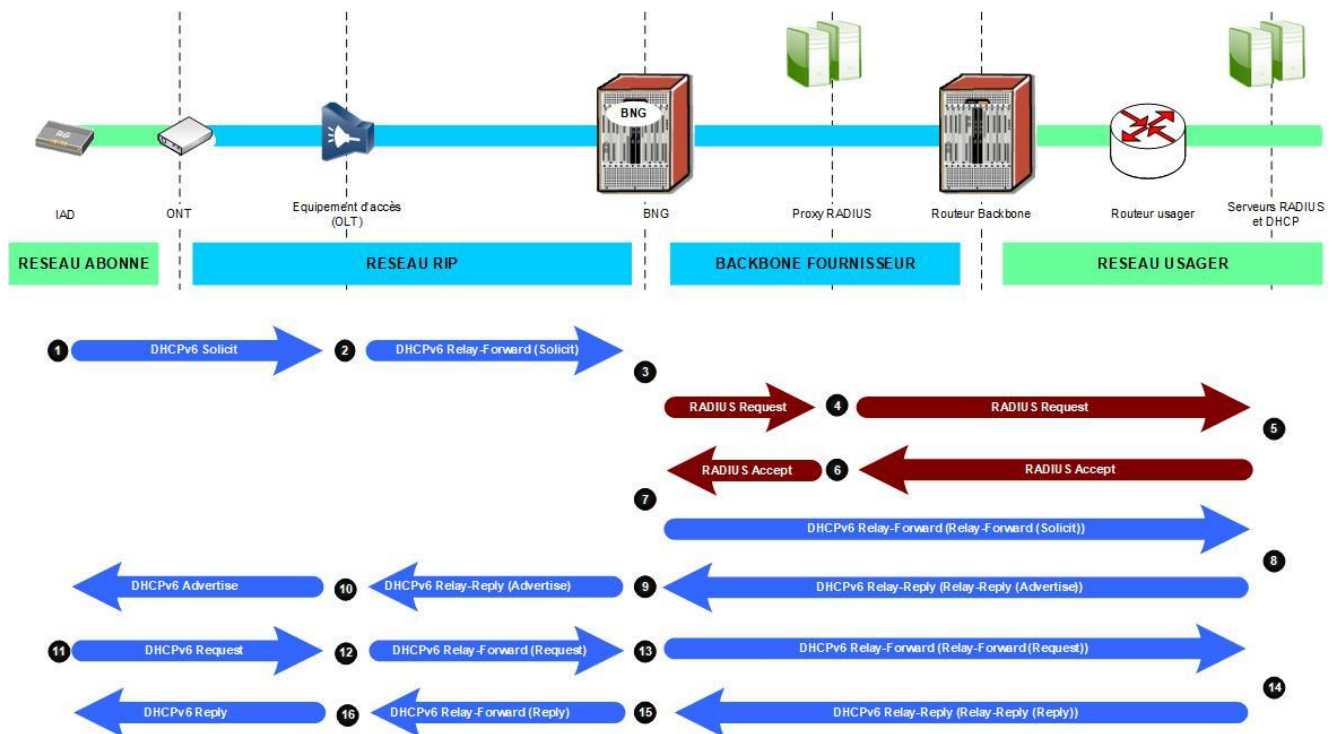


Figure 11 - Mode DHCP et RADIUS (transaction DHCPv6-Solicit)

IAD

(1) L'IAD envoie un DHCPv6-Solicit sur son port réseau.

Equipement d'accès (OLT)

(2) L'équipement d'accès se comporte en relai DHCPv6 en encapsulant la requête Solicit dans un message DHCPv6 Relay-Forward et y insère le circuit-id de l'abonné. Le circuit-ID étant l'option 18, Interface-ID, faisant apparaître les informations suivantes :

- Slot de l'équipement d'accès ;
- Port abonné ;
- Hostname de l'équipement d'accès.

BNG

Sur réception du message DHCPv6 Relay-Forward (Solicit), le BNG Nominal bloque la transaction jusqu'à ce que l'abonné soit identifié. Pour cela le BNG génère un RADIUS Access-Request à destination du Proxy RADIUS Fournisseur (3) en recopiant certains champs du message DHCP dans sa requête dont le circuit-id.

Proxy-RADIUS Fournisseur

Le Proxy-RADIUS Fournisseur identifie l'opérateur client de l'abonné sur la base de son circuit-id et proxifie l'Access-Request au RADIUS de l'opérateur client (4).

Le proxy-RADIUS peut si nécessaire en fonction du client opérateur rajouter et/ou supprimer des attributs de l'access-request initiale du BNG Fournisseur avant de le transmettre au RADIUS du client (cf chapitre suivant).

L'Access-Request transmis au client après traitement par le proxy-RADIUS contiendra à minima les informations suivantes :

- User-Name=<adresse_mac_IAD> ;
- User-Password = <mot-de-passe> ;
- NAS-IP-Address = <adresse IP du BNG auquel l'abonné est attaché > ;
- ADSL-Agent-Circuit-id = <circuit-id-access>;

Les attributs radius suivants seront transmis sur demande du client :

- Calling-Station-Id :
 - Pour un accès Point Multipoint = <nom-Fournisseur>#OLT#

RADIUS Client

Le RADIUS client authentifie l'abonné et renvoie un RADIUS Access-Accept (5) au proxy-RADIUS Fournisseur contenant les informations suivantes :

- Class = OPERA-Office-DL<hsiD>m<voipD>k-UL<hsiU>m<voipU>k-Bus<bus>m
 - <hsiD> : La valeur du débit HSI down max en Mbit/s
 - <hsiU> : La valeur du débit HSI up max en Mbit/s
 - <voipD> : La valeur du débit VoIP down max en Mbit/s
 - <voipU> : La valeur du débit VoIP up max en Mbit/s
 - <busD> : La valeur du débit Business up/down 10 Mbits/s ou 100 Mbits/s.

L'attribut Class permet de distinguer le profil de débit à appliquer à l'abonné. Il est construit en se référant aux valeurs maximales des débits descendants DATA/VOIP/BUSINESS et des débits montants DATA/VOIP/BUSINESS.

Exemple :

- Ligne OPERA Office avec débit symétrique Data 100Mbps, Business 10Mbps et voix de 500Kbps.

Class = **OPERA-Office-DL100m500k-UL100m500k-Bus10m**

Le proxy-Radius Fournisseur transmet le Radius Access-Accept au BNG Fournisseur en ajoutant les attributs propriétaires nécessaires à l'activation de l'abonné (6) :

- Identifiant Service du client ;
- Identifiant de l'abonné ;
- Profile de QoS (attribut Class renvoyé par le Radius Client).

A réception de l'Access-Accept, l'abonné est instancié, au sein du BNG, dans le VPN du client avec son profil de QoS.

A ce stade l'abonné n'a toujours pas obtenu d'IP. Le BNG relaie alors le message DHCPv6 qui a déjà été relayé par l'OLT vers le serveur DHCP du client (7).

Ici le BNG se comporte en relai DHCPv6 et vient ajouter une seconde encapsulation de type Relay-Forward au message Solicit de l'abonné.

S'ensuit alors un dialogue DHCPv6 standard entre l'IAD de l'abonné, les 2 relais DHCP (OLT et BNG) et le serveur DHCP du client :

- DHCPv6 Relay-Reply(Relay-Reply(Advertise)) (8) ;
- DHCPv6 Relay-Reply(Advertise) (9) ;
- DHCPv6 Advertise (10) ;
- DHCPv6 Request (11) ;
- DHCPv6 Relay-Forward (Request) (12) ;
- DHCPv6 Relay-Forward (Relay-Forward (Request)) (13) ;
- DHCPv6 Relay-Reply(Relay-Reply(Reply)) (14) ;
- DHCPv6 Relay-Reply(Reply) (15) ;
- DHCPv6 Reply (16).

Le DHCPv6 Relay-Reply(Relay-Reply(Reply)) (14) permet au BNG Fournisseur de connaître l'adresse IP de l'abonné, la durée du preferred-lifetime et la valeur des compteurs T1/T2 (Renew/Rebind DHCP).

5.4.3.2. DHCPv6-Renew

Chaque DHCPv6-Renew entraîne une nouvelle authentification de l'abonné. Si le profil de l'abonné a changé dans les bases RADIUS client la procédure de renouvellement de bail (réinitialisation du compteur preferred-lifetime) entrainera la mise à jour du profil de l'abonné.

Le schéma ci-dessous présente les échanges DHCPv6 et RADIUS relatifs à un renouvellement de bail :

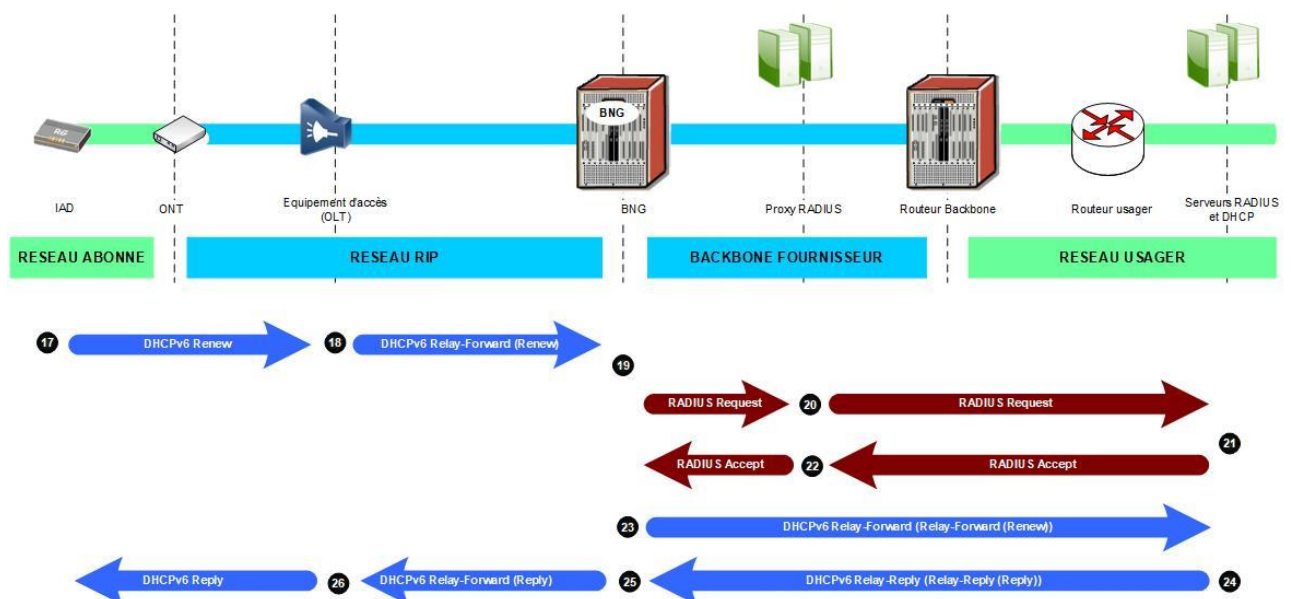


Figure 12 - Mode DHCP et RADIUS (renouvellement du Preferred-Lifetime DHCPv6)

(17) L'IAD de l'abonné envoie un message de type DHCPv6-Renew pour renouveler le bail dhcp en conservant la même adresse IP.

(18) DHCPv6-Renew est intercepté par l'équipement d'accès (OLT) et relayé dans un message DHCPv6 Relay-Forward (Renew) en y insérant le circuit-id de l'abonné. Le circuit-id étant l'option 18 DHCPv6.

(19) (20) Le message DHCPv6 Relay-Forward (Renew) est bloqué au niveau du BNG qui envoie un RADIUS Access-Request à destination du serveur client via le proxy Fournisseur.

(21) (22) En retour le RADIUS Client répond avec un RADIUS Access-Accept. Le BNG met à jour le profil de l'abonné sur la base des informations descendues par le serveur RADIUS.

(23) Le message DHCPv6 Relay-Forward (Renew) est alors relayé par le BNG jusqu'au serveur DHCP du client.

(24) Le serveur DHCP client répond alors par un DHCPv6 Reply encapsulé par un message Relay-Reply permettant d'adresser les 2 relais DHCPv6, BNG et OLT, pour joindre l'IAD de l'abonné.

(25) Le BNG enregistre les paramètres IP de l'abonné en analysant le message DHCPv6 reçu pour mettre à jour sa table DHCP. Celle-ci faisant entre autre correspondre l'adresse mac et l'adresse IP de l'abonné.

Le BNG retransmet le message DHCPv6 après avoir supprimé l'entête Relay-Reply le concernant.

(26) L'équipement d'accès (OLT) retransmet à l'IAD de l'abonné le message DHCPv6 après avoir supprimé l'entête Relay-Reply le concernant.

5.5. Mode Full RADIUS

Dans le mode Full RADIUS, le client n'a pas à maintenir un serveur DHCP, c'est le BNG Fournisseur qui prend ce rôle.

Le client a la possibilité :

- soit, d'attribuer des adresses IP fixes à ses abonnés ;
- soit, d'attribuer des adresses IP dynamiques pour une durée de 2 heures.

5.5.1. Authentification et adressage IP de l'abonné

A chaque nouvel échange IP/DHCP (DHCPv4-Discover / DHCPv4-Renew ou DHCPv6-Solicit / DHCPv6-Renew), une demande d'authentification RADIUS (RADIUS Access-Request) est envoyée au serveur RADIUS Client au travers d'un Proxy-RADIUS Fournisseur.

Une fois cette demande d'authentification validée par le serveur RADIUS client (RADIUS Access-Accept), le BNG Fournisseur joue le rôle de serveur DHCP en répondant à la demande DHCP (Discover ou Renew) de l'abonné.

Une fois la phase d'authentification passée, le dialogue IP/DHCP client/serveur se déroule de façon standard.

Le BNG Fournisseur attribuera des adresses IP pour une durée de 2 heures (**bail DHCPv4 / preferred-lifetime pour DHCPv6 = 2 heures**).

Pour une requête DHCPv4, le BNG servira une IPv4.

Pour une requête DHCPv6, le BNG servira un IA_NA et un IA_PD.

Dans le cas d'IAD adressés en double pile, IPv4/IPv6, le serveur Radius Client renvoie les paramètres IPv4 et IPv6 de l'abonné dans le même message Radius Access-Accept.

5.5.2. Détail des échanges RADIUS et DHCP

5.5.2.1. DHCPv4-Discover

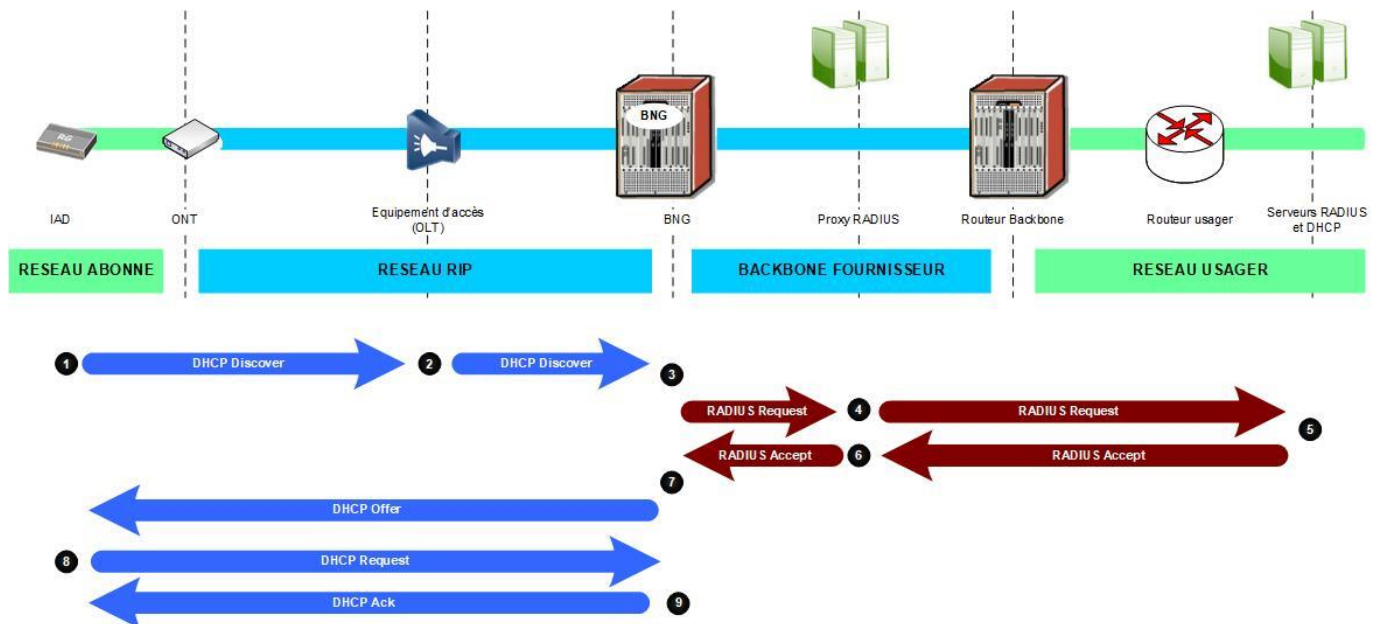


Figure 13 - Mode FULL RADIUS (transaction DHCPv4-Discover)

IAD

(1) L'IAD envoie un DHCP Discover sur son port réseau.

Equipement FTTH d'accès

(2) Celui-ci insère l'option 82 dans le DHCP Discover du client en y renseignant les informations suivantes :

- Slot de l'équipement d'accès ;
- Port abonné ;
- Hostname de l'équipement d'accès.

BNG

(3) A réception du DHCP Discover, le BNG Nominal bloquera le DHCP Discover de l'IAD Abonné. Il générera un RADIUS Access Request à destination du proxy-RADIUS Fournisseur afin d'identifier l'abonné en recopiant certains champs du DHCP Discover dans sa requête (circuit-id, remote-id et vendor-dhcp).

Proxy-RADIUS Fournisseur

Le Proxy-RADIUS Fournisseur identifie l'opérateur client de l'abonné sur la base de son circuit-id et proxifie l'access-request au RADIUS de l'opérateur client (4).

Le proxy-RADIUS peut si nécessaire en fonction du client opérateur rajouter et/ou supprimer des attributs de l'access-request initiale du BNG Fournisseur avant de le transmettre au RADIUS du client (cf chapitre suivant).

L'Access-Request transmis au client après traitement par le proxy-RADIUS contiendra à minima les informations suivantes :

- User-Name=<adresse_mac_IAD> ;
- User-Password = <mot-de-passe> ;
- NAS-IP-Address = <adresse IP du BNG auquel l'abonné est attaché > ;
- ADSL-Agent-Circuit-id=<circuit-id-access>;
- ADSL-Agent-Remote-id=<remote-id>.

Les attributs radius suivants seront transmis sur demande du client :

- Alc-DHCP-Vendor-Class-Id = <DHCP Option 60 (Vendor-ID)> ;
- Calling-Station-Id :
 - Pour un accès Point Multipoint = <nom-Fournisseur>#OLT#

RADIUS Client

Le RADIUS client authentifie l'abonné et renvoie un RADIUS access-accept (5) au proxy-RADIUS Fournisseur contenant les informations suivantes :

- Class ;
- Framed-IP-Address ;
- Framed-IP-Netmask ;
- Alc-Default-Router ;
- Alc-Primary-Dns ;
- Alc-Secondary-Dns.

Proxy-RADIUS Fournisseur

Le PROXY-RADIUS Fournisseur transmet le RADIUS Access-Accept au BNG Fournisseur en ajoutant les attributs propriétaires nécessaires à l'activation de l'abonné (6).

- Identifiant Service du client ;
- Identifiant de l'abonné ;

- Profil de QoS (dérive de l'attribut Class renvoyé par le client).

A réception de l'Access-Accept, l'abonné est instancié dans le VPN du client avec son profil de QoS.

Le BNG répond à l'abonné (DHCP-Offer) en proposant les paramètres réseaux qui lui ont été communiqués par le serveur RADIUS (7).

L'abonné envoie un DHCP-Request (8). Le BNG, qui joue le rôle de serveur DHCP, lui retourne un DHCP-Ack(9).

L'abonné dispose d'un bail de 2 heures.

5.5.2.2. DHCPv4-Renew

Chaque DHCP-Renew entraîne une nouvelle authentification de l'abonné. Si le profil de l'abonné a changé dans les bases RADIUS client la procédure de renouvellement de bail entrainera la mise à jour du profil de l'abonné.

Le schéma ci-dessous présente les échanges DHCP et RADIUS relatifs à un renouvellement de bail :

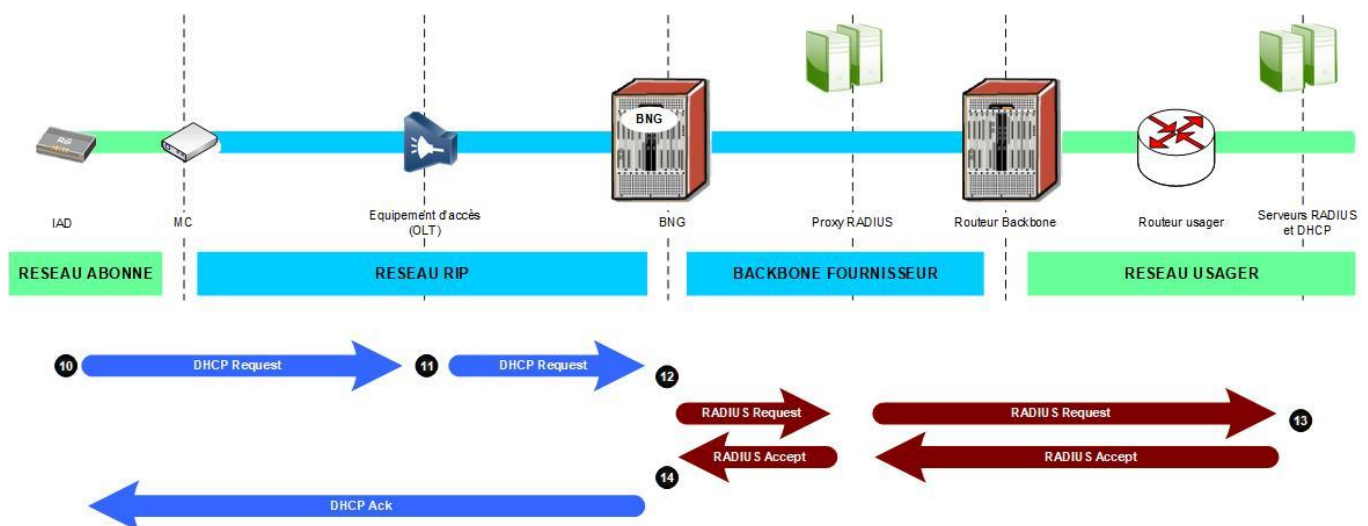


Figure 14 - Mode FULL RADIUS (renouvellement du Bail DHCPv4)

(10) L'IAD de l'abonné envoie un DHCP-Request.

(11) Le DHCP-Request est intercepté et l'option 82 de l'équipement d'accès est insérée.

(12) Le DHCP-Request est bloqué au niveau du BNG qui envoie un RADIUS Access-Request.

(13) En retour le RADIUS du client répond avec un RADIUS Access-Accept. Le message doit contenir les attributs suivants :

- Class ;
- Framed-IP-Address ;
- Framed-IP-Netmask ;
- Alc-Default-Router ;
- Alc-Primary-Dns ;
- Alc-Secondary-Dns.

(14) Le BNG met à jour le profil de l'abonné sur la base des informations descendues par le serveur RADIUS. Il envoie un message DHCPv6-ACK à l'abonné contenant les paramètres réseaux descendus par RADIUS.

5.5.3. Détail des échanges RADIUS et DHCPv6

5.5.3.1. DHCPv6-Solicit

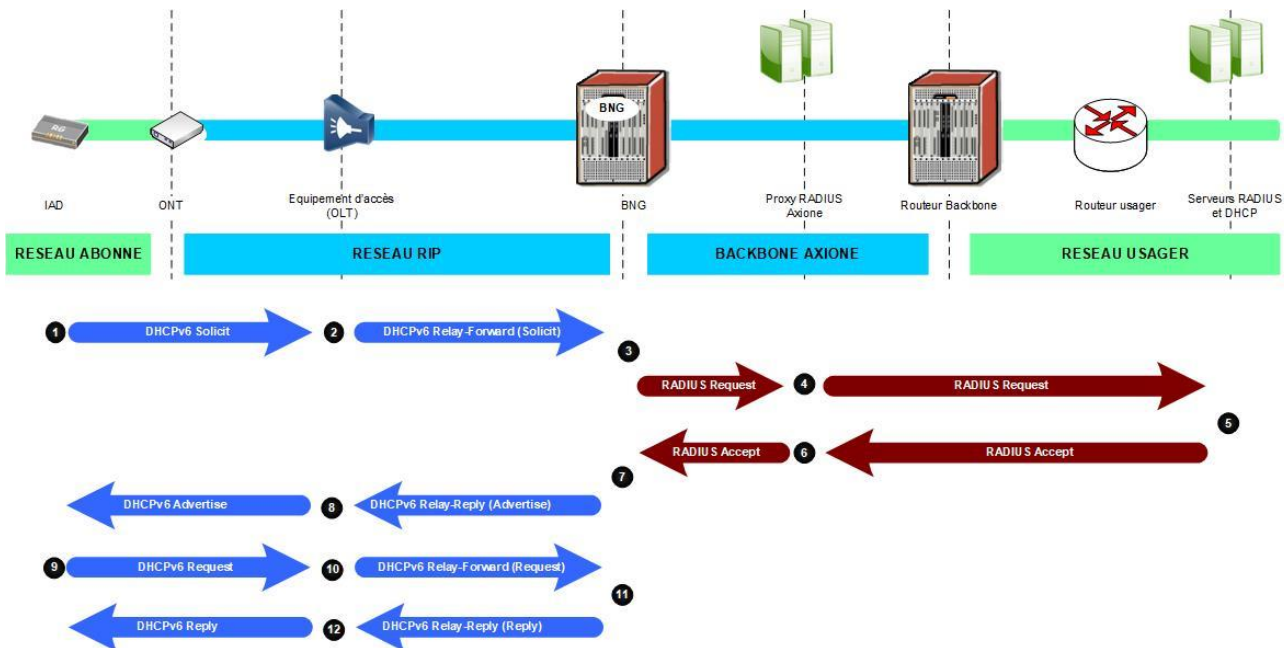


Figure 15 - Mode FULL RADIUS (transaction DHCPv6-Solicit)

IAD

(1) L'IAD envoie un DHCPv6-Solicit sur son port réseau.

Equipement d'accès (OLT)

(2) L'équipement d'accès se comporte en relai DHCPv6 en encapsulant la requête Solicit dans un message DHCPv6 Relay-Forward et y insère le circuit-id de l'abonné. Le circuit-ID étant l'option 18, Interface-ID, faisant apparaître les informations suivantes :

- Slot de l'équipement d'accès ;
- Port abonné ;
- Hostname de l'équipement d'accès.

BNG

Sur réception du message DHCPv6 Relay-Forward (Solicit), le BNG Nominal bloque la transaction jusqu'à ce que l'abonné soit identifié. Pour cela le BNG génère un RADIUS Access-Request à destination du Proxy RADIUS Fournisseur (3) en recopiant certains champs du message DHCP dans sa requête dont le circuit-id.

Proxy-RADIUS Fournisseur

Le Proxy-RADIUS Fournisseur identifie l'opérateur client de l'abonné sur la base de son circuit-id et proxifie l'access-request au RADIUS de l'opérateur client (4).

Le proxy-RADIUS peut si nécessaire en fonction du client opérateur rajouter et/ou supprimer des attributs de l'access-request initiale du BNG Fournisseur avant de le transmettre au RADIUS du client (cf chapitre suivant).

L'Access-Request transmis au client après traitement par le proxy-RADIUS contiendra à minima les informations suivantes :

- User-Name=<adresse_mac_IAD> ;
- User-Password = <mot-de-passe> ;
- NAS-IP-Address = <adresse IP du BNG auquel l'abonné est attaché > ;
- ADSL-Agent-Circuit-id=<circuit-id-access>;

Les attributs radius suivants seront transmis sur demande du client :

- Calling-Station-Id :
 - Pour un accès Point Multipoint = <nom-Fournisseur>#OLT#

RADIUS Client

Le RADIUS client authentifie l'abonné et renvoie un RADIUS access-accept (5) au proxy-RADIUS Fournisseur contenant les informations suivantes :

- Class ;
- Paramètres IPv4 en cas d'abonné en double pile :
 - Framed-IP-Address ;
 - Framed-IP-Netmask ;
 - Alc-Default-Router ;
 - Alc-Primary-Dns ;
 - Alc-Secondary-Dns ;
- Paramètres Ipv6 :
 - Alc-Ipv6-Address ;
 - Delegated-IPv6-Prefix ;
 - Alc-Ipv6-Primary-DNS ;
 - Alc-Ipv6-Secondary-DNS.

Proxy-RADIUS Fournisseur

Le PROXY-RADIUS Fournisseur transmet le RADIUS Access-Accept au BNG Fournisseur en ajoutant les attributs propriétaires nécessaires à l'activation de l'abonné (6) :

- Identifiant Service du client ;
- Identifiant de l'abonné ;
- Profil de QoS (dérive de l'attribut Class renvoyé par le client).

A réception de l'Access-Accept, l'abonné est instancié, au sein du BNG, dans le VPN du client avec son profil de QoS.

Le BNG prend le rôle de serveur DHCP. Il renseigne les paramètres réseaux de l'abonné, qui lui ont été communiqués par le serveur RADIUS, dans un message DHCPv6 Advertise puis l'encapsule par un entête Relay-Reply à destination de l'équipement d'accès, l'OLT (7).

S'ensuit alors un dialogue DHCPv6 standard entre l'IAD de l'abonné, 1 relais DHCP et le serveur DHCP du BNG :

- DHCPv6 Relay-Reply(Advertise) (7)
- DHCPv6 Advertise (8)
- DHCPv6 Request (9) ;
- DHCPv6 Relay-Forward (Request) (10) ;
- DHCPv6 Relay-Reply(Reply) (11) ;
- DHCPv6 Reply (12).

L'abonné dispose d'un bail (ou preferred-lifetime) de 2 heures.

5.5.3.2. DHCPv6-Renew

Chaque DHCP-Renew entraîne une nouvelle authentification de l'abonné. Si le profil de l'abonné a changé dans les bases RADIUS client la procédure de renouvellement de bail entrainera la mise à jour du profil de l'abonné.

Le schéma ci-dessous présente les échanges DHCP et RADIUS relatifs à un renouvellement de bail :

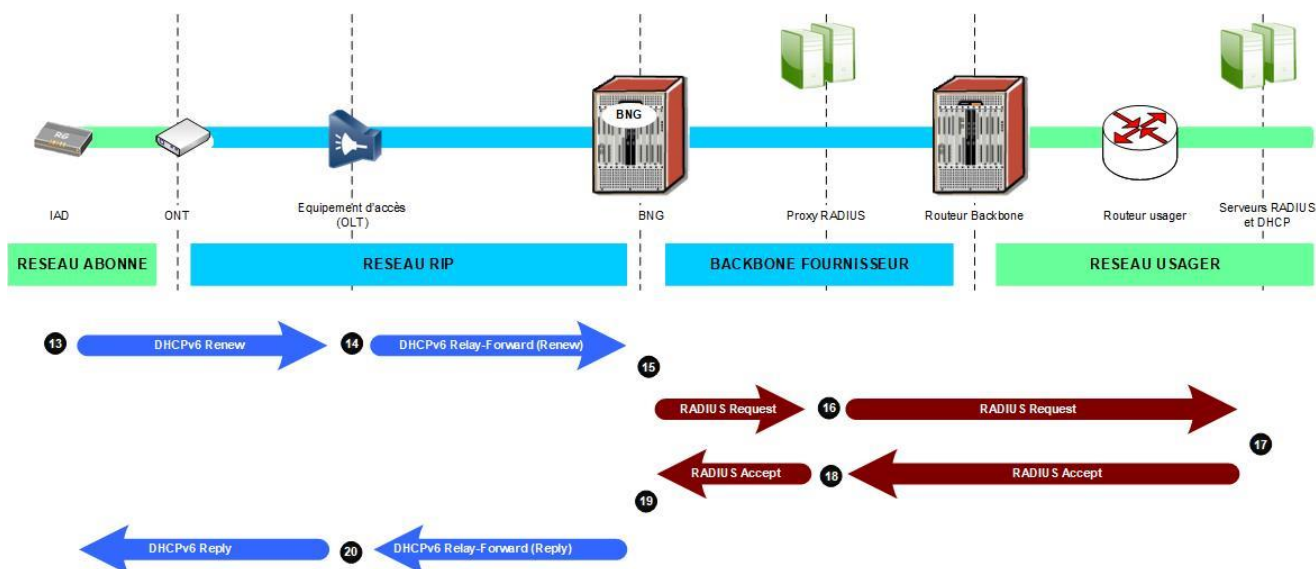


Figure 16 - Mode FULL RADIUS (renouvellement du Preferred-Lifetime DHCPv6)

(13) L'IAD de l'abonné envoie un message de type DHCPv6-Renew pour renouveler le bail dhcp en conservant la même adresse IP.

(14) DHCPv6-Renew est intercepté par l'équipement d'accès (OLT) et relayé dans un message DHCPv6 Relay-Forward (Renew) en y insérant le circuit-id de l'abonné. Le circuit-id étant l'option 18 DHCPv6.

(15) (16) Le message DHCPv6 Relay-Forward (Renew) est bloqué au niveau du BNG qui envoie un RADIUS Access-Request à destination du serveur client via le proxy Fournisseur.

(17) En retour le RADIUS du client répond avec un RADIUS Access-Accept. Le message doit contenir les attributs suivants :

- Class ;
- Paramètres IPv4 en cas d'abonné en double pile :
 - Framed-IP-Address ;
 - Framed-IP-Netmask ;
 - Alc-Default-Router ;
 - Alc-Primary-Dns ;
 - Alc-Secondary-Dns.
- Paramètres Ipv6 :
 - Alc-Ipv6-Address ;
 - Delegated-IPv6-Prefix ;
 - Alc-Ipv6-Primary-DNS ;
 - Alc-Ipv6-Secondary-DNS.

(18) Le BNG met à jour le profil de l'abonné sur la base des informations descendues par le serveur RADIUS.

(19) Le BNG renseigne les paramètres réseaux de l'abonné, qui lui ont été communiqués par le serveur RADIUS, dans un message DHCPv6 Reply puis l'encapsule par un entête Relay-Reply à destination de l'équipement d'accès, l'OLT.

(20) L'équipement d'accès OLT désencapsule le message DHCPv6 et le transmet à l'IAD de l'abonné.

5.5.4. Limitation connue

Dans le mode Full Radius, l'option DHCPv6 n°64 « Dual-Stack Lite AFTR Name » ne peut pas être délivrée au client DHCP. Le BNG Fournisseur est à l'origine de cette limitation car il ne reconnaît pas l'attribut RADIUS contenant le nom de domaine de l'AFTR.

5.6. Adressage IP des abonnés

5.6.1. Type d'adressage

L'adressage IP des abonnés est sous la responsabilité du client. Il peut être de type public, privé ou réservé selon les besoins de ses services.

Pour rappel les ranges d'adresses IP privées définis par l'IANA sont décrits dans le RFC1918 (Address Allocation for Private Internets) :

- 10.0.0.0 - 10.255.255.255 (10/8 prefix) ;
- 172.16.0.0 - 172.31.255.255 (172.16/12 prefix) ;
- 192.168.0.0 - 192.168.255.255 (192.168/16 prefix).

Le range d'adresses IP globales partagées est défini dans le RFC6598 (IANA-Reserved IPv4 Prefix for Shared Address Space) :

- 100.64.0.0 - 100.127.255.255 (100.64/10 prefix)

Cet espace d'adressage se rapproche, de par son utilisation, des ranges IP privés du RFC1918. Il n'est pas routé sur le réseau internet et est destiné à la numérotation des interfaces IPv4 des infrastructures mettant en relation les Carrier Grade Nat avec les équipements CPE des abonnés. Son usage permettant d'une part de contourner les éventuels dysfonctionnements du NAT des CPE lorsque la numérotation des interfaces inside et outside est de type privée, et d'autre part pour ne pas avoir de conflit entre l'adressage du lan des abonnés et wan des CPE.

5.6.2. Gestion des pools IP des abonnés

Lorsque les abonnés sont collectés dans les plaques Point-Multipoint (technologie GPON), le client ISP a la possibilité de gérer les pools IP en mode mutualisé ou par zone.

5.6.2.1. Mutualisation des pools IP

Avec ce mode d'adressage, le client ISP est en mesure de mutualiser les pools IP de ses abonnés entre plusieurs plaques Point-Multipoint du réseau du Fournisseur ou bien entre ses opérateurs de collecte.

En conséquence, les annonces de la session eBGP_Data sur l'interface de Collecte permettront de distinguer individuellement chacun des abonnés avec un préfixe spécifique /32 pour IPv4 ou les préfixes spécifiques IA_Na en /64 et IA_PD, de /32 à /64, pour IPv6 par IAD.

Dans ce mode, il est du ressort du client ISP de garantir l'unicité des adresses IP allouées aux abonnés. C'est-à-dire que le Fournisseur n'effectuera aucun contrôle sur les réponses Radius ; par exemple si une même adresse IP est allouée à deux abonnés différents sur 2 BNG différents, le préfixe spécifique sera annoncé en doublon.

En cas de transfert d'une plaque FTTH exploitée par le Fournisseur vers un autre opérateur de collecte, et vice-versa, il sera de la responsabilité du client ISP de gérer le nouvel adressage.

5.6.2.2. Gestion des pools IP par zone dans le réseau du Fournisseur

Dans ce mode d'adressage, le client ISP déclare au Fournisseur, à travers le fichier « Fiche d'interco OPERA Office », la liste des ranges d'adresses IPv4 et/ou IPv6 des abonnés ainsi que leur zone d'affectation.

Les routes spécifiques (/32 en IPv4 ou /32 à /64 en IPv6) des IAD sont filtrées par les BNG et seuls les ranges d'adresses sont annoncés dans le VPN IP.

En conséquence, les annonces de la session eBGP_Data sur l'interface de Collecte annonceront le préfixe correspondant à chacun des pools IP IAD.

Les pools IPv4 et/ou IPv6 fournis par le client sont associés au réseau de collecte d'une plaque.

Remarque : Pour chaque plaque, le client attribue une ou plusieurs plages IPv4 dont la taille à minima est celle d'un réseau de classe C (256 adresses).

5.6.3. Adresses IP réservées

Dans le mode « DHCP & Radius », les BNGs du Fournisseur utilisent une adresse de loopback active dans le contexte de routage dédié à l'opérateur client pour relayer les messages DHCP vers le serveur DHCP.

Au choix du client ces adresses de loopback, IPv4 ou IPv6 selon les besoins du service, sont :

- Soit les 2 premières adresses du premier sous réseau géré par les BNGs ;
- Soit 2 adresses appartenant à des sous réseaux distincts.

5.7. Profils de QoS Abonné IPoE

Le client peut demander l'implémentation de 3 profils de QoS maximum. Chaque profil est associé à une « Class » qui est échangée lors de l'authentification RADIUS comme décrit à la section « Echange Radius en mode IPoE ».

Les profils sont gérés au niveau du BNG Fournisseur.

Pour chaque profil de QoS, un maximum de 3 files d'attente ingress et egress (sens montant et descendant) est instancié par abonné.

Le trafic de l'abonné est mappé dans l'une ou l'autre de ces files d'attente en fonction du champ IP PRECEDENCE.

- VoIP : IP Precedence = 5, 6, 7 ;
- Business : IP Precedence = 3 ;
- DATA : IP Precedence = 0, 1, 2, 4.

Chaque file d'attente peut disposer d'une valeur de CIR et PIR qui lui est propre.

Un PIR global est défini pour l'abonné pour l'ensemble des files d'attente

Les valeurs de chaque classe de service sont données dans le tableau ci-dessous :

Service	CIR Up	PIR Up	CIR Down	PIR Down	Remarque
VoIP	500k	500k	500k	500k	Pour ce service : CIR=PIR
Business	10M / 100M	10M / 100M	10M / 100M	10M / 100M	Pour ce service : CIR=PIR
DATA	0M	300M	0M	1G	

Le débit maximum total pour un abonné est : 1Gbps / 300Mbps.

Le débit maximum de la classe Business dépend du débit Business souscrit (10 Mbits/s ou 100 Mbits/s).

Le schéma ci-dessous présente la gestion de la QoS pour un abonné OPERA Office :

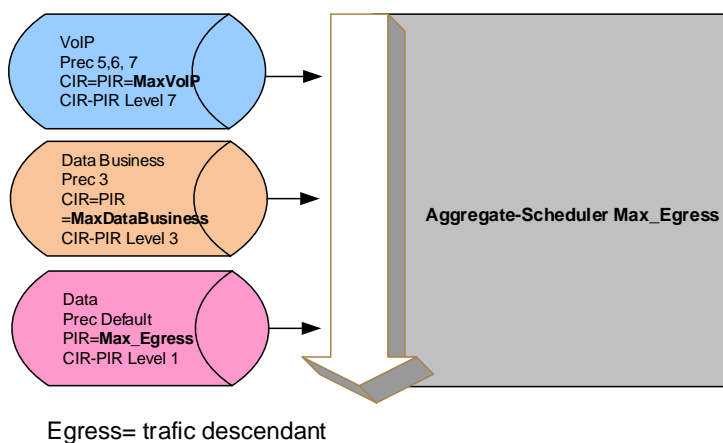
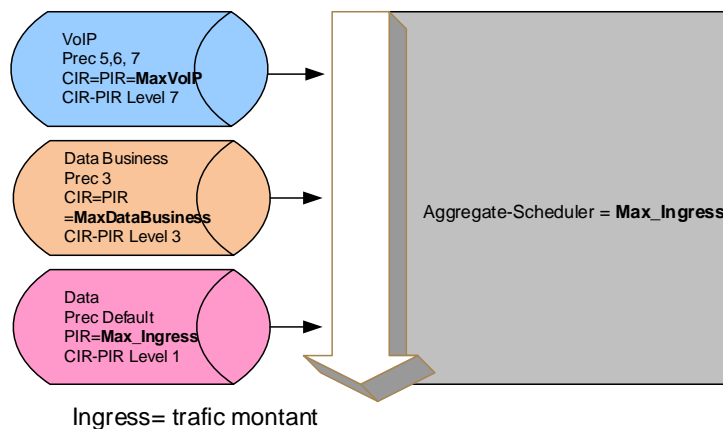


Figure 17 - Profil de QoS Abonné OPERA Office en mode IPoE

6.1. Principe et modélisation de la livraison L2TP



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

- Le Fournisseur est en charge du transport des sessions PPP depuis les sites Abonné jusqu'à l'interface de collecte ;
- 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 :

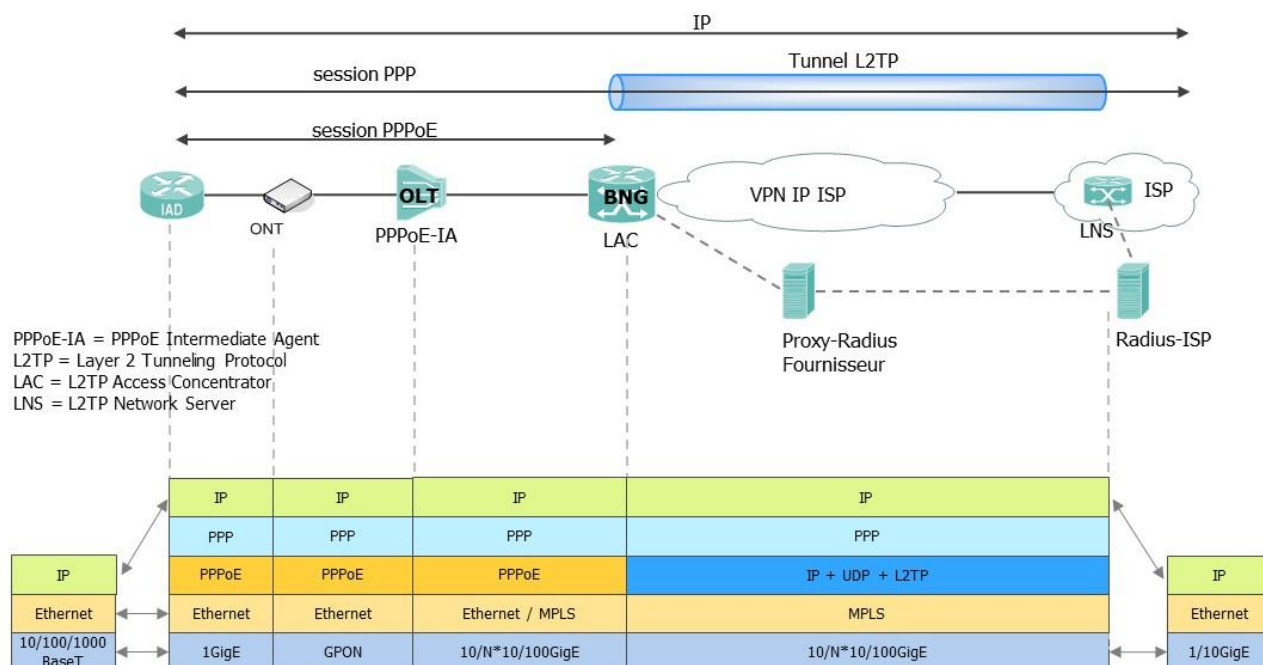


Figure 19 - Transport session PPP dans tunnel L2TP

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 authentifié 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'authentification 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.

6.2. 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 entraîne par conséquent un overhead de 52 octets maximum 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 sera monté sur le LNS de backup.

6.3. Identification Abonné

Le client peut identifier ses abonnés sur la base des attributs Radius « User-Name (attribut standard n°1) » et/ou « ADSL-Agent-Circuit-Id (attribut ADSL-Forum 3561 - n°1) ».

6.3.1. Identification sur la base du « User-Name »

Lors de la phase d'authentification, l'abonné se présente à travers le couple [« nom_abonné », « mot_de_passe »] attribué par le client.

Le format du « nom_abonné » devra être <identifiant-abonné>@<identifiant-client> avec :

- <identifiant-abonné> est une valeur alphanumérique. La chaîne de caractère doit contenir au moins un caractère et ne doit pas dépasser 64 caractères
- <identifiant-client> est une valeur alphanumérique qui identifie le client. Le client indique au moment de la commande « l'identifiant-client » à utiliser. L'identifiant du client 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 <identifiant-client> s'il est déjà utilisé par un autre client
 - L'identifiant-client doit contenir au moins 2 caractères et ne doit pas dépasser 63 caractères
 - Le client peut demander au Fournisseur d'ajouter l'<identifiant-client> dans le « nom_abonné » à condition que ce dernier ne contienne que l'<identifiant-abonné> lorsque l'abonné se présente

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.

L'attribut « ADSL-Agent-Circuit-Id » est utilisé par le Proxy RADIUS Fournisseur pour identifier l'Abonné et le serveur RADIUS client capable de traiter la requête.

6.3.2. Identification sur la base du «Agent-Circuit-Id »

Les équipements OLTs ajoutent le PPPoE Tag aux messages PADI/PADR/PADT avec la sous-option 0x01 (Agent-Circuit-Id).

Le format du PPPoE Tag est défini dans le document BBF TR-101 § 3.9.2. Il se compose de plusieurs champs dont le TAG_ID (0x0105 = Vendor-Specific) et le TAG_VALUE (vendor id= 0x000DE9 = BBF) suivis d'une suite de sous options selon les besoins. Par analogie à l'option 82 DHCPv4, les codes des sous options Agent Circuit ID et Agent Remote ID sont respectivement 1 et 2.

Le BNG recopie le Circuit-Id dans l'attribut Radius ADSL-Agent-Circuit-Id échangé avec le serveur Radius client.

Le format de l'attribut Radius ADSL-Agent-Circuit-Id est précisé au paragraphe « **3.2.6.Format du Circuit-ID spécifique aux OLTs** » du présent document.

6.4. Adressage IP des abonnés

Dans le mode de collecte PPPoE, les IAD doivent être adressés en IPv4 uniquement.

Le choix des adresses IPv4 des IAD Abonné est de la responsabilité du Client. Le Fournisseur ne participe pas au routage des adresses IPv4 du client.

6.5. Profils de QoS Abonné PPP

Le client peut demander l'implémentation de 3 profils de QoS maximum. Chaque profil est associé à une « Class » qui est échangée lors de l'authentification RADIUS comme décrit à la section « Echange Radius en mode PPPoE ». Les profils sont gérés au niveau du BNG Fournisseur.

Pour chaque profil de QoS, un maximum de 3 files d'attente ingress et egress (sens montant et descendant) est instancié par abonné. Chaque file d'attente peut disposer d'une valeur de CIR et PIR qui lui est propre.

Un PIR global est défini pour l'abonné pour l'ensemble des files d'attente.

Les valeurs de chaque classe de service sont données dans le tableau ci-dessous :

Service	CIR Up	PIR Up	CIR Down	PIR Down	Remarque
VoIP	500k	500k	500k	500k	Pour ce service : CIR=PIR
Business	10M / 100M	10M / 100M	10M / 100M	10M / 100M	Pour ce service : CIR=PIR
DATA	0M	300M	0M	1G	

Le débit maximum total pour un abonné est : 1Gbps / 300Mbps.

6.5.1. Trafic descendant

Dans le sens Client vers l'abonné, afin de différencier les différentes Classes de Service, le Client devra recopier 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. Par défaut tout le trafic abonné sera transporté en Best Effort.

- VoIP : IP Precedence = 5, 6, 7 ;
- Business : IP Precedence = 3 ;
- DATA : IP Precedence = 0, 1, 2, 4.

6.5.2. Trafic montant

Dans le sens Abonné vers Client, afin de différencier les différentes Classes de Service, le CPE abonné devra marquer la valeur des 3 bits de poids fort du champ DSCP (ou IP Precedence). Par défaut tout le trafic abonné sera transporté en Best Effort.

- VoIP : IP Precedence = 5, 6, 7 ;
- Business : IP Precedence = 3 ;
- DATA : IP Precedence = 0, 1, 2, 4.

7. Echanges RADIUS

7.1. Serveurs RADIUS Fournisseur et ISP

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 ISP 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 ISP. 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 ISP). Il faut noter que ce mécanisme n'est pas équivalent à un "Keep Alive" permanent et transmis à travers un Access-Request (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.

7.2. Echanges RADIUS en mode IPoE

Les sections « Détails des échanges RADIUS et DHCP » ont déjà décrit les échanges RADIUS.

Ce chapitre présente spécifiquement la médiation entre les attributs RADIUS communiqués par l'ISP et par le Fournisseur.

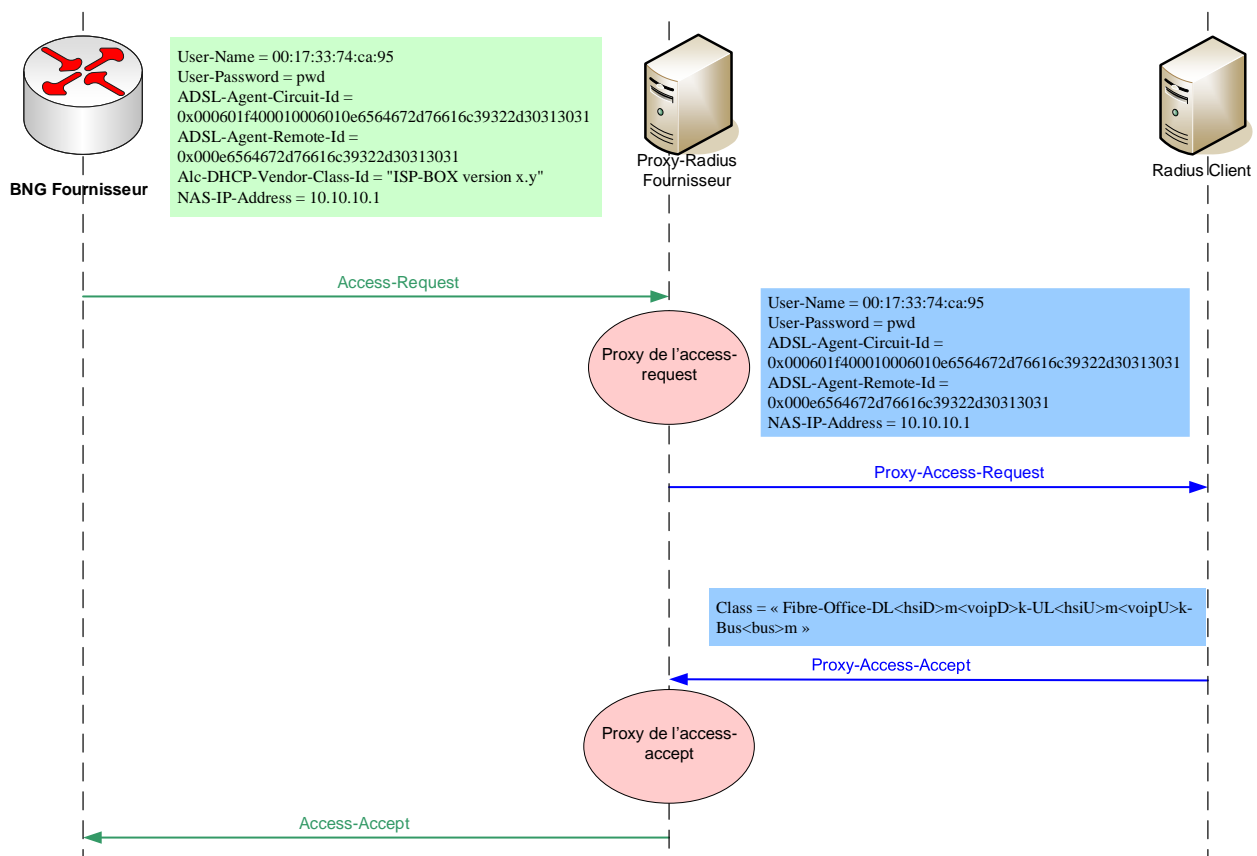


Figure 20 - Détails des Echanges Radius

7.2.1. Access-Request envoyé au client

Le message Access-Request, associé à un échange DHCPv4 et envoyé au client, contient les champs suivants :

- **User-Name** : l'adresse MAC de l'IAD est envoyée dans l'attribut User-Name. Le client peut demander au Fournisseur d'ajouter un realm (RFC 2486 §3) dans le User-name ;
- **User-Password** : mot de passe identique quel que soit l'abonné ;
- **NAS-IP-Address** : adresse IP du NAS (BNG) Fournisseur;
- **ADSL-Agent-Circuit-ID** et **ADSL-Agent-Remote-ID**. Il s'agit de la recopie des sous options 82 Circuit-id et Remote-id. Ils sont utilisés pour identifier la ligne de l'abonné.

Ces sous options sont encodées au format TLV (Type-Length-Value) dans le datagramme DHCP. Lorsque le BNG recopie le DHCP Circuit-ID (respectivement Remote ID) dans l'attribut Agent-Circuit-ID (respectivement Agent-Remote-ID), les 2 premiers octets (sub-option-type et length) sont retirés.

Pour un accès point multipoint :

- ▶ DHCP Circuit-ID : 0121**6f6c742d62736e34322d303120706f6e20312f312f30312f30312f342f312f312f**
- ▶ RADIUS Agent-Circuit-ID : 0x6f6c742d62736e34322d303120706f6e20312f312f30312f30312f342f312f312f

Remarque :

Pour les OLTs, la totalité de l'attribut radius Agent-Circuit-Id représente l'expression hexadécimale de codes ascii. Il peut être interprété comme une chaîne de caractères ASCII comme le stipule la RFC 4679 (DSL Forum Vendor-Specific RADIUS Attributes).

Les attributs radius suivants seront transmis sur demande du client :

- **Alc-DHCP-Vendor-Class-Id** : contenant l'option 60 DHCP (Vendor class identifier) de l'IAD. Cette option permet de connaître le type d'IAD installé chez l'abonné ;
- **Calling-Station-Id** : contenant le nom du fournisseur et le type d'équipement d'agrégation. Cette option peut être utilisée par le client pour identifier l'opérateur de collecte et le type d'infrastructure de collecte. Exemple :
 - Pour un accès point multipoint Calling-Station-Id = <nom-Fournisseur>#OLT#

7.2.2. Access-Accept du client

Le RADIUS client authentifie l'abonné et renvoie un RADIUS Access-Accept (5) au proxy-RADIUS Fournisseur contenant les informations suivantes :

- Class = OPERA-Office-DL<hsiD>m<voipD>k-UL<hsiU>m<voipU>k-Bus<bus>m
 - <hsiD> : La valeur du débit HSI down max en Mbit/s
 - <hsiU> : La valeur du débit HSI up max en Mbit/s
 - <voipD> : La valeur du débit VoIP down max en Mbit/s
 - <voipU> : La valeur du débit VoIP up max en Mbit/s
 - <bus> : La valeur du débit Business up/down 10 Mbits/s ou 100 Mbits/s.

Le champ Class, défini dans la RFC 2865, permet de différencier les profils à appliquer. Le BNG se base sur cet attribut pour identifier le profil de QoS devant être appliqué.

Les informations complémentaires suivantes sont requises dans le mode Full RADIUS

- Framed-IP-Address
- Framed-IP-Netmask
- Alc-Default-Router
- Alc-Primary-Dns
- Alc-Secondary-Dns

7.3. Echanges RADIUS en mode PPPoE

Le protocole d'authentification CHAP devra être utilisé pour l'authentification des abonnés.

Les attributs RADIUS échangés entre le Proxy RADIUS Fournisseur et le serveur RADIUS du client sont listés en annexe.

7.3.1. Etablissement des tunnels L2TP

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 publique 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 publique 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 ISP peut demander à ce 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 ISP déclare cette valeur au Fournisseur, à travers le fichier « Fiche d'interco OPERA Office ».

7.3.2. Synthèse des échanges lors de l'établissement d'une session PPP-L2TP

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

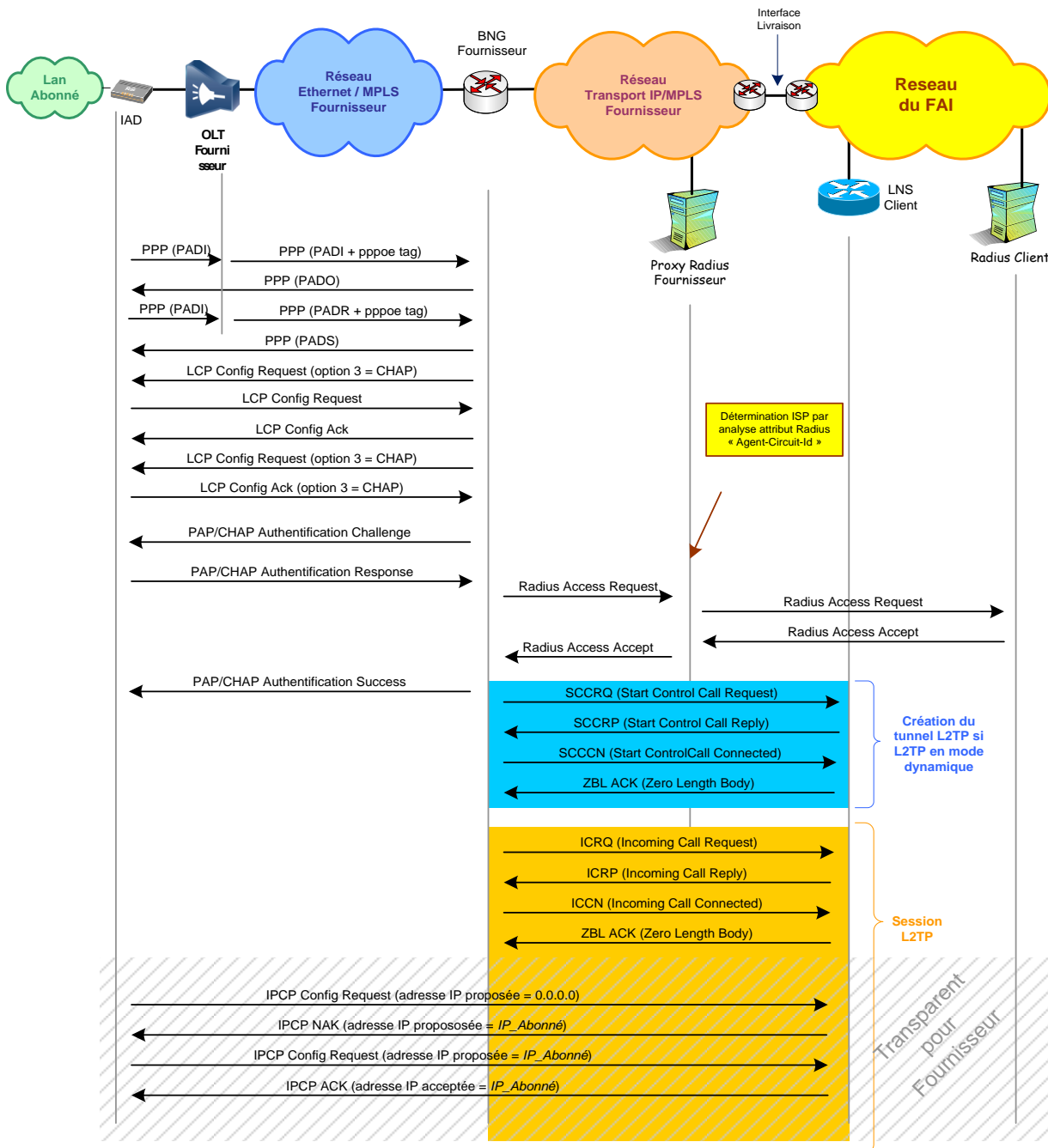


Figure 21 - Synthèse des échanges pour la création d'une session PPP-L2TP

7.3.3. 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.

L'authentification RADIUS

- Message « access-request » émis par le Proxy RADIUS Fournisseur vers le RADIUS du client

Attributs associés au paquet RADIUS « ACCESS_REQUEST »			
Nom de l'attribut	Numéro attribut	Description	Syntaxe
User-name	1	Nom de l'abonné	identifiant_abonné@identifiant_client
NAS-IP-Address	4	Adresse IP du BNG Fournisseur	XXX.XXX.XXX.XXX
Adsl-Agent-Circuit-Id	ADSL Forum N°1	Circuit Id de l'abonné	Access_Node_ID PON Rack/Frame/Slot/PON/ONU/OnuSlot/UNI/I-VID
NAS-Port-ID	87	NAS port ID	Interface logique de collecte du BNG associée à l'abonné
Alc-Client-Hardware-Addr	Alcatel N° 27	Adresse MAC IAD Abonné	xx.xx.xx.xx.xx
Acct-Session-Id	44	Identifiant de la session	
Calling-Station-Id	31	Identifiant Fournisseur et type équipement d'accès	#Nom-Fournisseur#OLT
CHAP-Password	3	Mot de Passe CHAP de l'abonné	Password
CHAP-Challenge	60	Challenge CHAP	Challenge

- Message « access-accept » émis par le RADIUS du client vers le Proxy RADIUS Fournisseur

Attributs associés au paquet RADIUS « ACCESS_ACCEPT »			
Nom de l'attribut	Numéro Attribut	Description	Syntaxe
Class	25	Profil à appliquer à l'Abonné	OPERA-Office-DL<hsiD>m<voipD>k-UL<hsiU>m<voipU>k-Bus<bus>m
Tunnel-Type ⁽¹⁾	64	Attribut obligatoire dans Access-Accept. Spécifie le type de tunnel à établir : valeur fixée à 3 pour L2TP.	3
Tunnel-Medium-Type ⁽¹⁾	65	Attribut obligatoire dans Access-Accept. Spécifie le type de protocole de transport pour le tunnel L2TP : valeur fixée à 1 pour IPv4.	1
Tunnel-Server-Endpoint ⁽¹⁾	67	Adresse IP publique du LNS terminant le tunnel L2TP	XXX.XXX.XXX.XXX
Tunnel-Assignment-ID ⁽¹⁾	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. L'identificateur du tunnel doit désigner de manière unique un LNS. Le Fournisseur recommande d'utiliser l'adresse IP publique du LNS pour cet identificateur. Dans le cas où plusieurs tunnels doivent être créés entre un BNG et un LNS, Le Fournisseur recommande d'ajouter une chaîne supplémentaire à l'adresse IP du LNS.	XXX.XXX.XXX.XXX

(1) : Envoyé uniquement lors d'un établissement dynamique du tunnel L2TP

- Message « access-reject » émis par le RADIUS du client vers le Proxy RADIUS Fournisseur

Aucun attribut n'est requis dans ce message.

Annexe 1 : Dictionnaire RADIUS

Standard

#

ATTRIBUTE	User-Name	1	string
ATTRIBUTE	User- Password	2	string
ATTRIBUTE	NAS-IP-Address	4	ipaddr
ATTRIBUTE	NAS-Port	5	integer
ATTRIBUTE	Service-Type	6	integer
ATTRIBUTE	Framed-IP-Address	8	ipaddr
ATTRIBUTE	Framed-IP-Netmask	9	ipaddr
ATTRIBUTE	Class	25	string
ATTRIBUTE	Configuration-Token	78	string
ATTRIBUTE	Calling-Station-Id	31	string
ATTRIBUTE	CHAP-Password	3	octets
ATTRIBUTE	CHAP-Challenge	60	octets
ATTRIBUTE	Tunnel-Type	64	string
ATTRIBUTE	Tunnel-Medium	65	string
ATTRIBUTE	Tunnel- Server-Endpoint	67	string
ATTRIBUTE	Tunnel- Assignment	82	string
ATTRIBUTE	NAS-Port-Id	87	string
ATTRIBUTE	Delegated IPv6 Prefix	123	ipv6pref

#

Alcatel vendor specifics

#

VENDORATTR6527	Alc-DHCP-Vendor-Class-Id	36	string
VENDORATTR6527	Alc-Default-Router	18	ipaddr
VENDORATTR6527	Alc-Primary-Dns	9	ipaddr
VENDORATTR6527	Alc-Secondary-Dns	10	ipaddr
VENDORATTR6527	Alc-Client-Hardware-Addr	27	MAC addr
VENDORATTR6527	Alc-Ipv6-Address	99	ipv6addr
VENDORATTR6527	Alc-Ipv6-Primary-DNS	105	ipv6addr
VENDORATTR6527	Alc-Ipv6-Secondary-DNS	106	ipv6addr

#

#ADSL-Forum

#

VENDORATTR3561	ADSL-Agent-Circuit-Id	1	string
VENDORATTR3561	ADSL-Agent-Remote-Id	2	string

Annexe 2 : Glossaire

ACL	Access Control List
BGP	Border Gateway Protocol
BNG	Broadband Network Gateway
CIR	Committed Information Rate
DHCP	Dynamic Host Configuration Protocol
DSCP	Differentiated Service Code Point
GPON	Gigabit Passive Optical Network
HSI	High Speed Internet
IAD	Integrated Access Device
IGMP	Internet Group Management Protocol
LAN	Local Area Network
MSDP	Multicast Source Discovery Protocol
NRO	Nœud de Raccordement Optique
OLT	Optical Line Terminal
ONT	Optical Network Terminal
PIM-SM	Protocol Independant Multicast – Sparse Mode
PIM-SSM	Protocol Independant Multicast – Source Specific Multicast
PIR	Peak Information Rate
PPP	Point-to-Point Protocol
PPPOE	Point-to-Point Protocol over Ethernet
RFC	Request For Comment
RP	Rendez-vous Point
STB	Set Top Box
VLAN	Virtual LAN
VoD	Vidéo on Demand
VoIP	Voice Over IP
VPN	Virtual Private Network
VPLS	Virtual Private Lan Service