Guideline related to the use of a 3rd party router on the Proximus residential network.

Table of contents

1 Terminology

- “must” or “shall” is used to indicate a mandatory element.
- “should” is used to express a strong recommendation.

2 Introduction

This document is provided as a reference guide for Equipment Manufacturers and End Users within the framework of the Decision of 26 September 2023 regarding the identification of the network termination point for broadband services. The information contained herein pertains to Proximus' network specifications.

The purpose of this document is to furnish insights into the current state of information and network specifications, serving as a guideline for third-party routers that might be deployed by end-users on the Proximus residential network.

Scope:

- This document provides details on the configuration requirements for third-party routers when interfacing with the Proximus residential network.
- It outlines the standards that must be adhered to by the third-party routers to ensure proper interoperability with the Proximus network.

Limitations:

- This document does not constitute a comprehensive router specification but specifically addresses essential points crucial for achieving interoperability with the Proximus residential network.
- The document does not cover the characteristics necessary for a modem to establish a connection to the physical line. For modem-specific requirements, please refer to the modem specifications provided separately:

    - DSL Modem Specification: “PXS_VDSLspecs”
    - ONT Specification: “PXSEndUser_ONTspecs_v03”

Usage Considerations:

- The information presented in this document is based on the current state of information and network specifications, subject to change. It is recommended to regularly check for updates and revisions.

Disclaimer: The guidelines outlined in this document are provided on an "as-is" basis. While every effort has been made to ensure accuracy, Proximus shall not be liable for any direct, indirect, incidental, consequential, or special damages arising out of the use of this information.

3 Basic Setup

3.1 Requirements

The following features must be supported by the router:

- VLAN Tagging on the WAN interface
- DHCPv4 (rfc 2131 and rfc 2132)
- SLAAC (rfc 4862)
- DHCPv6 (rfc8415, rfc3319, rfc3646, rfc4704, rfc5007 and rfc6221)
- IPv6 prefix delegation
- ARP (rfc 826)

The router must allow for the configurations described in the following paragraphs to be set by the end user.

3.2 Configuration

3.2.1 VLAN Tagging:

Proximus residential lines make use of a single VLAN (VLAN 20) for connectivity towards the network. The router must thus be configured so that its WAN interface encapsulates traffic in VLAN 20.

3.2.2 IP acquisition from the network:

IPv4 acquisition is done via DHCPv4.

IPv6 acquisition is done via SLAAC while IPv6 prefixes delegated for LAN use are acquired via DHCPv6. If the router supports IPv6 prefix delegation it should automatically use the provided Global IPv6 ranges to make them available on the LAN.

3.2.3 Keep alive:

To verify if a router is still connected to the network, the network will regularly send ARP messages to that router. The router will answer those ARPs.

3.3 Use of an external modem

If the router is connected to an external modem (e.g., DSL modem or ONT) by means of an Ethernet cable, the end user should make sure that the external modem is bridging traffic at the OSI Layer 2 level (this is the case for Proximus modems).

If the connection between the modem and the router is found to be unstable (packet loss), this might be due to one of the following elements:

- The Ethernet cable isn't properly plugged in.
- The Ethernet cable isn't adapted to the negotiated throughput. Make sure an Ethernet cable of the proper category is used (CAT 5E is good for connections up to 1 Gbps, CAT 6A or CAT 7 is to be used for connections up to 10 Gbps).
- Energy Efficient Ethernet is enabled.

4 Support of the Proximus TV Service

4.1 Requirements

The following features must be supported by the router:

- DHCPv4 Option Spoofing: Options received on WAN side need to be provided via DHCPv4 to the decoder on the LAN.
- DHCPv6 Option Spoofing (not used by the current TV service, will be used in the future).
- IGMP Snooping (Ideally v3 but will also work with v2).
- MLD v2 Snooping (not used by the current TV service, will be used in the future).

The router must also:

- Allow for the following Private IP ranges to be reached on the WAN: 172.28.40.0/21 and 172.28.48.0/21.
- Allow for the following Multicast ranges to be used on the WAN: 239.192.0.0/16 and 239.255.0.0/16.
- Not affect DSCP tags related to the decoder in upstream.

The router must allow for the configurations described in the following paragraphs to be set by the end user.

4.2 Configuration

4.2.1 DHCPv4 Option spoofing:

The following options provided on WAN side need to be provided to the Proximus decoder:

- Option 6 : DNS
- Option 42 : NTP server
- Option 67 : Bootfilename
- Option 43 : Vendor specific

If need be, the decoder can be isolated in a separate DHCPv4 pool by filtering on option 60 which in the case of Proximus decoders will start with “IPTV”.

4.3 Important Remarks

4.3.1 Availability of DHCPv4 options to the decoder

As the decoder requires for DHCPv4 options sent by the network to be present, it is important to check that:

- The options are requested by the router to the network. Option 55 sent in the DHCPv4 messages on WAN side should contain:
    - Option 1 (Subnet Mask)
    - Option 3 (Router)
    - Option 6 (Domain Name Server)
    - Option 12 (Host Name)
    - Option 15 (Domain Name)
    - Option 42 (Network Time Protocol Server)

  - Option 43 (Vendor Specific Information) - Used to communicate information to the Decoder as to the mode it needs to start in.
  - Option 51 (IP Address Lease Time)
  - Option 54 (DHCP Server Identifier)
  - Option 67 (Bootfile Name)
  - Option 121 (Classless Static Route)
- The options have been received by the router and are available for distribution to the decoder before an IPv4 address is assigned to it. If the configuration of the router doesn't allow for such a conditional configuration, the end user might need to wait until the router has acquired an IP address from the network before starting the decoder.

4.3.2 Stability of the decoder

To ensure the stability of the decoder it is important that it keeps the same IPv4 address when on (so from the time it is turned on until the time it is once again set into standby mode). This can be achieved in two ways,

- The DHCPv4 lease time given to the decoder is high enough to ensure it doesn't need to renew its IPv4 address for the period it is active.
- The DHCPv4 server present in the router is one that reassigns the same IP address to devices that come to renew it (This should be the case for most commercial routers)

4.3.3 Quality of Service

DSCP classes for the main traffic types that can reach the decoder are set as follows for traffic coming from the network (aka in Downstream):

- CS4 for TV Multicast and VQE
- CS3 for Signaling protocol for Video
- AF22 for TV Unicast
- 4 for Internet Traffic

In the event the decoder would be connected to the router over Wi-Fi, it is important to note that, if for routers following standard mapping practices towards Wi-Fi traffic access categories (cfr. rfc8325), CS4 and CS3 will be mapped to the Video Queue while AF22 and 4 will be mapped to the Best Effort Queue.

4.3.4 IGMP support

If the router supports IGMPv3 snooping, and switches are used by the end user in his local network, the end user should make sure those switches also support IGMPv3 snooping. If the switches only support IGMPv2 snooping, there will be an issue at IGMP level for interactions occurring through the switches installed between the router and any IGMPv2 end device (e.g. The decoder).

5 Support of the Proximus VoIP Service

5.1 Requirements

5.1.1 Basic Router requirements

The router must support:

- 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 rfc4733)
- 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)
- Multi part bodies in SIP messages (This feature shall conform to the requirements defined by the IETF standard body).

The router must allow for the configurations described in the following paragraphs to be set by the end user.

5.1.2 FXS Interface

The FXS interface, if present on the router, must conform to the following standards:

- ETSI ES 202 971 V1.2.1 (2006-03)

  Access and Terminals PSTN Harmonized specification of physical and electrical characteristics of a 2-wire analogue interface for short line interface

- ETSI TR 101 959 V1.1.1 (2002-10)

  Access and Terminals Ringing without DC for Terminal Equipment, Terminal Support Interfaces and Local Exchange Interfaces

- ETSI ES 201 729 V1.1.1 (2000-02)

  PSTN 2-wire analogue voice band switched interfaces Time break recall Specific requirements for terminals

- ETSI ES 201 235-1 V1.1.1 (2000-09)

  Specification of DTMF Transmitters and Receivers Part 1: General

- ETSI ES 201 235-2 V1.2.1 (2002-05)

  Specification of DTMF Transmitters and Receivers Part 2: Transmitters

- ETSI ES 201 235-3 V1.3.1 (2006-03)

  Specification of DTMF Transmitters and Receivers Part 3: Receivers

- ETSI ES 201 235-4 V1.3.1 (2006-03)

Specification of DTMF Transmitters and Receivers Part 4: Transmitters and Receivers for use in Terminal Equipment for end-to-end signalling

It must also conform to the following UNI specifications published by Proximus:

- BGC_D_48_9807_30_02_E_ed41.pdf - Analogue Subscriber Line Signaling (Basic Calls)
- BGC_D_48_9807_30_04_E_ed13.pdf - Information Tones
- BGC_D_48_9811_30_09_E_ed33.pdf - Subscriber line protocol for display (and related) services
- BGC_D_48_0001_30_02_E_ed21.pdf – Subscriber Control Interface (SCI)

5.1.3 Codecs

The following codecs are supported by the Proximus network:

- G.711
- G.729
- G.722 - That codec being an HD one it only makes sense to support it at router level If one of the interfaces present on the router supports HD Calls (e.g. If the router integrates a DECT CAT-iq base)

5.1.4 Features

Features, if supported by the router, shall be implemented according to the following specifications:

Message Waiting Indication (MWI) 3GPP TS 24.606 v14.0.0 or later.

The MWI service uses unsolicited SIP NOTIFY messages sent by the Voice mail system to the mailbox owner via the IMS core network. The unsolicited NOTIFY message contains a message-summary body in accordance with rfc3842 and the notify mechanisms of rfc3265. This SIP NOTIFY message-summary body contains an indication of the number of new messages versus the total number of messages in the mailbox.

The router shall be capable to receive the MWI notifications (SIP NOTIFY method) and to provide the audible and visual indication to the FXS interface. On the FXS interface, this will be done according to the Proximus UNI specification "BGC_D_48_9811_30_09_E_ed33.pdf".

Calling Line Identity Presentation and Restriction (CLIP/CLIR) 3GPP TS 24.607 v14.0.0 or later

The network-provided CLI is contained in the P-asserted-ID header of the incoming INVITE. User provided (unverified) CLI information MAY also be contained in the From header of the INVITE. The device shall transport this information to the end devices. On the FXS interface, this will be done by following the methods described in the Proximus UNI specifications "BGC_D_48_9811_30_09_E_ed33.pdf"

For an outgoing INVITE, the router is expected to include the CLI information in the FROM header and in the P-preferred-ID header. The Privacy header of the INVITE is used to transport the presentation allowed or restricted indication in the network.

Calling Name Identity Presentation (CNIP)

The router shall receive the calling name information in the incoming SIP INVITE method and transport this to the end device. On the FXS interface, this will be done by following the methods described in the Proximus UNI specifications "BGC_D_48_9811_30_09_E_ed33.pdf".

Connected Line Presentation and Restriction (COLP/COLR) 3GPP TS 24.608 v14.0.0 or later.

The requirement for the router is the capability to receive the called identity information in the 200 OK response to the SIP INVITE and to transport this to the end device. In the event COLR is active there will be no P-asserted-ID header in the 200 OK response to the INVITE delivered to the calling user. On the FXS interface this shall be done by following the methods described in the Proximus UNI specifications "BGC_D_48_9811_30_09_E_ed33.pdf".

Call hold / Music on hold support 3GPP specification TS 24.610 v14.0.0 or later

Note: An addition in version 14.0.0 mandates that if the CPE of the held user does NOT receive "music on hold", the CPE should generate this hold indication itself.

The router shall support and treat the hook flash or "R" button in following way:

A user involved in a communication can put the other party on HOLD by pushing the "R" button or via a hook flash according to § 6.2 of the Proximus specifications "BGC_D_48_9807_30_02_E_ed41.pdf" and annex B of the Proximus specification "BGC_D_48_0001_30_02_E_ed21.pdf".

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

Call Forwarding 3GPP TS 24.604 v14.1.0 or later.

Service offered by the network:

- Call forwarding unconditional:
- Call forwarding on busy:
- Call forwarding on no reply:

Anonymous Call Rejection / Outgoing Call Barring 3GPP specification TS 24.611 v14.0.0 or later

Service offered by the network:

- Outgoing call barring (OCB)
- Anonymous call rejection (ACR)

Call Waiting 3GPP TS 24.615 v14.0.0 or later.

Service offered by the network:

- Call waiting (activate/deactivate.)
- Reject call waiting (R0)
- Accept call waiting and release active call (R1)
- Accept call waiting and put the active call on hold (R2)

The expected behavior is according to the so-called loose coupled mode of the ETSI TISPAN standards.

In the event the router receives a second incoming call (for a user already in communication) it is the responsibility of the device to offer this second call to the phone. With regard to service interworking with the CLIP service, the requirement for the device is the capability to receive the calling identity information in the incoming SIP INVITE method of the second call and to transport this to the end device. On the FXS interface this shall be done according to 8.2 of the Proximus specification "BGC_D_48_9811_30_09_E_ed33.pdf".

Three Party Conference 3GPP TS 24.605 v14.0.0 or later

Service offered by the network:

- Three party conference (R3)

The expected behavior is according to the so-called loose coupled mode of the ETSI TISPAN standards.

Call Transfer 3GPP TS 24.629 v14.0.0 or later

Service offered by the network:

- Call Transfer (R4)

The expected behavior is according to the so-called loose coupled mode of the ETSI TISPAN standards.

Call Completion to Busy Subscriber 3GPP TS 24.642 v14.0.0 or later

Service offered by the network:

- Call Completion to Busy Subscriber (R5)

Fixed Destination Call

Service offered by the network and the router:

The Fixed destination call service shall be executed by the IMS application server. Two flavours exist:

- "FDC_Immediate" starts the call immediately after the user has gone off-hook. This is also called HOTLINE
- "FDC_Timed" routes the call after the phone has been off-hook for 5 seconds without any dialing for another number having been initiated. This is also called WARMLINE

The requirements for the router are as follow:

The router must determine when the Hotline or Warmline service is active. Warmline cannot be active at the same time as Hotline.

- HOTLINE specific:

  When the Hotline service is active the router must send an INVITE request to the IMS application server as soon as it detects off hook. The Request-URI of the INVITE must contain an IMS AS server specific value as the user part indicating the HOTLINE service.

  If a router allows for a user to dial digits before a call is initiated (e.g. a phone that has a SEND or NEW CALL button that will send digits previously entered by the caller), and the Hotline service is active, the router must still send an INVITE with the Hotline string in the Request-URI, but should also send the dialed digits in a P-Called-Number-ID header (as defined in rfc7315). Some services will be configured so that the router always sends an INVITE to a specific location (using the Hotline service), and the server at that location will use the dialed digits received in the P-Called-Number-ID header as the requested destination number.

- WARMLINE specific:

  A Warmline timer is to be used when Warmline is active. The timer should be configurable in steps of 1 second with a range that can vary between 2 and 30 seconds.

  When Warmline is active, the router must start the Warmline timer as soon as the end device goes off-hook. If the caller fails to enter any digits before the timer expires, the CPE device must send an INVITE to the IMS application server. The Request-URI of the INVITE must contain an IMS application server specific value as the user part indicating the WARMLINE service. If any digits are dialed by the caller before the timer expiry, then the dialed digits are included in the request URI just as is done for "normal" calls.

The IMS AS to be used for the Proximus service is "LU-FS5000-HOT-WARM"

The activation and deactivation codes that need to be supported by the router are:

- Activation code: *53*
- Deactivation code: #53#

5.1.5 Authentication

Authentication 3GPP TS 24.229 v14.0.0

Authentication of the SIP account shall occur with each outgoing call attempt.

Authentication for SIP Registration and call set-up is determined by the NETWORK and involves specific signaling procedures for which the device needs to act as a client. The router shall implement the authentication procedures as foreseen in the 3GPP standard and will use them for registration as well as for session set-up.

5.1.6 Fax Support

If the router supports the connection of a FAX on its FXS port(s) it must also support:

- Procedures for real-time Group 3 facsimile communication over IP networks (ITU-T T38 (09/2010) & Amendment 1 (10/2014))
- T-38 as a codec

5.2 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.

This is a very useful mechanism but also potentially dangerous. 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.

As the network will not respond to them, retransmission will occur. This pollutes the network and risks having the SBC go into DOS attack mode.

Therefore, it is essential for an end user device that any feature using SUBSCRIBE-NOTIFY has the capability to turn off the sending of SUBSCRIBE by configuration.

----------End of document----------