TECHNICAL REPORT

TR-207

Layer 2 Control Mechanism For Broadband Multi-Service Architectures part II

Issue: 1
Issue Date: November 2012

© The Broadband Forum. All rights reserved.

Notice

The Broadband Forum is a non-profit corporation organized to create guidelines for broadband network system development and deployment. This Broadband Forum Technical Report has been approved by members of the Forum. This Broadband Forum Technical Report is not binding on the Broadband Forum, any of its members, or any developer or service provider. This Broadband Forum Technical Report is subject to change, but only with approval of members of the Forum. This Technical Report is copyrighted by the Broadband Forum, and all rights are reserved. Portions of this Technical Report may be copyrighted by Broadband Forum members.

This Broadband Forum Technical Report is provided AS IS, WITH ALL FAULTS. ANY PERSON HOLDING A COPYRIGHT IN THIS BROADBAND FORUM TECHNICAL REPORT, OR ANY PORTION THEREOF, DISCLAIMS TO THE FULLEST EXTENT PERMITTED BY LAW ANY REPRESENTATION OR WARRANTY, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTY:

(A) OF ACCURACY, COMPLETENESS, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR TITLE;
(B) THAT THE CONTENTS OF THIS BROADBAND FORUM TECHNICAL REPORT ARE SUITABLE FOR ANY PURPOSE, EVEN IF THAT PURPOSE IS KNOWN TO THE COPYRIGHT HOLDER;
(C) THAT THE IMPLEMENTATION OF THE CONTENTS OF THE TECHNICAL REPORT WILL NOT INFRINGE ANY THIRD PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS.

By using this Broadband Forum Technical Report, users acknowledge that implementation may require licenses to patents. The Broadband Forum encourages but does not require its members to identify such patents. For a list of declarations made by Broadband Forum member companies, please see http://www.broadband-forum.org. No assurance is given that licenses to patents necessary to implement this Technical Report will be available for license at all or on reasonable and non-discriminatory terms.

ANY PERSON HOLDING A COPYRIGHT IN THIS BROADBAND FORUM TECHNICAL REPORT, OR ANY PORTION THEREOF, DISCLAIMS TO THE FULLEST EXTENT PERMITTED BY LAW (A) ANY LIABILITY (INCLUDING DIRECT, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES UNDER ANY LEGAL THEORY) ARISING FROM OR RELATED TO THE USE OF OR RELIANCE UPON THIS TECHNICAL REPORT; AND (B) ANY OBLIGATION TO UPDATE OR CORRECT THIS TECHNICAL REPORT.

Broadband Forum Technical Reports may be copied, downloaded, stored on a server or otherwise re-distributed in their entirety only, and may not be modified without the advance written permission of the Broadband Forum.

The text of this notice must be included in all copies of this Broadband Forum Technical Report.

Issue History

Issue Number	Approval Date	Publication Date	Editors	Changes
1	26 November 2012	28 January 2013	Bill Welch, Juniper Networks Hongyu Li, Huawei Technologies	Original

Comments or questions about this Broadband Forum Technical Report should be directed to info@broadband-forum.org.

Editors	Bill Welch Hongyu Li	Juniper Networks Huawei Technologies
End to End Architecture WG Chairs	David Allan David Thorne	Ericsson BT
Vice Chair	Sven Ooghe	Alcatel-Lucent
Chief Editor	Michael Hanrahan	Huawei Technologies

TABLE OF CONTENTS

© The Broadband Forum. All rights reserved

List of Figures

© The Broadband Forum. All rights reserved

Executive Summary

TR-147 defined a mechanism to perform QoS-related, service-related and subscriber-related operations between network nodes. TR-207 extends TR-147, *Layer 2 Control Mechanism For Broadband Multi-Service Architectures,* to support PON access as well as support new capabilities, such as multicast accounting and enhanced security.

1 Purpose and Scope

1.1 Purpose

Technical Report TR-147 *Layer 2 Control Mechanism For Broadband Multi-Service Architectures* defines a Layer 2 Control Mechanism between a BNG and an Access Node (e.g. DSLAM) in a multi-service reference architecture in order to perform QoS-related, service-related and subscriber-related operations directly between network nodes. TR-207 builds on and is backward compatible with TR-147.

The purpose of TR-207 is to extend Layer 2 Control Mechanism to support PON access as well as support new capabilities, such as multicast accounting and enhanced security.

In order to protect or increase both market share and revenue, service providers are expanding their existing services to support more value added services than those covered by TR-101. New services and business requirements are described by TR-144, which places a series of requirements on the network architecture and requires additional capabilities in network nodes. Tighter coordination between network nodes is more necessary than ever.

TR-147 covers a limited number of use cases requiring coordination functions between network nodes. Therefore, an enhanced Layer 2 Control Mechanism is necessary.

NOTE – TR-207 refers to a BRAS and a BNG as defined in TR-101, but uses the term BNG to refer to both unless explicitly stated otherwise.

1.2 Scope

The scope of TR-207 extends the concept of a Layer 2 Control Mechanism between network nodes and its applicability to multi-service architectures defined in TR-059, TR-101, TR-156, TR-145, TR-167, TR-177, TR-187 and WT-178.

TR-207 defines the network node requirements and describes information flows for the use of L2C mechanisms in the following scenarios:

- PON networks
- New wholesale and retail business agreements
- Multi-Edge Architectures
- Redundant and resilient access network Architectures
- Unified unicast and multicast admission Control
- The provision of remote OAM messages
- Network security
- Multicast accounting

The L2C framework defined in TR-147 covers DSL-based access but does not preclude its use on alternative access technologies. TR-207 goes beyond DSL access to cover additional access technologies and the associated architectures.

1.3 Relation to other Broadband Forum documents

TR-207 is part of the TR-144 family of documents. TR-207 provides L2C architectures and requirements to meet the new business requirements laid out in TR-144 *Broadband Multi-Service Architecture and Framework Requirements*.

2 References and Terminology

2.1 Conventions

In this Technical Report, several words are used to signify the requirements of the specification. These words are always capitalized. More information can be found be in RFC 2119. [11]

MUST This word, or the term “REQUIRED”, means that the definition is an absolute requirement of the specification.

MUST NOT This phrase means that the definition is an absolute prohibition of the specification.

SHOULD This word, or the term “RECOMMENDED”, means that there could exist valid reasons in particular circumstances to ignore this item, but the full implications need to be understood and carefully weighed before choosing a different course.

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

MAY This word, or the term “OPTIONAL”, means that this item is one of an allowed set of alternatives. An implementation that does not include this option MUST be prepared to inter-operate with another implementation that does include the option.

2.2 References

The following references are of relevance to this Technical Report. At the time of publication, the editions indicated were valid. All references are subject to revision; users of this Technical Report are therefore encouraged to investigate the possibility of applying the most recent edition of the references listed below.

A list of currently valid Broadband Forum Technical Reports is published at www.broadband-forum.org.

Document	Title	Source	Year
[1] TR-059	*DSL Evolution - Architecture Requirements for the Support of QoS-Enabled IP Services*	BBF	2003
[2] TR-101 Issue 2	*Migration to Ethernet-Based DSL Aggregation*	BBF	2011
[3] TR-134	*Broadband Policy Control Framework*	BBF	2012
[4] TR-144	*Broadband Multi-Service Architecture &*	BBF	2007

		Framework Requirements		
[5]	TR-147	*Layer 2 Control Mechanism For Broadband Multi-Service Architectures*	BBF	2008
[6]	TR-156 Issue 2	*Using GPON Access in the context of TR-101*	BBF	2010
[7]	TR-167 Issue 2	*GPON-fed TR-101 Ethernet Access Node*	BBF	2010
[8]	G.984.4	*ONT management and control interface (OMCI) specification*	ITU-T	2008
[9]	G.988	*ONU management and control interface (OMCI) specification*	ITU-T	2010
[10]	G.997.1	*Physical Layer Management for Digital Subscriber Line (DSL) Transceivers*	ITU-T	1999
[11]	RFC 2119	*Key words for use in RFCs to Indicate Requirement Levels*	IETF	1997
[12]	RFC 5851	*Framework and Requirements for an Access Node Control Mechanism in Broadband Multi-Service Network*	IETF	2010
[13]	RFC 6320	*Protocol for Access Node Control Mechanism in Broadband Networks*	IETF	2011
[14]	draft-ietf-ancp-pon	*Applicability of Access Node Control Mechanism to PON based Broadband Networks*	IETF	2012
[15]	draft-ietf-ancp-mc-extensions	*Multicast Control Extensions for ANCP*	IETF	2012

2.3 Definitions

This Technical Report uses the following terms:.

Access Node The Access Node is a node that terminates physical access media (e.g. DSL, PON, GE) and also provides the first or only aggregation function.

Actual Data Rate Within this Technical Report the term is used as defined by G.997.1.[10] This parameter reports the actual net data rate the bearer channel is operating at excluding the rate in L1 and L2 states.

BNG IP Edge Router where bandwidth and QoS policies may be applied, to support multi-service delivery.

BRAS The BRAS is a broadband network gateway and is the aggregation point for the subscriber traffic. It provides aggregation capabilities (e.g. IP, PPP, Ethernet) between the access network and the NSP or ASP. In addition to aggregation, it is also a policy management and QoS enforcement point for IP QoS in the access network.

Control Protocol The protocol that is used to implement the Layer 2 Control Mechanism.

Layer 2 Control Adjacency The relationship between an Access Node and a BNG for the purposes of exchanging Layer 2 Control Messages. The adjacency may either be down (i.e. no adjacency messages being exchanged or attempting transport layer connectivity establishment (cf. TCP)), in progress (i.e. adjacency negotiation is in progress) or up (i.e. established), depending on the status of the Layer 2 Control adjacency protocol operation.

Layer 2 Control Mechanism (L2C) A communication scheme that conveys status and control information – for a variety of use cases - between one or more ANs (not necessarily limited to DSLAMs) and one or more BNGs without using intermediate element managers.

Line Rate Within TR-207 the term is used as defined by Table 5-1/G.993.2 and Figure K-10/G.993.2. It contains the complete overhead including RS and trellis coding.

Optical Network Termination (ONT) A single subscriber device that terminates any one of the distributed (leaf) endpoints of an ODN, implements a PON protocol, and adapts PON PDUs to subscriber service interfaces. An ONT is a special case of an ONU.

Optical Network Unit (ONU) A generic term denoting a device that terminates any one of the distributed (leaf) endpoints of an ODN, implements a PON protocol, and adapts PON PDUs to subscriber service interfaces. In some contexts, an ONU implies a multiple subscriber device.

SYN flood A SYN flood is a form of denial-of-service attack in which an attacker sends a succession of SYN requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic

2.4 Abbreviations

AAA	Authentication, Authorization and Accounting
ACL	Access Control List
ADSL	Asymmetric Digital Subscriber Line
ALA	Active Line Access
AN	Access Node
ANCP	Access Node Control Protocol
AVC	Attribute Value Change
ASP	Application Service Provider
BFD	Bidirectional Forwarding Detection
BNG	Broadband Network Gateway
BRAS	Broadband Remote Access Server
CAC	Call Admission Control
CLI	Command Line Interface
C-VLAN ID	Customer VLAN ID
DHCP	Dynamic Host Configuration Protocol
DoS	Denial of Service
DPI	Deep Packet Inspection
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
EMS	Element Management System
FITH	Fiber Into The Home, Fibre delivery to a combined ONU/RG
FTTH	Fiber-To-The-Home, Fibre delivery to a standalone ONU
FTTB/C	Fiber To The Building/Curb
L2C	Layer 2 Control
MAC	Media Access Control
MDU	Multi-Dwelling Unit
MIB	Management Information Base
NSP	Network Service Provider
NAP	Network Access Provider
OAM	Operation, Administration and Maintenance
OLT	Optical Line Termination
OPEX	Operational Expenditure
OSS	Operations support systems,

PDP	Policy Decision Point
PON	Passive Optical Network
PPP	Point-to-Point Protocol
QoS	Quality of service
RADIUS	Remote Authentication Dial In User Service
RG	Residential Gateway
SFU	Single Fiber Unit
SNMP	Simple Network Management Protocol
SYN	Synchronize packet in transmission control protocol (TCP)
S-VLAN ID	Service VLAN ID
UNI	User Network Interface
VLAN	Virtual LAN
xDSL	Various DSL, e.g. ADSL, ADSL2, ADSL2+, VDSL2

3 Technical Report Impact

3.1 Energy Efficiency

TR-207 can deliver some improvement in efficiency of service delivery for a given unit of energy consumed. It can also be used to set or limit rates.

3.2 IPv6

TR-207 is equally applicable to IPv4 and IPv6 access.

3.3 Security

TR-207 addresses use cases that show how L2C can be used to increase network security.

3.4 Privacy

TR-207 has no impact on privacy.

4 Introduction

TR-207 extends TR-147 [5] to allow support of value-added services across GPON based access networks .TR-147 supports the TR-101 [2] architecture, which is based on DSL as last mile technology. TR-207 adapts TR-147 use cases to the PON environment, e.g. access line discovery and line configuration, and adds new use cases on wholesale and security. For implementation of TR-147 based use cases IETF has defined ANCP as protocol suite in RFC 6320 [13]. The IETF is now working on "*draft Applicability of Access Node Control Mechanism to PON based Broadband Networks*".

5 General Architecture

5.1 Reference Architecture for PON

The architecture in TR-207 is focused on PON, as this was not addressed in TR-147.

5.1.1 Overall architecture

An overall architecture of L2C applied to a PON network is depicted in Figure1. An OLT may provide FTTH and FTTB/C access at the same time. The OLT establishes a L2C adjacency with the BNG and is in charge of collecting and reporting status change of ONUs, as well as receiving configuration information from the BNG. A PON-fed Ethernet Access Node, as might be used in an MDU, can be a DSLAM or an Ethernet switch, and can also be a Layer 2 Control Point.

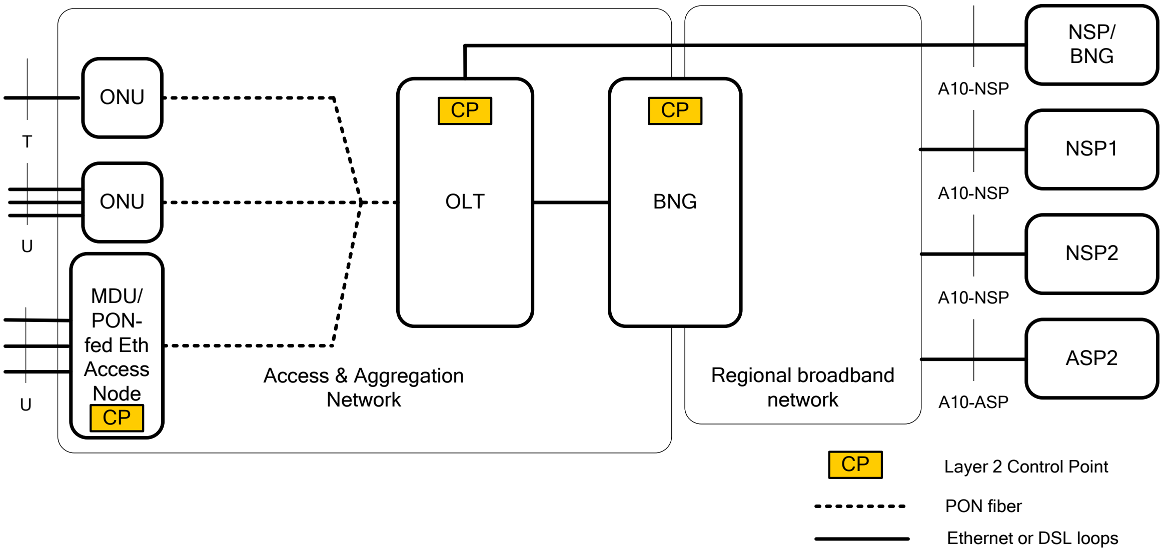

Figure 1 Overall architecture of Layer 2 Control applied to a PON network

5.1.2 L2C Deployment Options in PON networks

In a DSLAM, an access port is a physical DSL port. However, in an OLT device, an access port is shared by multiple ONUs, but bandwidth and QoS have to be allocated and managed between the OLT and the ONU on a per ONU basis. Therefore, an access port should be identified by an ONU. The OLT needs to report to the BNG the registration of each ONU and bandwidth it has allocated to it. This has implications for the partitioning model whereby multiple BNGs can control a single AN/OLT.

A PON-based access network may have different network architectures depending on the type of ONU, which will have an impact on the way L2C is used. Though a given PON port is normally attached to a single type of ONU, it is common for an OLT to have different types of ONUs attached (on different ports).

5.1.2.1 FITH with SFU ONUs

In this scenario, each ONU only serves one customer and so an integrated RG/ONU may be appropriate. The operators may not care about the status of integrated device's user facing ports, the T interface as it is an internal interface. The BNG and OLT establish a L2C adjacency, based on the principles defined in TR-147 [5]. Connections between each ONU and the OLT are taken as access ports, and use cases defined previously on DSL network should be adapted to apply to a PON network. All parameters on ONUs are preferred to be managed by OMCI to avoid impacting ONUs.

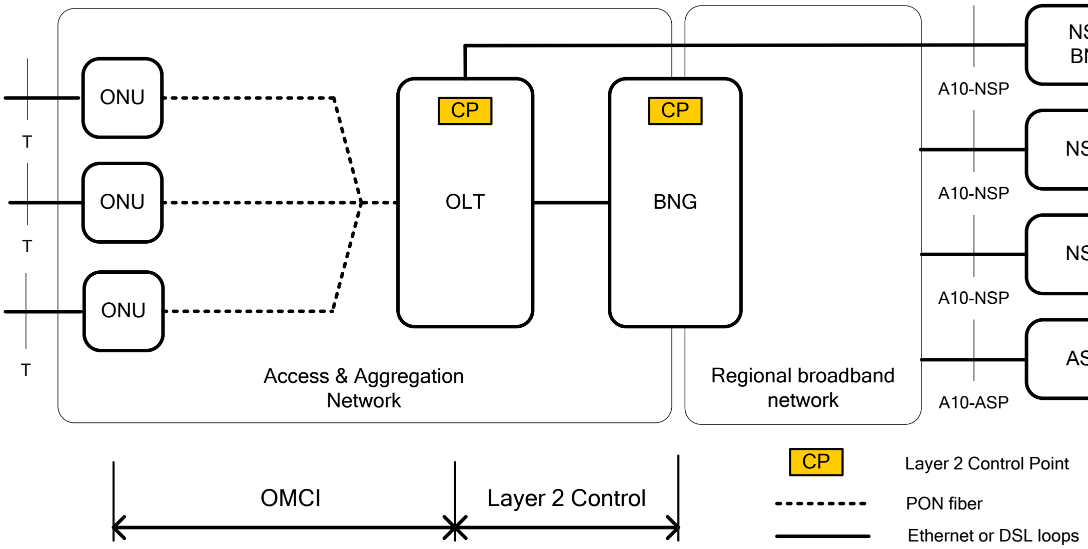

Figure 2 L2C Deployment Option for FITH

5.1.2.2 FTTH with mixed deployment of SFU and TR-156 MDU

In the case of FTTH with SFU or a TR-156 [6] MDU, each ONU may have one or more user ports, which are Ethernet or DSL and are typically connected to an RG. Each user port normally serves one customer. The U interface is between the ONU and RG. Status reporting and management of the U interface can be performed by the OLT by means of OMCI.

OMCI can report status change on an ONU by means of AVC (Attribute Value Change) notifications. When the ONU's DSL or Ethernet UNI's attributes changes, the related ME (Management Entity) will send an AVC notification to the OLT.

The OLT collates these notifications into a L2C report and which it sends to the BNG via its L2C session. As the L2C report contains information on both the ONU's UNI, and the OLT's PON port or ONU ID, the BNG can construct an accurate view of the topology.

When the BNG needs to send configuration information to an ONU's UNI, the OLT will terminate the L2C session, interpret the configuration parameters in the L2C messages and send them on to the ONU via OMCI.

In this case there is no need to change the ONU functionality, adding interworking support between L2C and OMCI is not a major undertaking on an OLT.

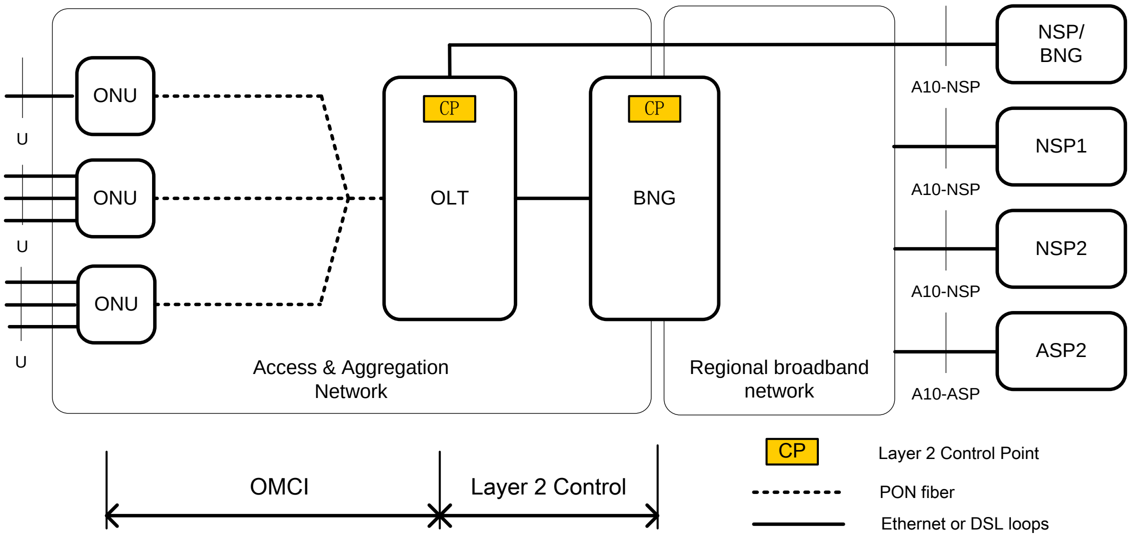

Figure 3 L2C Deployment with a TR-156 MDU

5.1.2.3 TR-167 MDU

In TR-167 [7], MDUs are served by PON-fed Ethernet Access Nodes as defined by TR-101, and managed by an EMS using SNMP. The OLT acts as an aggregation node for MDUs. However, there is one big difference between this case and that of Ethernet aggregation. Ethernet aggregation uses FE/GE/10GE ports, which have fixed bandwidth and few parameters to modify, as the aggregation switch and the Access Node are peers from the perspective of the Ethernet link between them. PON aggregation however uses PON ports, which have all the normal PON features, such as ONU ID, GEM Port, bandwidth management and QoS management. Further, the OLT and ONUs have a master-client relationship.

Before Ethernet packets can be transmitted over a PON link, the OLT and ONU must be synchronized with a registration process that is not required on a pure Ethernet link. For PON aggregation, the OLT has to be configured for each MDU’s PON uplink. This means the relationship between OLT and MDU must be managed.

There are two L2C deployment options:

Option 1 is to have separate L2C sessions between BNG and all its L2C adjacencies. This is simple, but considering the large number of MDUs that one BNG might manage, there is a scalability issue. Another problem with this option is that the BNG needs to correlate a given OLT and all the MDUs that it connects. This is necessary for CAC for example, as the controller has to be aware of the complete topology and bandwidth for any path. This would be a difficult job for a BNG, since the L2C sessions between the BNG and each OLT, and the OLT and each MDU have no automatic

© The Broadband Forum. All rights reserved

association. This could be done by manual configuration, but would have a significant impact on OPEX.

Option 2 is to correlate the L2C session between the BNG and OLT with all the L2C sessions between that OLT and its MDUs. Control messages sent to the OLT from BNG via L2C are translated by the OLT and sent on to its MDUs, again using L2C. L2C reports, e.g. Port Discovery of the MDU's access ports, are sent to the OLT via L2C. The OLT adds its PON port related information when necessary and sends it to the BNG via L2C. The BNG and MDU need no additional functionality with this option, but the OLT's function is more complex. However the advantage is that it provides complete topology information to BNG automatically, and makes management of the ONUs easier.

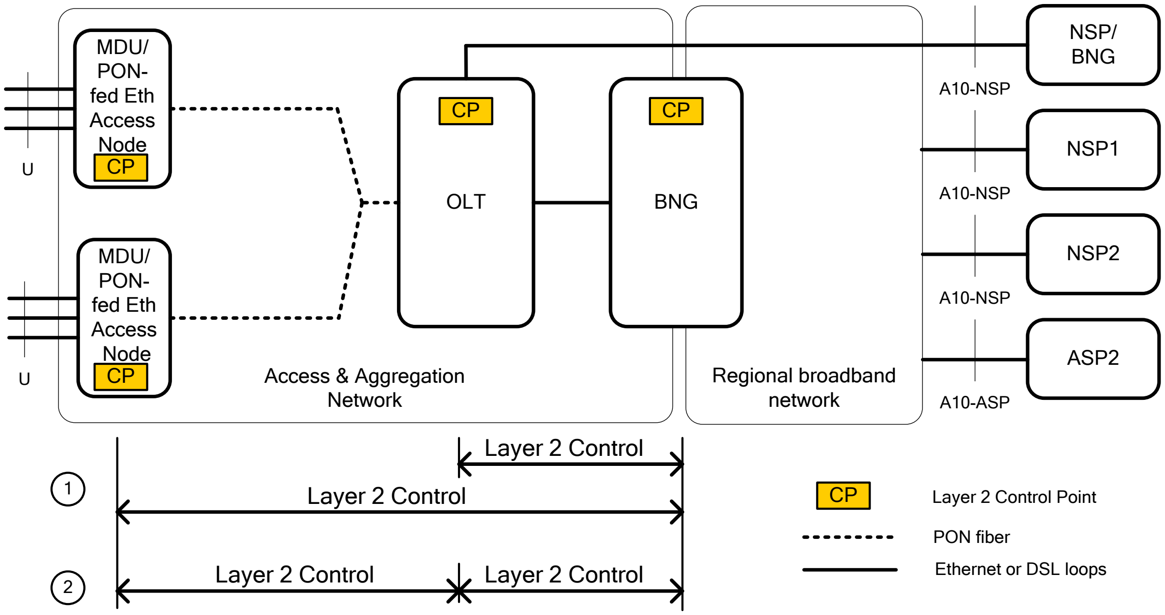

Figure 4 L2C Deployment Option with TR-167 MDU

5.2 Operation and Management

Since the mechanism introduced with Layer 2 Control in TR-147 also performs element management functions, there is need to define proper means to ensure the coexistence with the existing management system. Especially, when configuration changes are performed, there is the challenge of supporting multiple managers for the same network element at the same time.

Requirements on Operation and Network Management remain unchanged.
For details please refer to Section 8/TR-147.

5.3 Policy Management and AAA

Policy management framework TR-134 [3] defines in section 7.1.5.3 DSL based parameters between the PEP and the PDP via the R-Reference point. These parameters remain the same assuming DSL fed ONU. GPON related parameters referred to in section 6.1.2 and 6.1.3 of this document in conjunction with policy management requires GPON specific extensions which are left for further study. These parameters would also be sent over the B reference point to AAA server.

5.4 Multicast Architecture

At the time of writing GPON based multicast architecture is under finalization in IETF. Please see draft-ietf-ancp-pon [14] for further details.

5.5 Security Aspects

Security related description of section 5.6 and related requirements of section 9.7, TR-147 R-103 up to R-109 remain valid and must be applied to GPON based access technology as well.

5.6 Resilience

The principles of operation of a resilient architecture between BNG and AN described in Section 5.7/TR-147 also apply between BNG and OLT. The appropriate requirements are R-28 up to R-30 from TR-147.

6 Use Cases

This section describes new use cases grouped by “TR-147 Use cases for PON” and describe PON specific adaptation of existing DSL based use cases and their principles.. The detailed protocol specification of these use cases is beyond the scope of TR-207.

6.1 TR-147 Use cases for PON

6.1.1 Access Port Discovery in a Passive Optical Network

Access Port Discovery informs the BNG of the topology in an access network. In a Passive Optical Network, the OLT reports ONU’s status, e.g. online and offline. More detailed access network topology information may also be reported to the BNG using L2C. There are also some differences between discovery in DSL and PON networks, which are described in detail below.

6.1.1.1 FITH

6.1.1.1.1 Access Port Identification

One major difference between DSL and PON is the former has only one terminal device (CPE) on each physical port, while the latter has multiple terminal devices (ONUs) per physical port. In a DSLAM, an access port is identified by the physical DSL port. However, in an OLT, an access port cannot be identified by a physical PON port alone, as it is shared by multiple ONUs.

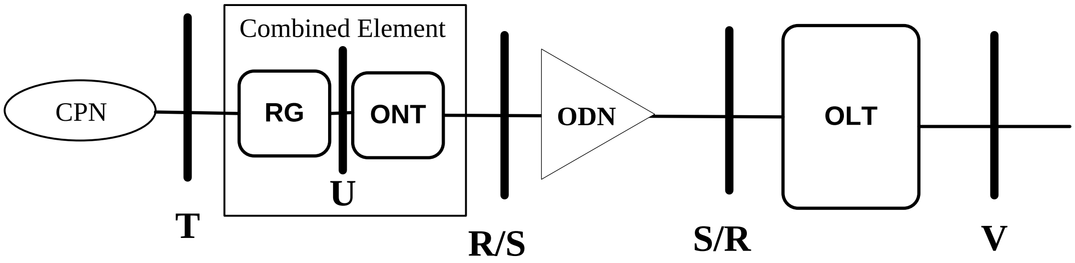

Figure 5 FITH deployment scenario

In the FITH case, each subscriber has one ONU that is integrated with an RG, therefore the U reference point in located inside the ONU. In order to identify the physical topology of each subscriber, an ONU ID is still necessary.

Each time an ONU goes online or offline, the OLT must send an Access Port Discovery Report to the BNG, containing the PON port as well as the ONU ID.

6.1.1.1.2 Data Rate of Access Port

In a DSL network, the actual data rate of a DSL port may change from synchronization event to synchronization event. The line rate can vary due to a change of environmental conditions or in the noise environment, and so the access node needs to send an Information Report to the BNG every time the Access Port Attributes change. However a PON port is fixed rate (e.g. 2.4 Gbit/s upstream, 2.4 Gbit/s downstream) and is not be influenced by environmental changes or noise. Further, the data rate of a PON port is shared between multiple ONUs, and actual bandwidth allocated to each ONU is managed dynamically by the OLT.

Therefore there is no need for an Information Report reflecting a physical data rate change of a PON port.

6.1.1.2 FTTH/TR-156 MDU

6.1.1.2.1 Access Port Identification

The difference between this case and FITH is that here the U reference point is not inside a physical box, but exposed and between the ONU and RG. One ONU may have multiple physical user side interfaces (UNIs) and provide network access for multiple subscribers. This means that in order to identify each subscriber the UNIs on the ONU need to be identified in addition to the ONU ID.

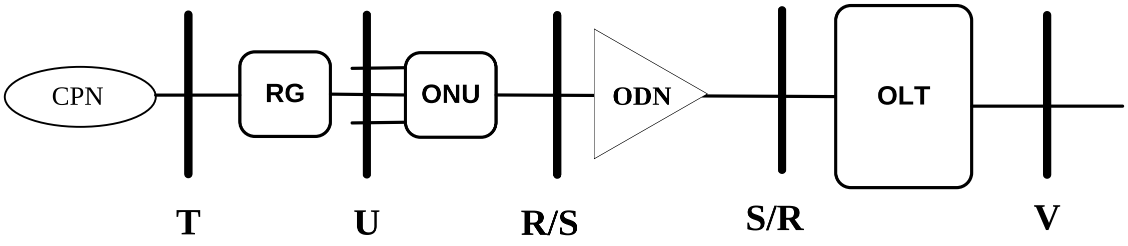

Figure 6 FTTH deployment scenario

There are two ways to send the status of ONU and its UNIs. One is to send each status independently; this provides the operator with complete information on each segment of access network. The other is to send a single message when both the ONU and UNI are activated. This is simpler, but the operator will not be aware of the status of the ONU if none of its UNIs are active.

6.1.1.2.2 Data Rate of Access Port

UNIs on an ONU could be 802.3Ethernet or xDSL interfaces. The line rate of the physical interface may vary, due to auto negotiation on the Ethernet interfaces, or the normal variability of the DSL interface. Therefore Information Reports reflecting the actual physical line rate are necessary.

6.1.1.3 Parameters to Be Reported

The ONU can provide physical information on its UNI through OMCI by means of the Management Entity Cardholder (Section 9.1.5/G.984.4 [8]). The Cardholder represents the fixed equipment slot configuration of the ONU and indicates the physical interface type of each UNI. When an ONU's UNI is activated, the OLT reports the actual rate of that UNI.
Any service profile applied on the ONU also needs to be reported to BNG. If the service profile is assigned on a pre-configured ONU which is inactive, the OLT should report the service parameters only when the ONU activates. If a service profile is assigned to an active ONU, the OLT should also report these updated service parameters to the BNG. The service parameters of an ONU include C-VLAN ID, S-VLAN ID, Line ID and bandwidth (Traffic Control).

Two categories of parameter must be supported in Port Status Report messages: device status parameters and service related parameters. These are:

Device topology and Status:

- ONU ID
- ONU Status
- PON port ID
- PON port bandwidth(to facilitate auto discovery)
- Physical interface type of UNI of ONU (Cardholder)
- Data rate of UNI of ONU

Service related parameters:

- C-VLAN ID
- S-VLAN ID
- Line ID of ONU
- Service bandwidth

6.1.1.4 Information flow

The following figure shows the access port discovery procedure using Layer 2 Control Messages.

- Each time the ONU goes online or offline, the OLT sends a Port Status Report Message to the BNG.
- In the case of FTTH/TR-156 MDU, each activation and deactivation of UNIs on an ONU triggers a Port Status message from the OLT to the BNG.
- In case of FTTH/TR-156 MDU, physical status change of each UNI on ONU triggers an Information Report message from OLT to BNG

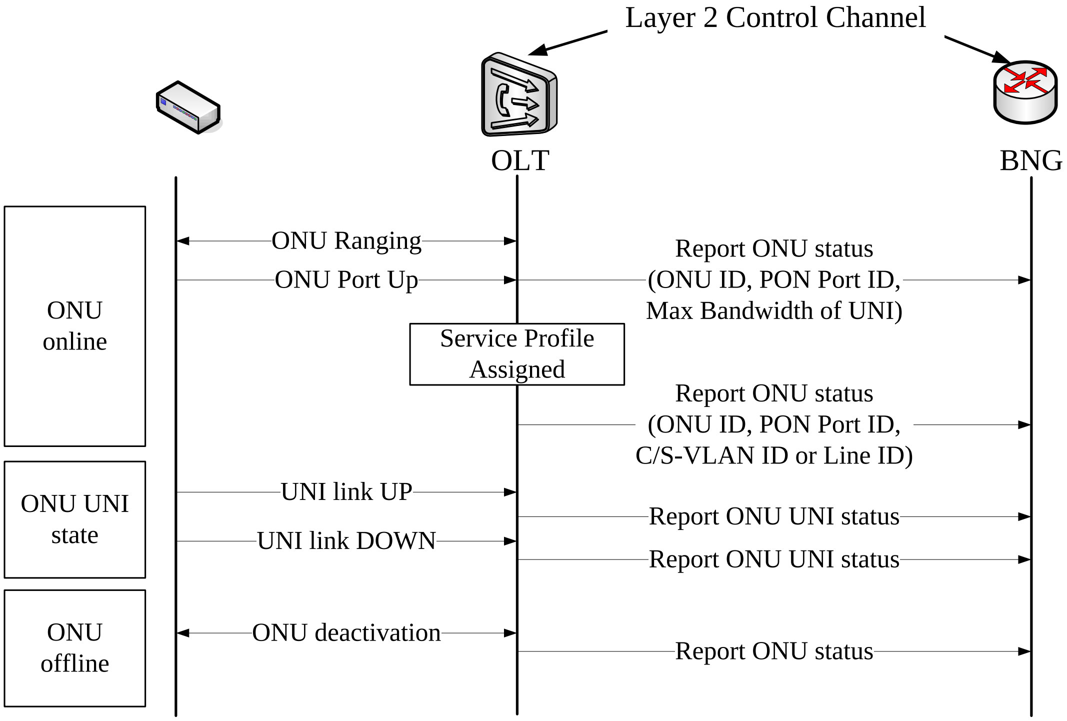

Figure 7 Access Port Discovery Information Flow

© The Broadband Forum. All rights reserved

6.1.2 Access Port Discovery in a PON network with L2C Relay Agent

The following figure depicts an example of two L2C sessions being correlated by the OLT in an MDU case. The flows in black are the L2C messages.
The gray flows are triggers for L2C reporting. Information on both MDU's DSL ports and OLT's PON ports need to be reported to the BNG. The OLT receives the MDU's information, adds its own, and then reports this to the BNG via L2C.

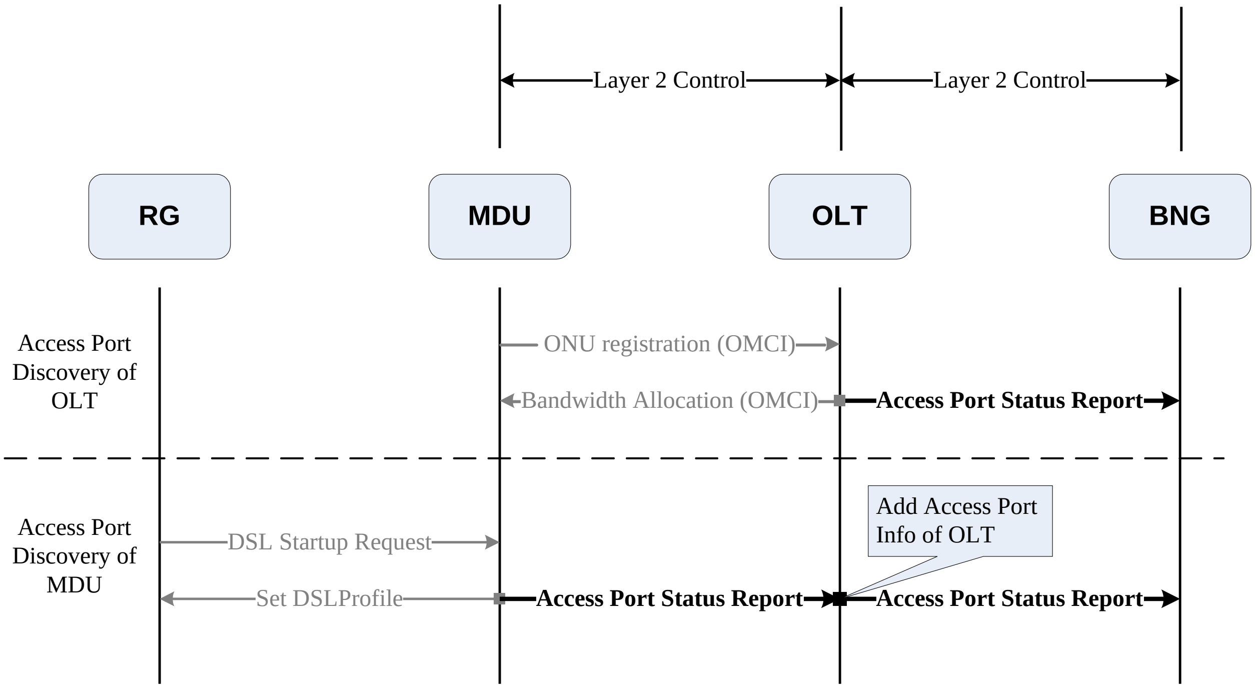
Layer 2 Control
Layer 2 Control
RG
MDU
OLT
BNG
Access Port Discovery of OLT
ONU registration (OMCI)
Bandwidth Allocation (OMCI)
Access Port Status Report
Access Port Discovery of MDU
Add Access Port Info of OLT
DSL Startup Request
Set DSLProfile
Access Port Status Report
Access Port Status Report

Figure 8 Access Port Discovery Flow with Relay Agent

6.1.3 Access Port Configuration in a Passive Optical Network

As described in Section 6.1.1, Access Port Discovery reports access port identification to the BNG when sending an Access Port Discovery message. This informs the BNG of the identity of a PON port on an Access Node. Based on the Access Port Identification and the customer identification, service related parameters can be configured on an OLT and an ONU.

Sending L2C Port Configuration messages from the BNG can be triggered by a management system or by customer identification and authentication after Access Port Discovery. It may be used for first time configuration (zero touch) or updating/upgrading a customer's profile (C-VLAN ID, S-VLAN ID), and service bandwidth.

Parameters of a UNI on an ONU can also be configured via L2C. When the ONU supports L2C, the parameters of the UNI are simply sent to the ONU via L2C. If the ONU does not support L2C, but only OMCI, the parameters have to be sent from the BNG to the OLT via L2C, and the OLT translates the configuration information into OMCI, and sends it to the ONU.

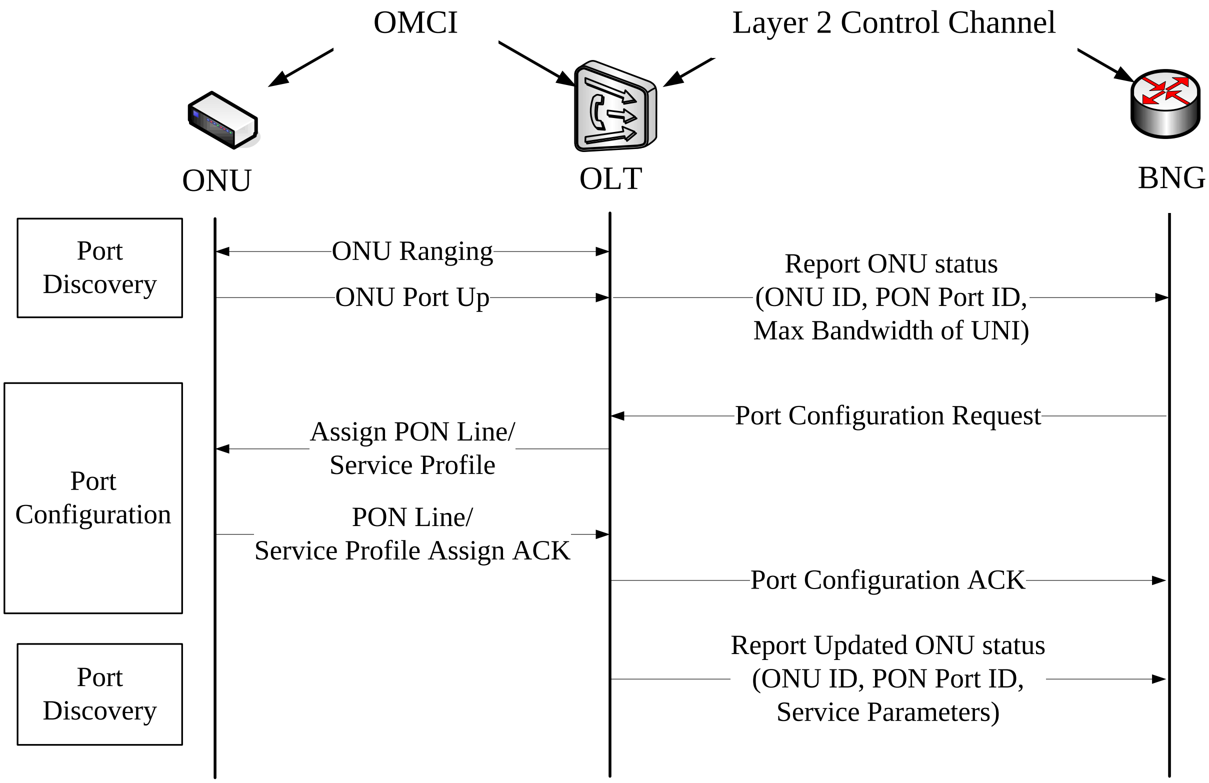
OMCI
Layer 2 Control Channel
ONU
OLT
BNG
Port Discovery
ONU Ranging
ONU Port Up
Report ONU status (ONU ID, PON Port ID, Max Bandwidth of UNI)
Port Configuration
Port Configuration Request
Assign PON Line/ Service Profile
PON Line/ Service Profile Assign ACK
Port Configuration ACK
Port Discovery
Report Updated ONU status (ONU ID, PON Port ID, Service Parameters)

Figure 9 Access Port Configuration Information Flow

6.2 Wholesale and retail access

6.2.1 Overview and Motivation

There are various standards development organisations producing specifications for wholesale services. Among wholesale models, Active Line Access (ALA) wholesale requires communication and control between devices in a wholesale operator’s network, and those in a retail service provider’s. L2C is an efficient mechanism for such a purpose.

Below is a typical wholesale access scenario:

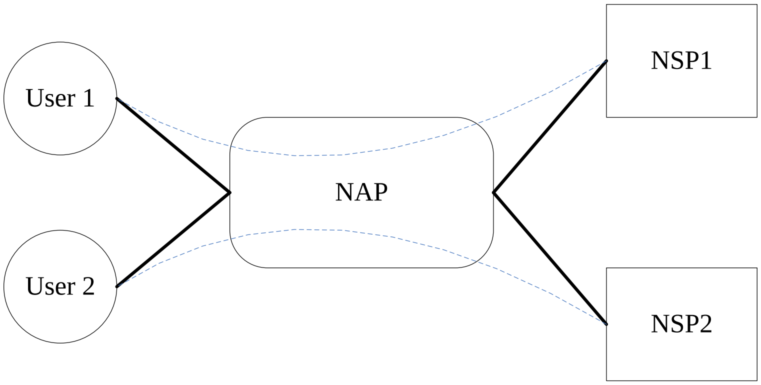

Figure 10 Active Line Access Wholesale Scenario

User1 is a subscriber of NSP1. User2 is a subscriber of NSP2. User1 and user2 connect to NSP1 and NSP2 respectively via NAP (wholesale network provider). Layer 2 control mechanisms can be used to coordinate between the NAP and NSP to enable the former to deploy value-added services.

6.2.2 Control Interaction

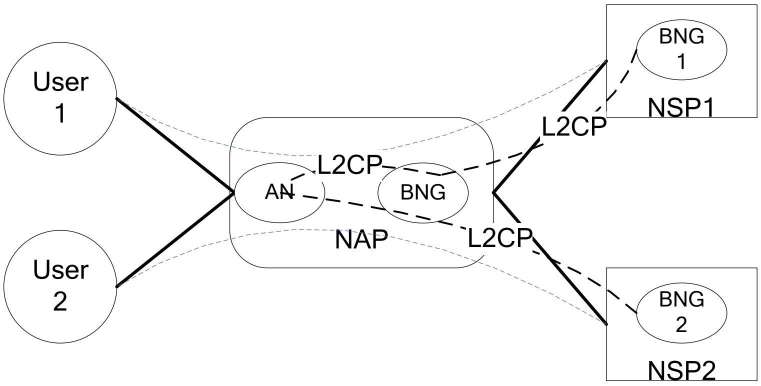

Figure 11 L2C for Wholesale Service Reference Model

An Access Node in the NAP's network provides active line access to subscribers of both NSP1 and NSP2. The Access Node needs to interact with BNGs in both the NSPs' networks. The AN, BNG1, BNG2 are all L2C control points.

L2C sessions between the Access Node and BNGs in the NSPs' networks could be either a single hop or a relayed one. In the above figure, the L2C session between the Access Node and BNG2 is setup directly between them; the BNG in the NAP's network is not aware of this L2C session. In contrast, the L2C session between the Access Node and BNG1 is relayed by the BNG in NAP's network. Such a relay function could be implemented but has not been standardized.

6.3 Unified Unicast and Multicast Resource Control

6.3.1 Overview and motivation

Layer 2 Control can be used in the Policy Framework defined in TR-134 to coordinate resources between the Access Node and BNG using the L-reference point.

There are two resource control models. In the first model, the BNG may perform resource control without any bandwidth delegation to the Access Node; in this case, multicast and unicast CAC are both performed by the BNG with optional interaction with a policy Server. The AN will replicate multicast flows as instructed by the BNG. In the second model, the BNG may perform resource control with bandwidth delegation to the Access Node, with multicast CAC being performed on the AN, and unicast CAC on the BNG and/or policy server.

In the bandwidth delegation scenario, dedicated resources are pre-provisioned to unicast and multicast services respectively in a specific network segment. Thresholds of aggregate resources are adjustable, based on network policy and resource status. For multicast services, the AN performs multicast resource admission control based on the available resource within a pre-provisioned allocation. For unicast services, the BNG performs resource admission control based on available resource within another pre-provisioned allocation. When the allocated resources reach a configured threshold in the AN, either the policy server can authorize the BNG to adjust the AN's allocation, or the AN can request an increased allocation from the BNG. If the allocation is not increased, then further admission requests may be denied.

6.3.2 Control interactions

The typical interaction between the unified unicast and multicast resource control is as follows. Firstly the BNG specifies the AN's resource management mode using an L2C provisioning message. In adjustable mode, the following interaction is possible. When the BNG's unicast allocation is insufficient, the BNG may trigger a bandwidth reallocation procedure. When the AN's resource available for multicast services is insufficient, AN can attempt to request more by triggering the bandwidth reallocation procedure.

In fully shared mode, the AN must report the currently used amount of multicast bandwidth to the BNG, so as to make the BNG aware of the AN's resource usage. Finalization of detailed message flow and ANCP protocol extensions supporting that use case are currently subject of work of ANCP WG. For further details please see draft-ietf-ancp-mc-extensions [15].

6.3.3 Information flow

This section describes exemplary message flows in the adjustable resource scenario derived from draft-ietf-ancp-mc-extensions.

As soon as the AN's port comes up, the AN sends an ANCP PORT_UP message to the BNG specifying the Access Loop Circuit ID. The BNG replies with an ANCP PORT_MNGT message. The PORT_MNGT message includes a flag indicating the ratio between multicast and unicast resource is adjustable, and the amount of delegated multicast bandwidth for each access line.

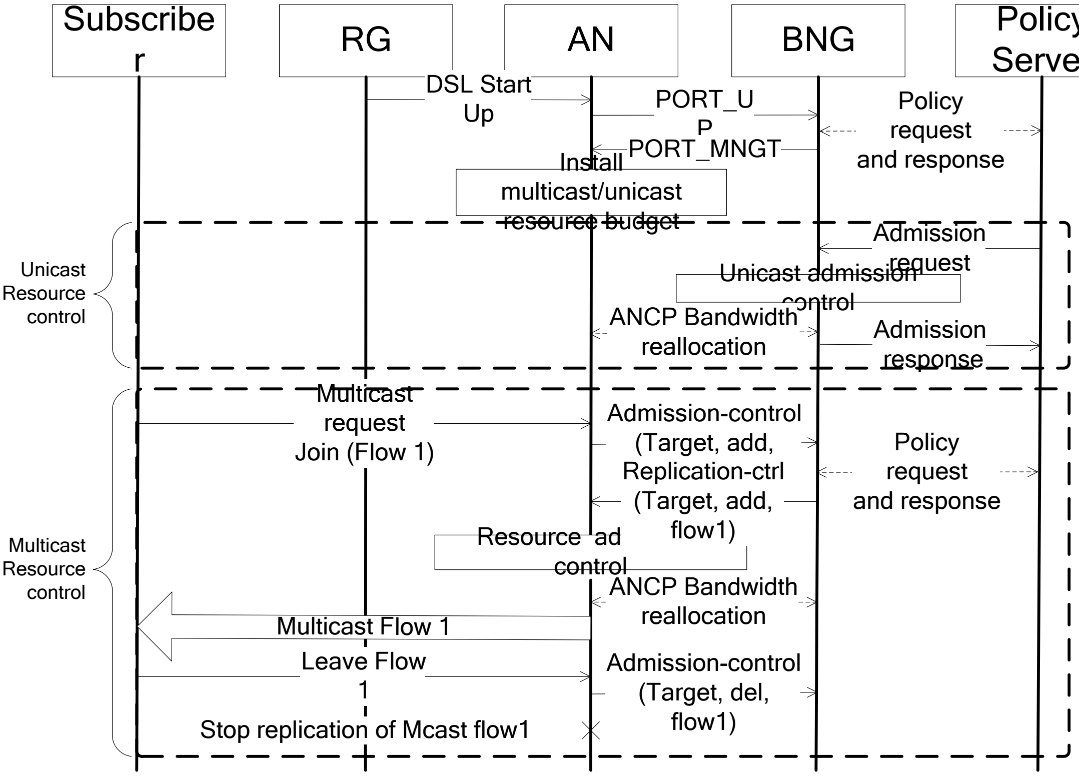
Subscribe r
RG
AN
BNG
Policy Server
DSL Start Up
PORT_U P
PORT_MNGT
Policy request and response
Install multicast/unicast resource budget
Unicast Resource control
Admission request
Unicast admission control
ANCP Bandwidth reallocation
Admission response
Multicast Resource control
Multicast request Join (Flow 1)
Admission-control (Target, add, Replication-ctrl (Target, add, flow1)
Policy request and response
Resource ad control
ANCP Bandwidth reallocation
Multicast Flow 1
Leave Flow 1
Admission-control (Target, del, flow1)
Stop replication of Mcast flow1

Figure 12 Information Flow of Unified Resource Control

The bandwidth reallocation interaction in unicast resource control only happens when the BNG's available bandwidth for unicast is insufficient. The BNG will trigger an adjustment to the amount of that access line's delegated unicast/multicast bandwidth, subject to agreement by the policy server.

The bandwidth reallocation interaction in multicast resource control appears only when AN's current available bandwidth for multicast is insufficient, the AN will trigger an adjustment for the amount of access line's delegated unicast/multicast bandwidth.

6.4 PON based and Ethernet based Remote OAM procedures for PON

OAM use case of Section 6.3/TR-147 and Section 7.2.3/TR-147 for PON scenarios using DSL-fed ONU in case of FTTC/B still apply. OAM for native PON in case of FTTH is left for further study.

© The Broadband Forum. All rights reserved

6.5 Network Security Countermeasures

6.5.1 Overview and Motivation

Traditionally, network attacks by users are detected at the BNG and may involve additional functions such as DPI. Types of attack include denial of service (SYN flood, fraggle, smurf, etc.), scanning and snooping attacks (address scanning, port scanning, tracert, etc.), malformed packet attacks (ping of death, teardrop, etc.), control message flood towards BNG (PPP/DHCP protocol control message, etc.). The BNG is the device that blocks any attack traffic, and so such upstream flows traffic will be transmitted from the AN to the BNG without any limitation or control. This centralized mode normally requires the BNG to have high performance hardware, since widespread attacks may be launched (knowingly or unknowingly) by a large number of subscribers at the same time.

Access Nodes frequently have some functions (such as ACLs, MAC address filtering) which could be used to prevent attacking traffic being forwarded to the BNG. These functions can be configured through CLI or NMS, but typically without any interaction with other network elements. In order to perform dynamic filtering of attacking packets, the BNG can use L2C to configure filtering tables in the Access Node, and so perform packet filtering or rate limiting on malicious packets thereby reducing the load on the BNG.

6.5.1.1 Control Message Countermeasures

Some attacks use large numbers of control messages to the BNG, such as PPP/DHCP discover messages.

The BNG sends suspected attacking messages to its internal control plane for analysis. The traffic management mechanism in the control plane will determine if this is an attacking event. After an attack is detected, the BNG could find the attacker’s location by information in the attacking message, such as option 82 which is attached by the Access Node. The BNG can then set up packet filters on specific AN interfaces.

6.5.1.2 Anti DOS-attack

TCP SYN attacks are used to attack application servers. Currently, it can be detected by an internal BNG function or a dedicated DPI box. Then the BNG will implement the anti-attack policy itself, but again this centralized processing places a heavy burden to the BNG.

The BNG could use L2C to mitigate the processing stress of massively concurrent SYN flood attacks. When the BNG detects such an attack and has identified the related access circuit, it can instruct the Access Node to filter or rate limit packets on the basis of layer 2 information, e.g. MAC address. The layer 3 and upper layer policies will still be implemented on the BNG.

6.5.2 Control Interactions

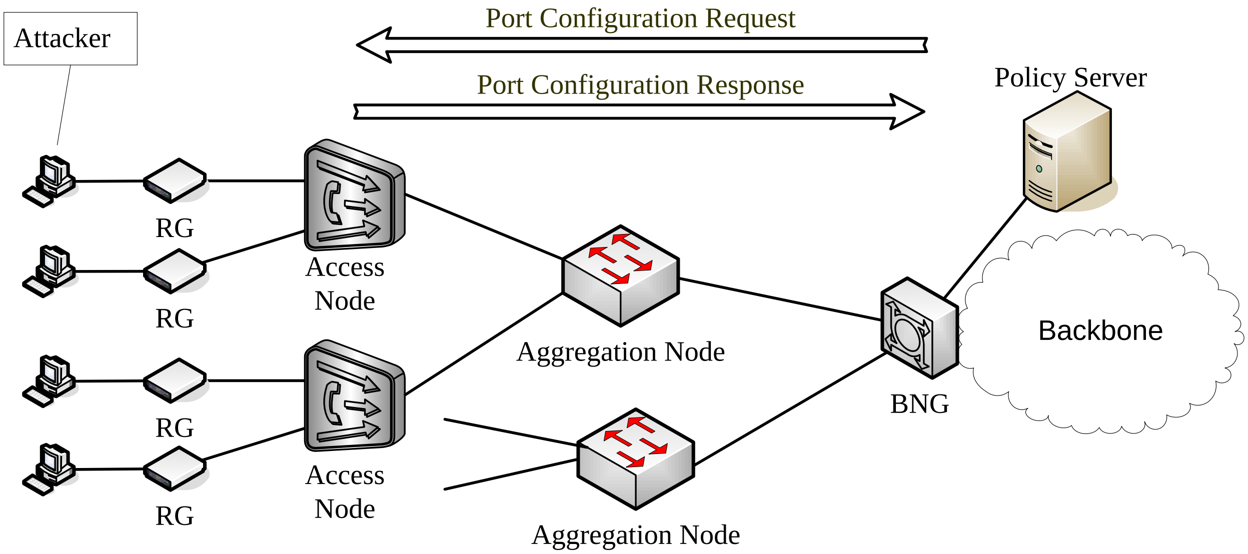

Figure 13 Network Anti-Attack Interaction

In this use case, BNG uses Port Configuration Request message to configure filter settings on the Access Node. The filtering parameters may include specific MAC addresses, limiting the number of source MAC addresses, rate limiting and ACLs. The Access Node sends a Port Configuration Response message back to the BNG.

6.5.3 Information Flow

The following figure gives an example of this procedure. Parameters configured on the Access Node should be valid for a certain time, so service is not permanently disabled. The time of validity could be set along with the anti-attack policy. Otherwise, the BNG should remove the policy configuration via a Port Configuration message.

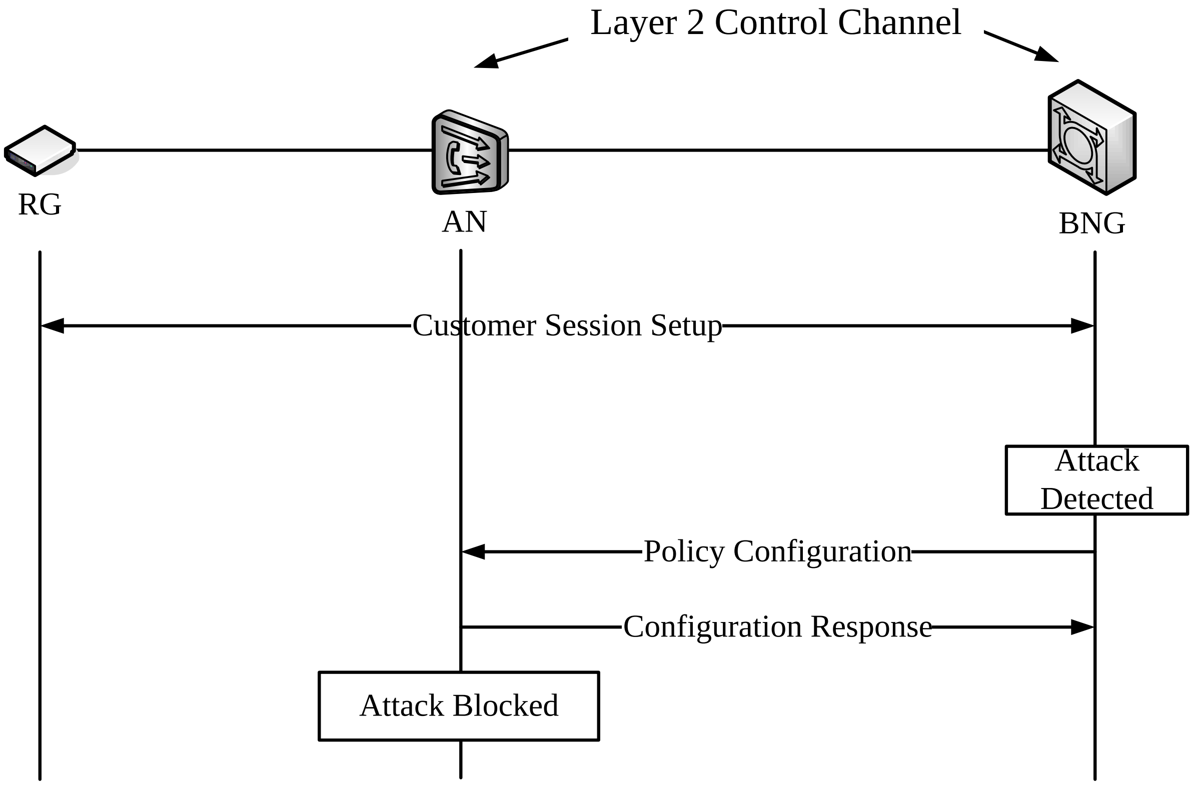

Figure 14 Network Anti-Attack Information Flow

6.6 Multicast Accounting Use Case

6.6.1 Overview and motivation

According to RFC 5851 [12](*Framework and Requirements for an Access Node Control Mechanism in Broadband Multi-Service Networks*), It may be desirable to perform time and/or volume-based accounting for certain multicast flows sent on particular Access Ports. In the case where the AN is performing the traffic replication process, only it knows when replication of a multicast flow to a particular Access Port or user start and stops.

6.6.2 Specific TLVs for replicating start/end time and volume are needed; the Control Interaction

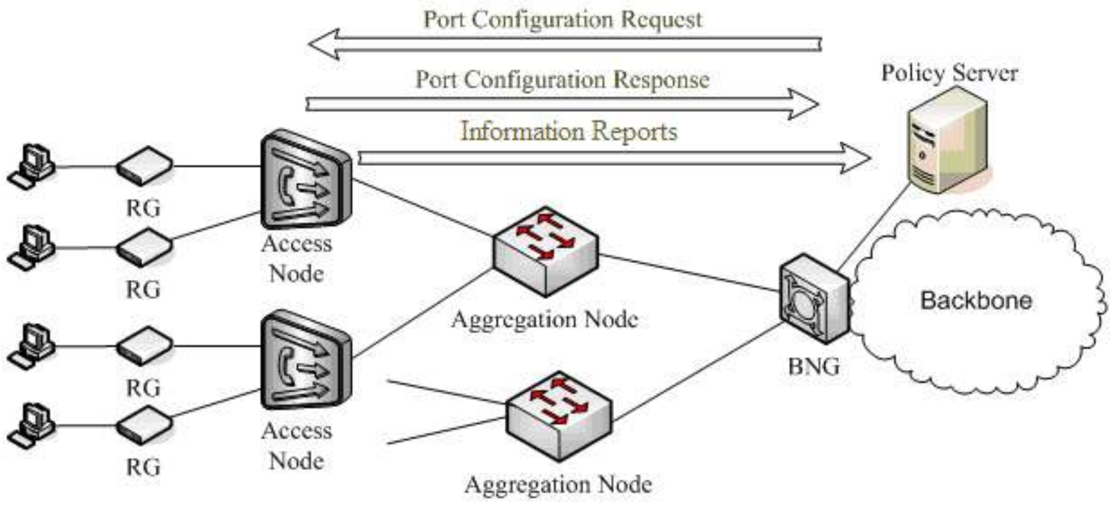

Figure 15 Multicast Accounting Interaction

In this use case, the BNG uses a Port Configuration Request message to inform the AN about the type of accounting needed for a given multicast flow on a particular Access Port for a particular subscriber's MAC address. Types include: no accounting, basic accounting (based on replicating start and end times) and detailed accounting (based on replicating start and end times together with volume information). The AN will send a Port Configuration Response to the BNG to accept or reject the request (based on the AN's capability). If the request is accepted by the AN, the AN will send accounting information (within the Information Reports message) to the BNG when the specified subscriber joins or leave a multicast group, and may send information periodically while multicast replication is active.

This multicast accounting procedure is applicable to both BNG initiated multicast replication and conditional access and admission control based replication.

© The Broadband Forum. All rights reserved

6.6.3 Information Flow

The following figure gives an example of this procedure. When the BNG receives the information report message, it finds the appropriate subscriber and sends the accounting information to the AAA server, either separately, or within the normal accounting messages.

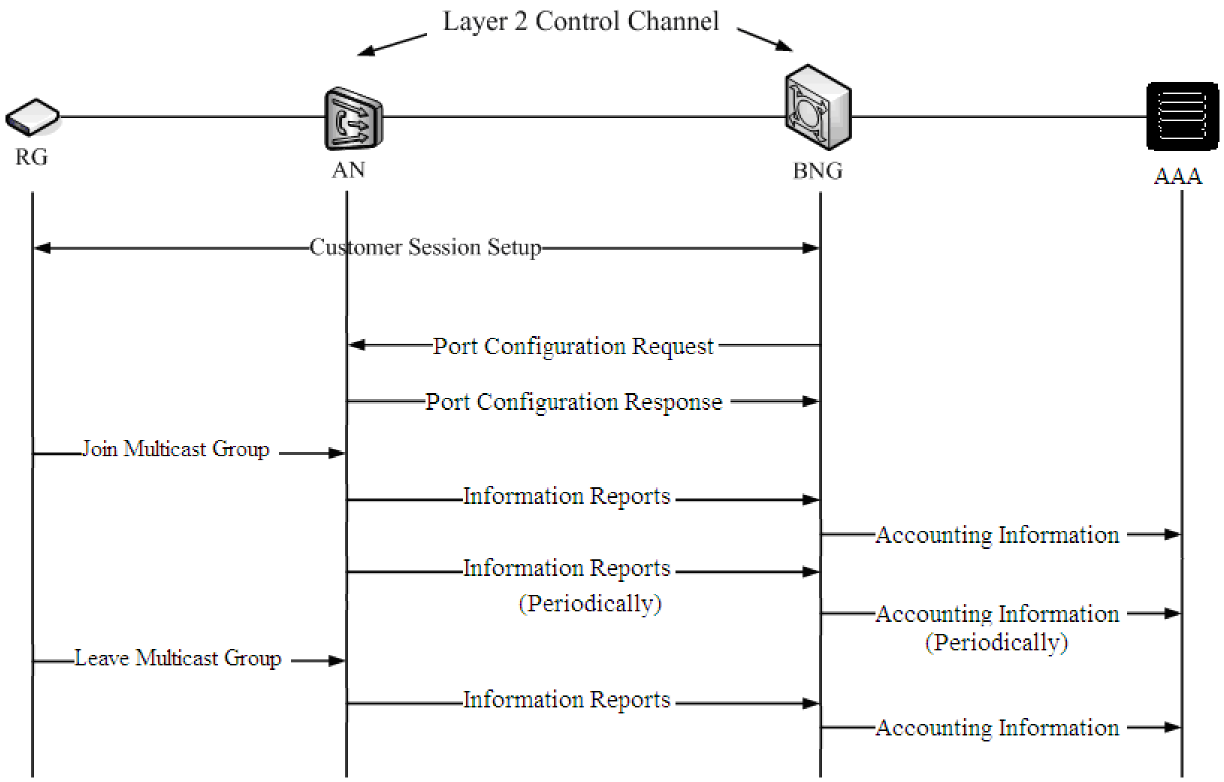

Figure 16 Multicast Accounting Information Flow

7 General Requirements

7.1 High-Level Protocol Requirements

R-01 There MUST be information elements containing multicast replication start/end times and volumes with the information reports message for multicast accounting.

7.2 Access Node Requirements

7.2.1 General Requirements

R-02 The Access Node MUST send a Port Configuration Response to the BNG accepting or rejecting a multicast accounting request.

R-03 The Access Node SHOULD be able to collect accounting information (multicast replication start and end times, and volume information) according to the Port Configuration Request for multicast accounting sent from a BNG.

R-04 The Access Node SHOULD be able to send Information Reports to the BNG, containing accounting information according to the multicast accounting type within the Port Configuration Request.

R-05 The OLT MUST support a L2C partition that includes ONUs across an arbitrary group of OLT PON ports.

R-06 The GPON-fed Access Node MUST support L2C partitioning.

R-07 The Access Node SHOULD support configuration of the maximum number of source MAC addresses allowed to be learned on a specific access port, via L2C.

7.2.2 Requirements for FITH/FTTH/TR-156 MDU

R-08 Each time an ONU/ONT gets activated or de-activated, the OLT MUST send the BNG a Port Status Report message containing the parameters related to device topology and status as defined in Section 6.1.1.3. (Activated means registered successfully and ranging).AAE

R-09 The OLT MUST be able to send layer 1 parameters of an ONU's xDSL UNI in a Port Status Report message, as defined in Section 7.2.1/TR-147 .

R-10 The OLT MUST report the port status of an active ONU's xDSL UNI when its status changes according to R-60, R-61 and R-62 in TR-147.

R-11 The OLT MUST insert the PON port ID ONU ID in a Port Status Report message, when reporting status of an ONU's xDSL UNI.

R-12 The OLT MUST be able to report an ONU's service parameters in a Port Status Report message as defined in Section 6.1.1.3.

R-13 The OLT MUST report any changes to an ONU's service parameters in a Port Status Report message

R-14 The OLT MUST be able to configure the layer 1 parameters of an ONU's xDSL UNI received in a Port Configuration message.

R-15 The OLT MUST be able to report access line status changes on the ONU to the BNG via L2C. .

R-16 The OLT MUST be able to receive L2C Port Configuration Requests from the BNG and configure the corresponding ONU.

R-17 When acting as a L2C relay agent, the OLT MUST be able to receive L2C reports from its ONU/MDUs and send them to BNG after adding its own information.

R-18 When acting as a L2C relay agent, the OLT MUST be able to receive L2C Port Configuration Requests from the BNG and send them to the corresponding ONU/MDU after decomposition.

7.3 BNG Requirements

R-19 The BNG MUST be able to configure ACL and filtering tables on an AN for network anti-attack purposes when it detects network attacks from users.

R-20 The BNG MUST be able to configure layer 1 parameters of an ONU's xDSL UNI via a Port Configuration message.

R-21 The BNG MUST be able to send a Port Configuration Request to the AN to indicate the accounting type for certain multicast flows sent on particular Access Ports for particular subscriber.

R-22 The BNG MUST be able to send the multicast accounting information to a AAA server for particular subscribers.

R-23 The BNG SHOULD support sending L2C message to the Access Node, specifying the maximum number of source MAC addresses allowed to be learned on a specific access port on the Access Node.

7.4 Management Requirements

For management related requirements Section 9.6/TR-147 still apply.

7.5 Security Related Requirements

For security related requirements Section 9.7/TR-147 still apply.

End of Broadband Forum Technical Report TR-207