



Telenet FTTH
XGS-PON CPE specification
for Free Modem regulation

Author: Telenet
Version: 1.0

Date: July 2024

Version	Date	Author	Comment
0.1	19 June 2024	Dean Allison	Draft version
0.2	22 July 2024	Dean Allison	Revised draft
1.0	26 July 2024	Dean Allison	Release Version

Table of Contents:

1. ABBREVIATIONS	5
1. CONVENTIONS	6
2. CONTACT	6
3. SCOPE	6
4. OVERVIEW OF THE TELENET FIBER SERVICE	7
5. DETAILED REQUIREMENTS	8
A. XGS-PON REQUIREMENTS	8
B. HARDWARE / REGULATORY REQUIREMENTS	9
C. RESIDENTIAL GATEWAY REQUIREMENTS	10
D. VOICE SERVICE REQUIREMENTS	11
I. BASIC VOICE REQUIREMENTS	11
II. CODECS	11
III. FEATURES	12
MESSAGE WAITING INDICATOR	12
CALLING LINE IDENTITY PRESENTATION AND RESTRICTION (CLIP/CLIR)	12
CALL HOLD / MUSIC ON HOLD SUPPORT	13
UNCONDITIONAL CALL FORWARD	13
CALL FORWARD ON NO REPLY	13
CALL FORWARD ON BUSY	13
ANONYMOUS CALL REJECTION	14
OUTGOING CALL BARRING	14
CALL WAITING	14
THREE PARTY CONFERENCE	14
CALLING NAME DELIVERY	14
AUTOMATIC RECALL	14
IV. AUTHENTICATION	15
V. REGISTRATION	15

VI. SIP ACCOUNT & CREDENTIALS	15
VII. FAX SUPPORT	15
VIII. ADDITIONAL IMPORTANT REMARKS	15
E. SUPPORT FOR TELENET TV SERVICES	16
F. GENERAL REQUIREMENTS	16

1. Abbreviations

The following abbreviations are used in this document.

AP	Access point device
CO	Central Office
CPE	Customer Premise Equipment
FTTH	Fiber to the Home
GUI	Graphical User Interface
HGW	Home Gateway
OLT	Optical Line Termination
OMCI	ONU Management and Control Interface
ONT	Optical Network Terminal
ONU	Optical Network Unit
OTDR	Optical Time Domain Reflectometry
PON	Passive Optical Network
RGW	Residential gateway
SFP	Small Form-factor Pluggable
XGS-PON	10Gigabit Symmetrical Passive Optical Network

1. Conventions

Throughout this document, the words that are used to define the significance of particular requirements are capitalized. These words are:

"MUST, SHALL" This word means that the item is an absolute requirement of this specification.

"MUST NOT" This phrase means that the item is an absolute prohibition of this specification.

"SHOULD" This word means that there MAY exist valid reasons in particular circumstances to ignore this item, but the full implications SHOULD be understood and the case carefully weighed before choosing a different course.

"SHOULD NOT" This phrase means that there MAY exist valid reasons in particular circumstances when the listed behaviour is acceptable or even useful, but the full implications SHOULD be understood and the case carefully weighed before implementing any behaviour described with this label.

"MAY" This word means that this item is truly optional.

2. Contact

The contact for queries regarding this specification can be found on www.telenet.be

Please note that this contact is an address for hardware vendors only.

3. Scope

Telenet operates a "one box" model for CPE used to deliver data and voice services over the Telenet Fiber To The Home (FTTH) network, combining an XGS-PON ONT and Residential Gateway/Router in a single unit. This document describes the Telenet requirements for attaching such a device to the Telenet FTTH network in order to use data and voice services provided by Telenet. Requirements relating to both the XGS-PON ONT functionality of the device selected by an end user for use on the Telenet FTTH network, and its Residential Gateway capabilities are referenced.

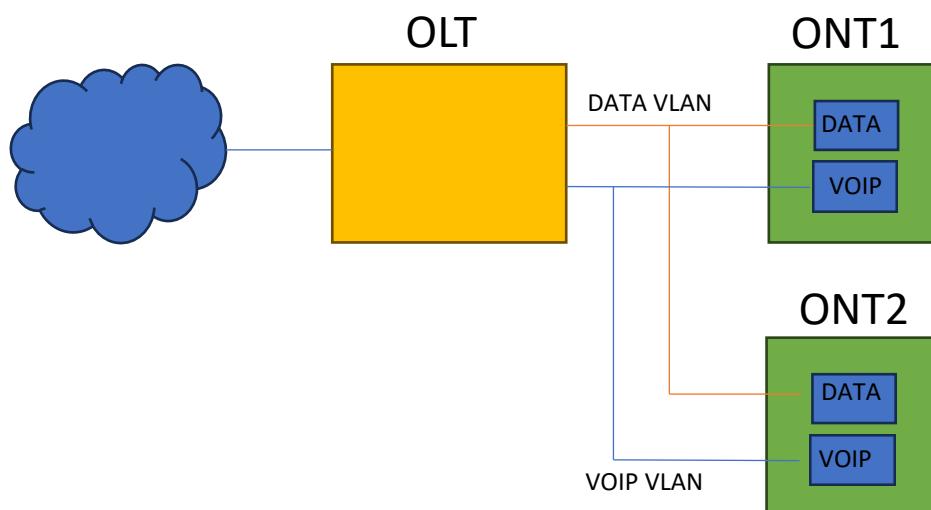
Third party devices used by end users in the context of the decision of the BIPT concerning the location of the network termination point for broadband services delivered by network operators must comply with the requirements listed in this document to ensure proper operation on Telenet's network.

4. Overview of the Telenet Fiber Service

The Telenet FTTH network is based on XGS-PON technology. Customers are connected to the Telenet network via a Passive Optical Network (PON) which is terminated on an Optical Line Termination port located at a Central Office location. End users should note that devices based on the earlier Gigabit Passive Optical Network technology are NOT compatible for use on Telenet's network.

The customer premises equipment (CPE) is then connected to the optical fiber termination point that is installed by Telenet in their premises, via a single mode simplex fiber patch cable. The optical fiber termination will be provided as a SC/APC 8 outlet to which the patch fiber cable to the CPE will be connected.

Network data services (including over-the-top TV services) and telephony services are delivered over separate VLAN allocations. The end user CPE MUST therefore be capable of configuring a different VLAN ID for data/internet and voice services. A diagrammatic representation of this is shown below:



The table below also details the current customer VLAN IDs and associated p-bit settings for data and voice services:

Service	C-VLAN ID	p-bit
DATA	1081	0
VoIP Signalling	981	3
VoIP Media	981	5

Telenet does not support the delivery of both voice and data services over a single VLAN.

5. Detailed Requirements

a. XGS-PON Requirements

[REQ-1.1] The end user CPE MUST support the following ITU-T standards:

- ITU-T G.9807.1 10 Gigabit Symmetrical – Passive Optical Network
- ITU-T G.988 ONU management and control (OMCI) Specification
- ITU-T G.664 Optical safety procedures and requirements for optical transmission systems
- ITU-T G.652 Characteristics of a single-mode optical fiber and cable

[REQ-1.2] The CPE MUST be able to co-exist with an OTDR system that may be deployed in order monitor optical network health and performance

[REQ-1.3] The Broadband Forum defines a number of standards relating to operation of a PON network and certification against these standards:

- TR-101 Migration to Ethernet-Based Broadband Aggregation
- TR-156 issue 3 Using GPON access in the context of TR-101
- BBF.247 GPON ONU Interoperability and Certification Testing
- TR-247 Abstract Test Plan for GPON ONU Conformance
- TR-309 XG-PON and XGS-PON TC Layer Interoperability Test Plan
- TR-287 PON Optical-Layer Management

The CPE MUST comply with the above standards and evidence successful testing against the associated test plans

[REQ-1.4] Forward Error Correction MUST be supported

[REQ-1.5] Downstream AES encryption MUST be supported

[REQ-1.6] Automatic device discovery of the CPE PON serial number MUST be supported for activation purposes

[REQ-1.7] It MUST NOT be possible to change the PON Serial Number via the CPE's end user interface, or by any other means

[REQ-1.8] The device MUST be identified by an Equipment ID and Model Number, and this MUST reference the model identification used in regulatory and compliance documentation. It MUST NOT be possible to change these identifiers by any means.

[REQ-1.9] For operator monitoring purposes the CPE MUST support supervision and performance monitoring parameters as outlined in the ITU-T standards:

- Optical transmit power
- Optical receive power
- XGS-PON ONT state
- Module temperature
- Module voltage
- Module laser bias current

[REQ-1.10] The CPE MUST send a dying gasp notification in the event that power to the device is lost, or intentionally switched off.

[REQ-1.11] The CPE MUST conform to the following PON slot ID and UNI port numbering:

- Slot number: 1
- UNI port number: 1

[REQ-1.12] The CPE selected by the end user MAY be of a type where the XGS-PON function is provided via a plug-in SFP module. This being the case, the module MUST comply with the same XGS-PON requirements that are set out in this document.

[REQ-1.13] The CPE device MUST implement rogue ONU detection as detailed in the ITU-T XGS-PON standards.

[REQ-1.14] The device SHOULD support a minimum of 8 GEM ports.

b. Hardware / Regulatory Requirements

[REQ-2.1] The CPE device MUST comply with all applicable regulatory and safety standards required for CE compliance and use within the European Union.

[REQ-2.2] User LAN ports MUST comply with the relevant IEEE standards according to the LAN port type (eg 802.3ab 1000Base-T). For 10Gb/s LAN ports these MUST comply with IEEE 802.3an 10GBase-T Ethernet over unshielded twisted pair.

[REQ-2.3] Where implemented, WiFi functionality MUST comply with all required regulatory standards and IEEE standards (eg 802.11ax)

c. Residential Gateway Requirements

[REQ-3.1] The RGW MUST provide an embedded router to enable multiple end user client devices to share the XGS-PON WAN connection provided.

[REQ-3.2] IPv4 and IPv6 dual stack operation MUST be supported.

[REQ-3.3] The RGW MUST support Network Address Translation (NAT) and implement a NAT firewall that enables multiple LAN clients to simultaneously share a single IPv4 address.

[REQ-3.4] DHCPv4 MUST be supported for assignment of private IPv4 addresses to LAN clients.

[REQ-3.5] The RGW MUST support DHCPv6 and stateless address autoconfiguration for assignment of IPv6 addresses to LAN clients.

[REQ-3.6] IPv6 prefix delegation MUST be supported.

[REQ-3.7] The embedded router WAN interface MUST be able to obtain a public IPv4 address from the network using DHCP; and a public IPv6 address via DHCPv6.

[REQ-3.8] Device MUST conform to the latest WAN and IP RFCs, and specifically where relevant to IPv6:

- RFC4443 Internet Control Message Protocol (ICMPv6) for the Internet Protocol version 6
- RFC8200 Internet Protocol version 6 July 2017
- RFC8201 Path MTU Discovery for IP version 6
- RFC8415 Dynamic Host Configuration Protocol for IPv6
- RFC3646 DNS Configuration options for Dynamic Host Configuration Protocol for IPv6
- RFC3769 Requirements for IPv6 Prefix Delegation
- RFC7084 Basic Requirements for IPv6 Customer Edge Routers
- RFC9096 Improving the Reaction of Customer Edge Routers to IPv6 Renumbering Events
- RFC6333 Dual-Stack Lite Broadband Deployments following IPv4 Exhaustion
- RFC6334 Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Option for Dual-Stack Lite
- RFC8106 IPv6 Router Advertisement Options for DNS Configuration
- RFC4861 Neighbor Discovery Protocol for IP version 6
- RFC4862 IPv6 Stateless Address Autoconfiguration

[REQ-3.9] The device MUST NOT introduce any new QoS settings on the WAN IP interface

[REQ-3.10] The residential gateway WAN interface MUST support the VLAN / p-bit tagging of upstream egress packets as described in section 4 of this document.

d. Voice Service Requirements

These requirements describe the SIP interface only. It is the responsibility of device vendors to ensure that the PSTN interface is suitable for use in the Belgian market.

i. Basic Voice Requirements

Telenet uses the loose coupled model to interface with the SIP client at the user side.

[REQ-4.1] The RGW MUST provide at least one RJ11 FXS voice port to allow telephony services to be delivered to end users via the RGW.

[REQ-4.2] Voice services will be delivered over IPv6 only, therefore It MUST be possible to support SIP voice service over IPv6.

[REQ-4.3] It MUST be possible to configure voice services to use a separate VLAN to that used for data/internet service, in order to guarantee quality of service for voice services.

[REQ-4.4] The VoIP WAN interface MUST support the VLAN / p-bit tagging of upstream egress packets as described in section 4 of this document.

[REQ-4.5] It MUST be possible to localize the voice service configuration for use in Belgium.

[REQ-4.6] The CPE MUST support the following RFCs and protocols:

- Session Initiation Protocol (SIP) (RFC 3261, RFC 3262, RFC 3263, RFC 3323, RFC 3325, RFC 3327, RFC 3608, RFC 4028, RFC 4412 and RFC 6665)
- Session Description Protocol (SDP) (RFC 3264 and RFC 4566)
- Real Time Transport Protocol (RTP) (RFC 3550, RFC 3551 and RFC 4733)
- IP multimedia call control protocol based on SIP and SDP (3GPP TS 24.229 V 14.0.0)
- The tel URI for Telephone Numbers (RFC 3966)
- The Message Session Relay Protocol (MSRP) (RFC 4975 and RFC 4976)
- End-to-End Session Identification in IP-Based Multimedia Communication Networks (RFC 7989)

ii. Codecs

[REQ-4.7] The CPE MUST support the G.711 codec.

iii. Features

The following features are supported by Telenet. Telephony features that are not mentioned are not supported.

For the purposes of this document <DN> refers to a directory number with:

- National: one leading zero
- International: two leading zeros

Message Waiting Indicator

Reference: RFC 3265 Session Initiation Protocol (SIP)-Specific Event Notification

RFC 3842 A Message Summary and Message Waiting Indication event package for SIP

In order to receive the MWI from the network, the user has to subscribe to the event.

- Method : Subscribe
 - Header : Event : message-summary

The user will be informed about the status of the MWI via a Notify

- Method : Notify
 - Headers
 - Subscription-Expires : ...
 - Event : message-summary
 - Subscription-State : Active;Expires=...
 - Body
 - Message-Waiting: yes/no
 - Message-Account <sip:<fqdn>>

The Notify is sent approximately every +/- 490 sec from the network towards the user, this is to ensure that if one of the settings would fail a subsequent Notify can set the MWI to the correct status.

In order to avoid a recurring ring splash due to this audit mechanism, make sure towards the phoneset to use DT-AS (dualtone) instead of RP-AS (Ring pulse alerting signal).

Calling Line Identity Presentation and Restriction (CLIP/CLIR)

The network-provided CLI is contained in the P-asserted-ID header of the incoming INVITE towards the ONT.

If the user has subscribed to a permanent privacy service, the network will implement this functionality without the need of the user sending a Privacy-header. Moreover, we don't expect the P-Asserted-Identity to be sent by the user towards the network.

For an outgoing call we expect the P-Preferred-Identity (<sip:username@domainname>)

The user can deactivate this service on a per call basis by dialling #31(tone)DN

A user without a permanent subscription to a privacy service dials *31(tone)DN to enable privacy on a per call basis.

Expected pattern of the RURI becomes sip:*31%23<DN>@domainname or <sip:#31%23<DN>@domainname>

Note:

Inclusion of a (tone) is the responsibility of the ONT since we have a loose coupled configuration.

Call Hold / Music On Hold support

A user involved in a communication can put the other party on HOLD by pushing the “R” button or via a hook flash

For hold and resume of media stream the router shall comply with the behaviour described in 3GPP TS 24.610 for sending (in the SDP offer) directionality attributes in SDP. Additionally, the Home Gateway shall be able to accept (in the SDP offer) directionality attributes as described in clause 5.3 of RFC 6337.

The behaviour expected is according to the so-called loose coupled mode of the 3GPP and ETSI TISPAN standards.

Unconditional Call Forward

The user can activate the call forwarding via *21(tone)DN or deactivate via #21

Expected pattern of the RURI becomes

- Activation : sip:*21%23<DN>@domainname
- Deactivation : <sip:%2321<DN>@domainname>

Once the network confirmed successful treatment of activation or deactivation it will provide an appropriate tone via his media server.

Note:

Inclusion of a (tone) is the responsibility of the ONT since we have a loose coupled configuration.

Call Forward on No Reply

This is part of the voicemail functionality and cannot be programmed by the user.

Timer is set to a fixed value of 30 seconds.

Call Forward on Busy

This is part of the voicemail functionality and cannot be programmed by the user.

Anonymous Call Rejection

This functionality cannot be programmed by the user.
Can be set via a request towards the Telenet helpdesk.

Outgoing Call Barring

This functionality can be set via the Telenet “Mijn Telenet” portal where several types of outgoing calls can be blocked.

Call Waiting

Service offered by the network is to accept call waiting and put the active call on hold.

Three Party Conference

The expected behaviour is according to the so-called loose coupled mode of the ETSI TISPAN standards.
The mixing of the voice streams is the responsibility of the ONT.

Calling Name Delivery

Automatic Recall

A user can dial 1919 to hear date and time + the last number that called him and the option to call this number.

Expected pattern of the RURI becomes

- Activation : <sip:1919@domainname>

iv. Authentication

Authentication of the SIP account happens during the initial registration and subscription to the message summary package.

At periodic intervals (+/- 10 min) the re-registrations will be challenged and authentication will happen again.

v. Registration

In order to work properly, the user SIP-client must include the below mandatory header specifications while registering:

- Expires : 180
- Supported: path
- User-Agent: freemodem

vi. SIP Account & Credentials

SIP account & credentials will be provided by Telenet and must be used as provided. Otherwise, the network will respond with a 403-Forbidden fault code.

vii. Fax Support

Telenet only allows the use of G.711 group 3 facsimile. T.38 is not supported.

viii. Additional Important Remarks

RFC 3265 “Session Initiation Protocol (SIP)-Specific Event Notification” defines a general mechanism of SUBSCRIBE-NOTIFY methods which can be used by end user devices to subscribe to event notifications. When end user devices use SUBSCRIBE-NOTIFY for a particular “feature”, while that feature is not activated or even not offered by the operator, the end user device will send unnecessary and useless SUBSCRIBE messages to the network.

The network will respond to them; however this will only result in an obsolete notification every +/- 490 sec (see Message Waiting Indicator). This pollutes the network.

Therefore, it is essential for an end user device that it only subscribes to the message summary event package if a voicemail service in the network has been configured.

e. Support for Telenet TV Services

Delivery of Telenet TV services over IP using a so-called IP Set Top Box only is supported. Support for legacy TV services connected via a coax cable are not in scope.

[REQ-5.1] The CPE MUST ensure that any DHCP options provided by the network or specifically requested by a connected Telenet IP STB are passed to the STB.

[REQ-5.2] The CPE MAY support IGMPv3 Snooping. Where supported, this SHALL be configured only as directed by Telenet.

[REQ-5.3] The CPE MAY support MLDv2. Where supported, this SHALL be configured only as directed by Telenet.

[REQ-5.4] The CPE MUST preserve DSCP classification and other QoS marking in packets received from a connected Telenet STB when forwarding these upstream.

[REQ-5.5] For a STB connected wirelessly to the CPE, the CPE MUST adhere to 802.11e WMM traffic mappings.

f. General Requirements

[REQ-6.1] Best practice cybersecurity practices MUST be followed for any CPE. In preparation for upcoming CE RED new cybersecurity regulation, the CPE must already support these basic security aspects:

- Unique login name and password for end-user access to device configuration, so unique per device
- Regular software updates to be made available for any required security updates
- Pen testing and related reviews should be done by the device manufacturer
- The equipment shall be resilient against brute force attacks to any authentication mechanisms
- Auto-generated passwords must be randomly seeded

[REQ-6.2] Telenet will not provide managed software updates for end-user CPE devices. End users MUST ensure that devices are maintained with a secure configuration and are kept updated with the latest software provided by device manufacturers.

[REQ-6.3] If the device implements Wi-Fi functionality, then it SHOULD follow best practices to ensure good co-existence in typical Belgium density and the challenges of Wi-Fi shared spectrum aspects.

- 2.4GHz band frequency settings should be only selectable for channels 1, 6 and 11 to avoid overlap
- 5GHz bandwidth setting should be 80MHz maximum or lower bandwidth
- There should be a channel selection algorithm that chooses the lowest utilized channel
- The 5GHz radio should support the full spectrum available including DFS channels
- Wi-Fi 6 should be the minimal norm for FTTH gateways
- CE regulation and EIRP emission limits must be strictly adhered to and should be assessed using audits of mass production samples to ensure continuous regulatory compliancy and fair usage of the Wi-Fi medium.

End of document