Access Backhauling Using L2TP - Technical Specifications

Current version: 1.1.7

Date: 2023.11.16

1. Introduction 4
2. L2TP Backhauling ServiceOverview 5
3. Access Line 6
   3.1 Access Links Physical Specifications 6
      3.1.1 Copper Access Lines 6
      3.1.2 Fiber Access Lines 9
   3.2 Access Links Layer 2 Specifications 10
      3.2.1 Ethernet Frames Specifications 11
      3.2.2 End User Equipment MTU 11
      3.2.3 Frame Marking 11
      3.2.4 Access Protocol 12
      3.2.5 User Circuit Identification 12
4. ENNI 13
   4.1 Delivery Site 13
   4.2 ENNI Physical Specifications 13
      4.2.1 ENNI Connection Rates 13
      4.2.2 LAG (Link Aggregation) Feature Implementation 14
   4.3 ENNI Layer 2 Specifications 14
      4.3.1 Ethernet Frames Specifications 14
      4.3.2 Interconnection Port Frame Marking 14
5. Service Operation 16
   5.1 RADIUS Role 16
      5.1.1 Proxy RADIUS 16
      5.1.2 Static RADIUS 16
   5.2 L2TP Protocol 16
   5.3 L2TP Tunnel Establishment 16
      5.3.1 L2TP Tunnel Establishment In Dynamic Mode 16
      5.3.2 L2TP Tunnel Establishment In Static Mode 17
   5.4 PPP Session Establishment 18
   5.5 LNS Resiliency 18

5.6 RADIUS Accounting 18
6. Service Configuration 19
6.1 IP Addressing 19
6.1.3 Proxy RADIUS IP Adresses 19
6.1.4 LNS IP Addresses 19
6.1.5 Customer RADIUS Addresses 20
6.1.6 User's IP Addresses 20
6.2 Routing 20
6.2.1 EBGP Session Characteristics 20
6.2.2 Resiliency 21
6.3 Traffic 23
6.3.1 RADIUS Traffic 23
6.3.1 User Traffic 23
6.4 RADIUS In ProxyMode 23
6.4.1 RADIUS Server Configuration 23
6.4.3 RADIUS Accounting Attributes 26
6.4.4 RADIUS Tags Usage 27
6.4.5 Users Identification Format 28
6.4.6 RADIUS Health Check 28
16.5. Static RADIUS Mode 28
7. Billing Of The ENNI Traffic 30
Annex A - Glossary 31
Annex C - Covage's 100G Sites 33

Changelog

Date	Version	Changelog
2017-12-13	0.9	Document creation
2018-04-24	0.9.1	Deleted the NO-EXPORT community rule for BGP routes advertised by COVAGE
2018-07-09	0.9.2	Added MTU value rules for the ENNI The document now states clearly that COVAGE will not accept fragmented L2TP packets
2018-08-22	0.9.3	Added the ONT requirement for the service operation Added the recommandation to shape traffic for sub rate fiber services
2018-09-01	0.9.4	Added VDSL profiles
2019-02-28	1.0	Added static RADIUS mode
2019-03-06	1.1	Changed VDSL Max profiles
2019-07-25	1.1.1	Introduced backhauling from Orange's network
2020-02-25	1.1.3	Reworked section 3 for clarity
2021-04-21	1.1.4	Added fiber profile 1Gbps/800Mbps
2021-09-15	1.1.5	Added CONFORT FIBER Offer
2022-12-08	1.1.6	Added technical specifications for Orange’s Public Initiative Networks

1. Introduction

This document defines the technical specifications for the **« L2TP Access Backhauling »** Service, referred to as **« the Service »**. This service relies on **xDSL** and **GPON** access lines.

The following terminology is used throughout the document:

- **Customer:** A Customer is a Telecommunication Operator using the Service from Covage for an End User.
- **End User:** The End User is the natural or legal person who has subscribed with the Customer to a service which is provided by the Customer on the basis of the L2TP Access Backhauling Service.
- **Network Element:** A Network Element is an architectural concept that represents telecommunication equipment that performs network element functions.
- **End User's Site:** The End User's Site is the geographical location hosting the End User.
- **End User's Network Element:** An End User's Network Element is a Network Element located at the End User's Site.
- **ENNI:** The External Network-to-Network Interface (ENNI) is a reference point representing the boundary between two Networks that are operated as separate administrative domains.

This document describes:

- The L2TP Access Backhauling Service.
- The requirements to be borne by the **Customer**.
- The xDSL or GPON traffic backhauling from **Covage's network** to the **Customer's network** using an L2TP tunnel.

2. L2TP Backhauling Service Overview

The Service is an authentication and traffic backhaul offer, from Covage's network to the Customer's network.

The service is comprised of:

- An xDSL or GPON **Access Line** on each **End User's Site**.
- A Customer connectivity to Covage's network through an **ENNI**. This connectivity can be supported on **10GE** or **100GE** interfaces.

  This ENNI is delivered on a site where a **Covage's network Element** supportting the Service is present.

  This site is called the **Delivery Site**.
- An End User authentication and session management layer through **RADIUS** and **L2TP** exchanges between Covage's network and the Customer's network. Covage's RADIUS server can behave as a **Proxy RADIUS**, relaying authentication requests to the customer to be processed, or respond locally to authentication requests in a predefined manner. The former method is called hereafter **Static RADIUS**
  Once authenticated, the **End User's Network Element** establishes a **PPP** session towards a Customer's network Element.
  This PPP session is backhauled on Covage's network through an L2TP tunnel, and provides a means to collect the End User's **IP Traffic**.

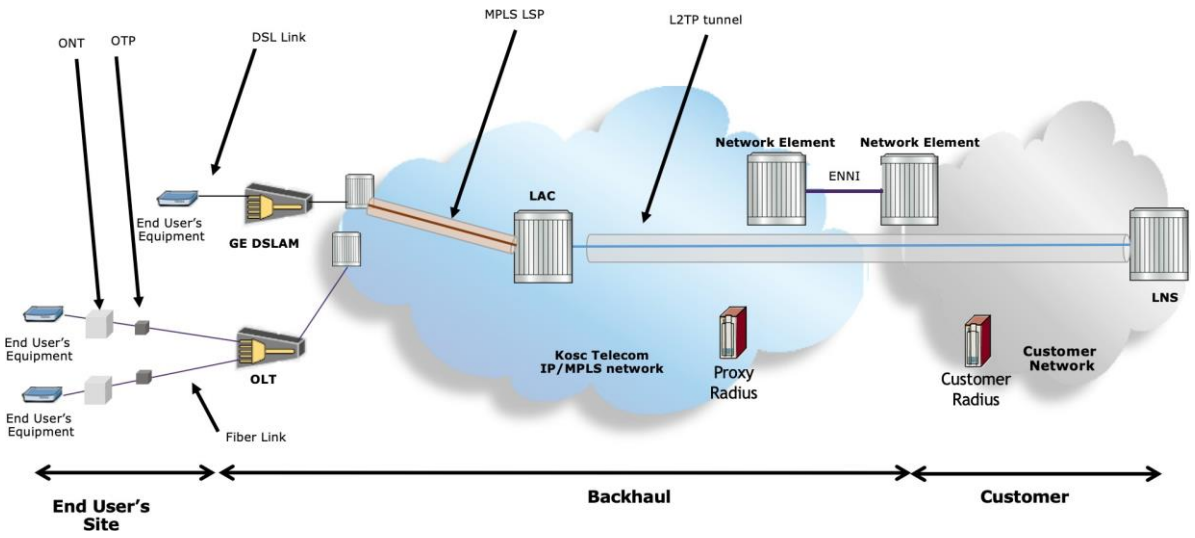

Figure 1 : Service Topology Overview

The traffic is backhauled solely in Mainland France and Corsica and does not include French overseas departments and territories.
On Covage's network, the End User's PPP sessions flowing through xDSL or GPON Access Lines are treated similarly and tunneled in L2TP tunnels to the Customer's network.

A list of Covage's Sites on which the service can be delivered is provided in **Annex B**.

3. Access Line

Access Lines are provided through the following Network Elements: A

- **DSLAM** for copper Access Lines
- An **OLT** for fiber Access Lines

PPP frames are transported from a DSLAM or OLT towards a Covage's Network Element behaving as a **LAC** and forwarded to the Customer's Network Element, behaving as an **LNS**, using an L2TP tunnel.

Some Access Lines are connected to a third party network.

Product Family Name	Access Network	Technology	Support	Maximum Downstream Rate (Mbps)	Maximum Upstream Rate (Mbps)	MTU (octets)	Demarcation Device
ADSL Max	Covage	ADSL ATM	Copper Pair	24	1	1500	None
ADSL Max	Orange	ADSL ATM	Copper Pair	24	1	1500	None
VDSL Max	Covage	VDSL PTM	Copper Pair	100	30	1500	None
VDSL Max	Orange	VDSL PTM	Copper Pair	100	30	1500	None
SDSL Max	Covage	SDSL EFM	Copper Pair	5,7	5,7	1500	None
ESSENTIEL Fibre	Covage	GPON	Single Fiber	1000	800	1500	Yes
CONFORT Fibre	Covage	GPON	Single Fiber	1000	800	1500	Yes

Table 1: Access-Lines for L2TP Service

3.1 Access Links Physical Specifications

3.1.1 Copper Access Lines

The End User's Sites connectivity on Copper Access Lines is provided through the following commercial offerings:

- **ADSL Max**
- **VDSL MAX**

The physical connectivity of the End User's Site is supported by a twisted copper pair delivered on a **Copper Termination Point (CTP)**. The Customer must provide an xDSL End User's Equipment that will be connected to the CTP. Theses offerings are based on the xDSL technologies.

The synchronization informations provided in sections ***3.1.1.1*** and ***3.1.1.2*** are indicative as the access synchronization for xDSL links is dependent of the quality of the copper line.
Notwithstanding the synchronization characteristics, the bandwidth provided to the End User's Site is not guaranteed.

3.1.1.1 ADSL Max on Covage's network

ADSL link synchronization can reach **24 Mbps downstream** and **1 Mbps upstream** in optimal conditions.

ADSL link conditions are constrained by the physical characteristics of copper lines. In order to adapt the ADSL link to the line characteristics the following ADSL profiles are available on Covage's DSLAMs.

ADSL Profile	Channel Mode	Downstream Physical Rate in Kbps	Upstream Physical Rate in Kbps	SNR Downstream Target	SNR Upstream Target
ADSL_24M	interleaved	160-24000	96-1024	6	6
ADSL_512K	interleaved	500-608	60-160	6	6
ADSL_2M	interleaved	608-2432	320-1024	6	6
ADSL_SAFE1	interleaved	160-16128	96-1024	10	8
ADSL_SAFE2	interleaved	160-16128	96-1024	15	12
ADSL_PERF1	fast	160-30000	96-1024	3	3
ADSL_PERF2	fast	160-30000	96-1024	1	1

Table 2: ADSL Profiles

Remark:

> The **ADSL_24M** profile is the one applied per default on ADSL links.

3.1.1.2 ADSL Max on Orange's network

ADSL link synchronization can reach **24 Mbps downstream** and **1 Mbps upstream** in optimal conditions.

ADSL link conditions are constrained by the physical characteristics of copper lines. The traffic from those lines is backhauled through Orange DSLAMs.

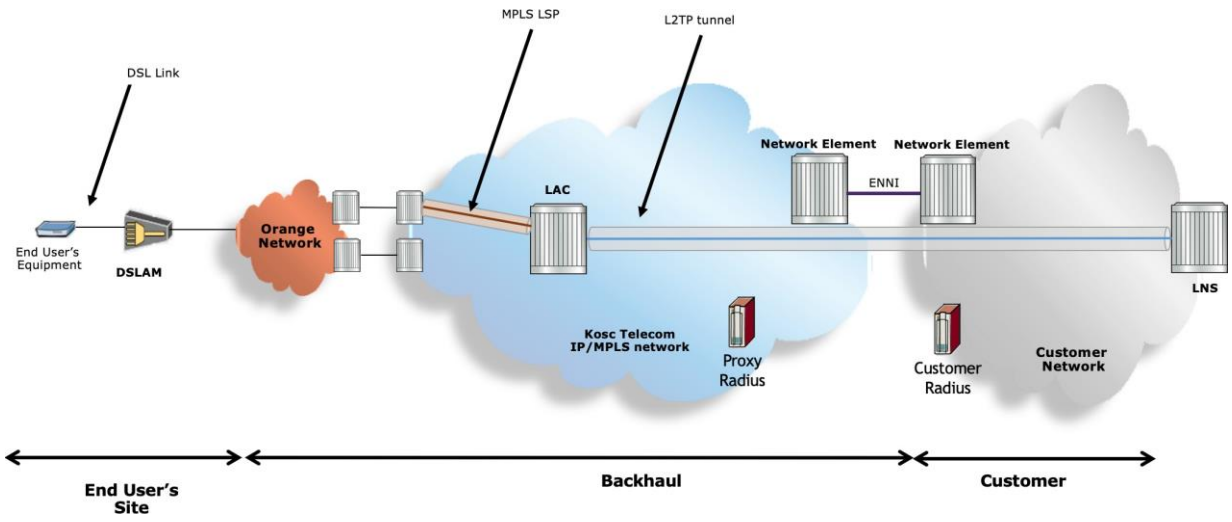

Figure 2 : Bitstream via Orange Topology Overview

Remark:

> - Orange tested a number of ADSL modems for compatibility with its DSLAM equipments. The devices list as well as test methodology are available at the following link https://www.orange.com/fr/Groupe/Activites/Les-reseaux/Documentation/Documentation-reseaux under the title *"Offre d'accès et collecte DSL"*. Any Client subscribing to an access-line through Orange's network must comply to the interoperability requirements listed in this documentation.

- It is not possible to change the ADSL profile

3.1.1.3 VDSL Max on Covage's network

VDSL link synchronization can reach **100 Mbps downstream** and **30 Mbps upstream** in optimal conditions.

VDSL link are activated using **Ethernet in the First Mile** (EFM/PTM) path mode

VDSL link conditions are constrained by the physical characteristics of copper lines. In order to adapt the VDSL link to the line characteristics the following VDSL profiles are available on Covage's DSLAMs. These are using either 17a or 8b spectrum profile

VDSL Profile	Channel Mode	Downstream Physical Rate in Kbps	Upstream Physical Rate in Kbps	SNR Downstream Target	SNR Upstream Target
VDSL_17a	interleaved	5000-100000	600-30000	8	8
VDSL_17a_SAFE1	interleaved	5000-70000	600-20000	12	12
VDSL_17a_SAFE2	interleaved	5000-70000	600-20000	16	16
VDSL_17a_PERF1	fast	5000-100000	600-30000	3	3
VDSL_17a_PERF2	fast	5000-100000	600-30000	1	1
VDSL_8b	interleaved	5000-40000	600-10000	8	8
VDSL_8b_SAFE1	interleaved	5000-35000	600-15000	12	12
VDSL_8b_SAFE2	interleaved	5000-35000	600-15000	16	16
VDSL_8b_PERF1	fast	5000-40000	600-10000	3	3
VDSL_8b_PERF2	fast	5000-40000	600-10000	1	1

Table 3: VDSL Profiles

3.1.1.4 VDSL Max on Orange's network

VDSL link synchronization can reach **100 Mbps downstream** and **30 Mbps upstream** in optimal conditions.

VDSL link are activated using **Ethernet in the First Mile** (EFM/PTM) path mode The traffic

from those lines is backhauled through Orange DSLAMs.

Remark:

> - Orange tested a number of VDSL modems for compatibility with its DSLAM equipments. The devices list as well as test methodology are available at the following link https://www.orange.com/fr/Groupe/Activites/Les-reseaux/Documentation/Docume ntation-reseaux under the title *"Offre d'accès et collecte DSL"*. Any Client subscribing to an access-line through Orange's network must comply to the interoperability requirements listed in this documentation.
> - It is not possible to change the VDSL profile

3.1.1.5 Unbundling

The ADSL MAX or VDSL MAX service is offered on unbundled local loops. These loops may be:

- Fully unbundled

- Partially unbundled

For totally unbundled local loops, POTS support will be removed after the transfer of the copper line on Covage's Network Element and the phone number associated will be lost.

For areas where Covage chose not to unbundle the local loop, bitstream traffic will be collected using the *"Optimum Collect"* offering from Orange.

3.1.2 Fiber Access Lines

The End User's Sites connectivity on Fiber Access Lines is provided through the following commercial offering:

- ESSENTIEL FIBRE
- CONFORT FIBRE

These offering are based on the **GPON** technology.

3.1.2.1 ESSENTIEL FIBRE

The physical connectivity of the End User's Site is supported by a single fiber delivered on an **Optical Termination Point (OTP)**. The OTP is a passive device installed at the optical penetration point in the End User's Site.

For each Fiber Access Line, Covage provides an **Optical Network Terminal (ONT)** behaving as the demarcation point for the Service. The ONT is equipped with an RJ45 Gigabit Ethernet interface behaving as the **UNI**. **The use of the ONT device provided by COVAGE is mandatory to operate the Service. No third party ONT will be tolerated.**

GPON access synchronization is **2.5 Gbps downstream** and **1.25 Gbps upstream**.

On the UNI, End User's IP Traffic can reach the following values depending on the commercial offer.

Offer	Upstream Peak Rate	Downstream Peak Rate
PROFESSIONAL FIBER 300	250 Mbps	300 Mbps
PROFESSIONAL FIBER 1000	250 Mbps	1 Gbps
ESSENTIEL FIBRE 1000	800 Mbps	1 Gbps

Table 4: Fiber Rates

IP Bandwidth is not guaranteed for End User's Site as resources are shared on the GPON tree.

In order to be protected from bandwidth throttling, the End User's Equipment should implement a traffic shaping mechanism. The shaper should limit the traffic to the rate subscribed to by the Customer.

3.1.2.2 CONFORT FIBRE

The physical connectivity of the End User's Site is supported by a single fiber delivered on an **Optical Termination Point (OTP)**. The OTP is a passive device installed at the optical penetration point in the End User's Site.

For each Fiber Access Line, Covage provides an **Optical Network Terminal (ONT)** behaving as the demarcation point for the Service. The ONT is equipped with an RJ45 Gigabit Ethernet interface behaving as the **UNI**. **The use of the ONT device provided by COVAGE is mandatory to operate the Service. No third party ONT will be tolerated.**

GPON access synchronization is **2.5 Gbps downstream** and **1.25 Gbps upstream**.

On the UNI, End User's IP Traffic can reach the following values depending on the commercial offer.

Offer	Upstream Peak Rate	Downstream Peak Rate	Guaranteed Rate (symmetrical)
CONFORT FIBRE 5M	800 Mbps	1 Gbps	5 Mbps
CONFORT FIBRE 20M	800 Mbps	1 Gbps	20 Mbps

Table 4: Fiber Rates

In order to protect the guaranteed rate, Covage has implemented a traffic prioritization of CONFORT Fibre traffic over non-guaranteed accesses. By Default, Covage network equipment will classify packets from CONFORT Fibre depending on the guaranteed rate subscribed by the User.

If congestion occurs, the exceeded packets will be dropped.

In order to be protected from bandwidth throttling, the End User's Equipment should implement a traffic shaping mechanism. The shaper should limit the traffic to the maximum peak rate subscribed to by the Customer.

3.1.2.3 ONT Specifications

The Customer must guarantee that the End User's Site where the ONT will be deployed is equipped with a power outlet.
Covage will not provide the cabling between the ONT and the End User's Equipment.

Specification item	Value
Uplink	G.984, G.988 standard compliant
Downlink	RJ-45 10/100/1000 auto negotiating Ethernet port
Dimensions	Less than 150x115x30 mm
Weight	Less than 500 g (including power adapter)
Operating Temp	-5°C to 45°C
Mounting	Desk or wall mounted
Power Spec.	11-14V (with external AC adapter)
Power Consumption	Less than 6W

Table 5: ONT general specifications

Remark:

> These informations are indicative and may vary slightly for a given site.

3.2 Access Links Layer 2 Specifications

3.2.1 Ethernet Frames Specifications

Ethernet frames generated by the End User's equipment must conform to the **IEEE 802.3** standard.

3.2.2 End User Equipment MTU

The **End User** is a subscriber of the services offered by the Customer. The End User connects an equipment to one of Covage's Access Links in order to use the Customer's services.

The MTU for frames generated and received by the Customer’s End User must be smaller than or equal to **1500 bytes**.

Any frame bigger than **1500 bytes** will be discarded in Covage's network.

3.2.3 Frame Marking

3.2.3.1 ADSL Max on Covage's network

Only the VPI/VCI 8/35 marking should be used at the ATM layer. Other markings will be dropped. At the Ethernet layer the Customer's End User equipment **must not** use **802.1q** or **802.1p** marking. Any frame that fails to comply to this rule is **discarded** at DSLAM or OLT level.

3.2.3.2 ADSL Max on Orange's network

The ADSL Max offering through Orange's network supports single or bi-VC marking.

The following values must be used for the VPI/VCI.

- VPI/VCI = 8/35 for the first VC, also used for single VC services.
- VPI/VCI = 8/50 for the second VC.

3.2.3.3 VDSL Max on Covage's network

At the Ethernet layer the Customer's End User equipment **must not** use **802.1q** or **802.1p** marking. Any frame that fails to comply to this rule is **discarded** at DSLAM or OLT level.

3.2.3.4 VDSL Max on Orange's network

The VDSL Max offering through Orange's network supports single or bi-VLAN marking. The following values must be used for the VLAN_ID.

- VLAN_ID = 835 for the first VLAN, also used for single VLAN services.
- VLAN_ID = 850 for the second VLAN.

3.2.3.5 Essentiel Fibre / Confort Fibre on Covage's network

At the Ethernet layer the Customer's End User equipment **must not** use **802.1q** or **802.1p** marking. Any frame that fails to comply to this rule is **discarded** at OLT level.

3.2.3.6 Essentiel Fibre on Orange's Public Initiative Networks

At the Ethernet layer the Customer's End User equipment **must** use **802.1q** or **802.1p** marking. Any frame that

fails to comply to this rule is **discarded** at OLT level.

- For **Essentiel Fibre** offer, the tag to use is **835**.

3.2.4 Access Protocol

Only PPPoE protocol can be used at the access.

Only *one* PPPoE session can be provided for an Access Line. This is enforced by limiting to one the number of PPPoE sessions based on End User MAC address on the LAC.

3.2.5 User Circuit Identification

User circuit identification is based on the use of the **"circuit-id"** attribute. The "circuit-id" gives information about the DSLAM/OLT identifier, and the physical characteristic of the End User Equipment's connection to the DSLAM/OLT (chassis/card/port).

Circuit-id examples:

```
DSLAM.123.abc.paris.net.kosc atm 0/11/0/21:8.35
```

This identification is relayed by the Proxy RADIUS to the Customer RADIUS during RADIUS exchange.

4. ENNI

4.1 Delivery Site

The Delivery Site is where the External Network to Network Interface or ENNI between the networks of Covage and the Customer is located. The ENNI is used to deliver all the L2TP encapsulated PPP sessions collected for the Customer.

No demarcation device is delivered by Covage to the Customer, the Service is directly delivered on one or more optical fiber pairs to the **Optical Distribution Frame (ODF)** at the Delivery site.

If the Customer subscribes to other services offered by Covage, it is possible to use the same physical ENNI and use dot1q tags to separate the traffic issued from different services.

4.2 ENNI Physical Specifications

4.2.1 ENNI Connection Rates

The offered rates at the Delivery Site are 10 Gbps, 20 Gbps, 40 Gbps or 100 Gbps. 20 Gbps and 40 Gbps links are achieved using LAG. The ENNI carries the Service traffic, including RADIUS flows.

Data rate (Gbps)	No. and Service Interface Type	Optical Fiber Type	Nominal Wavelength	Receiver Optical Power Range	Launch Optical Power Range	Max. Dist.	No. of Optical Pairs
10	1 port 10G LR	Monomode	1310 nm	2 dBm max -7 dBm min	2 dBm max -7 dBm min	10 km	1
20	2 ports 10G LR	Monomode	1310 nm	2 dBm max -7 dBm min	2 dBm max -7 dBm min	10 km	2
40	4 ports 10G LR	Monomode	1310 nm	2 dBm max -7 dBm min	2 dBm max -7 dBm min	10 km	4
100	1 port 100G LR4	Monomode	1310 nm	2.4 dBm max -8.4 dBm min	2.4 dBm max -8.4 dBm min	10 km	2

Table 6: ENNI physical specifications

Remarks:

- The connection rates are expressed at Ethernet level.
- If the required Connection cannot be delivered through the above interface choices, a tailor-made offer could be implemented on-demand at the discretion of Covage.
- The provisioning of optical attenuators to adjust the optical levels between Covage equipment and the Customer equipment is the responsibility of the Customer. The Service Interface type is determined by Covage during the preliminary technical survey.
- The connector type (e.g. SC/APC, LC/LC, SC/LC) will depend of on-site requirements at the ODF location where Covage and the Customer are both located.

Accordingly, the Customer must limit its traffic to the subscribed contractual rate for the Service to operate correctly.

The implementation of a traffic shaping mechanism is recommended on the Customer's equipment at both ends.

The total of the Access Lines speeds may exceed the ENNI connection rate (overbooking of the ENNI). In case of ENNI overbooking the full data rate subscribed for each access link cannot be guaranteed. The overbooking rate is free and under the responsibility of the Customer who must ensure the smooth flow of traffic to its own End Users. A list of the sites that can support 100 Gbps rate is available in Annex C.

4.2.2 LAG (Link Aggregation) Feature Implementation

The LAG feature is implemented on Covage equipment for all data rate types at the ENNI. This allows for higher bandwidth on the ENNI.

Covage recommends enabling LACP on the Customer equipment (**802.3ad** Link Aggregation). Auto-

negotiation feature must be enabled on all ports of the LAG.

The **« Minimum Link »** feature is not deployed by Covage. As long as a link is operational, the LAG remains active.

LAGs are configured in load-balancing mode on all the links set of Covage equipment. **Active- Standby mode is not implemented.**

If this shall not be possible for the Customer to enable LAG feature in its network, LACP feature will be disabled on Covage equipment to allow the Customer to operate with a physical port without LAG or with a LAG without LACP.

4.3 ENNI Layer 2 Specifications

4.3.1 Ethernet Frames Specifications

Ethernet frames generated by the Customer equipment must conform to the **IEEE 802.3** standard:

- **802.3ae** for 10GE interface
- **802.3bm** for 100GE interface

Ethernet frames must be VLAN tagged in compliance with the **802.1q** standard.

The transmission mode on the different service interfaces is **Full Duplex**, and must comply to the **IEEE 802.3x** standard.

The Ethertype value used must be of 0x8100 on both dot1q and QinQ interfaces. Any frame using another Ethertype will be dropped.

COVAGE implements a 9212 MTU value on the ENNI. The customer **must** support at least an MTU of 2000 in order to guarantee the proper operation of the service.

COVAGE will **not** accept fragmented L2TP packets.

4.3.2 Interconnection Port Frame Marking

The Ethernet link between the Customer’s peering node and Covage's network supports dot1q VLAN tagging for L2TP delivery. The VLAN tag to be used is provided by the Customer in the range 1-4090.

Remark:

- If the same physical port is used to provide the Customer with an E-Access/Premium service termination, VLAN tags must be distinct for the two services. The E-Access service is described in another document.

5. Service Operation

5.1 RADIUS Role

5.1.1 Proxy RADIUS

The Proxy RADIUS relays all authentication and accounting information to the Customer RADIUS server. In this mode of operation, the subsequent L2TP tunnel establishment is done dynamically.

5.1.2 Static RADIUS

In the static RADIUS configuration mode, the Customer provides COVAGE with the Attribute Value Pairs needed for the service to operate. In this mode of operation, the subsequent L2TP tunnel establishment is done statically.

Note that in this mode of operation no RADIUS accounting is available to the Customer.

5.2 L2TP Protocol

The Service is based on the “L2TP” protocol (Layer Two Tunneling Protocol) in compliance with **RFC 2661**.

The L2TP protocol is connection-oriented. When established, an L2TP session creates a tunnel between a LAC (L2TP Access Concentrator) and an LNS (L2TP Network Server):

- The LAC function is performed by an equipment belonging to Covage's network,
- The LNS function is performed by a BNG in the Customer's Network. This feature is not performed by Covage equipment. The LNS belonging to the Customer must comply with **DSL Forum TR-032** recommendation from the Broadband Forum.

5.3 L2TP Tunnel Establishment

5.3.1 L2TP Tunnel Establishment In Dynamic Mode

In the proxy RADIUS configuration, the L2TP tunnel establishment is done dynamically. In this mode, the Proxy RADIUS and Customer RADIUS, in which L2TP tunnels information are stored, exchange RADIUS attributes in order to allow L2TP tunnel establishment between the LAC and the LNS.

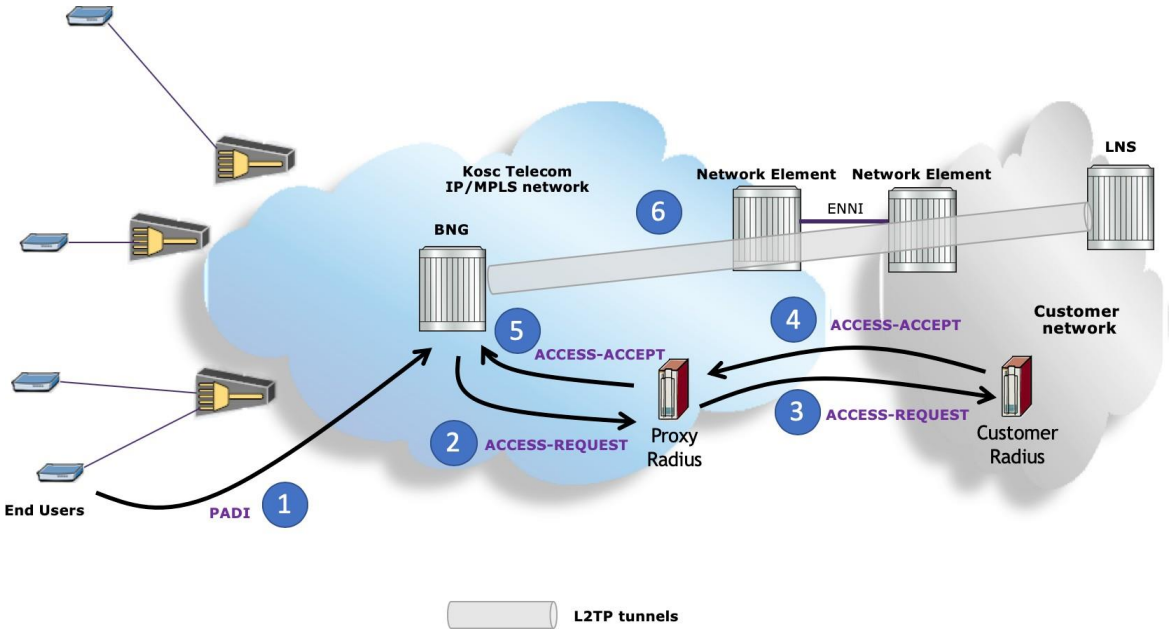

Figure 3: L2TP Tunnel Establishment In Dynamic Mode

1. User connection request: sending of username/password tuple, which is relayed by the LAC belonging to Covage to the Proxy RADIUS,
2. Sending of an “ACCESS-REQUEST” RADIUS message by the Proxy RADIUS to the Customer RADIUS,
3. Sending of an “ACCESS-ACCEPT” RADIUS message in case of user identification success by the Customer RADIUS to the Proxy RADIUS. This “ACCESS-ACCEPT” contains L2TP tunnel information in which the user PPP session will be transported and gives all characteristics (including the IP address of the LNS to be used to terminate the L2TP session). This information is relayed by the Proxy RADIUS to the BNG.
4. The LAC performs negotiation of L2TP tunnel establishment with the LNS indicated by Customer RADIUS in “ACCESS-ACCEPT” message.

5.3.2 L2TP Tunnel Establishment In Static Mode

In the static RADIUS configuration, all the needed information to establish L2TP tunnels towards the Customer network is stored locally on COVAGE's RADIUS servers.

This mode is static in the sense that once the tunnel characteristics are shared and implemented, the Customer cannot change them without asking COVAGE for a configuration change.

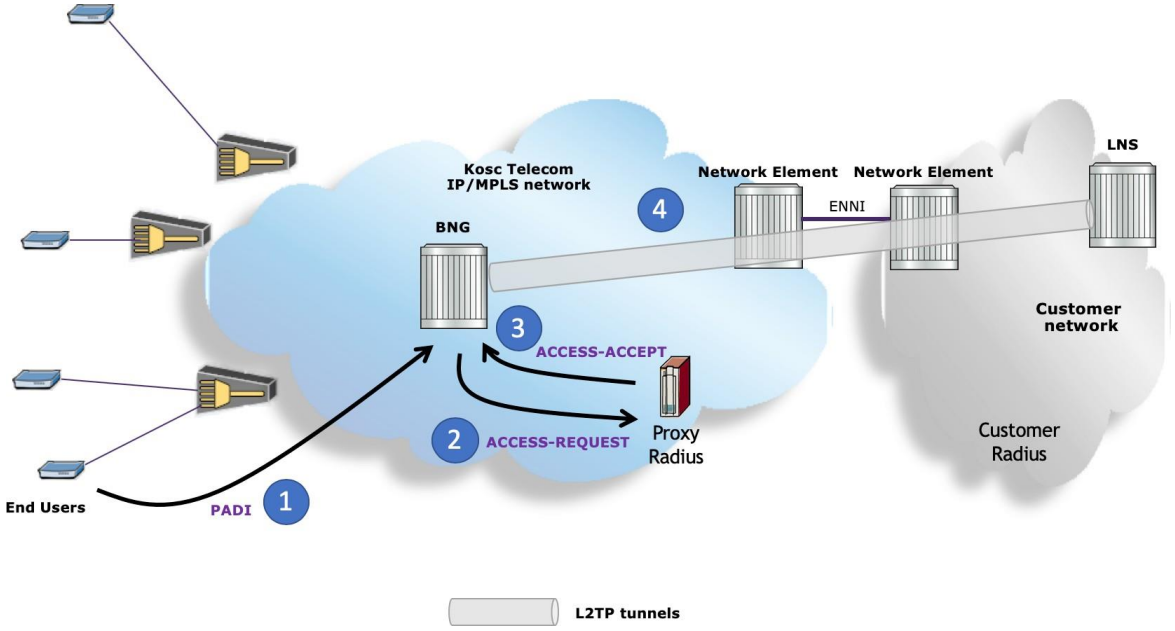

Figure 4: L2TP Tunnel Establishment In Static Mode

5.4 PPP Session Establishment

This phase allows the End User to establish **one unique PPP session** that is encapsulated and transported in the already established L2TP tunnel from the previous phase. Covage's network is transparent to the kind of traffic flowing through this session.

The PPP session lifetime is 7 days.

5.5 LNS Resiliency

RADIUS tags usage allows the Customer to send back several LNS in a single **"ACCESS-ACCEPT"** message.

This feature allows to perform either load-sharing or active/standby between LNS. The Tunnel-

Preference (83) RADIUS attribute allows to indicate each LNS preference:

- If each LNS has the same preference, then the LAC will perform load-sharing between those LNS.
- If one LNS has a better preference, then the LAC will always try to establish primarily a tunnel towards this LNS. In case of failure, the LAC will try to establish a tunnel towards the LNS with lower preference.

LNS resiliency can only be made by another LNS, the reason being RADIUS tags usage.

See sections *"6.4.2 RADIUS Authentication Attributes"* and *"6.4.4 RADIUS Tags Usage"* for more details about RADIUS tags.

5.6 RADIUS Accounting

The Service can transmit **START** and **STOP** accounting messages to the Customer RADIUS for statistics or connection management purposes. This is compliant to **RFC 2866**.

Each ticket corresponds to one End User session established in an L2TP tunnel.

6. Service Configuration

6.1 IP Addressing

The Layer 3 protocol used is IPv4.

6.1.1 Interconnection IP addresses

The interconnection IP addressing between Covage and the Customer is the responsibility of the Customer. Hence, the Customer will provide Covage the following information:

- One /30 or /31 public subnet to be used on the interconnection interface
    - One address will be used by the Customer
    - The other address will be used by Covage

6.1.2 LAC IP Addresses

Covage uses multiple Network Elements nodes as LACs to operate L2TP tunnels with the Customer's LNS. Each LAC uses a public IP address taken from the following range.

Nodes	IP address pool
Covage-LAC-Node	185.169.90.192/26

6.1.3 Proxy RADIUS IP Adresses

The primary and backup Proxy RADIUS IP addresses are defined and announced by Covage. The Customer's RADIUS servers must be able to process requests originating from both Proxy RADIUS nodes.

Proxy server	IP address
Covage-Proxy-1	185.169.90.1/32
Covage-Proxy-2	185.169.90.2/32

6.1.4 LNS IP Addresses

The LNS IP addresses are defined and announced by the Customer. The

Customer's LNS addresses must comply to the following rules:

- LNS addresses must be public.
- LNS addresses must be different from loopback addresses used for EBGP sessions.
- LNS addresses must not belong to the interconnection networks.
- LNS addresses must be different from RADIUS servers' addresses.

It is recommended for the Customer to declare its LNS in its DNS server and give them a name which identifies

the Customer and its LNS.

The Customer must announce its LNS addresses in /32.

Remarks:

> - LNS addresses are not announced outside Covage's network.
> - The Customer must provide ALL LNS addresses intended to be used with Covage's network. Any route to an unknown LNS will be discarded.

6.1.5 Customer RADIUS Addresses

The Customer RADIUS IP addresses are defined and announced by the Customer. The following information will be provided to Covage:

- The IP address for the authentication RADIUS server and optionally a second IP address for a backup server.
- The IP address for the accounting RADIUS server (if different from the authentication server), and optionally a second IP address for a backup server.

These IP addresses must be public.

The Customer must announce its RADIUS server(s) address(es) in /32.
Remark:

> RADIUS server addresses are not announced outside Covage's network. The Customer must provide ALL RADIUS server addresses intended to be used with Covage's network. Any route to an unknown RADIUS server will be discarded.

6.1.6 User's IP Addresses

The users IP addresses are the responsibility of the Customer. These addresses are not visible by Covage.

The Customer is responsible for the user IP address allocation. Covage cannot be held responsible if the Customer tries to allocate a specific IP address twice (on the same DSL Region or different DSL Regions).

6.2 Routing

The addresses exchanges between the Customer and Covage are done using an **External Border Gateway Protocol (BGP)** session.

This EBGP session allows:

- Covage's network Element to announce to the Customer's network:
  - the LAC routes
  - the Proxy RADIUS server routes
- The Customer's network Element to announce to Covage's network:
  - its LNS routes
  - its RADIUS server routes

6.2.1 EBGP Session Characteristics

6.2.1.1 Common Rule Sets For All Interconnections

The following rules apply to EBGP:

- The Customer must have a unique public AS number
- **Covage's Autonomous System (AS) number is 206958**
- MD5 authentication with a key shared by the Customer. The password must be composed at least of 8 ASCII characters and up to 16 ASCII characters.

Remark:

> In case the Customer's network Element supporting the EBGP session does not support 32-Byte AS numbers, Covage will use **AS_TRANS (23456)** for the peering in conformance with **RFC 4893**

6.2.1.2 Route Filtering

Covage protects its network with the following filter rules:

- Check on /32 mask for each announced route, in order to be prioritized in Covage's network
- Only addresses part of the addresses blocks previously declared by the Customer to Covage are redistributed to Covage's network
- A maximum of 1000 BGP prefixes can be learned on each EBGP session. Any BGP session that fails to conform to this rule will be disabled.

6.2.1.3 Attributes For BGP Routes

The MED (MULTI-EXIT-DISCRIMINATOR) attribute allows the Customer to define the usage of the secured connections (primary / backup or load-sharing).

AS pre-pending can be also used for this purpose.

The communities used by the Customer are ignored by Covage.

6.2.2 Resiliency

If the Customer subscribes to more than one ENNI with Covage, each interconnection will host one EBGP session between the two networks.

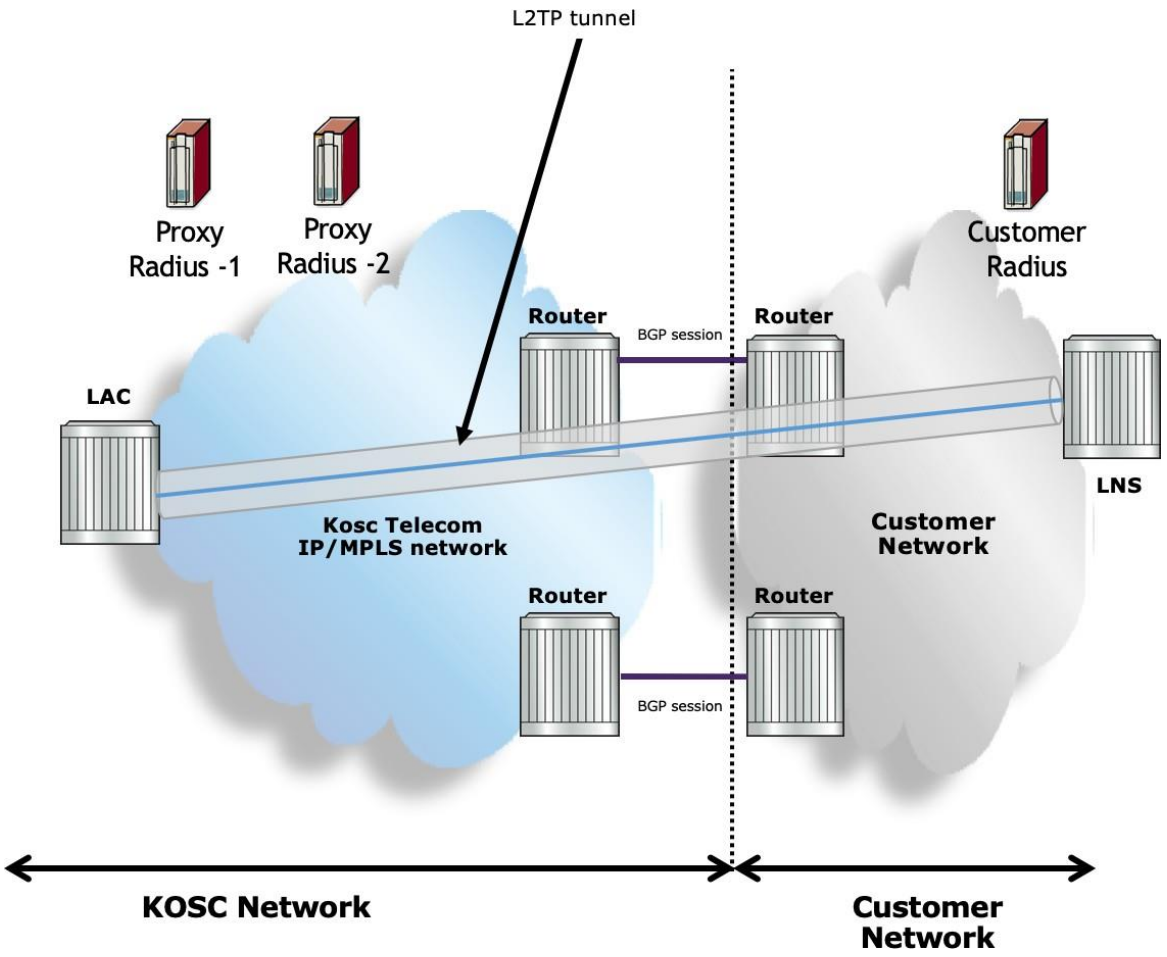

Figure 5: BGP Redundancy Overview

The Customer defines the way the two connections are used.

Redundancy e.g.:

- *A set of the Customer's LNS routes is announced via the primary BGP session, upon failure of the primary link, the routes are announced via the second BGP Session*

Remark:

> Covage's network supports the use of BFD sessions for fast fault detection. This functionality can be provided upon request.
>
> The BFD sessions are configured with the following default values:
>
> - Transmit interval : 100 ms
> - Multiplier : 3

6.3 Traffic

Two traffic types will transit on the ENNI

1. RADIUS traffic in the form of authentication requests and replies and accounting tickets
2. PPP user traffic encapsulated in L2TP flowing between end users and the Customer's LNS

6.3.1 RADIUS Traffic

- RADIUS traffic flowing from Covage to the Customer:
    - every ENNI on which Customer RADIUS routes are announced is susceptible to deliver this traffic. The Customer's network must be able to handle it.
- RADIUS traffic flowing from the Customer to Covage:
    - every ENNI can receive this traffic. If multiple ENNIs are used, the Customer chooses to which one authentication traffic is delivered.
- Only RADIUS authentication and accounting traffic is accepted by Covage Proxy servers.
- Proxy servers only use :
    - Port 1812 for Authentication requests
    - Port 1813 for Accounting requests

6.3.1 User Traffic

- User traffic from the End User's Site to the Customer's network:
    - User traffic is delivered through L2TP tunnel on the ENNI using the specified VLAN.
- User traffic from the Customer's network to the End User's Site:
    - The Customer must send downstream user traffic to the ENNI through an L2TP tunnel on the specified VLAN interface.

6.4 RADIUS In Proxy Mode

6.4.1 RADIUS Server Configuration

Customer RADIUS server must support the UDP protocol. It must detect Proxy RADIUS source port and send back its response on that specific port.

Covage must get from Customer the following mandatory information for RADIUS server identification:

- RADIUS secret (password exchanged between RADIUS server and Proxy RADIUS)
- UDP ports used for communication (RADIUS server receiving port) if not standard

These informations are given for both RADIUS authentication and accounting servers.

6.4.2 RADIUS Authentication Attributes

RADIUS attributes are described in **RFC 2865** and **RFC 2868** for authentication and **RFC 2866** for accounting.

- **RADIUS attributes generated by the Proxy RADIUS to the Customer RADIUS (ACCESS- REQUEST)**

If the authentication method is PAP:

AttributeName	Attribute number	Description
User-Name	1	Name of user
User-Password	2	PAP password of user
NAS-IP-Address	4	BNG IP address
Called-Station-Id	30	This attribute represents the DSL Access type of the user
Calling-Station-Id	31	DSL line identifier
NAS-identifier	32	BNG identifier
Proxy-State	33	Attribute added for each relay through Proxy RADIUS and used as identifier for RADIUS exchange
Acct-Session-Id	44	Session identifier

This table lists the modified attributes if the authentication method is CHAP:

AttributeName	Attribute number	Description
CHAP-Password	3	CHAP password of user
CHAP-Challenge	60	Response of user to a CHAP challenge
NAS-IP-Address	4	BNG IP address

- **RADIUS attributes generated by the Customer RADIUS to the Proxy RADIUS (ACCESS- ACCEPT)**

AttributeName	Attribute number	Description
Service-Type	6	Service type provided to the user
Framed-Protocol	7	Used protocol for connection (PPP)
Proxy-State	33	Attribute added for each relay through Proxy RADIUS and used as identifier for RADIUS exchange. This attribute received from Proxy RADIUS in ACCESS-REQUEST must be copied by Customer RADIUS in ACCESS-ACCEPT message
Tunnel-Type	64*	Tunnel type to establish (3 for L2TP)
Tunnel-Medium-Type	65*	Media type encapsulating the tunnel (1 for IPv4)
Tunnel-Server-Endpoint	67*	LNS IP address
Tunnel-Password	69*	Tunnel password to be used for authentication by Covage BNG
Tunnel-Assignment-ID	82*	Tunnel identification to establish or use. COVAGE BNGs use this attribute to identify the tunnel in which PPP sessions are carried. A tunnel name must be associated to a unique LNS address. Covage recommends to use LNS public IP address as string for the attribute. If the Customer requires to establish several tunnels on a given BNG for a given service, it must give different attribute values for different tunnels
Tunnel-Preference	83*	This attribute represents the priority associated with the tunnel. It is used in the case where L2TP tunnels attributes are tagged. The lowest value is preferred
Tunnel-Client-Auth-Id	90*	LAC name. The string returned in this attribute must match the string defined in Customer LNS configuration as LAC name.

Remark:

> Attributes with an asterisk (*) can be tagged.

- **RADIUS attributes generated by the Customer RADIUS to the Proxy RADIUS (ACCESS- REJECT)**

  No attribute is necessary.

Remark:

> The Customer must be able to manage two different authentication phases, one for L2TP tunnel establishment and one for PPP session establishment.

6.4.3 RADIUS Accounting Attributes

- **RADIUS accounting START attributes generated by the Proxy RADIUS**

AttributeName	Attribute number	Description
User-name	1	Name of user
NAS-IP-Address	4	BNG IP address
NAS-Port	5	BNG virtual port number
Called-Station-Id	30	This attribute represents the DSL Access type of the user
Calling-Station-Id	31	DSL line identifier
NAS-Identifier	32	BNG identifier
Proxy-State	33	Attribute added for each relay through Proxy RADIUS and used as identifier for RADIUS exchange
Acct-Status-Type	40	Accounting start (1) message
Acct-Delay-Type	41*	Duration of ticket
Acct-Session-Id	44	Session identifier
Acct-Authentic	45	Specifies how user has been authenticated

- **RADIUS accounting STOP attributes generated by the Proxy RADIUS**

AttributeName	Attribute number	Description
User-name	1	Name of user
NAS-IP-Address	4	BNG IP address
NAS-Port	5	BNG virtual port number
Called-Station-Id	30	This attribute represents the DSL Access type of the user
Calling-Station-Id	31	DSL line identifier
NAS-Identifier	32	BNG identifier
Proxy-State	33	Attribute added for each relay through Proxy RADIUS and used as identifier for RADIUS exchange
Acct-Status-Type	40	Accounting start (1) message
Acct-Delay-Type	41*	Duration of ticket
Acct-Input-Octets	42	Number of received bytes
Acct-Output-Octets	43	Number of sent bytes
Acct-Session-Id	44	Session identifier
Acct-Authentic	45	Specifies how user has been authenticated
Acct-Session-Time	46	Call duration
Acct-Input-Packets	47	Number of received packets
Acct-Output-Packets	48	Number of sent packets
Tunnel-Assignment-ID	82	Identification of established tunnel

START and **STOP** packets will hold all or some part of these attributes.

6.4.4 RADIUS Tags Usage

Some attributes can be tagged as described in **RFC 2868** in order to allow LNS resiliency.

If the Customer wants to use tags, all L2TP tunnels related attributes must be tagged (64 to 91).

Tags values must be comprised between 0x01 and 0x1F included. If the Tag field is unused, it MUST be zero (0x00).

6.4.5 Users Identification Format

The redirection of a user flow towards the Customer's network is based on the analysis of the domain name by Covage.

The identification process relies on the tuple [**user-name**, **password**] allocated by the Customer to every user.

The following format should be used: **user-name = user-ID@domain-ID** with:

- **user-ID** = alphanumeric value
- **domain-ID** = **ISP-ID.carrier-ID**
    - **ISP-ID** = alphanumeric value
    - **carrier-ID** = Covage
- **password** = alphanumeric value

Covage relies on the **ISP-ID** part to manage RADIUS requests using redirection of RADIUS requests towards Customer RADIUS.

The Customer declares to Covage all the desired DOMAIN-ID strings that will be used for the service.

Remarks:

> - Covage can refuse an ISP-ID, e.g. for some terms which are reserved such as ICANN terms.
> - Covage can refuse an ISP-ID if already used by another Customer for the Service or if the ISP-ID is not defined explicitly enough to discriminate between all Customer's Alphanumeric is defined as any alphabet character from A to Z or a number from 0 to 9. Upper case letter or lower-case letter are two distinct alphabet characters. "**/**" character must not be used in fields **<user-ID>** and **<domain-ID>**.

6.4.6 RADIUS Health Check

Covage tracks the health status of its Customer's RADIUS servers using a periodic authentication check. This check is performed every 5 minutes and must use a valid login on the Customer's network.

6.5 Static RADIUS Mode

For the static RADIUS mode of operation, the customer must provide COVAGE with the following information:

- The LNS IP address(ses) for tunnel termination.
- A tunnel password, if used.
- A tunnel ID to use for each LNS. COVAGE will use the LNS's IP address per default. A tunnel preference in the case of multiple LNSs being used.

- A tunnel authentication ID if used.

If the customer uses more than one LNS, it is possible to use up to four different endpoints. The redundancy mode can be round-robin or active / backup.

7. Billing Of The ENNI Traffic

The 95th percentile method is used for the billing of the Customer traffic. Every five minutes Covage measures the In/Out octets on the ENNI. For any given day, Covage sums the measures for every hour in order to obtain 24 values. These 24 daily values are then added up monthly to obtain 720 values. The 720 values are then ordered and the top 5% values are discarded. The remaining top value for the In traffic and the remaining top value for the Out traffic are then compared and the biggest value is used for the billing period.

Annex A - Glossary

Term	Definition
AAA	Authentication, Authorization, and Accounting
Customer	The Customer is the network operator contracting with Covage for the service
Access Site	The Access Site designates the site from which the Customer's traffic is collected, as opposed to the Delivery Site where said traffic is delivered
ADSL	Asymmetric Digital Subscriber Line - A type of digital sunbscriber line that enables data transmission over copper telephone lines
CTP	Copper Termination Point
Data Center	A Data Center is a facility used to house computer systems
Delivery Site	The Delivery Site designates the site to which the Customer's traffic is sent, as opposed to the Access Site from which said traffic is collected
L2TP	Layer 2 Tunneling Protocol is a tunneling protocol used as part of the delivery services offered by ISPs
LAC	L2TP Access Concentrator
LNS	L2TP Network Server
GPON Access	Gigabit Passive Optical Network
PoP	A Point of Presence typically houses network equipment and servers. It is typically located in a Data Center
RADIUS	RADIUS servers are responsible for receiving user connection requests, authenticating the user, and then returning all configuration information necessary for the client to deliver service to the user
xDSL Access	All types of Digital Subscriber Lines

Annex B - Covage's Sites

List of Covage's PoPs Below is the list of Covage's PoPs on which the service can be delivered:

Site Name	Address
TH2	137 Boulevard Voltaire, 75011 Paris. France
PA2	114 Rue Ambroise Croizat, 93200 Saint-Denis, France
CBV	124 Boulevard de Verdun, 92400 Courbevoie, France
ITX2	20-22 Rue des Gardinoux, 93534 Aubervilliers, France
DIJ	9 Rue du professeur Louis Neel, 21600 Longvic, France
TLS	14 Rue Ferdinand Lassale , 31200 Toulouse, France
BDX	3 Rue du Docteur Gabriel Péri, 33300 Bordeaux, France
REN	7-9 Allée Bray ZA de Bray 35000, Cesson-Sévigné, France
NTS	Rue Felix Eboue, 44000 Rezé, France
NCY	Parc d’activité Lafayette, 54200 Maxéville, France
ROU	Rond point des vaches, 76800 Saint-Etienne-du-Rouvray, France

Annex C - Covage's 100G Sites

List of Covage's PoPs Below is the list of Covage's PoPs on which the service can be delivered on 100G Ethernet interfaces:

Site Name	Address
TH2	137 Boulevard Voltaire, 75011 Paris. France
PA2	114 Rue Ambroise Croizat, 93200 Saint-Denis, France
CBV	124 Boulevard de Verdun, 92400 Courbevoie, France
ITX2	20-22 Rue des Gardinoux, 93534 Aubervilliers, France