Network Working Group

Internet Draft
Intended Status: Informational

Expires: August 25, 2013

Nabil Bitar(ed.)
Verizon

Sanjay Wadhwa (ed.)
Alcatel-Lucent

Thomas Haag
Deutsche Telekom

Hongyu Li
Huawei Technologies

February 25, 2013

Applicability of Access Node Control Mechanism to PON based Broadband Networks

draft-ietf-ancp-pon-05.txt

Abstract

The purpose of this document is to provide applicability of the Access Node Control mechanism to Passive Optical Network (PON)-based broadband access. The need for an Access Node Control mechanism between a Network Access Server (NAS) and an Access Node Complex (a combination of Optical Line Termination (OLT) and Optical Network Termination (ONT) elements) is described in a multi-service reference architecture in order to perform QoS-related, service-related and Subscriber-related operations. The Access Node Control mechanism is also extended for interaction between components of the Access Node Complex (OLT and ONT). The Access Node Control mechanism will ensure that the transmission of information between the NAS and Access Node Complex (ANX) and between the OLT and ONT within an ANX does not need to go through distinct element managers but rather uses a direct device-to-device communication and stays on net. This allows for performing access link related operations within those network elements to meet performance objectives.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on August 25,2013.

Copyright Notice

Table of Contents

1. Introduction

Passive Optical Networks (PONs) based on BPON [G.983.1] and GPON [G.984.1] are being deployed across carrier networks. There are two

models for PON deployment: Fiber to the building/curb (FTTB/FTTC), and Fiber to the Premises (FTTP). In the FTTB/C deployment, the last mile connectivity to the subscriber premises is provided over the local Copper loop, often using Very High Speed Digital Subscriber line (VDSL). In the FTTP case, PON extends to the premises of the subscriber. In addition, there are four main PON technologies: (1) Broadband PON (BPON), (2) Gigabit PON (GPON), (3) 10-Gigabit PON (XG-PON), and (4) Ethernet PON (EPON). This document describes the applicability of Access Node Control Protocol (ANCP) in the context of FTTB/C and FTTP deployments, focusing on BPON, GPON and XG-PON. Architectural considerations lead to different ANCP compositions. Therefore, the composition of ANCP communication between Access Nodes and Network Access Server (NAS) is described using different models.

BPON, GPON and XG-PON in FTTP deployments provide large bandwidth in the first mile, bandwidth that is an order of magnitude larger than that provided by xDSL. In the downstream direction, BPON provides 622 Mbps per PON while GPON provides 2.4 Gbps, and XG-PON provides 10 Gbps.

In residential deployments, the number of homes sharing the same PON is limited by the technology and the network engineering rules. Typical deployments have 32-64 homes per PON.

The motive behind BPON, GPON and XG-PON deployment is providing triple-play services over IP: voice, video and data. Voice is generally low bandwidth but has low-delay, low-jitter, and low packet-loss requirements. Data services (e.g., Internet services) often require high throughput and can tolerate medium latency. Data services may include multimedia content download such as video. However, in that case, the video content is not required to be real-time and/or it is low quality video. Video services, on the other hand, are targeted to deliver Standard Definition or High Definition video content in real-time or near-real time, depending on the service model. Standard Definition content using MPEG2 encoding requires on the order of 3.75 Mbps per stream while High definition content using MPEG2 encoding requires on the order of 15-19 Mbps depending on the level of compression used. Video services require low-jitter and low-packet loss with low start-time latency. There are two types of video services: on demand and broadcast (known also as liner programming content). While linear programming content can be provided over Layer1 on the PON, the focus in this document is on delivering linear programming content over IP to the subscriber, using IP multicast. Video on demand is also considered for delivery

to the subscriber over IP using a unicast session model.

Providing simultaneous triple-play services over IP with unicast video and multicast video, VoIP and data requires an architecture that preserves the quality of service of each service. Fundamental to this architecture is ensuring that the video content (unicast and multicast) delivered to the subscriber does not exceed the bandwidth allocated to the subscriber for video services. Architecture models often ensure that data is guaranteed a minimum bandwidth and that VoIP is guaranteed its own bandwidth. In addition, QoS control across services is often performed at a Network Access Server (NAS), often referred to as Broadband Network Gateway (BNG) for subscriber management, per subscriber and shared link resources. Efficient multicast video services require enabling multicast services in the access network between the subscriber and the subscriber management platform. In the FTTP/B/C PON environment, this implies enabling IP multicast on the Access Node (AN) complex composed of the Optical Network Terminal (ONT) or Unit (ONU) and Optical Line Terminal (OLT), as applicable. This is as opposed to Digital Subscriber Line (DSL) deployments where multicast is enabled on the DSL Access Multiplexer (DSLAM) only. The focus in this document will be on the ANCP requirements needed for coordinated admission control of unicast and multicast video in FTTP/B/C PON environments between the AN complex (ANX) and the NAS, specifically focusing on bandwidth dedicated for multicast and shared bandwidth between multicast and unicast.

[RFC5851] provides the framework and requirements for coordinated admission control between a NAS and an AN with special focus on DSL deployments. This document extends that framework and the related requirements to explicitly address PON deployments.

2. Terminology

- PON (Passive Optical Network) [G.983.1][G.984.1]: a point-to-multipoint fiber to the premises network architecture in which unpowered splitters are used to enable the splitting of an optical signal from a central office on a single optical fiber to multiple premises. Up to 32-128 may be supported on the same PON. A PON configuration consists of an Optical Line Terminal (OLT) at the Service Provider's Central Office (CO) and a number of Optical Network Units or Terminals (ONU/ONT) near end users, with an optical distribution network (ODN) composed of fibers and splitters between them. A PON configuration reduces the amount of fiber and CO equipment required compared with point-to-point architectures.

- Access Node Complex (ANX): The Access Node Complex is composed of two geographically separated functional elements OLT and ONU/ONT. The general term Access Node Complex (ANX) will be used when describing a functionality which does not depend on the physical location but rather on the "black box" behavior of OLT and ONU/ONT.

-Optical Line Terminal (OLT): is located in the Service provider's central office (CO). It terminates and aggregates multiple PONs (providing fiber access to multiple premises or neighborhoods) on the subscriber side, and interfaces with the Network Access server (NAS) that provides subscriber management.

- Optical Network Terminal (ONT): terminates PON on the network side and provides PON adaptation. The subscriber side interface and the location of the ONT are dictated by the type of network deployment. For a Fiber-to-the-Premise (FTTP) deployment (with Fiber all the way to the apartment or living unit), ONT has Ethernet (FE/GE/MoCA) connectivity with the Home Gateway (HGW)/Customer Premise Equipment(CPE). In certain cases, one ONT may provide connections to more than one Home Gateway at the same time.

-Optical Network Unit (ONU): A generic term denoting a device that terminates any one of the distributed (leaf) endpoints of an Optical Distribution Node (ODN), implements a PON protocol, and adapts PON PDUs to subscriber service interfaces. In case of an MDU multi-dwelling or multi-tenant unit, a multi-subscriber ONU typically resides in the basement or a wiring closet (FTTB case), and has FE/GE/Ethernet over native Ethernet link or over xDSL (typically VDSL) connectivity with each CPE at the subscriber premises. In the case where fiber is terminated outside the premises (neighborhood or curb side) on an ONT/ONU, the last-leg-premises connections could be via existing or new Copper, with xDSL physical layer (typically VDSL). In this case, the ONU effectively is a "PON fed DSLAM".

-Network Access Server (NAS): Network element which aggregates subscriber traffic from a number of ANs or ANXs. The NAS is often an injection point for policy management and IP QoS in the access network. It is also referred to as Broadband Network Gateway (BNG) or Broadband Remote Access Server (BRAS).

-Home Gateway (HGW): Network element that connects subscriber devices to the AN or ANX and the access network. In case of xDSL, the Home Gateway is an xDSL network termination that could either operate as a

Layer 2 bridge or as a Layer 3 router. In the latter case, such a device is also referred to as a Routing Gateway (RG). In the case of PON, it is often a Layer3 routing device with the ONT performing PON termination.

-PON-Customer-ID: This is an identifier which uniquely identifies the ANX and the access loop logical port on the ANX to the subscriber (customer) premises, and is used in any interaction between NAS and ANX that relates to access-loops. Logically it is composed of information containing identification of the OLT (the OLT may be physically directly connected to the NAS), the PON port on the OLT, the ONT/ONU, and the port on the ONT/ONU connecting to the subscriber HGW. When acting as a DHCP relay agent, the OLT can encode PON-Customer-ID in the "Agent-Circuit-Identifier" Sub-option in Option-82 of the DHCP messages [RFC3046].

3. Motivation for explicit extension of ANCP to FTTx PON

The fundamental difference between PON and DSL is that a PON is an optical broadcast network by definition. That is, at the PON level, every ONT on the same PON sees the same signal. However, the ONT filters only those PON frames addressed to it. Encryption is used on the PON to prevent eavesdropping.

The broadcast PON capability is very suitable to delivering multicast content to connected premises, maximizing bandwidth usage efficiency on the PON. Similar to DSL deployments, enabling multicast on the Access Node Complex (ANX) provides for bandwidth use efficiency on the path between the Access Node and the NAS as well as improves the scalability of the NAS by reducing the amount of multicast traffic being replicated at the NAS. However, the broadcast capability on the PON enables the AN (OLT) to send one copy on the PON as opposed to one copy to each receiver on the PON. The PON multicast capability can be leveraged in the case of GPON and BPON as discussed in this document.

Fundamental to leveraging the broadcast capability on the PON for multicast delivery is the ability to assign a single encryption key for all PON frames carrying all multicast channels or a key per set of multicast channels that correspond to service packages, or none. When supporting encryption for multicast channels, the encryption key is generated by the OLT and sent by the OLT to each targeted ONT via the ONT Management and Control Interface (OMCI) as described in section 15.5.2 of ITU-T G.987.3 [G.987.3] for XG-PON. It should be

noted that the ONT can be a multi-Dwelling Unit (MDU) ONT with multiple Ethernet ports, each connected to a living unit. Thus, the ONT must not only be able to receive a multicast frame, but must also be able to forward that frame only to the Ethernet port with receivers for the corresponding channel.

In order to implement triple-play service delivery with necessary "quality-of-experience", including end-to-end bandwidth optimized multicast video delivery, there needs to be tight coordination between the NAS and the ANX. This interaction needs to be near real-time as services are requested via application or network level signaling by broadband subscribers. ANCP as defined in [RFC5851] for DSL based networks is very suitable to realize a control protocol (with transactional exchange capabilities), between PON enabled ANX and the NAS, and also between the components comprising the ANX, i.e., between OLT and the ONT. Typical use cases for ANCP in PON environment include the following:

- Access topology discovery
- Access Loop Configuration
- Multicast
    - Optimized multicast delivery
    - Unified video resource control
    - NAS based provisioning of ANX
- Remote connectivity check

4. Reference Model for PON Based Broadband Access Network

An overall end-to-end reference architecture of a PON access network is depicted in Figure 1 and Figure 2 with ONT serving a single HGW, and ONT/ONU serving multiples HGWs, respectively. An OLT may provide FTTP and FTTB/C access at the same time but most likely not on the same PON port. Specifically, the following PON cases are addressed in the context of this reference architecture:

- BPON with Ethernet uplink to the NAS and ATM on the PON side.
- GPON/XG-PON with Ethernet uplink to the NAS and Ethernet on the PON side

In case of an Ethernet aggregation network that supports new QoS-enabled IP services (including Ethernet multicast replication), the architecture builds on the reference architecture specified in the Broadband Forum (BBF) [TR-101]. The Ethernet aggregation network

between a NAS and an OLT may be degenerated to one or more direct physical Ethernet links.

Given the industry move towards Ethernet as the new access and aggregation technology for triple play services, the primary focus throughout this document is on GPON/XG-PON and BPON with Ethernet between the NAS and the OLT.

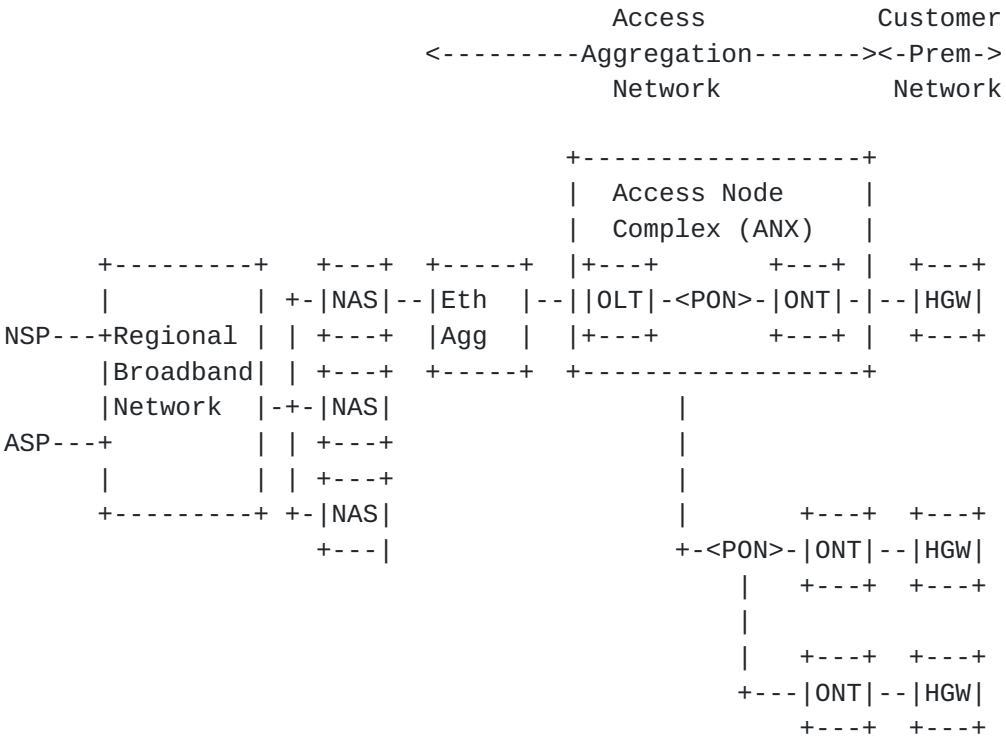


Figure 1: Access Network with PON.

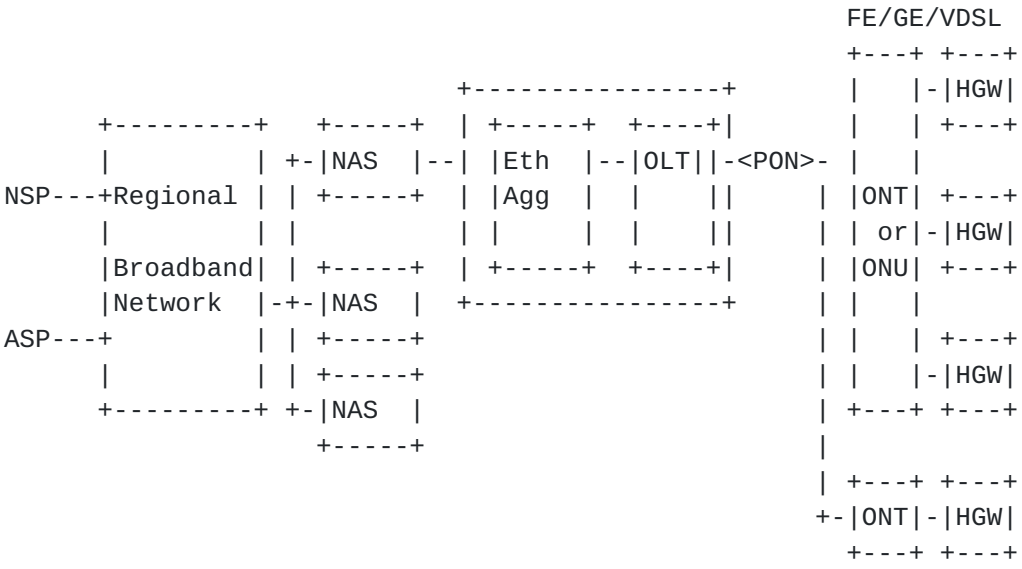


Figure 2: FTTP/FTTB/C with multi-subscriber ONT/ONU serving MTUs/MDUs. The following sections describe the functional blocks and network segments in the PON access reference architecture.

4.1. Functional Blocks

4.1.1. Home Gateway

The Home Gateway (HGW) connects the different Customer Premises Equipment (CPE) to the ANX and the access network. In case of PON, the HGW is a layer 3 router. In this case, the HGW performs IP configuration of devices within the home via DHCP, and performs Network Address and Port Translation (NAPT) between the LAN and WAN side. In case of FTTP/B/C, the HGW connects to the ONT/ONU over an Ethernet interface. That Ethernet interface could be over an Ethernet physical port or over another medium. In case of FTTP, it is possible to have a single box GPON CPE solution, where the ONT encompasses the HGW functionality as well as the GPON adaptation function.

4.1.2. PON Access

PON access is composed of the ONT/ONU and OLT. PON ensures physical connectivity between the ONT/ONU at the customer premises and the OLT. PON framing can be BPON (in case of BPON) or GPON (in case of GPON). The protocol encapsulation on BPON is

based on multi-protocol encapsulation over AAL5, defined in [RFC2684]. This covers PPP over Ethernet (PPPoE, defined in [RFC2516]), or bridged IP (IPoE). The protocol encapsulation on GPON is always IPoE. In all cases, the connection between the AN (OLT) and the NAS (or BNG) is assumed to be Ethernet in this document.

4.1.3. Access Node Complex

This is composed of OLT and ONT/ONU and is defined in section 2.

4.1.4. Access Node Complex Uplink to the NAS

The ANX uplink connects the OLT to the NAS. The fundamental requirements for the ANX uplink are to provide traffic aggregation, Class of Service distinction and customer separation and traceability. This can be achieved using an ATM or an Ethernet based technology. The focus in this document is on Ethernet as stated earlier.

4.1.5. Aggregation Network

The aggregation network provides traffic aggregation towards the NAS. The Aggregation network is assumed to be Ethernet in this document.

4.1.6. Network Access Server

The NAS is a network device which aggregates multiplexed Subscriber traffic from a number of ANXs. The NAS plays a central role in per-subscriber policy enforcement and QoS. It is often referred to as a Broadband Network Gateway (BNG) or Broadband Remote Access Server (BRAS). A detailed definition of the NAS is given in [RFC2881]. The NAS interfaces to the aggregation network by means of 802.1Q or 802.1 Q-in-Q Ethernet interfaces, and towards the Regional Network by means of transport interfaces (e.g., GigE, PPP over SONET). The NAS functionality corresponds to the BNG functionality described in BroadBand Forum (BBF) TR-101 [TR-101]. In addition, the NAS supports the Access Node Control functionality defined for the respective use cases in this document.

4.1.7. Regional Network

The Regional Network connects one or more NAS and associated Access Networks to Network Service Providers (NSPs) and Application Service

Providers (ASPs). The NSP authenticates access and provides and manages the IP address to Subscribers. It is responsible for overall service assurance and includes Internet Service Providers (ISPs). The ASP provides application services to the application Subscriber (gaming, video, content on demand, IP telephony, etc.). The NAS can be part of the NSP network. Similarly, the NSP can be the ASP.

4.2. Access Node Complex Control Reference Architecture Options

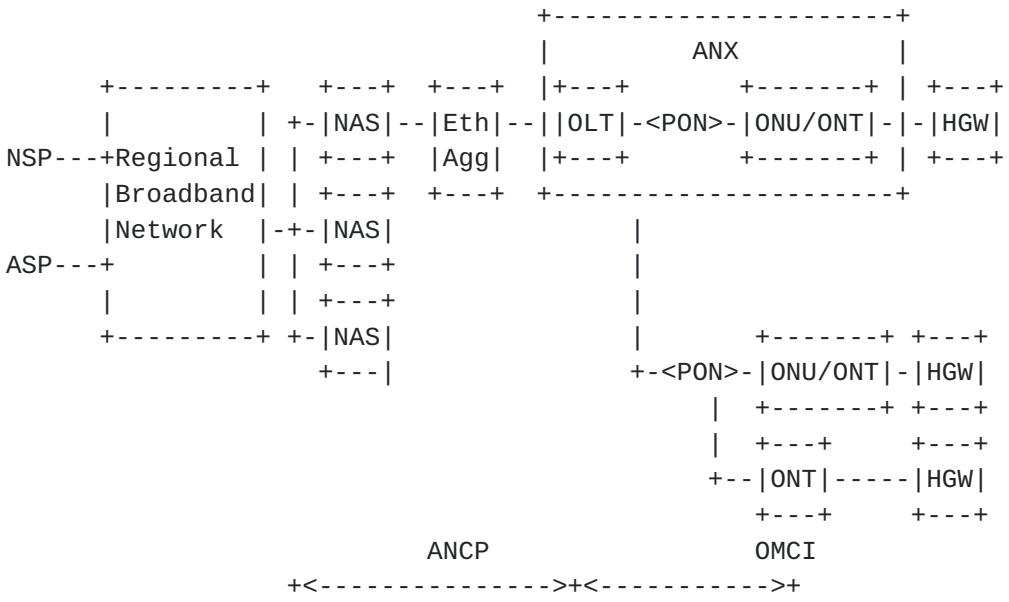
Section 3 details the differences between xDSL access and PON access and the implication of these differences on DSLAM control vs. OLT and ONT/ONU (access node complex (ANX)) control. The following sections describe two reference models: (1) ANCP+OMCI ANX control, and (2) all-ANCP ANX control. That is, the two models differ in the ONT/ONU control within the ANX. Implementations, out of the scope of this document, may choose to implement one or the other based on the ONT/ONU type and the capabilities of the ONT/ONU and OLT. It is possible for an OLT or an OLT PON port to connect to ONTs/ONUs with different capabilities and for these two models to co-exist on the same OLT and same PON. Section 12 describes the differences between OMCI and ANCP in controlling the ONU/ONT.

OMCI is designed as a protocol between the OLT and ONT/ONU. It enables the OLT to configure and administer capabilities on the ONT/ONU in BPON, GPON and XG-PON. ANCP is designed as a protocol between the NAS and access node. It enables the NAS to enforce dynamic policies on the access node, and the access node to report events to the NAS among other functions.

4.2.1. ANCP+OMCI ANX Control

Figure 3 depicts the reference model for ANCP+OMCI ANX control. In this model, ANCP is enabled between the NAS and a connected OLT, and OMCI is enabled between the OLT and an attached ONT/ONU. NAS communicates with the ANX via ANCP. The OLT acts as an ANCP/OMCI gateway for communicating necessary events and policies between the OLT and ONT/ONU within the ANX and for communicating relevant policies and events between the ONT/ONU and the NAS. The functionality performed by the OLT as ANCP/OMCI gateway will be application dependent (e.g., multicast control, topology discovery) and should be specified in a related specification. It should be noted that some applications are expected to require ANCP and/or OMCI extensions to map messages between OMCI and ANCP. OMCI extensions are likely to be defined by the ITU-T. It should also be noted that OMCI,

in addition to configuration and administration, provides the capability to report status changes on an ONT/ONU with AVC (Attribute Value Change) notifications. When ONT/ONU's DSL or Ethernet UNI attributes change, a related ME (management Entity) will send a corresponding notification (AVC) to the OLT. The OLT interworks such notification into an ANCP report and sends it to the connected NAS via the ANCP session between the OLT and the NAS. As the ANCP report contains information of ONT/ONU's UNI and OLT's PON port, NAS can obtain accurate information of access topology.



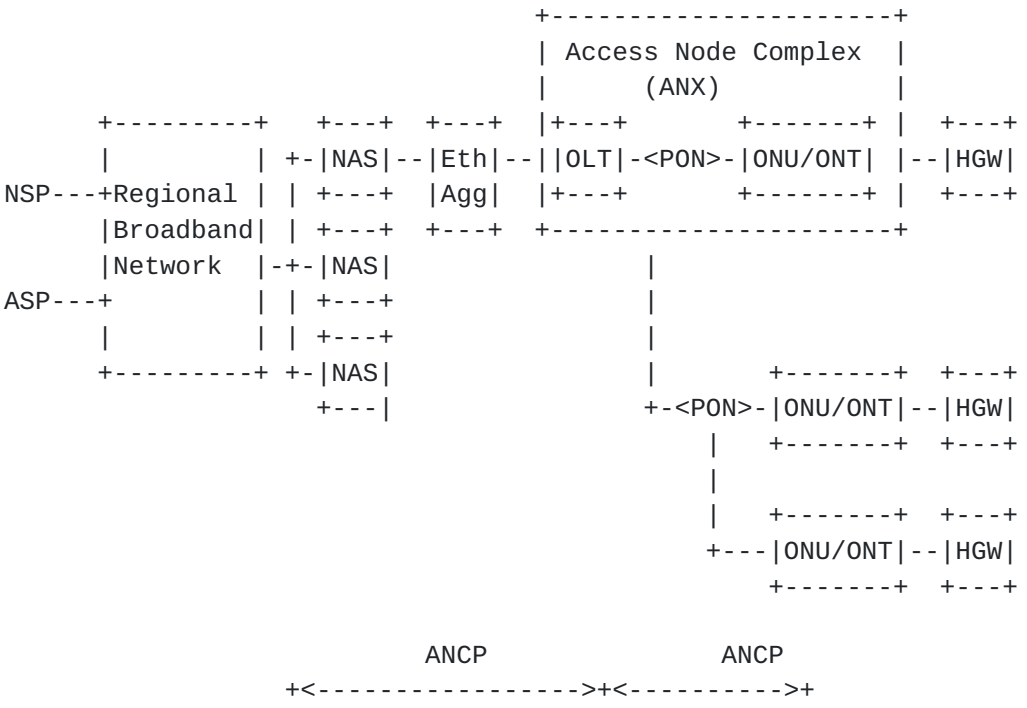
HGW: Home Gateway
NAS: Network Access Server
PON: Passive Optical Network
OLT: Optical Line Terminal
ONT: Optical Network Terminal
ONU: Optical Network Unit

Figure 3: Access Network with single ANCP+OMCI access control

4.2.2. All-ANCP ANX Control

Figure 4 depicts the All-ANCP ANX control reference model. In this model, an ANCP session is enabled between a NAS and a connected OLT, and another ANCP session is enabled between the OLT and a connected ONT/ONU. ANCP enables communication of policies and events between the OLT and the ANX. The OLT acts as a gateway to relay policies and events between the NAS and ONT/ONU within the ANX in addition to

communicating policies and events between the OLT and ONT/ONU. It should be noted that in this model, OMCI(not shown) is expected to be simultaneously enabled between the ONT and OLT, supporting existing OMCI capabilities and applications on the PON, independent of ANCP or applications intended to be supported by ANCP.



HGW: Home Gateway
NAS: Network Access Server
PON: Passive Optical Network
OLT: Optical Line Terminal
ONT: Optical Network Terminal
ONU: Optical Network Unit

Figure 4: All-ANCP ANX Reference Model

5. Concept of Access Node Control Mechanism for PON Based Access

The high-level communication framework for an Access Node Control mechanism is shown in Figure 5 for the ALL-ANCP ANX control model. The Access Node Control mechanism defines a quasi real-time, general-purpose method for multiple network scenarios with an extensible communication scheme, addressing the different use cases that are described in the sections that follow. The access node control mechanism is also extended to run between OLT and ONT/ONU. The mechanism consists of control function, and reporting and/or

enforcement function. Controller function is used to receive status information or admission requests from the reporting function. It is also used to trigger a certain behavior in the network element where the reporting and/or enforcement function resides.

The reporting function is used to convey status information to the controller function that requires the information for executing local functions. The enforcement function can be contacted by the controller function to enforce a specific policy or trigger a local action. The messages shown in Figure 5 show the conceptual message flow. The actual use of these flows, and the times or frequencies when these messages are generated depend on the actual use cases, which are described in later sections.

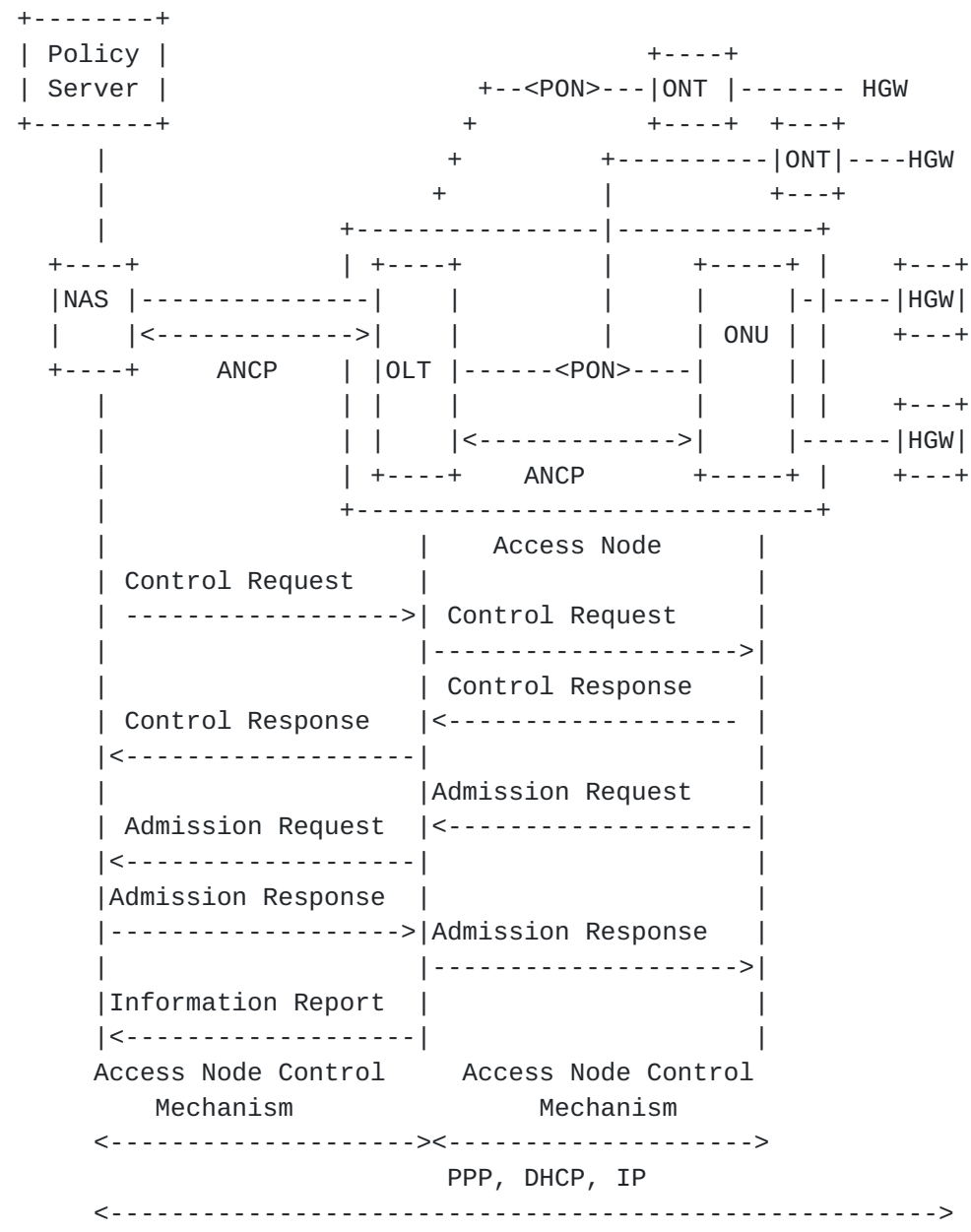


Figure 5: Conceptual message flow for Access Node Control mechanism in all-ANCP ANX control model.

As discussed previously, in different PON deployment scenarios, ANCP may be used in variant ways and may interwork with other protocols, e.g., OMCI. In the ANCP+OMCI model described earlier, the NAS maintains ANCP adjacency with the OLT while the OLT controls the ONT/ONU via OMCI. The messages shown in Figure 6 show the conceptual message flow for this model. The actual use of these flows, and the times or frequencies when these messages are generated depend on the actual use cases.

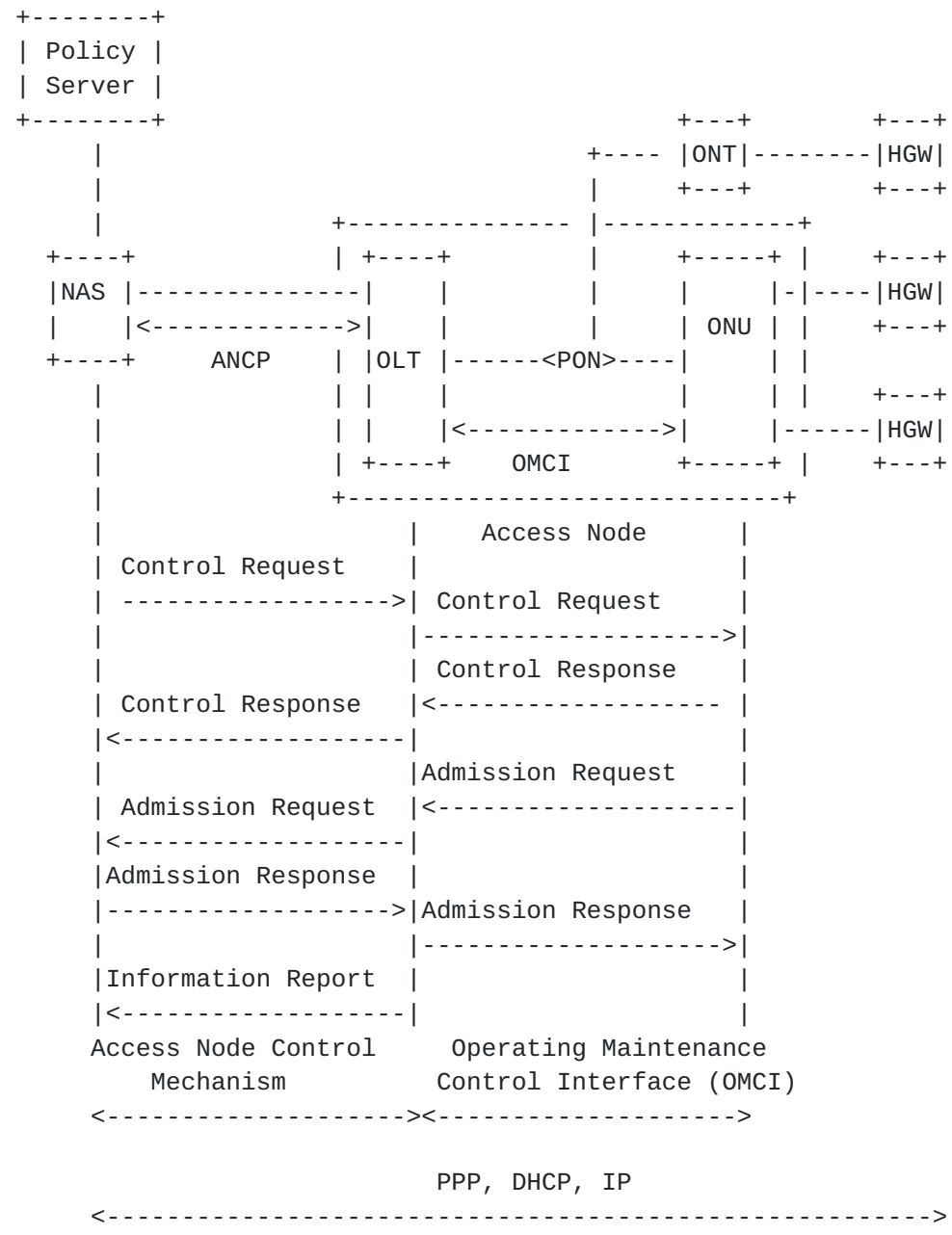


Figure 6: Conceptual Message Flow for ANCP+OMCI ANX control model.

6. Multicast

With the rise of supporting IPTV services in a resource-efficient way, multicast services are becoming increasingly important.

In order to gain bandwidth optimization with multicast, the replication of multicast content per access-loop needs to be distributed to the ANX. This can be done by ANX (OLT and ONT/ONU) becoming multicast aware by implementing an IGMP [RFC3376]

snooping and/or proxy function [RFC4605]. The replication thus needs to be distributed between NAS, aggregation nodes, and ANX. In case of GPON, and in case of BPON with Ethernet uplink, this is very viable. By introducing IGMP processing on the ANX and aggregation nodes, the multicast replication process is now divided between the NAS, the aggregation node(s) and ANX. This is in contrast to the ATM-based model where NAS is the single element responsible for all multicast control and replication. In order to ensure backward compatibility with the ATM-based model, the NAS, aggregation node and ANX need to behave as a single logical device. This logical device must have exactly the same functionality as the NAS in the ATM access/aggregation network. The Access Node Control Mechanism can be used to make sure that this logical/functional equivalence is achieved by exchanging the necessary information between the ANX and the NAS.

An alternative to multicast awareness in the ANX is for the subscriber to communicate the IGMP "join/leave" messages with the NAS, while the ANX is being transparent to these messages. In this scenario, the NAS can use ANCP to create replication state in the ANX for efficient multicast replication. The NAS sends a single copy of the multicast stream towards the ANX. The NAS can perform network-based conditional access and multicast admission control on multicast joins, and create replication state in the ANX if the request is admitted by the NAS.

The following sections describe various use cases related to multicast.

6.1. Multicast Conditional Access

In a Broadband FTTP/B/C access scenario, Service Providers may want to dynamically control, at the network level, access to some multicast flows on a per user basis. This may be used in order to differentiate among multiple Service Offers or to realize/reinforce conditional access based on customer subscription. Note that, in some environments, application layer conditional access by means of Digital Rights Management (DRM) for instance may provide sufficient control so that network-based Multicast conditional access may not be needed. However, network level access control may add to the service security by preventing the subscriber from receiving a non-subscribed channel. In addition, it enhances network security by preventing a multicast stream from being sent on a link or a PON based on a non-subscriber request.

Where network-based channel conditional access is desired, there are two approaches. It can be done on the NAS along with bandwidth-based admission control. The NAS can control the replication state on the ANX based on the outcome of access and bandwidth based admission control. This is covered in a later section. The other approach is to provision the necessary conditional access information on the ANX (ONT/ONU and/or OLT) so the ANX can perform the conditional access decisions autonomously. For these cases, the NAS can use ANCP to provision black and white lists as defined in [RFC5851] on the ANX so that the ANX can decide locally to honor a join or not. It should be noted that in the PON case, the ANX is composed of the ONT/ONU and OLT. Thus, this information can be programmed on the ONT/ONU and/or OLT. Programming this information on the ONT/ONU prevents illegitimate joins from propagating further into the network. A third approach, outside of the scope, may be to program the HGW with the access list. A White list associated with an Access Port identifies the multicast channels that are allowed to be replicated to that port. A Black list associated with an Access Port identifies the multicast channels that are not allowed to be replicated to that port. It should be noted that the black list if not explicitly programmed is the complement of the white list and vice versa.

If the ONT/ONU performs IGMP snooping and it is programmed with a channel access list, the ONT/ONU will first check if the requested multicast channel is part of a White list or a Black list associated with the access port on which the IGMP join is received. If the channel is part of a White list, the ONT/ONU will pass the join request upstream towards the NAS. The ONT/ONU must not start replicating the associated multicast stream to the access port if such a stream is received until it gets confirmation that it can do so from the upstream node (NAS or OLT). Passing the channel access list is one of the admission control criteria whereas bandwidth-based admission control is another. If the channel is part of a Black list, the ONT/ONU can autonomously discard the message because the channel is not authorized for that subscriber.

The ONT/ONU, in addition to forwarding the IGMP join, sends an ANCP admission request to the OLT identifying the channel to be joined and the premises. Premises identification to the OLT can be based on a Customer-Port-ID that maps to the access port on the ONT/ONU and known at the ONT/ONU and OLT. If the ONT/ONU has a white list and/or a black list per premises, the OLT need not have such a list. If the ONT/ONU does not have such a list, the OLT may be programmed with

such a list for each premises. In this latter case, the OLT would perform the actions described earlier on the ONT/ONU. Once the outcome of admission control (conditional access and bandwidth based admission control) is determined by the OLT (either by interacting with the NAS or locally), it is informed to the ONT/ONU. OLT Bandwidth based admission control scenarios are defined in a later section.

The White List and Black List can contain entries allowing:

- An exact match for a (*,G) Any Source Multicast (ASM) group (e.g., <G=g.h.i.l>);

- An exact match for a (S,G) Source Specific Multicast (SSM)channel (e.g., <S=s.t.u.v,G=g.h.i.l>);

- A mask-based range match for a (*,G) ASM group (e.g., <G=g.h.i.l/Mask>);

- A mask-based range match for a (S,G) SSM channel (e.g., <S=s.t.u.v,G=g.h.i.l/Mask>);

The use of a White list and Black list may be applicable, for instance, to regular IPTV services (i.e., Broadcast TV) offered by an Access Provider to broadband (e.g., FTTP) subscribers. For this application, the IPTV subscription is typically bound to a specific FTTP home, and the multicast channels that are part of the subscription are well-known beforehand. Furthermore, changes to the conditional access information are infrequent, since they are bound to the subscription. Hence the ANX can be provisioned with the conditional access information related to the IPTV service.

Instead of including the channel list(s) at the ONT/ONU, the OLT or NAS can be programmed with these access lists. Having these access lists on the ONT/ONU prevents forwarding of unauthorized joins to the OLT or NAS, reducing unnecessary control load on these network elements. Similarly, performing the access control at the OLT instead of the NAS, if not performed on the ONT/ONU, will reduce unnecessary control load on the NAS.

6.2. Multicast Admission Control

The successful delivery of Triple Play Broadband services is quickly becoming a big capacity planning challenge for most of the Service

Providers nowadays. Solely increasing available bandwidth is not always practical, cost-economical and/or sufficient to satisfy end-user experience given not only the strict QoS requirements of unicast applications like VoIP and Video on Demand, but also the fast growth of multicast interactive applications such as "video conferencing", digital TV, and digital audio. These applications typically require low delay, low jitter, low packet loss and high bandwidth. These applications are also typically "non-elastic", which means that they operate at a fixed bandwidth, which cannot be dynamically adjusted to the currently available bandwidth.

An Admission Control (AC) mechanism covering admission of multicast traffic for the FTTP/B/C access is required in order to avoid over-subscribing the available bandwidth and negatively impacting the end-user experience. Before honoring a user request to join a new multicast flow, the combination of ANX and NAS must ensure admission control is performed to validate that there is enough video bandwidth remaining on the PON, and on the uplink between the OLT and NAS to carry the new flow (in addition to all other existing multicast and unicast video traffic) and that there is enough video bandwidth for the subscriber to carry that flow. The solution needs to cope with multiple flows per premises and needs to allow bandwidth to be dynamically shared across multicast and unicast video traffic per subscriber, PON, and uplink (irrespective of whether unicast AC is performed by the NAS, or by some off-path Policy Server). It should be noted that the shared bandwidth between multicast and unicast video is under operator control. That is, in addition to the shared bandwidth, some video bandwidth could be dedicated to Video on Demand, while other video bandwidth could be dedicated for multicast.

The focus in this document will be on multicast-allocated bandwidth including the shared unicast and multicast bandwidth. Thus, supporting admission control requires some form of synchronization between the entities performing multicast AC (e.g., the ANX and/or NAS), the entity performing unicast AC (e.g., the NAS or a Policy Server), and the entity actually enforcing the multicast replication (i.e., the NAS and the ANX). This synchronization can be achieved in a number of ways:

- One approach is for the NAS to perform bandwidth based admission control on all multicast video traffic and unicast video traffic that requires using the shared bandwidth with multicast. Based on the outcome of admission control, NAS then controls the replication state on the ANX. The subscriber

generates an IGMP join for the desired stream on its logical connection to the NAS. The NAS terminates the IGMP message, and performs conditional access and bandwidth based admission control on the IGMP request. The bandwidth admission control is performed against the following:

1. Available video bandwidth on the link to OLT

2. Available video bandwidth on the PON interface

3. Available video bandwidth on the last mile (access-port on the ONT/ONU).

The NAS can locally maintain and track video bandwidth it manages for all the three levels mentioned above. The NAS can maintain identifiers corresponding to the PON interface and the last mile (customer interface). It also maintains a channel map, associating every channel (or a group of channels sharing the same bandwidth requirement) with a data rate. For instance, in case of 1:1 VLAN representation of the premises, the outer tag (S-VLAN) could be inserted by the ANX to correspond to the PON interface on the OLT, and the inner-tag could be inserted by the ANX to correspond to the access-line towards the customer. Bandwidth tracking and maintenance for the PON interface and the last-mile could be done on these VLAN identifiers. In case of N:1 representation, the single VLAN inserted by ANX could correspond to the PON interface on the OLT. The access loop is represented via Customer-Port-ID received in "Agent Circuit Identifier" sub-option in DHCP messages.

The NAS can perform bandwidth accounting on received IGMP messages. The video bandwidth is also consumed by any unicast video being delivered to the CPE. NAS can perform video bandwidth accounting and control on both IGMP messages and on requests for unicast video streams when either all unicast admission control is done by the NAS or an external policy server makes a request to the NAS for using shared bandwidth with multicast as described later in the document.

This particular scenario assumes the NAS is aware of the bandwidth on the PON, and under all conditions can track the changes in available bandwidth on the PON. On receiving an IGMP Join message, NAS will perform bandwidth check on the subscriber bandwidth. If this passes, and the stream is already being forwarded on the PON by the OLT (which also means that it is already forwarded by the NAS to the OLT), NAS will admit the JOIN, update the available subscriber

bandwidth, and transmit an ANCP message to the OLT and in turn to the ONT/ONU to start replication on the customer port. If the stream is not already being replicated to the PON by the OLT, the NAS will also check the available bandwidth on the PON, and if it is not already being replicated to the OLT it will check the bandwidth on the link towards the OLT. If this passes, the available PON bandwidth and the bandwidth on the link towards the OLT are updated. The NAS adds the OLT as a leaf to the multicast tree for that stream. On receiving the message to start replication, the OLT will add the PON interface to its replication state if the stream is not already being forwarded on that PON. Also, the OLT will send an ANCP message to direct the ONT/ONU to add or update its replication state with the customer port for that channel. The interaction between ANX and NAS is shown in Figures 7 and 8. For unicast video streams, application level signaling from the CPE typically triggers an application server to request bandwidth based admission control from a policy server. The policy server can in turn interact with the NAS to request the bandwidth for the unicast video flow if it needs to use shared bandwidth with multicast. If the bandwidth is available, NAS will reserve the bandwidth, update the bandwidth pools for subscriber bandwidth, the PON bandwidth, and the bandwidth on the link towards the OLT, and send a response to the policy server, which is propagated back to the application server to start streaming. Otherwise, the request is rejected.

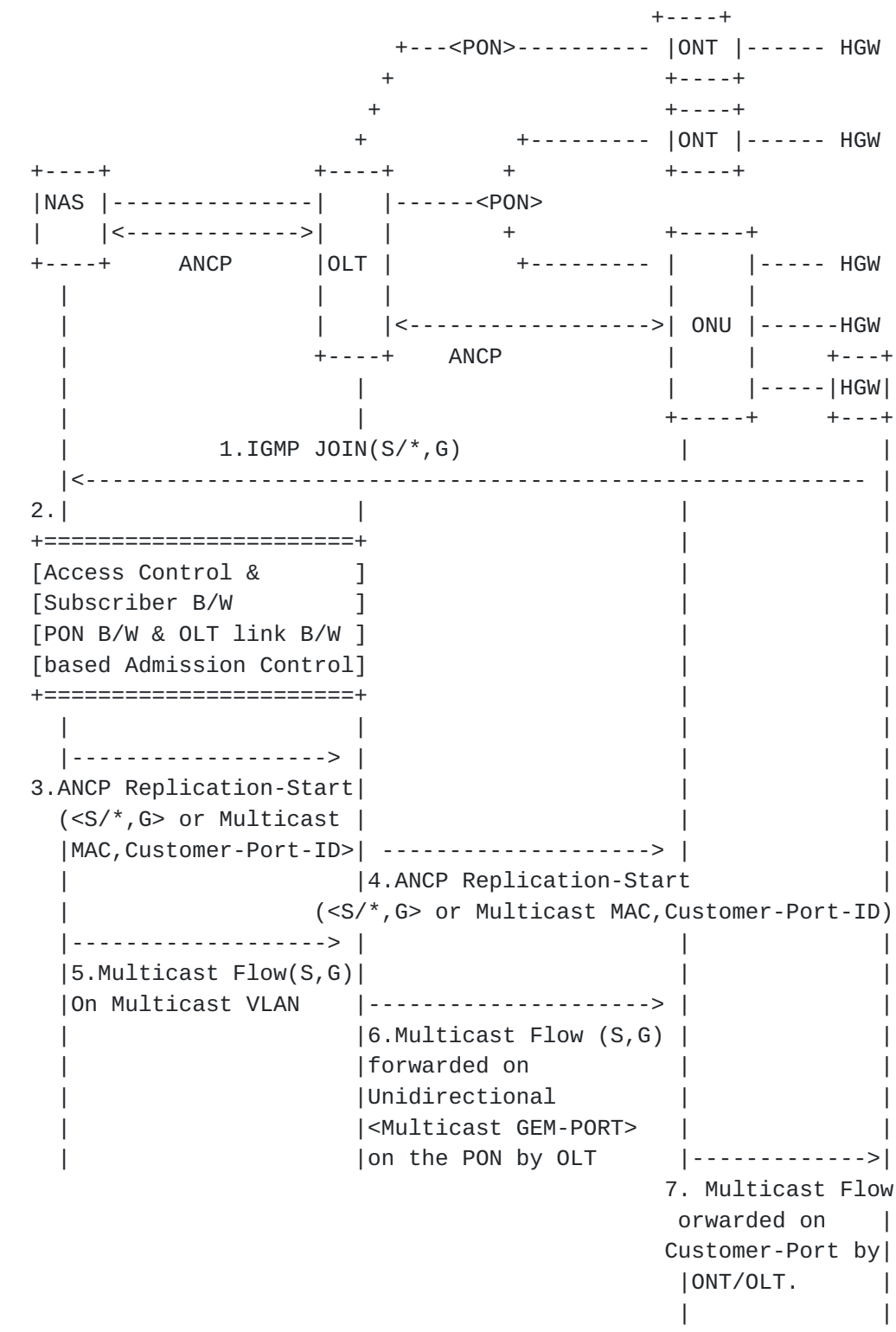


Figure 7: Interactions for NAS based Multicast Admission Control (no IGMP processing on ANX, and NAS maintains available video bandwidth for PON) upon channel join.

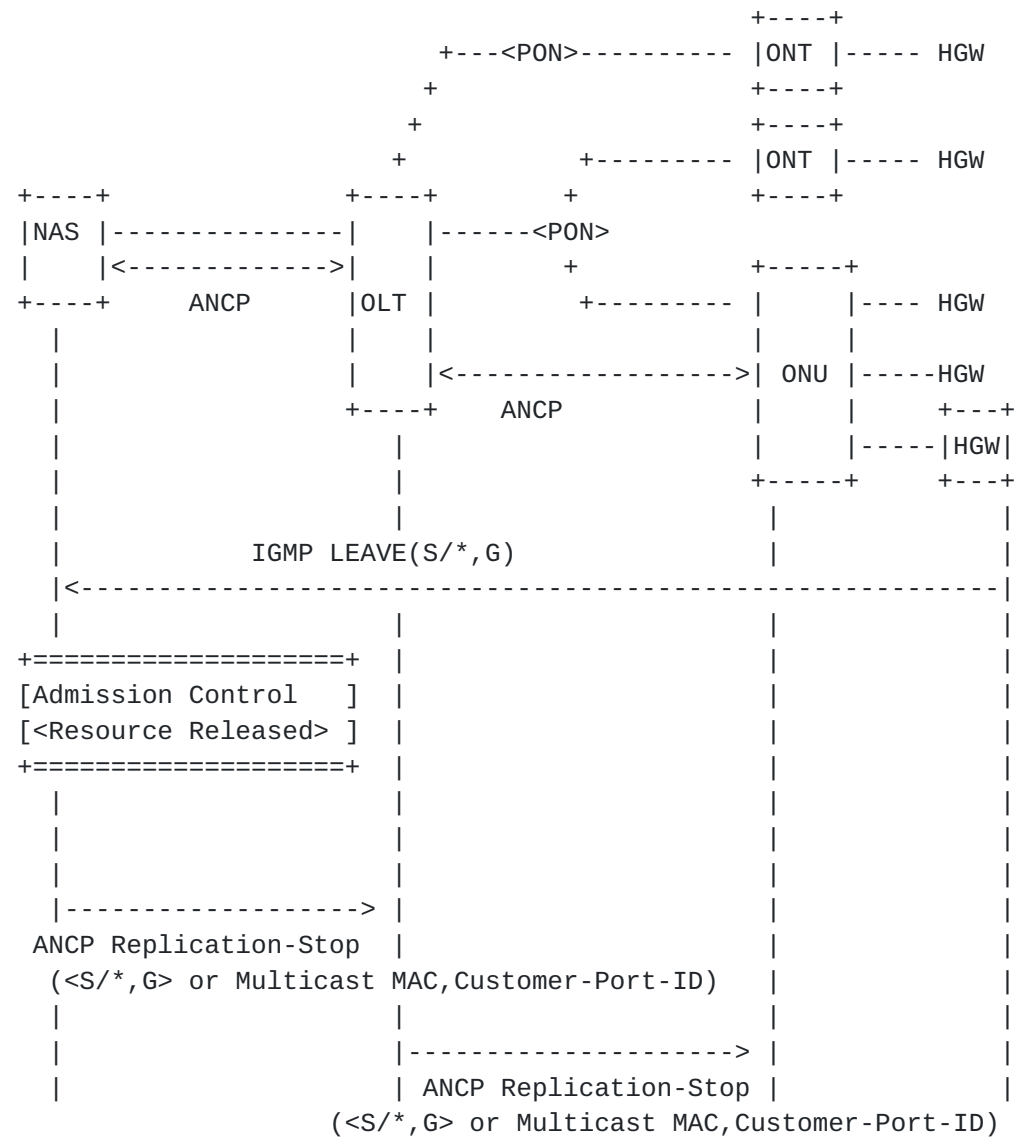


Figure 8: Interactions for NAS based Multicast Admission Control (no IGMP processing on ANX, and NAS maintains available video bandwidth for PON) upon channel leave.

- An alternate approach is required if the NAS is not aware of the bandwidth on the PON. In this case the OLT does the PON bandwidth management, and requests NAS to perform bandwidth admission control on subscriber bandwidth and the bandwidth on the link to the OLT. Following are operations of various elements:

ANX operation:

- ONT/ONU can snoop IGMP messages. If conditional access is configured and the channel is in the Black list (or it is not on the White list), ONT will drop the IGMP Join. If the channel passes the conditional access check, the ONT will forward the IGMP Join, and will send a bandwidth admission control request to the OLT. In case the multicast stream is already being received on the PON, the ONT/ONU does not forward the stream to the access port where IGMP is received till it has received a positive admission control response from the OLT.

- OLT can snoop IGMP messages. It also receives a bandwidth admission control request from the ONT/ONU for the requested channel. It can be programmed with a channel bandwidth map. If the multicast channel is already being streamed on the PON, or the channel bandwidth is less than the multicast available bandwidth on the PON, the OLT forwards the IGMP request to the NAS and keeps track of the subscriber (identified by customer-Port-ID) as a receiver. If the channel is not already being streamed on the PON, but the PON has sufficient bandwidth for that channel, the OLT reduces the PON multicast video bandwidth by the channel bandwidth and may optionally add the PON to the multicast tree without activation for that channel. This is biased towards a forward expectation that the request will be accepted at the NAS. The OLT forwards the IGMP join to the NAS. It also sends a bandwidth admission request to the NAS identifying the channel, and the premises for which the request is made. It sets a timer for the subscriber multicast entry within which it expects to receive a request from the NAS that relates to this request. If the PON available bandwidth is less than the bandwidth of the requested channel, the OLT sends an admission response (with a reject) to the ONT/ONU, and does not forward the IGMP join to the NAS.

NAS operation:

The NAS receives the IGMP join from the subscriber on the subscriber connection. When NAS receives the admission control request from ANX (also signifying the bandwidth on the PON is available), it performs admission control against the subscriber available multicast bandwidth. If this check passes, and the NAS is already transmitting that channel to the OLT, the request is accepted. If the check passes and the NAS is not transmitting the channel to the OLT yet, it performs admission control against the multicast video available bandwidth (this includes the dedicated multicast bandwidth and the shared bandwidth between multicast and video on demand) on the

link(s) to the OLT. If the check passes, the request is accepted, the available video bandwidth for the subscriber and downlink to the OLT are reduced by the channel bandwidth, and the NAS sends an ANCP admission control response (indicating accept) to the OLT, requesting the addition of the subscriber to the multicast tree for that channel. The OLT activates the corresponding multicast entry if not active and maintains state of the subscriber in the list of receivers for that channel. The OLT also sends an ANCP request to the ONT/ONU to enable reception of the multicast channel and forwarding to the subscriber access port. Otherwise, if the request is rejected, the NAS will send an admission reject to the OLT, which in turn removes the subscriber as a receiver for that channel (if it were added), and credits back the channel bandwidth to the PON video bandwidth if there is no other receiver on the PON for that channel. The interactions between ANX and NAS are shown in Figures 9 and 10.

If the OLT does not receive a response from the NAS within a set timer, the OLT removes the subscriber from the potential list of receivers for the indicated channel. It also returns the allocated bandwidth to the PON available bandwidth if there are no other receivers. In this case, the NAS may send a response to the OLT with no matching entry as the entry has been deleted. The OLT must perform admission control against the PON available bandwidth and may accept the request and send an ANCP request to the ONT/ONU to activate the corresponding multicast entry as described earlier. If it does not accept the request, it will respond back to the NAS with a reject. The NAS shall credit back the channel bandwidth to the subscriber. It shall also stop sending the channel to the OLT if that subscriber was the last leaf on the multicast tree towards the OLT.

On processing an IGMP leave, the OLT will send an ANCP request to NAS to release resources. NAS will release the subscriber bandwidth. If this leave causes the stream to be no longer required by the OLT, the NAS will update its replication state and release the bandwidth on the NAS to OLT link.

If the subscriber makes a request for a unicast video stream (i.e., Video on Demand), the request results in appropriate application level signaling, which typically results in an application server requesting a policy server for bandwidth-based admission control for the VoD stream. The policy server after authorizing the request, can send a request to the NAS for the required bandwidth if it needs to use bandwidth that is shared with multicast. This request may be based on a protocol outside of the scope of this document. The NAS

checks if the available video bandwidth (accounting for both multicast and unicast) per subscriber and for the link to the OLT is sufficient for the request. If it is, it temporarily reserves the bandwidth and sends an ANCP admission request to the OLT for the subscriber, indicating the desired VoD bandwidth. If the OLT has sufficient bandwidth on the corresponding PON, it reserves that bandwidth and returns an accept response to the NAS. If not, it returns a reject to the NAS. If the NAS receives an accept, it returns an accept to the policy server which in turn returns an accept to the application server, and the video stream is streamed to the subscriber. This interaction is shown in Figure 11. If the NAS does not accept the request from the policy server, it returns a reject. If the NAS receives a reject from the OLT, it returns the allocated bandwidth to the subscriber and the downlink to the OLT.

Figure 9: Interaction between NAS & ANX for Multicast Bandwidth Admission Control in the All-ANCP ANX control model upon success. Similar functionality will be required when OMCI is enabled between the OLT and ONT/ONU in the ANCP+OMCI ANX control model. In this latter case, the OLT will act as ANCP-OMCI gateway.

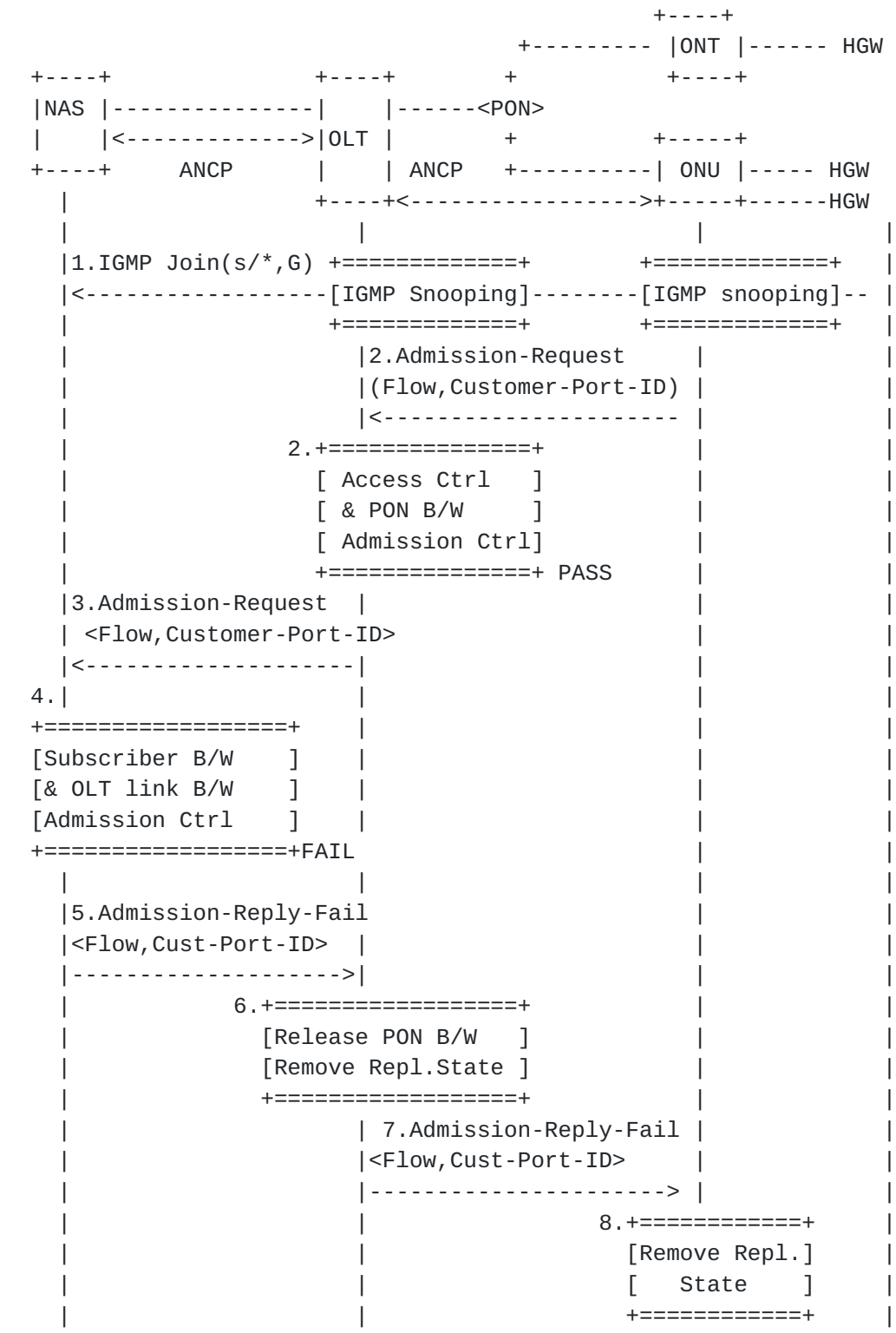


Figure 10: Interaction between NAS and ANX for Multicast Bandwidth Admission Control in the All-ANCP ANX control model upon failure. Similar functionality will be required when OMCI is enabled between the OLT and ONT/ONU in the ANCP+OMCI ANX control model. In this latter case, the OLT will act as ANCP-OMCI gateway.

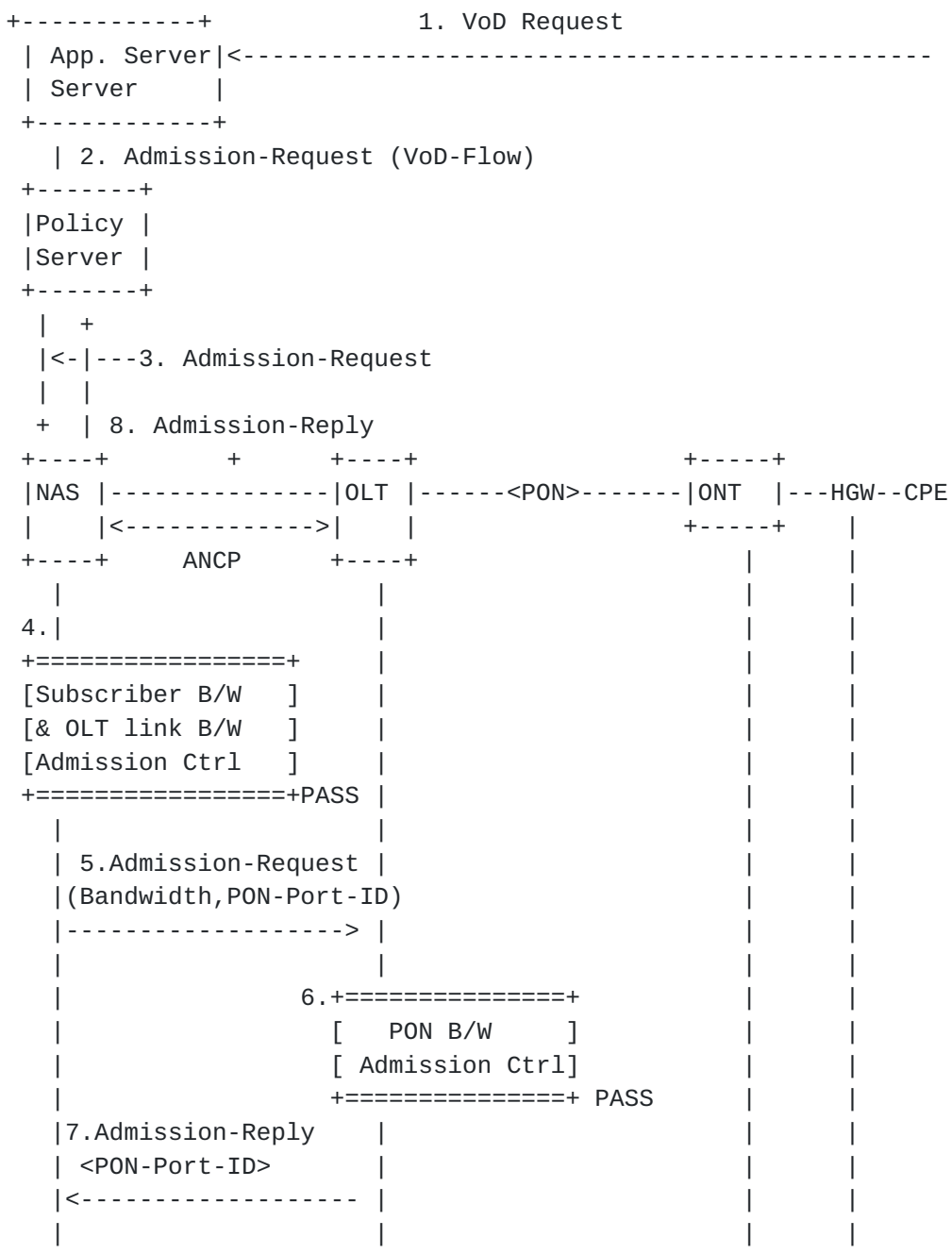


Figure 11: Interactions for VoD Bandwidth Admission Control in the All-ANCP ANX control model. Similar functionality will be required when OMCI is enabled between the OLT and ONT in the ANCP+OMCI ANX control model. In this latter case, the OLT will act as ANCP-OMCI gateway.

-A third possible approach is where the ANX is assumed to have a full knowledge to make an autonomous decision on admitting or rejecting a multicast and a unicast join. With respect to the interaction between

ONT/ONU and OLT, the procedure is similar to the first approach (i.e., NAS controlled replication). However, when the OLT receives an IGMP request from a subscriber, it performs admission control against that subscriber multicast video bandwidth (dedicated and shared with Video on Demand), the PON and uplink to the NAS. It should be noted in this case that if there are multiple NAS-OLT links, either the link on which the multicast stream must be sent is pre-determined, needs to be selected by the OLT based on downstream bandwidth from NAS to OLT and the selection is communicated to the NAS, or the OLT has to be ready to receive the stream on any link. If the check passes, the OLT updates the video available bandwidth per PON and subscriber. The OLT adds the subscriber to the list of receivers and the PON to the multicast tree, if it is not already on it. It also sends an ANCP request to the ONT/ONU to add the subscriber access port to that channel multicast tree, and sends an ANCP message to the NAS informing it of the subscriber and link available video bandwidth and the channel the subscriber joined. The NAS upon receiving the ANCP information message, updates the necessary information, including the OLT to the multicast tree if it is not already on it. It should be noted in this case that the ANCP message from the OLT to the NAS is being used to add the OLT to a multicast tree as opposed to an IGMP message. The IGMP message can also be sent by the OLT with the OLT acting as an IGMP proxy at the expense of added messages. In this option, the OLT acts as the network IGMP router for the subscriber.

For unicast video streams, the policy server receiving an admission request from an application server, as described before, may query the OLT for admission control as it has all information. If the OLT has sufficient bandwidth for the stream it reserves that bandwidth for the subscriber, PON and OLT uplink to the NAS and returns an accept to the policy server. It also updates the NAS via an ANCP message of the subscriber available video bandwidth. If the OLT rejects the policy server request, it will return a reject to the policy server.

It should be noted that if the policy server adjacency is with the NAS, the policy server may make the admission request to the NAS. The NAS then sends an ANCP admission request to the OLT on behalf of the policy server. The NAS returns an accept or reject to the policy server if it gets a reject or accept, respectively, from the OLT.

6.3. Multicast Accounting

It may be desirable to perform accurate per-user or per Access Loop time or volume based accounting. In case the ANX is performing the traffic replication process, it knows when replication of a multicast flow to a particular Access Port or user starts and stops. Multicast accounting can be addressed in two ways:

- ANX keeps track of when replication starts or stops, and reports this information to the NAS for further processing. In this case, ANCP can be used to send the information from the ANX to the NAS. This can be done with the Information Report message. The NAS can then generate the appropriate time and/or volume accounting information per Access Loop and per multicast flow, to be sent to the accounting system. The ANCP requirements to support this approach are specified in [RFC5851]. If the replication function is distributed between the OLT and ONT/ONU, a query from the NAS will result in OLT generating a query to the ONT/ONU.

- ANX keeps track of when replication starts or stops, and generates the time and/or volume based accounting information per Access Loop and per multicast flow, before sending it to a central accounting system for logging. Since ANX communicates with this accounting system directly, the approach does not require the use of ANCP. It is therefore beyond the scope of this document. It may also be desirable for the NAS to have the capability to asynchronously query the ANX to obtain an instantaneous status report related to multicast flows currently replicated by the ANX. Such a reporting functionality could be useful for troubleshooting and monitoring purposes. If the replication function in the ANX is distributed between the OLT and the ONT/ONU, then for some of the information required by the NAS (such as the list of access-ports on which a flow is being forwarded or list of flows being forwarded on an access-port), a query to the OLT from the NAS will result in a query from OLT to ONT/ONU. The OLT responds back to the NAS when it receives the response from the ONT/ONU. Also, if the list of PONs on which replication is happening for a multicast channel or the list of channels being replicated on a PON is what is desired, the OLT can return this information.

7. Remote Connectivity Check

In an end-to-end Ethernet aggregation network, end-to-end Ethernet OAM as specified in IEEE 802.1ag and ITU-T Recommendation Y.1730/1731 can provide Access Loop connectivity testing and fault isolation.

However, most HGWs do not yet support these standard Ethernet OAM procedures. Also, in a mixed Ethernet and ATM access network (e.g., Ethernet based aggregation upstream from the OLT, and BPON downstream), interworking functions for end-to-end OAM are not yet standardized or widely available. Until such mechanisms become standardized and widely available, Access Node Control mechanism between NAS and ANX can be used to provide a simple mechanism to test connectivity of an access-loop from the NAS.

Triggered by a local management interface, the NAS can use the Access Node Control Mechanism (Control Request Message) to initiate an Access Loop test between Access Node and HGW or ONT/ONU. On reception of the ANCP message, the OLT can trigger native OAM procedures defined for BPON in [G.983.1] and for GPON in [G.984.1]. The Access Node can send the result of the test to the NAS via a Control Response message.

8. Access Topology Discovery

In order to avoid congestion in the network, manage and utilize the network resources better, and ensure subscriber fairness, NAS performs hierarchical shaping and scheduling of the traffic by modeling different congestion points in the network (such as the last-mile, access Node uplink, and the access facing port).

Such mechanisms require that the NAS gains knowledge about the topology of the access network, the various links being used and their respective rates. Some of the information required is somewhat dynamic in nature (e.g., DSL line rate in case the last mile is xDSL based, e.g., in case of "PON fed DSLAMs" for FTTC/FTTB scenarios), hence cannot come from a provisioning and/or inventory management Operations Support System (OSS). Some of the information varies less frequently (e.g., capacity of the OLT uplink), but nevertheless needs to be kept strictly in sync between the actual capacity of the uplink and the image the NAS has of it.

OSS systems are rarely able to enforce in a reliable and scalable manner the consistency of such data, notably across organizational boundaries under certain deployment scenarios. The Access Topology Discovery function allows the NAS to perform these advanced functions without having to depend on an error-prone and possibly complex integration with an OSS system.

The rate of the access-loop can be communicated via ANCP (Information Report Message) from the ONT/ONU to the OLT in the All-ANCP ANX control model or via OMCI in the ANCP+OMCI ANX control model, and then from OLT to the NAS via ANCP. Additionally, during the time the DSL NT is active, data rate changes can occur due to environmental conditions (the DSL Access Loop can get "out of sync" and can retrain to a lower value, or the DSL Access Loop could use Seamless Rate Adaptation making the actual data rate fluctuate while the line is active). In this case, ANX sends an additional Information Report to the NAS each time the Access Loop attributes change above a threshold value. Existing DSL procedures are not applicable in this case because an adapted message flow and additional TLVs are needed.

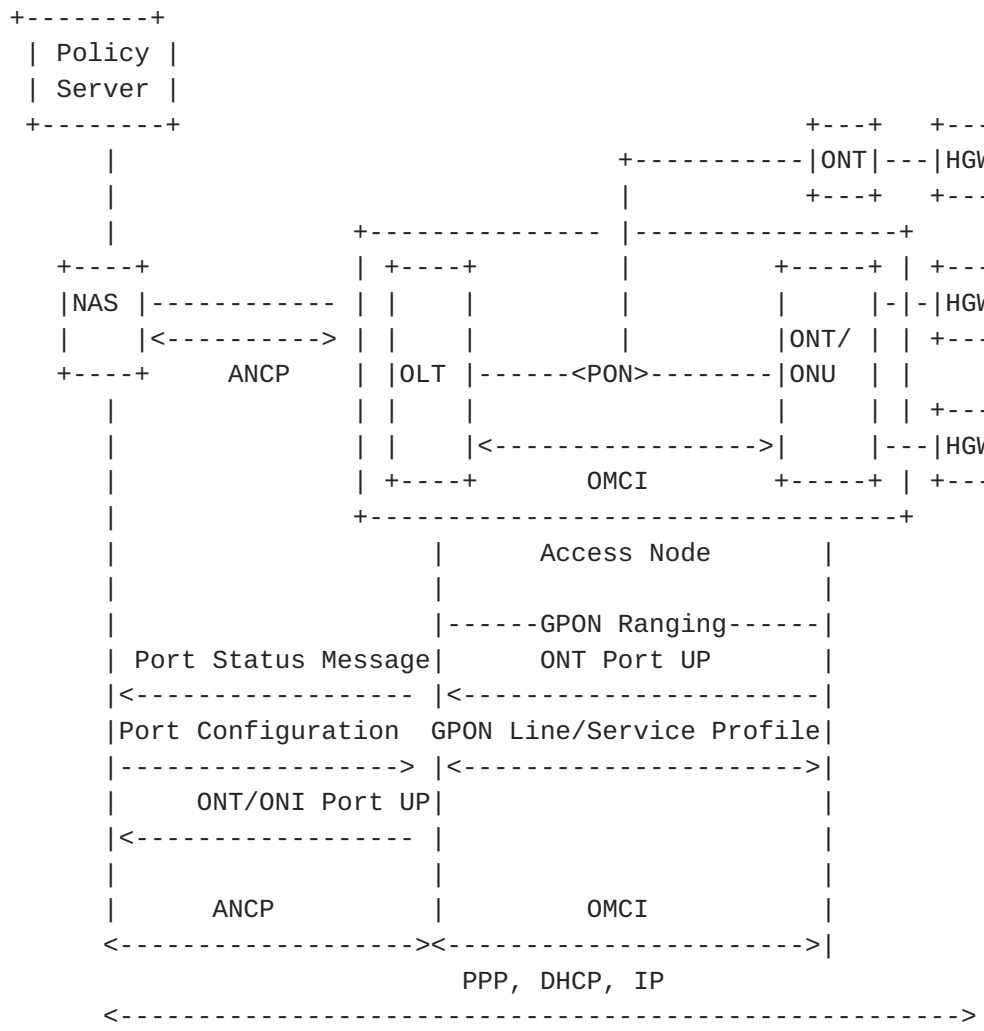


Figure 12: Message Flow for the use case of Topology Discovery for the ANCP+OMCI access control model.

Figure 12 depicts a message flow for topology discovery when using the ANCP+OMCI access control model. Basically, when an ONT/ONU gets connected to a PON, the OLT detects a new device and a GPON Ranging process starts. During this process the ONT/ONU becomes authorized by the OLT and identified by ONT/ONU ID, PON Port ID and max Bandwidth. This port status is reported via ANCP to the NAS and then potentially the policy server via another mechanism that is out of scope of this document. In a second step after GPON Service profile is assigned from OLT to ONT/ONU, the OLT reports the final status to NAS with information about service profile and other information such as the ONT/ONU port rate to the subscriber for instance.

9. Access Loop Configuration

Topology Discovery reports access port identification to NAS when sending an Access Port Discovery message. This informs NAS identification of PON port on an Access Node. Based on Access Port Identification and on customer identification, service related parameters could be configured on an OLT and an ONU/ONT.

Service related parameters could be sent to OLT via ANCP before or after an ONU/ONT is up. Sending of ANCP loop Configuration messages from NAS can be triggered by a management system or by customer identification and authentication after Topology Discovery. It may be used for first time configuration (zero touch) or for updating/upgrading customer's profile like C-VLAN ID, S-VLAN ID, and service bandwidth.

Parameters of the User to Network Interface (UNI), which is the subscriber interface to HGW/CPE of ONU/ONT, can also be configured via ANCP. When the ONU/ONT supports ANCP, parameters of the UNI on ONU/ONT are sent to the ONU/ONT via ANCP. If the ONU/ONT does not support ANCP, but only OMCI, parameters have to be sent from the NAS to the OLT via ANCP first. Then, the OLT translates such configuration into OMCI and sends it to the ONU/ONT.

10. Security Considerations

[RFC5713] lists the ANCP related security threats that could be encountered on the Access Node and the NAS. It develops a threat model for ANCP security, and lists the security functions that are required at the ANCP level.

With Multicast handling as described in this document, ANCP protocol activity between the ANX and the NAS is triggered by join/leave requests coming from the end-user equipment. This could potentially be used for denial of service attack against the ANX and/or the NAS.

To mitigate this risk, the NAS and ANX may implement control plane protection mechanisms such as limiting the number of multicast flows a given user can simultaneously join, or limiting the maximum rate of join/leave from a given user.

Protection against invalid or unsubscribed flows can be deployed via provisioning black lists as close to the subscriber as possible (e.g., in the ONT).

User activity logging for accounting or tracking purposes could raise privacy concerns if not appropriately protected. To protect such information, logging/accounting information can be exchanged with the corresponding server over a secure channel, and the information can be stored securely with policy-driven controlled access.

11. Differences in ANCP applicability between DSL and PON

As it currently stands, both ANCP framework [RFC5851] and protocol [RFC6320] are defined in context of DSL access. Due to inherent differences between PON and DSL access technologies, ANCP needs a few extensions for supporting the use-cases outlined in this document for PON based access. These specific differences and extensions are outlined below.

- In PON, the access-node functionality is split between OLT and ONT. Therefore, ANCP interaction between NAS and AN translates to transactions between NAS and OLT and between OLT and ONT. The processing of ANCP messages (e.g., for multicast replication control) on the OLT can trigger generation of ANCP messages from OLT to ONT. Similarly, ANCP messages from ONT to the OLT can trigger ANCP exchange between the OLT and the NAS (e.g., admission-request messages). This is illustrated in the generic message flows in Figures 5 and 6 of section 5. In case of DSL, the ANCP exchange is contained between two network elements (NAS and the DSLAM).

- The PON connection to the ONT is a shared medium between multiple ONTs on the same PON. The local-loop in case of DSL is point-to-point. In case of DSL access network, the access facing port on the NAS (i.e., port to the network between NAS and the DSLAM), and the access-facing ports on the DSLAM (i.e., customer's local-loop) are the two bandwidth constraint points that need to be considered for performing bandwidth based admission control for multicast video and VoD delivered to the customer. In case of PON access, in addition to the bandwidth constraint on the NAS to OLT facing ports, and the subscriber allocated bandwidth for video services, the bandwidth available on the PON for video is an additional constraint that needs to be considered for bandwidth based admission control. If the bandwidth control is centralized in NAS (as described in option 1 of section 6.2), then the NAS needs to support additional logic to consider available PON bandwidth before admitting a multicast request or a VoD request by the user. Accordingly, ANCP needs to identify the customer access port and the PON on which the customer ONT is. If the PON bandwidth control is performed on the OLT (as defined in second

option in section 6.2), then additional ANCP request and response messages are required for NAS to query the OLT to determine available PON bandwidth when a request to admit a VOD flow is received on the NAS (as shown in Figure 9 in section 6.2) or for the OLT to inform the NAS what stream bandwidth is sent to the subscriber for the NAS to take appropriate action (e.g., bandwidth adjustment for various types of traffic).

- In PON, the multicast replication can potentially be performed on three different network elements: (1) on the NAS (2) on the OLT for replication to multiple PON ports, and (3) on the ONT/ONU for replication to multiple customer ports. In case of DSL, the replication can potentially be performed on NAS and/or the DSLAM. Section 6.2 defines options for multicast replication in case of PON. In the first option, the multicast replication is done on the AN, but is controlled from NAS via ANCP (based on the reception of per-customer IGMP messages on the NAS). In this option, the NAS needs to supply to the OLT the set of PON-customer-IDs (as defined in section 2) to which the multicast stream needs to be replicated. The PON-customer-ID identifies the OLT and the PON ports on the OLT as well as the ONT and the access-ports on the ONT where the multicast stream needs to be replicated. Upon receiving the request to update its multicast replication state, the OLT must update its replication state with the indicated PON ports, but may also need to interact with the ONT via ANCP to update the multicast replication state on the ONT with the set of access-ports (as indicated by the NAS). In case of DSL, the DSLAM only needs to update its own replication state based on the set of access-ports indicated by the NAS.

- For reporting purposes, ANCP must enable the NAS to query the OLT for channels replicated on a PON or a list of PONs and to specific access ports. The latter should trigger the OLT to query the ONT for a list of channels being replicated on all access ports or on specific access ports to the premises. In DSL case, it is sufficient to query the DSLAM for a list of channels being replicated on an access port or a list of access ports.

12. ANCP versus OMCI between the OLT and ONT/ONU

ONT Management and Control Interface (OMCI) [OMCI] is specified for in-band ONT management via the OLT. This includes configuring parameters on the ONT/ONU. Such configuration can include adding an access port on the ONT to a multicast tree and the ONT to a multicast tree. Thus, OMCI can be a potential replacement for ANCP between the

OLT and ONT/ONU, albeit it may not a be suitable protocol for dynamic transactions as required for the multicast application.

If OMCI is selected to be enabled between the OLT and ONT/ONU to carry the same information elements that would be carried over ANCP, the OLT must perform the necessary translation between ANCP and OMCI for replication control messages received via ANCP. OMCI is an already available control channel, while ANCP requires a TCP/IP stack on the ONT/ONU that can be used by an ANCP client and accordingly it requires that the ONT/ONU be IP addressable for ANCP. Most ONTs/ONUs today have a TCP/IP stack used by certain applications (e.g., VoIP, IGMP snooping). ANCP may use the same IP address that is often assigned for VoIP or depending on the implementation may require a different address. Sharing the same IP address between VoIP and ANCP may have other network implications on how the VoIP agent is addressed and on traffic routing. For instance, the VoIP traffic to/from the ONT is often encapsulated in a VLAN-tagged Ethernet frame and switched at layer2 through the OLT to the NAS where it is routed. The VoIP agent in this case looks like another subscriber to the NAS. On the other hand, the ANCP session between the ONT and OLT is terminated at the OLT. Thus, the OLT must be able to receive/send IP traffic to/from the OLT, which will not work using this setting. Using a separate IP address for the purpose of ONT/ONU management or ANCP specifically may often be required when supporting ANCP. These considerations may favor OMCI in certain environments. However, OMCI will not allow some of the transactions required in approach 2, where the ONT/ONU sends unsolicited requests to the OLT rather than being queried or configured by OLT requests.

13. IANA Considerations

This document does not require actions by IANA.

14. Acknowledgements

The authors are thanksful to Rajesh Yadav and Francois Le Faucheur for valuable comments and discussions.

15. References

15.1. Normative References

[RFC2516] Mamakos, L., Lidl, K., Evarts, J., Carrel, D., Simone, D., and R. Wheeler, "A Method for Transmitting PPP Over Ethernet (PPPoE)", RFC 2516, February 1999.

[RFC2684] Grossman, D. and J. Heinanen, "Multiprotocol Encapsulation over ATM Adaptation Layer 5", RFC 2684, September 1999.

[RFC3376] Cain, B., et al, "Internet Group Management Interface, Version 3", RFC 3376, October 2002.

[RFC4605] Fenner, W., et al, "Internet Group Management Protocol (IGMP)/Multicast Listener Discovery (MLD)-Based Multicast Forwarding ("IGMP/MLD Proxying")", RFC 4605, August 2006.

15.2. Informative References

[RFC2881] Mitton, D. and M. Beadles, "Network Access Server Requirements Next Generation (NASREQNG) NAS Model", RFC 2881, July 2000.

[RFC5851] Ooghe, S., et al., "Framework and Requirements for Access Node Control Mechanism in Broadband Networks", RFC 5851, May 2010.

[G.983.1] ITU-T G.983.1, "Broadband optical access systems based on Passive Optical Networks (PON)".

[G.984.1] ITU-T G.984.1, "Gigabit-capable Passive Optical Networks (G-PON): General characteristics".

[RFC3046] Patrick, M., "DHCP Relay Agent Information Option", RFC3046, January 2011.

[TR-101] Cohen, A. and E. Shrum, "Migration to Ethernet-Based DSL Aggregation", DSL Forum TR-101, May 2006.

[RFC5713] Moustafa, H., Tschofenig, H., and S. De Cnodder, "Security Threats and Security Requirements for the Access Node Control Protocol (ANCP)", RFC 5713, January 2010.

[OMCI] ITU-T G.984.4, "GPON ONT Management and Control Interface (OMCI) Specifications".

[RFC6320] Taylor, T., et al, "Protocol for Access Node Control Mechanism in Broadband Networks", RFC 6320, October 2011.

[G.987.3] ITU-T G.987.3, "10-Gigabit-capable passive optical networks(XG-PON): Transmission convergence (TC) layer specification".

Authors' Addresses

Nabil Bitar
Verizon
60 Sylvan Road
Waltham, MA 02451
Email: nabil.n.bitar@verizon.com

Sanjay Wadhwa
Alcatel-Lucent
701 East Middlefield Road
Mountain View, CA, 94043
Email: sanjay.wadhwa@alcatel-lucent.com

Thomas Haag
Deutsche Telekom
Email: HaagT@telekom.de

Hongyu Li
Huawei Technologies
Email: hongyu.lihongyu@huawei.com