TECHNICAL REPORT

TR-147

Layer 2 Control Mechanism For Broadband Multi-Service Architectures

Issue: 1
Issue Date: December 2008

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 DOCUMENTATION 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	Issue Date	Issue Editor	Changes
1	December 2008	Norbert Voigt, Nokia Siemens Networks Sven Ooghe, Alcatel-Lucent	Original

Technical comments or questions about this Broadband Forum Technical Report should be directed to:

Editors:	Norbert Voigt	Nokia Siemens Networks	norbert.voigt@nsn.com
	Sven Ooghe	Alcatel-Lucent	sven.ooghe@alcatel-lucent.be
	Michel Platnic	ECI Telecom	michel.platnic@ecitele.com
A&T WG Chairs:	David Allan	Nortel	dallan@nortel.com
	David Thorne	BT	david.j.thorne@bt.com

Table of Contents

List of Figures

List of Tables

Summary

When deploying value-added services across broadband access networks, special attention regarding Quality of Service and service control is required. This implies a tighter coordination between network nodes, notably Access Nodes (e.g. a Digital Subscriber Line Access Multiplexer (DSLAM)) and Broadband Network Gateways.

Coordination between these network nodes could be performed by means of interworking via the management plane. However, this is not always possible because of the organizational boundaries between business entities operating the local loop, the aggregation network and the IP network. Further, management networks are usually not designed to transmit management data between the different entities in real time.

Therefore, there is a need for a Layer 2 Control Mechanism that runs directly between a BNG and an Access Node, in order to perform QoS-related, service-related and subscriber-related operations. The Layer 2 Control Mechanism means that the transmission of the information does not need to go through distinct element managers but rather can use direct device-device communication. This allows access link related operations to be performed within those network elements, while avoiding any impact on the existing management systems.

This Technical Report provides a framework for the Layer 2 Control Mechanism and identifies a number of use cases for which this mechanism may be appropriate. It then presents the requirements for the Layer 2 Control Mechanism and the network elements that need to support it.

1 Purpose and Scope

1.1 Purpose

The purpose of this Technical Report is to define 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.

The Layer 2 Control Mechanism ensures the transmission of the information does not need to go through distinct element managers but rather can use direct device-device communication. This allows access link related operations to be performed within those network elements, while avoiding any impact on the existing management systems.

NOTE – This Technical Report refers to a BRAS and a BNG as defined in TR-101. From this point onward this document uses the term BNG to refer to both unless explicitly stated otherwise.

1.2 Scope

The scope of this Technical Report comprises the concept of a Layer 2 Control Mechanism between a BNG and an Access Node (e.g. VDSL Remote Access Node, Central Office DSLAM) and its applicability to multi-service architectures including those defined in TR-059 and TR-101.

Use of this mechanism between network elements other than the BNG and Access Node is not excluded, but is beyond the scope of this document.

This Technical Report defines the network element requirements and describes information flows for the following use cases:

- Reporting the characteristics of the access links and/or general Access Node capabilities to a BNG that uses this information for QoS purposes;
- Configuration of service parameters on selected access ports. This may include physical layer service parameters (e.g. DSL maximum net data rate) or network layer service parameters (e.g. 802.1p scheduling configuration on the access link);
- Triggering a point-to-point OAM mechanism on selected access links. This may include ATM OAM in the case of ATM-Ethernet interworking (cf. TR-101), or Ethernet OAM in the case of an end-to-end Ethernet network;
- Communicating multicast related information between a BNG and an Access Node in order to configure, for example, multicast Access Control Lists.

The framework defined by this Technical Report is targeted at DSL-based access (either by means of ATM/DSL or Ethernet/DSL). The principles of this framework are applicable to non-DSL technologies, like PON, FTTx and WiMAX. However the actual technical details of such an application are not addressed in this Technical Report.

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 when used in this sense.

MUST This word, or the adjective "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 adjective "RECOMMENDED", means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications must be understood and carefully weighted before choosing a different course.

MAY This word, or the adjective "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 the currently valid Broadband Forum Technical Reports is published at www.broadband-forum.org.

[1] TR-059: *DSL Evolution - Architecture Requirements for the Support of QoS-Enabled IP Services*, Broadband Forum 2003

[2] TR-101: *Migration to Ethernet-Based DSL Aggregation*, Broadband Forum 2006

[3] TR-058: *Multi-Service Architecture & Framework Requirements*, Broadband Forum 2003

[4] TR-068: *Base Requirements for an ADSL Modem with Routing*, Broadband Forum 2006

[5] TR-144: *Broadband Multi-Service Architecture & Framework Requirements*, Broadband Forum 2007

[6] ITU-T I.361: *B-ISDN ATM layer specification* (02/99)

[7] ITU-T I.610: *B-ISDN Operation and Maintenance Principles and Functions* (02/99)

[8] ITU-T G.997.1: *Physical Layer Management for Digital Subscriber Line (DSL) Transceivers* (06/99)

[9] ITU-T G.993.2: *Very high speed digital subscriber line transceivers 2 (VDSL2)* (02/06)

[10] IEEE 802.1D: *Media Access Control (MAC) Bridges* (06/04)

[11] IEEE 802.1ag: *Connectivity Fault Management* (04/08)

[12] IEEE 802.1p: *Traffic Class Expediting and Dynamic Multicast Filtering* (09/95); incorporated into 802.1D

[13] IETF RFC 894: *Transmission of IP Datagrams over Ethernet* (04/84)

[14] IETF RFC 894: *Multiprotocol Encapsulation over ATM Adaptation Layer 5* (09/99)

2.3 Definitions

This Technical Report uses the terms defined in TR-101, e.g. Access Node and BNG.

Access Node	The Access Node may implement the ATU-C function (DSL signal termination), may physically aggregate other ATM or Ethernet nodes implementing ATU-C functionality, or may perform both functions at the same time. This can be CO based or non-CO based equipment. In the scope of this specification, this node contains at least one standard Ethernet interface that serves as its uplink interface into which it aggregates traffic from several ATM-based (user ports) or Ethernet-based southbound interfaces.
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.
BNG	IP Edge Router where bandwidth and QoS policies may be applied, to support multi-service delivery.

Further, it uses the following terms:

Actual Data Rate	Within this Technical Report the term is used as defined by ITU-T G.997.1. This parameter reports the actual net data rate the bearer channel is operating at excluding the rate in L1 and L2 states.
Net Data Rate	Within this Technical Report the term is used as defined by ITU-T G.993.2, cf. Table 5-1 and Figure K-10. It is the portion of the total data rate that can be used to transmit ATM cells or Ethernet frames. It excludes the overhead related to the physical media (e.g. trellis coding). It includes TPS-TC (Transport Protocol Specific - Transmission Convergence)

	encapsulation; this is zero for ATM encapsulation, and non-zero for 64/65 encapsulation.
Line Rate	Within this Technical Report the term is used as defined by ITU-T G.993.2, cf. Table 5-1 and Figure K-10. It contains the complete overhead including RS and trellis coding.
L2C	Layer 2 Control Mechanism
Layer 2 Control Mechanism	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.
Layer 2 Control Channel	A bidirectional IP communication interface between the L2C controller function (in the BNG) and L2C reporting/enforcement function (in the Access Node).
Layer 2 Control Adjacency	The relationship between an Access Node and a BNG for the purpose 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.
Control Protocol	The protocol that is used to implement the Layer 2 Control Mechanism

2.4 Abbreviations

This Technical Report defines the following abbreviations:

AAA	Authentication, Authorization and Accounting
ACI	Access Circuit Identifier
ACL	Access Control List
ADSL	Asymmetric Digital Subscriber Line
AN	Access Node
ASP	Application Service Provider
ATM	Asynchronous Transfer Mode
ATU-C	ADSL Transceiver Unit Central Office
BNG	Broadband Network Gateway
BPON	broadband Passive Optical Network
BRAS	Broadband Remote Access Server

CLP	Cell Loss Priority
CO	Central Office
COPS	Common Open Policy Service
C-VID	Customer VLAN ID
DHCP	Dynamic Host Configuration Protocol
DSCP	Differentiated Services Code Point
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
EMS	Element Management System
FTTx	Fiber-To-The-X
IGMP	Internet Group Management Protocol
IPSec	Internet Protocol Security
IPTV	Internet Protocol Television
L2C	Layer 2 Control
L2TP	Layer 2 Tunneling Protocol
LAC	L2TP Access Concentrator
LNS	L2TP Network Server
NSP	Network Service Provider
OAM	Operation, Administration and Maintenance
OLT	Optical Line Termination
OPEX	Operational Expenditure
PON	Passive Optical Network
PPP	Point-to-Point Protocol
PPPoE	Point-to-Point Protocol over Ethernet
PVC	Permanent Virtual Circuit
QoS	Quality of service
RADIUS	Remote Authentication Dial In User Service
RAN	Remote Access Node
RG	Residential Gateway
RSTP	Rapid Spanning Tree Protocol
SDSL	Symmetric Digital Subscriber Line
SHDSL	Single-Pair High-speed Digital Subscriber Line
SNMP	Simple Network Management Protocol
SSM	Source Specific Multicast
S-VID	Service VLAN ID
TCP	Transmission Control Protocol

UDP	User Datagram Protocol
VBRrt	Variable Bit Rate Real Time
VC	Virtual Circuit
VCC	Virtual Circuit Connection
VDSL2	Very High Speed Digital Subscriber Line 2
VID	VLAN ID
VLAN	Virtual LAN
VoIP	Voice over IP
VP	Virtual Path
VPC	Virtual Path Connection
VSA	Vendor Specific Attribute
WiMAX	Worldwide Interoperability for Microwave Access

3 Technical Report Impact

3.1 Energy Efficiency

TR-147 has no impact on Energy Efficiency.

3.2 IPv6

TR-147 has no impact on IPv6.

3.3 Security

TR-147 has no impact on Security

4 Introduction

DSL technology is widely deployed for Broadband Access for Next Generation Networks. Several documents, for example Broadband Forum TR-058, Broadband Forum TR-059 and Broadband Forum TR-101, describe possible architectures for these access networks. These specifications support the delivery of voice, video and data services.

The framework defined in this Technical Report is targeted at DSL-based access (either by means of ATM/DSL or Ethernet/DSL).

Traditional access architectures require one or more permanent virtual circuits per subscriber. These virtual circuits are configured at Layer 2 and are terminated at the first Layer 3 device (e.g. BRAS). Beside the data plane, such access architectures also define the architecture for element, network and service management. However, due to organizational boundaries between the business entities operating the local loop, the aggregation network and the IP backbone network, interworking between these entities via the management plane is not always applicable. Further, management networks are usually not designed to transmit management data between the different entities in real time.

When deploying value-added services across DSL access networks, special attention regarding Quality of Service and user management is required. This implies a tighter coordination between network nodes (e.g. Access Nodes and BNG), without burdening the management layer with impractical expectations.

Driven by these facts this Technical Report provides a framework for the Layer 2 Control Mechanism. Section 5 describes the general concept of the Layer 2 Control Mechanism, including the network architecture, security, redundancy and operational aspects. Section 6 then describes the different use cases for the Layer 2 Control Mechanism in detail. Given these use cases, Section 7 provides the necessary top-level message descriptions and lists the message parameters for the different use cases. Section 8 describes how the Layer 2 Control mechanism interworks with Element Management systems. Finally, Section 9 presents the protocol requirements for the Layer 2 Control Mechanism, as well as the requirements for the network elements that support it.

5 General Architecture Aspects

In this section the principles and the concept of the Layer 2 Control Mechanism is firstly described and then the reference architecture is introduced.

5.1 Concept of Layer 2 Control Mechanism

The high-level communication framework for a Layer 2 Control Mechanism is defined in Figure 1. The Layer 2 Control Mechanism defines a general-purpose method for multiple network scenarios with an extensible communication scheme, addressing the different use cases that are described within this Technical Report.

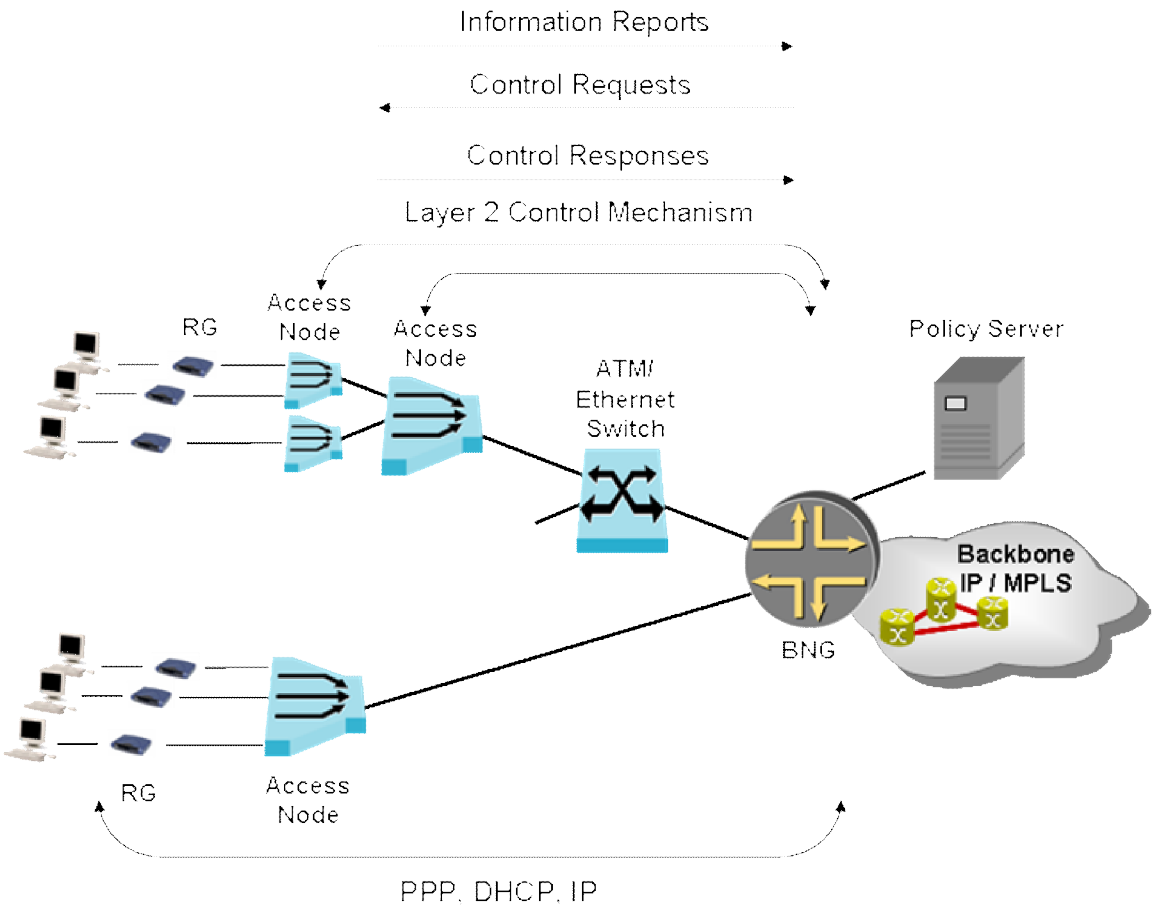

Figure 1: Layer 2 Control Mechanism

A number of functions can be identified:

- A **controller** function: this function is used to either send out requests for information to be used by the network element where the controller function resides, or to trigger a certain behavior in the network element where the reporting and/or enforcement function resides;

- A **reporting** function: this function is used to convey status information to the controller function. An example of this is the transmission of the Access Loop data rate from an Access Node to a BNG tasked with shaping traffic to that rate.
- An **enforcement** function: this function is contacted by the controller function to trigger a remote action on the Access Node. An example is the initiation of a port testing mechanism on an Access Node.

The connectivity between the Access Node and the BNG may differ depending on the actual layer 2 technology used (ATM or Ethernet). Therefore the identification of unicast and multicast flows/channels will also differ (see also section 5.3.1).

The control plane interactions are transactional in nature and imply a reliable communication channel to share states. Bidirectional operations are needed, as well as dynamic negotiation of capabilities.

The messages in this Technical Report are described in an abstract way, independent from any actual protocol mapping. The IETF ANCP working group is in the process of developing the Access Node Control Protocol (ANCP) that meets the requirements listed in this Technical Report. In the naming convention of the IETF, the BNG has the role of the controller and the Access Node represents the controlled switch. The actual protocol specification is out of scope of this Technical Report, but certain characteristics of the protocol are required so as to allow simple specification, implementation, debugging and troubleshooting, and also to be easily extensible in order to support additional use cases. This is discussed in Chapter 9.1.

5.2 Reference Architecture

The reference architecture used in this Technical Report is based on TR-101 and TR-059. Specifically:

- In the case of a legacy ATM aggregation network that is to be used for the introduction of new QoS-enabled IP services, the architecture builds on the reference architecture specified in TR-059;
- In the 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 TR-101.

Given the industry's move towards Ethernet as the future access and aggregation technology for triple play services, the primary focus throughout this Technical Report is on a TR-101 architecture. However the concepts are equally applicable to an ATM architecture based on TR-059. The reference architectures are shown in Figure 2.

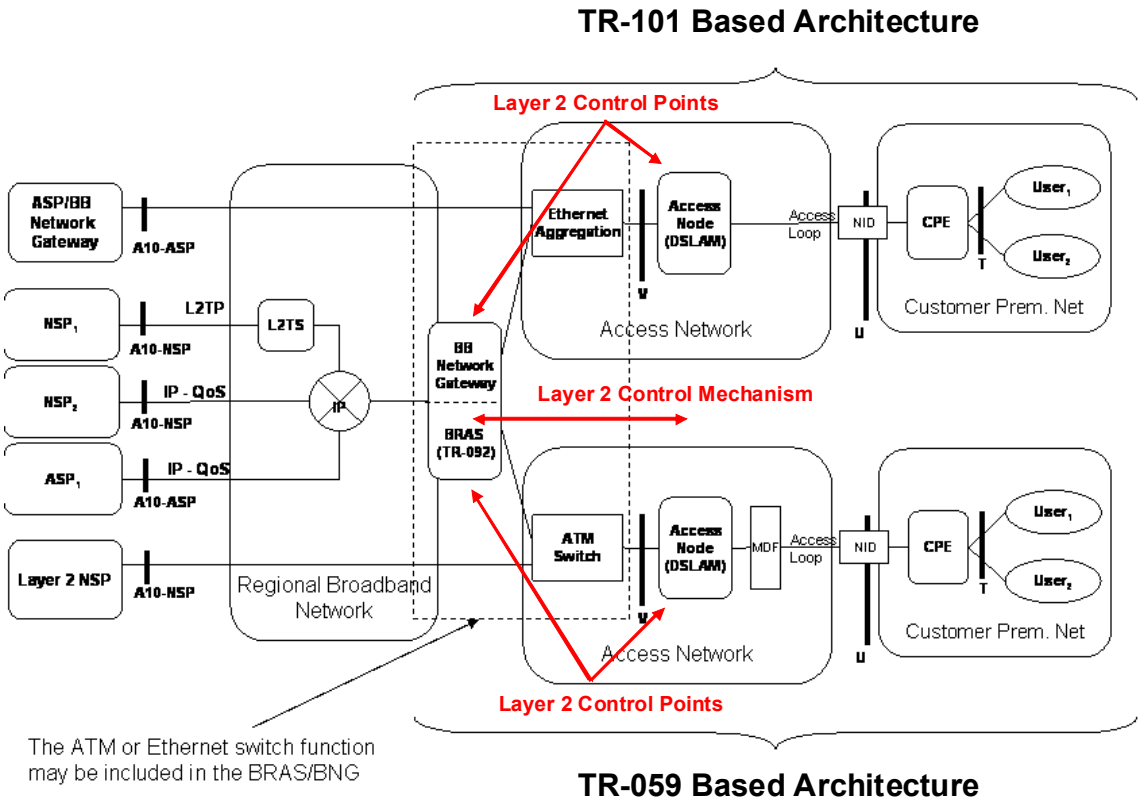

Figure 2: TR-059 and TR-101 Network Architecture with L2C-Mechanism

5.2.1 The Residential Gateway

The requirements of the Residential Gateway (RG) are consistent with those detailed in TR-068 and TR-101. No additional RG requirements arise as a result of this Technical Report.

5.2.2 Access Node

The Access Node is a network element as defined in TR-101 that terminates the Access Loops. It supports one or more Access Loop technologies and allows them to interwork with a common aggregation network technology. For example, an Access Node can support ADSL2+, SHDSL, VDSL2 and PON as Access Loop types and then backhaul the data to the aggregation network using Ethernet. There is an emerging requirement that ANs support multiple loop technologies, rather than only one.
Besides the DSL signal termination, the AN can also aggregate other ATM or Ethernet nodes implementing the ATU-C functionality. Both functions may also be performed at the same time.

The framework defined by this Technical Report is targeted at DSL-based access (either by means of ATM/DSL or Ethernet/DSL). However, the framework is open to non-DSL technologies, such as PON, FTTx and WiMAX.

The reporting and/or enforcement function defined in section 5.1 typically resides in an Access Node.

5.2.3 Access Node Deployment Options

The typical Access Node deployment options have been described in detail in Section 2.4/TR-101. This section looks more closely at how the Layer 2 Control functionality can be mapped onto these deployment options.

5.2.3.1 Base Deployment

A basic deployment option is shown in Figure 3. In this architecture, each Access Node behaves autonomously and will have its own Layer 2 Control Adjacency towards the BNG. Nodes that are subtended from a Hub Access Node will also establish their individual Layer 2 Control Adjacencies with the BNG. The Layer 2 Control messages sent to/from the subtended nodes will be switched through the Hub Access Node like other data packets, without processing of the actual message payload.

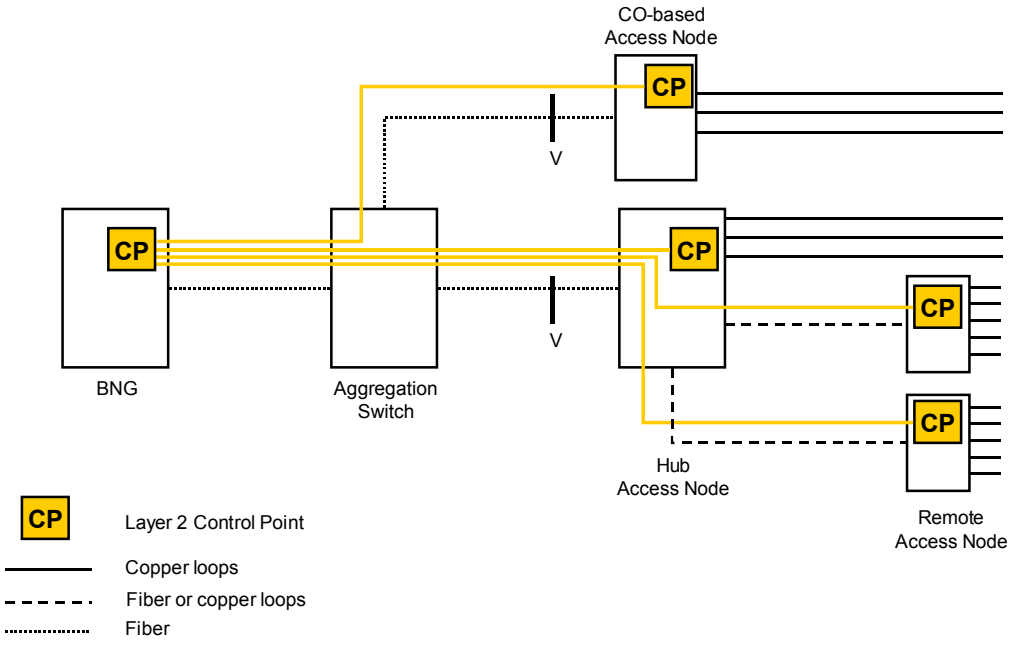

Figure 3: Basic Access Node Deployment Option

5.2.3.2 Deployment with Clustering

A second deployment scenario is shown in Figure 4. In this architecture, the Hub Access Node performs "clustering": the subtended network topology is abstracted towards the aggregation network, so that it looks like a single physical Access Node.

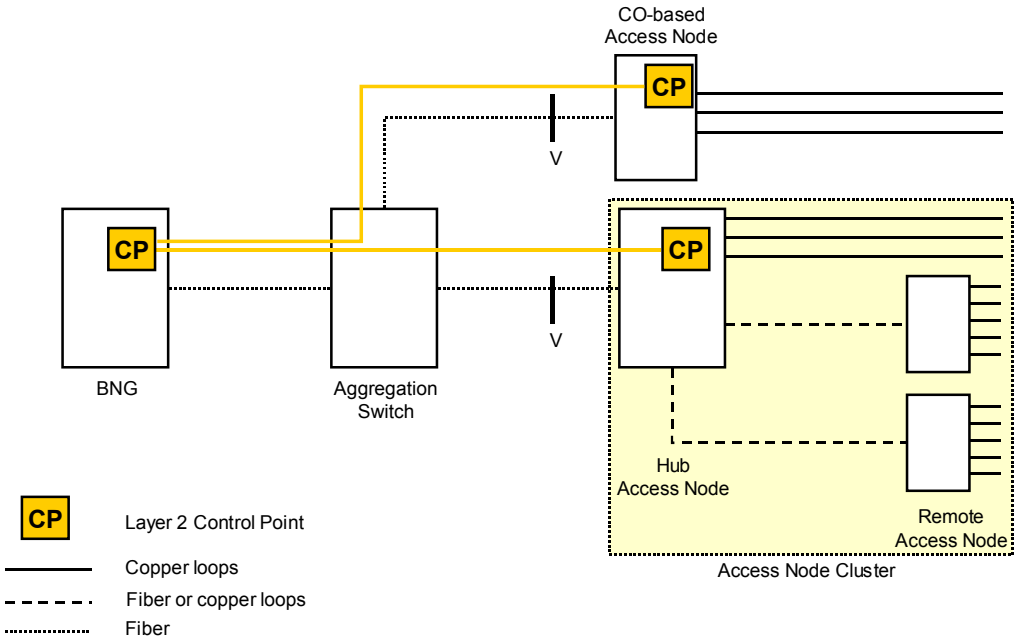

Figure 4: Access Node Deployment Option with Clustering

The Layer 2 Control interactions between the BNG and the Hub Access Node are the same as those to any other physical Access Node. The BNG has a Layer 2 Control Adjacency with the Hub Access Node, but not with the individual subtended nodes.

Whenever the BNG sends a downstream Layer 2 Control message pertaining to an access port on a subtended node, the Hub Access Node will process the message and take the necessary steps to contact the correct subtended node. Similarly, in the upstream, the remote nodes will communicate with the Hub Access Node, which will send the appropriate Layer 2 Control message to the BNG. The details of how to achieve clustering are beyond the scope of this document.

5.2.4 Aggregation Network

The aggregation network provides traffic aggregation towards the BNG(s). The aggregation technology can be based on ATM (in the case of a TR-059 architecture) or Ethernet (in the case of a TR-101 architecture).

5.2.5 Broadband Network Gateway

The BNG is a network element as defined in TR-101. It interfaces to the aggregation network by means of standard ATM or Ethernet interfaces, and towards the regional broadband network by means of transport interfaces for Ethernet frames (e.g. GigE, Ethernet over SONET or SDH). In addition to the functionality specified in TR-101, the BNG supports the Layer 2 Control functionality defined for the respective use cases throughout this Technical Report.
The controller function defined in section 5.1 typically resides in a BNG.

5.3 Operation and Management

When introducing a Layer 2 Control Mechanism, care is needed to ensure that the impact on the existing management mechanisms is minimized. The implications of possibly having multiple managers for the same object need to be fully taken into account.

Specifically when using the Layer 2 Control Mechanism for performing a *configuration* action on a network element, there is the challenge of supporting multiple managers for the same network element: both the Element Manager as well as the Layer 2 Controller function may now perform configuration actions on the same network element. Mechanisms are defined in order to synchronize the configuration actions and databases of all managers and avoid conflicts between them.
Also, when using the Layer 2 Control Mechanism for performing a *reporting* action, this raises the possibility of having more than one reporting method for a given network parameter. Care is needed that inconsistencies or race conditions are avoided.

The Layer 2 Control Mechanism could also form part of a Subscriber policy system.

5.3.1 Port Addressing Scheme

In deployments using an ATM aggregation network, access port identification is facilitated by the typical one-to-one mapping between an access port and an ATM PVC between the Access Node and the BNG. Based on such a property, in a PPP scenario, the BNG typically includes a NAS-Port-Id, NAS-Port or Calling-Station-Id attribute in RADIUS authentication and accounting messages sent to the policy server(s). Such an attribute includes the identification of the ATM PVC for this subscriber, which allows in turn identification of the access port.

In an Ethernet-based aggregation network, the port addressing scheme is defined in TR-101. Two mechanisms can be used:

- A first approach is to use the 1:1 VLAN assignment model for all Access Ports. This allows the access port identification to be directly derived from the VLAN tagging, i.e. S-VID or S-VID plus C-VID, of the frames coming from this DSL port.
- A second approach is to use the N:1 VLAN assignment model and to encode the Access Port identification in the “Agent Circuit ID” sub-option to be added to a DHCP or PPPoE message. The details of this approach are specified in Section 3.9/TR-101.

This Technical Report reuses the port addressing scheme specified in TR-101. It should be noted however that the use of such a scheme does not imply the actual existence of a PPPoE or DHCP session, nor the specific interworking function present in the Access Node. In some cases, no PPPoE or DHCP session may be present, while a persistent port address independent of protocol session would be desirable.

5.4 Policy management and admission control

The Layer 2 Control Mechanism can be part of an overall policy management framework. This includes aspects of QoS control and multicast conditional access, as described in sections 6.2 and 6.4.

Resource admission control for a given IP service may require coordination between several network elements including Access Node, BNG and Policy Server. The Layer 2 Control Mechanism could be used to perform such coordination. The details of such an approach are not addressed in this Technical Report.

5.5 Multicast Architecture

With the need to support IPTV services in a resource efficient way, multicast support is becoming more important.

In the reference architecture specified in TR-059, multicast traffic replication is performed in the BNG (BRAS). In that model, IGMP is typically used to control the multicast replication. As a result, network resources are wasted within the access/aggregation network.

To overcome this resource inefficiency, the Access Node, aggregation node(s) and the BNG must all be involved in the multicast replication process. This prevents several copies of the same stream being sent within the access/aggregation network. This may be achieved by means of IGMP snooping or IGMP proxy in the Access Node and aggregation node(s).

In this scenario BNG, aggregation node and Access Node need to behave as a single logical device and the Layer 2 Control Mechanism can be used to make sure that this logical/functional equivalence is achieved by exchanging the necessary information between the AN and the BNG.

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 for sensitive content. In this case, it is possible to provision the necessary conditional access information into the Access Node so it can then perform the conditional access decisions autonomously.

Provisioning the conditional access information on the Access Node can be done using a “White list” and/or a “Black list”. A White list associated with an Access Port identifies the multicast flows that are allowed to be replicated to that port. A Black list associated with an Access Port identifies the multicast flows that are not allowed to be replicated to that port. The BNG can use the L2C Mechanism to provision the necessary conditional access information in the Access Node so that the Access Node can decide locally whether or not to accept an IGMP Report.

5.6 Security Aspects

Potential attacks may be directed to the access network in order to:

- Disrupt the communication of individual subscribers, a large fraction of subscribers or the access network itself,
- Gain own profit (e.g., by modifying the QoS settings), or
- Intercept subscriber-related data.

Thus, the L2C Mechanism needs to provide a means of protecting messages against eavesdropping, modification, injection and replay while in transit. Furthermore, it is important to protect Access Nodes and BNGs from Denial of Service Attacks on resources like bandwidth and processing power. Any form of impersonation has to be avoided.

In the following, these potential attacks are explained in more detail:

- **Message Modification** involves integrity violations that modify the message flow. This includes reordering, delaying, dropping, injecting, truncating and other forms of message or message flow modification
- **Replaying of Signaling Messages** involves eavesdropping and collecting messages. Messages are then replayed at a later time or at a different place. This attack could cause denial of service or even theft of service.
- **Denial of Service Attacks** happen when a large number of messages are transmitted by a compromised node or by a man-in-the-middle. Also injecting false messages or truncating messages could lead to unexpected protocol behavior or to excessive resource consumption.
- **Eavesdropping or Traffic Snooping** assumes an attacker is able to capture all packets between the AN and the BNG. The eavesdropper might learn QoS parameters, communication patterns, policy information, application identifiers, user identities, authorization objects, network configuration and performance information, and more. This attack allows traffic analysis or replay attacks. The gathered information about the network can later be used to gain unauthorized access or to alter QoS settings for a flow.

5.7 Redundancy

In order to create a resilient network architecture, different levels of redundancy may need to be deployed, e.g. link/port redundancy and redundancy of the aggregation switches to protect the network between the Access Node and the BNG. These redundancy mechanisms are described in TR-144 and are largely orthogonal to the use of the Layer 2 Control Mechanism.

Redundancy becomes important from the Hub Access Node or CO-based Access Node toward the network core. The operator must avoid a node at this point in the network becoming a single point of failure.

In the case of an Ethernet aggregation network, the Rapid Spanning Tree Protocol (RSTP) defined in IEEE 802.1D (2004 edition), can be used to provide link and node failure protection between the Access Node and the BNG. Care is needed that the Layer 2 Control Adjacency will not go down when RSTP sets up a new spanning tree. The Adjacency will remain up if the keepalive timeout mechanism built into the protocol is set to a value that is higher than the RSTP convergence time (which may differ depending on network topology and sizing; worst case a few seconds).

In general, the protection mechanisms in the aggregation network should protect against link or aggregation node failures in such a way that the Layer 2 Control Adjacency will not go down.

Note: Ethernet Network resiliency can also be achieved using Ethernet protection mechanisms as defined in ITU-T recommendations G.8031 (Ethernet Linear Protection) and G.8032 (Ethernet Ring Protection).

Protection is also needed against failure of the BNG itself. In order to protect against facility failures (e.g. due to fire or a power outage), two physical BNGs can be deployed at geographically different locations. Given that the Layer 2 Control Mechanism is defined between the Access Node and the BNG, this creates additional considerations when establishing the Layer 2 Control Adjacencies to the Access Nodes, i.e. the need for additional state synchronization mechanisms between the Access Node and the redundant BNG. Note however, that the mechanism for achieving synchronization between two BNGs is presently not standardized; details of such approach are beyond the scope of this document.

Depending on the specific redundancy mechanism, the operation of the Layer 2 Control mechanism will be slightly different. A distinction can be made between “cold standby”, “warm standby” and “hot standby” as explained below.

5.7.1 Cold Standby

Traditional architectures mostly employ “cold standby”. In such a redundancy scheme, the backup system is not synchronized with the active system.

When using cold standby, the Access Node only establishes a Layer 2 Control Adjacency with the active BNG. This is shown in Figure 5. When the BNG fails, the Layer 2 Control Adjacency will go down and all state information (e.g. DSL line states) will be lost. The Access Node has to establish a new Layer 2 Control Adjacency with the backup BNG, and exchange all state information.

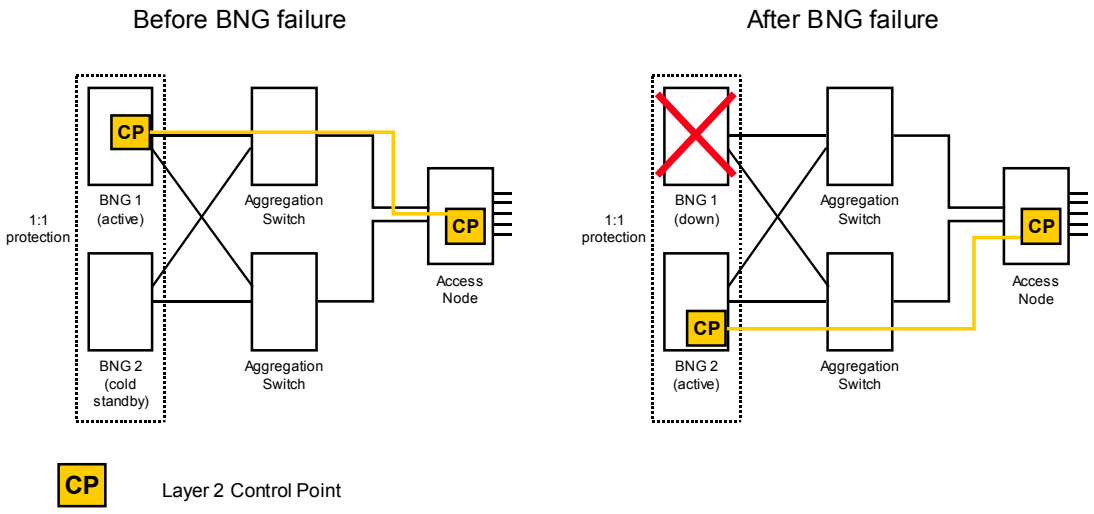

Figure 5: BNG Redundancy - Cold Standby

5.7.2 Warm Standby / Hot Standby

When using **"warm standby"**, the backup BNG is kept in sync with the active BNG at regular time intervals (e.g. every 15 minutes). This way, the backup BNG will be largely in sync with the previously active BNG. Nevertheless, at failure time, there may still be a need to provide some additional state information to the backup BNG upon a BNG failure.

When using "**hot standby**", the redundant BNG is kept fully synchronized with the active BNG. This is achieved by mirroring the state information from the active to the standby BNG in real time, so that both systems contain identical state information. When the active BNG goes down, the standby BNG provides for seamless protection without having to establish a new Layer 2 Control Adjacency, or having to provide additional state information to the backup BNG.

Warm/hot standby could be implemented in different ways. One approach is to have the Access Node establish a Layer 2 Control Adjacency to both the active and the standby BNG beforehand. This is shown in Figure 6:

- In case of warm standby, the Access Node exchanges state information to the backup BNG at regular time intervals.
- In case of hot standby, state information is sent to both BNGs in real time. Upon every state change, the Access Node sends a message to the standby BNG.

Note that when two Adjacencies are established and maintained, only the active BNG must be allowed to send Layer 2 Control messages (e.g. for remote port testing or port configuration) to the Access Node.

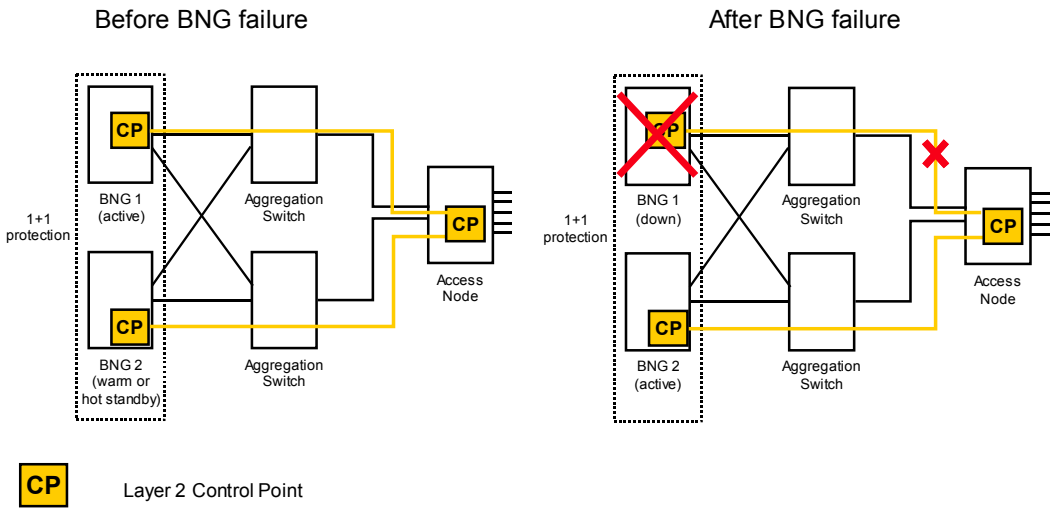

Figure 6: BNG Redundancy: Warm or Hot Standby Using Two Layer 2 Control Adjacencies

Another approach to achieve warm or hot standby is to let the two BNGs exchange state information directly. This is shown in Figure 7. In this model, the Access Node establishes a single Layer 2 Control Adjacency with the active BNG. The mechanism for achieving synchronization between two BNGs is presently not standardized; details of such approach are beyond the scope of this document.

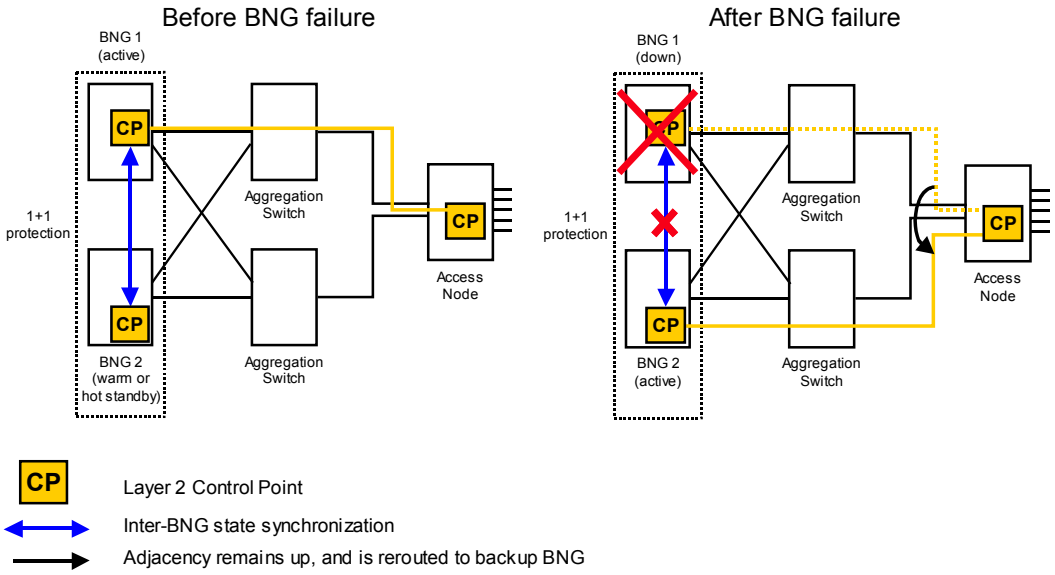

Figure 7: BNG Redundancy: Warm or Hot Standby Using BNG State Synchronization

6 Use Cases for the Layer 2 Control Mechanism

Based on a defined reference architecture use cases are defined supported by the layer 2 Control Mechanism.

6.1 Access Port Discovery

6.1.1 Overview and Motivation

Broadband Forum TR-059 identifies various queuing/scheduling mechanisms to avoid congestion in the access network while dealing with multiple flows with distinct QoS requirements. In networks that use a BNG performing hierarchical scheduling, the BNG needs to have an accurate view of the access network, including the various links being used and their respective rates.

Some of the information required is dynamic in nature (e.g. DSL line rate) and hence cannot come from a provisioning and/or inventory management system. Especially, when the subscriber line is operated in Rate Adaptive Mode (RAM) or in Seamless Rate Adaptation (SRA) mode it is very important to enforce consistency of the view of the Access Loop characteristics as seen by the Access Node and the BNG.

Dynamic and automated discovery of the different links in the access network addresses these issues. Access Port Discovery allows the BNG to perform these advanced functions without having to depend on an error-prone and possibly complex integration with a management system. The Layer 2 Control Mechanism allows the Access Node to communicate to the BNG the characteristics of the access links and any corresponding updates.

The actual data rate that is obtained when a DSL line is training up, is bound by configuration of the different DSL parameters, including the minimum net data rate, maximum net data rate and minimum net data rate in low power state. Within these bounds, the actual net data rate is determined by current noise conditions

In current approaches, the shaper is set in the BNG according to the service rate, which is part of the service profile. This rate may or may not correspond to the configured maximum net data rate; furthermore, the actual DSL net data rate may turn out to be lower than the configured service rate. If the distance between Access Node and RG is such that the DSL line synchronizes to a lower data rate than the shaping rate configured on the BNG, data packets are buffered in the Access Node and will be discarded upon buffer overflow. Traffic that is sent using TCP/IP automatically adapts to the new rate. If traffic is transferred using UDP, data loss can occur if no Layer 5-7 safeguard mechanisms are used. Rejected cells/frames and the associated IP packets are then not noticed and this leads to impairments of the connection.

In the case where the data rate on the subscriber line is modified, it may be necessary to control and check all elements along the data path (BNG and Access Node), so that the desired data rate is in line with the available data rate. The latter is usually limited by

noise conditions on the subscriber line. If the overall data path cannot support the desired data rate the management or billing system may need to be informed.

Communicating Access Port attributes is important in the case where the rate of the Access Loop changes over time. The DSL actual data rate may be different every time the RG is turned on. In this case, the Access Node sends an Information Report message to the BNG once the DSL line has synchronized.

Additionally, during the time the RG is active, data rate changes can occur due to environmental conditions (the DSL line can get lose sync and can retrain to a lower value, or the DSL line could use Seamless Rate Adaptation (SRA) making the actual data rate fluctuate while the line remains active). Both in the case of a retrain as well as when using SRA, the Access Node sends an Information Report to the BNG each time the Access Port attributes changes above a threshold value.

The use case includes more information than the Access Port identification and corresponding actual data rate. It also includes the Interleaving Delay, Minimum, Maximum and Attainable Data Rates. A complete list of DSL parameters that are to be conveyed to the BNG is specified in Table 3 of TR-101. These parameters could for instance be used by the BNG for admission control or QoS purposes.

6.1.2 Control Interactions

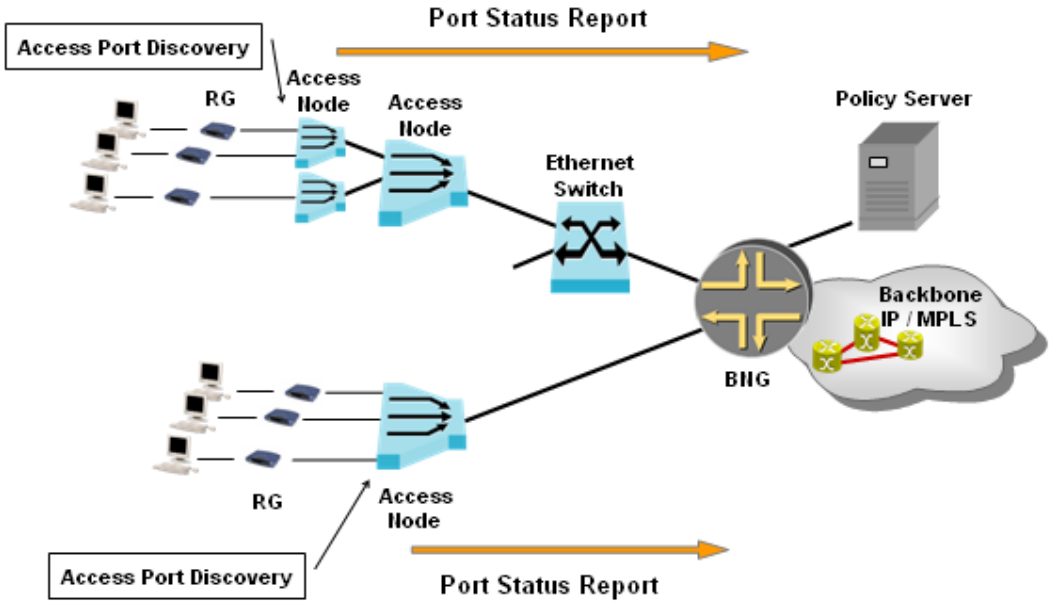

Figure 8: Access Port Discovery Interaction

To allow the BNG to dynamically adapt its schedulers, the Access Node informs the BNG with a Port Status Report Message when a new link is discovered or when the data rate on one of its links changes. This allows the BNG to rebuild the hierarchy of links in the access network and automatically (re-)configure its hierarchical QoS packet scheduler. A policy server can also use such information for admission control purposes.

The principles are valid for ATM-based as well as for Ethernet-based Access Nodes.

The hierarchy and the rates of the various links to enable the BNG hierarchical scheduling and policing mechanisms are the following:

- The identification and speed (data rate) of the DSL line (i.e. the net data rate)
- The identification and speed (data rate) of the Remote Access Node (RAN) /Access Node link (when relevant)

The BNG can adjust downstream shaping to current Access Loop actual data rate, and more generally re-configure the appropriate scheduler in the scheduling hierarchy (support of advanced capabilities according. to TR-101).

6.1.3 Information Flow

When using Access Port Discovery, the Access Node queries the current state of the synchronization of the DSL line and then sends this information (i.e. actual net data rate, minimum net data rate, maximum net data rate etc.) to the BNG. The BNG uses this information as input to its Hierarchical Scheduling process in order to limit the data traffic in the downstream direction so that no cell loss occurs in the Access Node. Note that as part of this process, the BNG could also interact with an AAA or Policy Server to retrieve per-subscriber authorization data and reduce the shaping limit to a different value.

Upon loss of the DSL signal, the Access Node informs the BNG with a Port Status Report Message that the DSL line went down.

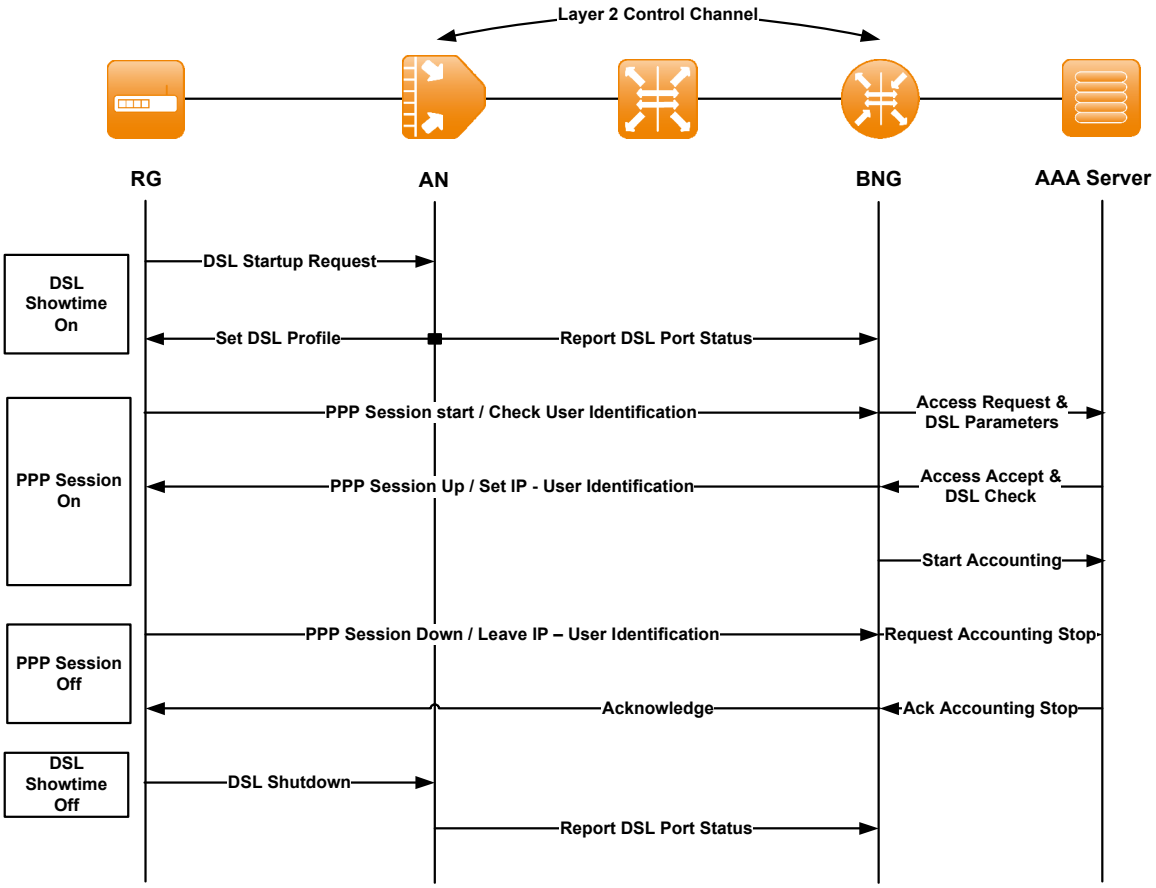

Figure 9: Access Port Discovery Flow

6.2 Access Port Configuration

6.2.1 Overview and Motivation

DSL Configuration

Most of the subscriber authorization data (i.e. service profiles, also known as "user entitlement") are typically enforced by the BNG itself. There are a few cases where it is useful to push such service parameters to the Access Node for local execution of a mechanism (e.g. DSL related) on the corresponding subscriber line.

DSL access parameters are typically configured in a static way. If a subscriber wants to change the access parameters required by a certain service, this normally requires an OPEX intensive reconfiguration of the port via the network operator, possibly implying a business-to-business transaction between an ISP and an Access Provider.

By means of the Layer 2 Control Mechanism such cross-organizational business-to-business interactions are avoided. This also allows centralizing subscriber-related service data in, for example, a AAA or Policy Server.

The BNG could configure a number of physical layer service parameters for a particular access line. Such a configuration change does not need to happen in real-time. Rather, it is a subscription change that will be valid for a long period of time.

Ethernet/IP Configuration
Besides the configuration of physical layer parameters, Access Port Configuration also includes network layer service parameters, e.g. 802.1p scheduling configuration on the access link.

When deploying multiple services over the access link, it is necessary to provide different QoS levels for the different services. Additionally, services such as VoIP with real-time performance requirements may require end-to-end QoS strategies.

In this context, QoS attributes of the Access Node can be configured via the L2C Mechanism by sending the information from the BNG to the Access Node. Using such an approach simplifies the management infrastructure for service management, allowing fully centralizing subscriber-related service data (e.g. Policy Server) and avoiding complex cross-organization business-to-business interactions.

6.2.2 Control Interactions

Following dynamic Access Port identification (subscriber local loop) as assisted by the mechanism described in the section 6.1 (Access Port Discovery), the BNG queries a subscriber management system (e.g. AAA and/or Policy Server) to retrieve subscriber authorization data (service profiles, also known as “user entitlement”).

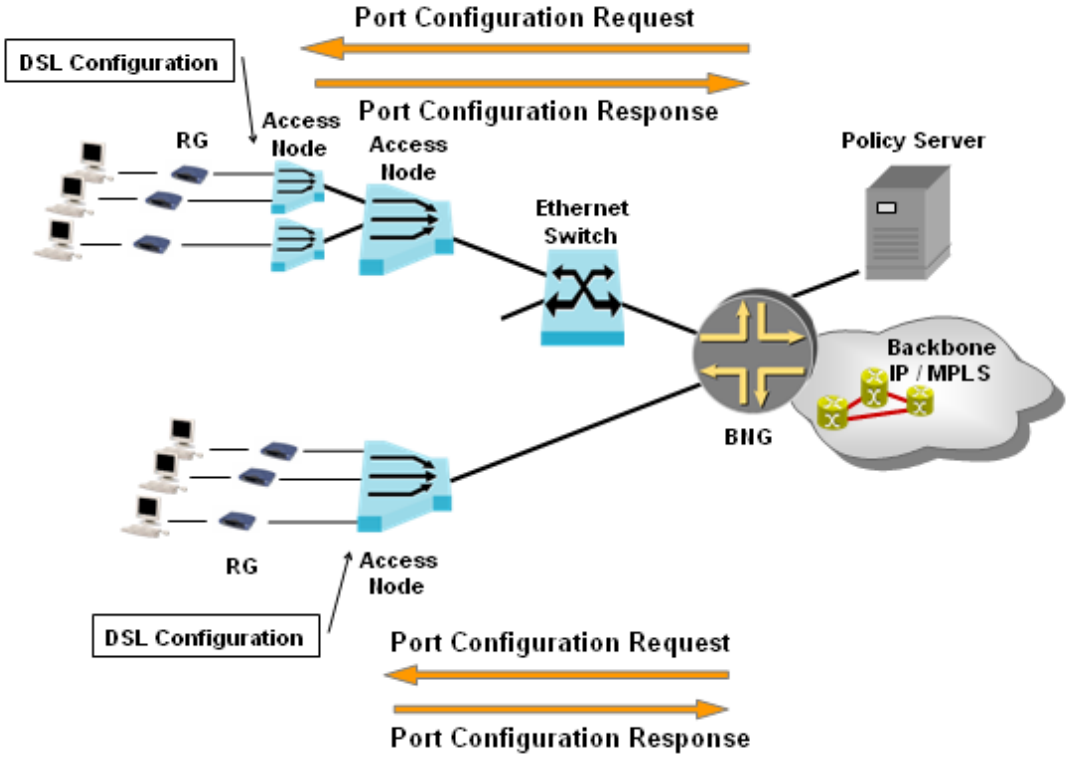

Figure 10: DSL Configuration Interaction

One way to change line parameters is by using profiles. These profiles (DSL profiles for different services) are pre-configured by the management system of the Access Nodes. The L2C interaction then only needs to transmit a reference to the right DSL profile.
Another way to change line parameters is by conveying discrete DSL parameters in the L2C interaction.

Triggered by the communication of the Access Port attributes described in section 6.1, the BNG may send Access Port Configuration information (e.g. a reference to a DSL profile) to the Access Node using a Port Configuration Request Messages. The BNG may get such line configuration data from either AAA or Policy Server. The BNG may update the Access Loop configuration due to a subscriber service change (e.g. triggered by the policy server).

Example message sequence:

- The BNG is informed by a policy server (e.g. using COPS or Change or Authorization (CoA) message) about a subscriber requesting bandwidth;
- The BNG instructs the Access Node to reconfigure for example the maximum data rate for a specific Access Port to a higher value, such that the line can train to a higher rate
- The Access Node reconfigures the Access Port maximum data rate and after retraining the DSL line, informs the BNG of the new data rate

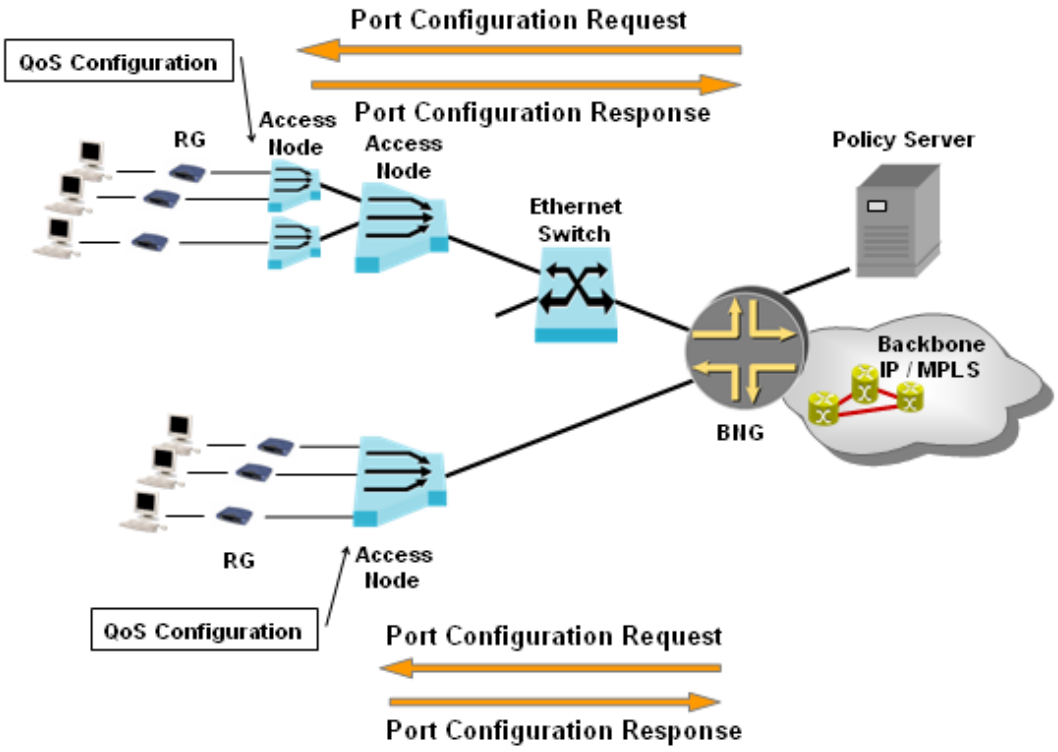

Figure 11: Ethernet/IP Configuration Interaction

Triggered by the **subscriber's access request**, the BNG, interacting with AAA Server, authenticates the subscriber. Then the BNG retrieves QoS policy information per subscriber and per service from either AAA or Policy Server. A Port Configuration Request Message is sent to the Access Node, which triggers the configuration of QoS attributes for the corresponding subscriber and service. This could include policing rate control, queue mapping and queue scheduling etc.
The Access Node sends a Port Configuration Response Message back to the BNG, notifying about the configured QoS attributes.
When the subscriber terminates the service, the BNG detects the service termination and notifies the Access Node to release the network resources and the QoS policy enforcement.

Example message sequence:

- The BNG conveys QoS attributes to the Access Node
- The Access Node informs the BNG about the configuration result
- The Access Node releases network resources dynamically

6.2.3 Information Flow

After the Access Port enters "showtime", the subscriber can initiate a session. With a successful authentication, the AAA server sends subscriber parameters to the BNG.

These parameters will be configured on the Access Port where the subscriber is located; this is done by the BNG using the Port Configuration Request message. The DSL line may retrain after such port configuration action has been performed. In that case, the subscriber session will need to be re-established after the retrain. The BNG may later modify parameters on the Access Port using the Port Configuration Request message.

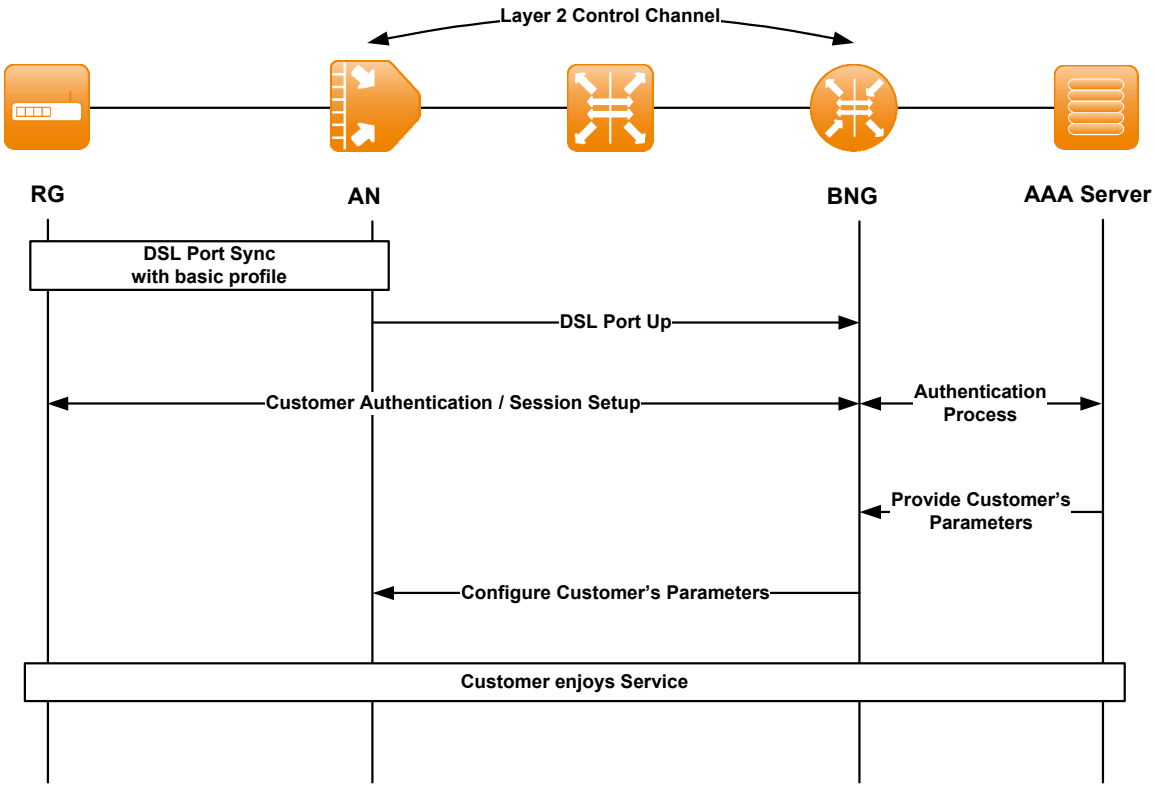

Figure 12: Access Port Configuration Flow

6.3 Layer 2 OAM

6.3.1 Overview and Motivation

Traditionally, ATM circuits are point-to-point connections between BNG and RG. In order to test the connectivity at Layer 2, appropriate OAM functionality is used for operation and troubleshooting. An end-to-end ATM OAM loopback can be performed between the edge devices (BNG and RG) of the broadband access network.

When migrating to Ethernet-based aggregation networks (as defined by TR-101), end-to-end ATM OAM functionality becomes impossible. In such a mixed Ethernet and ATM access network (including the local loop), operators desire to keep the same ways to test and troubleshoot connectivity as those used in an ATM based architecture. To reach consistency with the ATM based approach, the Layer 2 Control Mechanism can be used until end-to-end Ethernet OAM mechanisms are more widely available.

When Ethernet-based VDSL2 access is used, ATM OAM is no longer applicable. Although end-to-end Ethernet OAM mechanisms have been standardized in IEEE802.1ag, these techniques are not yet widely supported by deployed RGs. Therefore, even in an end-to-end Ethernet access network, a port status test triggered by the BNG management system and conveyed via Layer 2 Control Mechanism remains a useful mechanism for the foreseeable future.

DSL access is commonly used to establish broadband connectivity between RG and BNG. Some trouble tickets are related to access line connectivity problems. Therefore, a mechanism is desired that enables remotely testing access line connectivity. The Layer 2 OAM use case demonstrates how to perform such troubleshooting remotely, triggered by the BNG. In order to achieve this, the following basic requirements need to be met:

1. Unique point to point connection between RG and BNG within layer 2 for addressing customer connection(s) (with or without a PPP or DHCP session being established)
2. In the case of ATM access, use of a default Loopback Location ID (LLID) when addressing the connection endpoint at the RG, combined with a connection ID which identifies the virtual connection between the RG and BNG. This provides a unique addressing scheme for DSL connections between RG and BNG (administering the RG's MAC addresses is too complex for operation in a mass market environment due to the fact that various RG's could be connected over the open U-reference point)

ATM and Ethernet use different forwarding paradigms. ATM uses a label swapping connection oriented forwarding mechanism. ATM loopback assumes a connection and the integrity of the connection is verified by a successful loopback of the OAM cell inserted into a particular VCC or VPC. As long as there is ATM end-to-end connectivity between the BNG and the RG, OAM loopback cells can be used for on-demand connectivity monitoring, fault localization and pre-service connectivity verification. The subscriber is identified by the VPC or VCC assignment. Therefore the loopback endpoint can be addressed by the default Loopback Location ID (LLID) value. That simplifies the operation because no administration of different subscriber specific Connection Point IDs (CPID) is needed.

Ethernet uses a forwarding paradigm that uses the destination MAC address. An Ethernet loopback would verify integrity by getting a response from a message directed towards a specific MAC address. The provider does not administer customer MAC addresses, therefore mechanisms would be required to "learn" or "discover" this information (and track corresponding changes).

Ethernet has defined multiple standardized OAM mechanisms e.g. in ITU-T Y.1731 and IEEE 802.1ag. There are some concerns however in terms of the scalability of the current method of manually administering MEPs in a residential mass-market environment. It remains to be investigated if and how the Layer 2 Control Mechanism might be used to solve this problem. This however is not addressed in this Technical Report.

6.3.2 Control Interactions

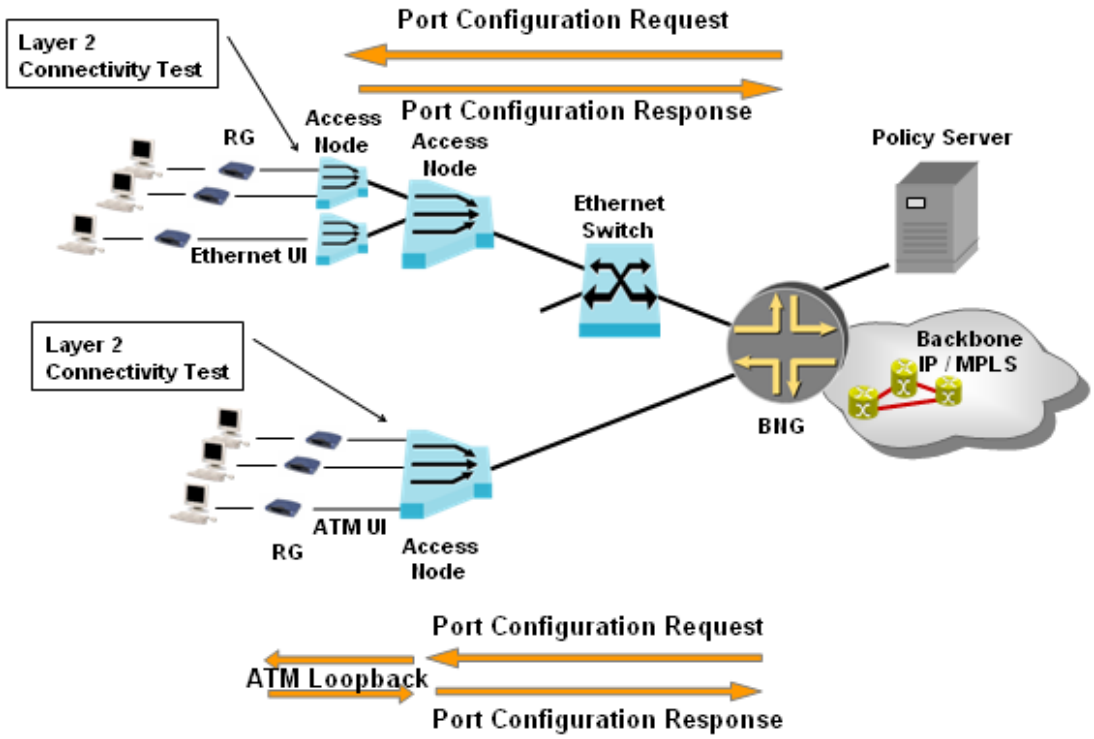

Figure 13: Layer 2 OAM Interaction

Triggered by a local management interface, the BNG can use the Layer 2 Control Mechanism to initiate an Access Loop test between Access Node and RG. A Port Configuration Request is sent to the Access Node to trigger the Access Loop test. In the case of an ATM based Access Loop, the Access Node generates ATM F5 loopback cells on the Access Loop. In the case of Ethernet, the Access Node can perform a port synchronization and administrative test for the Access Loop. The Access Node can send the result of the test to the BNG via a Port Configuration Response Message. The BNG may then report the results via a local management interface.
Thus, the connectivity between Access Node and the RG can be monitored by the BNG without the BNG needing to know how the Access Node actually performs troubleshooting.

As described in Section 6.3.1, new deployment scenarios may support end-to-end Ethernet transport. When using RGs that do not support Ethernet OAM functionality, the Access Node may terminate the BNG's Port Configuration Request Message and rely on the Access Loop synchronization state to answer the request.

Layer 2 connectivity test:

- Supports both Ethernet and ATM Layer 2 at U-reference point
- Supports Ethernet at V-reference point

- Is irrelevant for ATM at V- reference point

Example message sequence:

- The BNG sends a Port Configuration Request Message to the Access Node to request the ATM (or Ethernet) Access Loop test
- The Access Node sends ATM F5 OAM loopback cells in case of ATM over DSL, or the Access Node sends an equivalent loopback frame in case of Ethernet over DSL in order to test Access Loop connectivity
- The Access Node informs the BNG about the test result

6.3.3 Information Flow

Referring to Section 7.4/TR-101, describing requirements for interworking between Ethernet and ATM OAM in the Access Node, the following information flow shows OAM interworking using Layer 2 Control Messages.

Triggered by the BNG's management system, the interworking function (IWF) in the Access Node will insert ATM F5 Loopback cells at the respective Access Port of the Access Node. The answer from the RG is evaluated at the Access Port and the appropriate result is sent to the BNG in a Layer 2 Control Message. The result is then passed on to the management system.

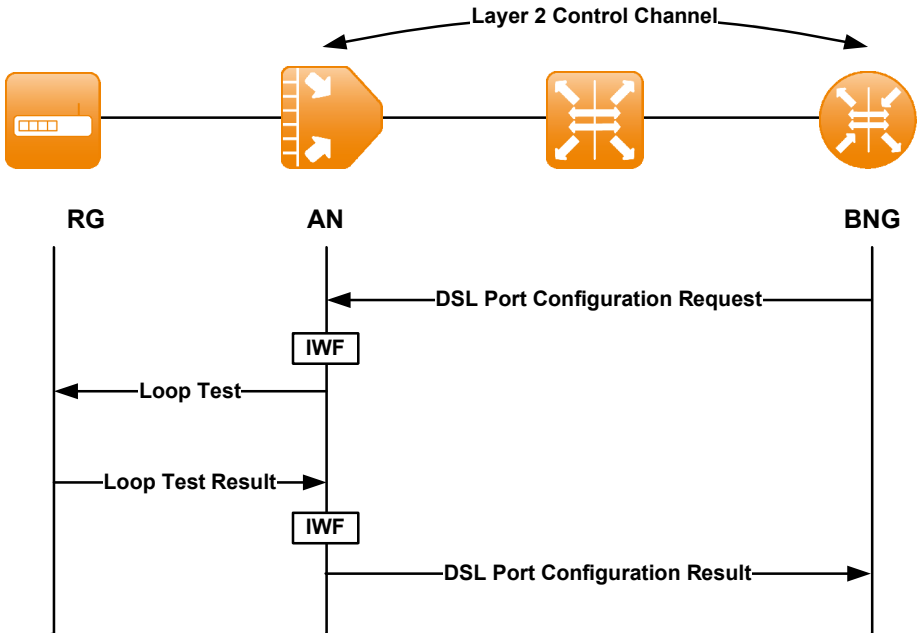

Figure 14: OAM Flow with L2C-Triggered Access Loop Test

6.4 Multicast

6.4.1 Overview and Motivation

With the requirement to support IPTV services in a resource efficient way in an Ethernet-based access/aggregation network, multicast support is getting increasingly important. IGMP is typically used to control the multicast content replication process. This is achieved by means of IGMP snooping or IGMP proxy in the different layer 2 nodes in the network (e.g. Access Node, Ethernet aggregation switch). In order to allow for centralized QoS and policy control, the BNG and the Access Node may have to communicate on the configuration/state of the multicast replication process.

As mentioned in Section 5.4, service providers may want to dynamically control, at the network level, access to some multicast flows on a per user basis. The BNG can use the L2C Mechanism to provision the necessary information in the Access Node so that the Access Node can decide locally whether or not to accept an IGMP Report message. The BNG may retrieve such information from an external Policy Server.

Multicast ACLs

For enabling multicast at an Access Node port, an Access Control List (ACL) – the so-called "white list" and/or "black list" – must be provided per Access Port. The ACL must contain customer multicast related information in order to provide the end-customer permission to join particular IP multicast groups. The ACL allows a network provider to authorize or deny access to specific multicast content to a customer.

The addressing scheme of an ACL is derived from the 'Access Circuit Identifier' convention provided in the use case "Access Port Discovery" (chapter 6.1).

Multicast replication control

The criteria that might be checked by the AN while receiving a channel request are:

- Is the customer entitled to receive any multicast content?
- Is the customer entitled to receive the specific multicast content he requested?
- Is the customer making a request that would exceed the maximum number of authorized simultaneous channels he is entitled to receive?

ACL population

Several models are available to populate the ACL via the Layer 2 Control Protocol. In the same way, several models are relevant regarding the disconnection of the service.

In a first model, the BNG uses the PPPoE session establishment together with the intermediate agent in the Access Node in order to identify the customer and download the entitlements to the ACL instances associated with the Circuit ID.

A similar model can be applied when using DHCP.

Another option for ACL population is to provision the ACL using static data linking the customer entitlements to the relevant Circuit ID.

Multicast Service Disconnection

In the case where the customer entitlements are linked statically with the relevant Circuit ID, service disconnection should be done in the same static way – using an operator command.

For dynamic customer identification, two scenarios are possible depending on whether the customer identification protocol (PPPoE/DHCP) is bound to the multicast service or not.

- In the first case where both are bound, the PPPoE (or DHCP) termination implies the disconnection of the multicast service. If customer is later discovered on a new port, the ACL should be sent via L2C to this new port. The channels following this model are called 'Nomad' channels.

- In the second case where the customer identification protocol is independent or not directly linked to the multicast service (e.g. not sharing the same data link or being initiated by a different physical entity than the one receiving the service), once the customer is identified, the multicast service should be independent from the PPPoE session termination. A PPPoE session can then be established and terminated on a single port without having the video service disrupted. The channels following this model are called 'Semi-Nomad' channels.

Both scenarios allow several business models, where the customer dedicated ACL may be separated into at least two parts. One part of the customer entitlements may be port dependent and the other part may be customer dependent thus following him when changing location.

Multicast Information collection

The BNG can use the L2C Mechanism to asynchronously query the AN to obtain an instantaneous status report related to multicast flows currently replicated by the AN. Such a reporting functionality could be useful for auditing and troubleshooting purposes. The BNG can query the AN to find out the following:

- Which flows are currently being sent on a specific Access Port;
- On which Access Ports a specified multicast flow is currently being sent;
- Which multicast flows are currently being sent on each and every individual Access Port.

Note that the last two types of query may not be feasible in real-time.

6.4.2 Control Interactions

The control interactions for ACL population are conceptually identical to those of the Access Port Configuration use case. Details of the information elements provided as part of the multicast ACL are described in Section 7.2.4.

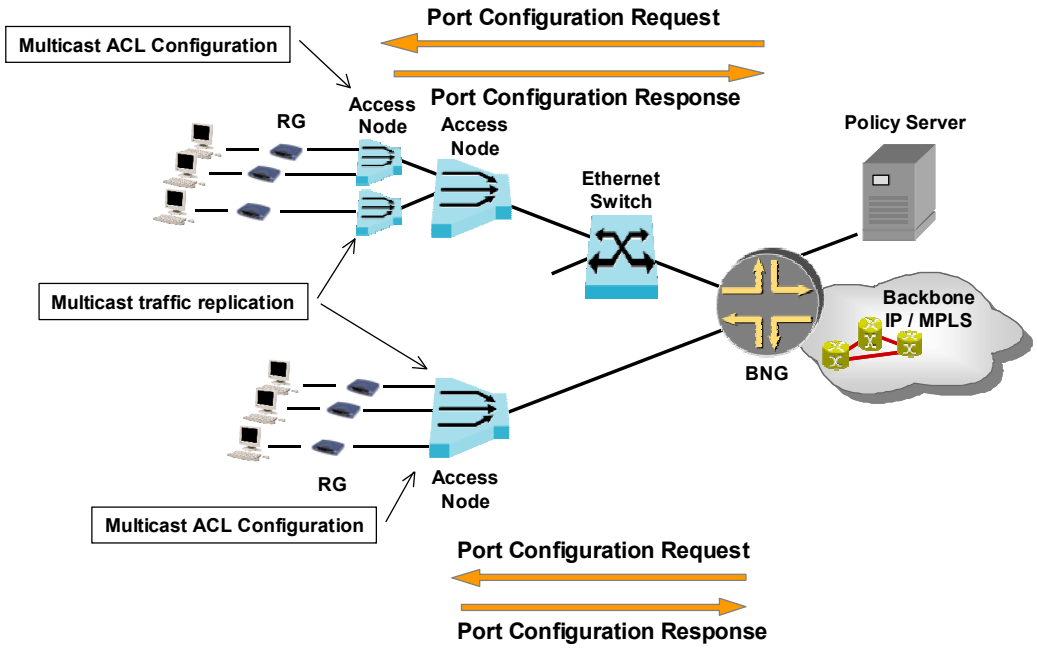

Figure 15: Multicast Interaction

6.4.3 Information Flows

The following flow chart gives an example on an ACL population depending on PPP, Operator or Service Provider Events. The messages used for configuring the ACLs are sent from the BNG to the Access Node.

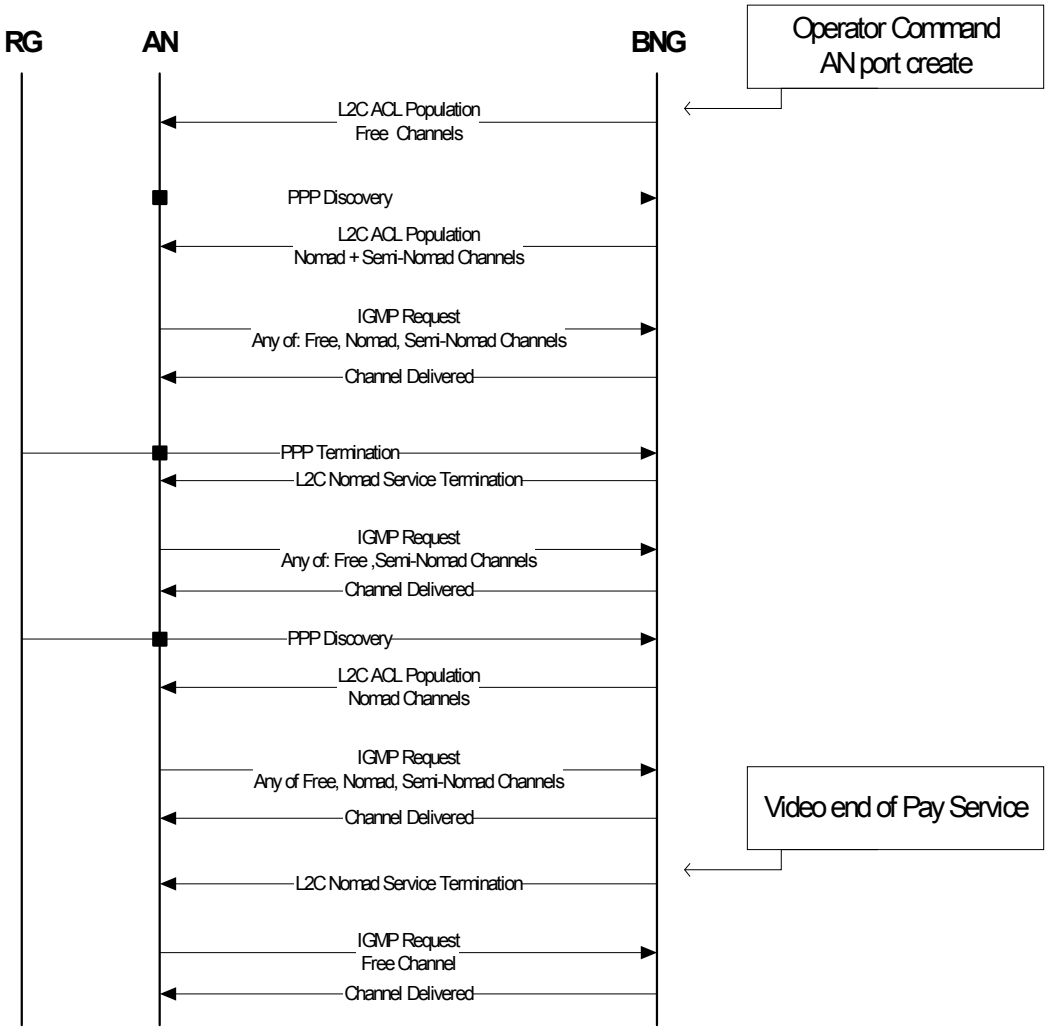

Figure 16: Multicast Flow

7 Message Descriptions and Parameters for L2C

7.1 Message Descriptions

The following message types need to be defined to facilitate the exchange of this control information

- A Boot Request Message sent by BNG or Access Node
- A Boot Response Message by the peer device
- A Port Configuration Request Message sent by the BNG to Access Node
- A Port Configuration Response Message that is sent by the Access Node to the BNG
- A Port Status Report Message sent by the Access Node to the BNG to support an asynchronous exchange of control data

7.1.1 Boot Request Message

The Boot Request Message is sent in a directed or broadcast manner by BNG or Access Node, typically at start-up time. It is intended to solicit capability information from an Access Node for a BNG or from a BNG for an Access Node. The Boot Request Message needs to contain at least the following parameters

- <Holding Time>
- <Device Type>
- <Access Port Discovery Capable>
- <OAM Capable>
- <Access Port Configuration Capable>
- <Multicast Capable>

The receiver, to allow for future extensions, must ignore unknown capabilities.

7.1.2 Boot Response Message

The Boot Response Message needs to contain at least the following parameters:

- <Holding Time>
- <Device Type>
- <Access Port Discovery Capable>
- <OAM Capable>
- <Access Port Configuration Capable>
- <Multicast Capable>

7.1.3 Port Configuration Request Message

The Port Configuration Request Message allows the BNG to configure subscriber level information in the Access Node, query data from or initiate an action in the Access Node. Examples of when such a message may be sent by the BNG include:

- When a user is first identified and authenticated
- When a subscriber service level changes
- When OAM tests need to be performed
- When Multicast related information is communicated

The operation is intended to be transactional in nature (i.e. the transaction is either fully completed, or rolled-back to the previous state; in the case of failure, no change should occur on the Access Node side).
The following parameters need to be contained in this message type:

- <The Subscriber ID with which Access Node can identify the subscriber (e.g.: MAC Address, ATM VC associated with a subscriber, Line ID)>
- <Access Port Configuration Parameters | Optional>
- <OAM Test Parameters | Optional>
- <Multicast Information | Optional>

7.1.4 Port Configuration Response Message

An Access Node sends the Port Configuration Response Message to a BNG in reply to a Port Configuration Request Message received by.
The parameters of this message need to include:

- <Subscriber ID>
- <Line ID | Optional>
- <Access Port Configuration Result | Optional>
- <OAM Test Results | Optional>

7.1.5 Port Status Report Message

The Port Status Report Message will typically be sent from Access Node to BNG and is used to transmit data such as Access Loop characteristics to the BNG.
This message may be triggered by one of the following events:

- After a DSL line entering a stable link status (idle, silent or showtime)
- After recovery of the communication channel
- When one or more of the configured Access Port parameters are modified by means of the management system (i.e. not L2CP)

The message needs to include the following parameters:

- <Subscriber ID | Optional>
- <DSL Parameters | Optional>
  - <Line ID & Bandwidth | Optional>
  - <RT/Access Node Link ID & Bandwidth | Optional>
- <Port Status | Optional>

The bandwidth description of a given link provides both the upstream and downstream capacity of that link. In the case of a DSL line, this is the actual data rate on the DSL line (sometimes referred to as the Access Loop sync rate). The DSL parameters above are exemplified. A more complete list can be found in Table 3/TR-101.

7.2 Message Parameters

7.2.1 Access Port Discovery - xDSL Parameters

The complete set of Access Loop characteristics that need to be conveyed for the Access Port Discovery use case is listed in the following table:

Pos.	Message Type	Information	Reference	Read-only (R) / Read-write (RW)[1]
1	DSL Type: xDSL Transmission System	This parameter defines the transmission system in use (e.g. ADSL, ADSL2, ADSL2+, VDSL2)	ITU-T G.997.1 Section 7.5.1.1	R
2	DSL Port State	Port up (showtime, L0) / Port down (not synchronized powered, L3) / Low power down (reduced net data rate, L1 or L2)	ITU-T G.997.1 Section 7.5.1.5	R
3	Actual data rate Up- and Downstream	Actual net data rate upstream and downstream of a synchronized DSL port	ITU-T G.997.1 Section 7.5.2.1	R
4	Attainable Data Rate Up- and Downstream	Maximum net data rate which can be achieved	ITU-T G.997.1 Section 7.5.1.20 and 7.5.1.19	R
5	Minimum Data Rate	minimum net data rate desired by the operator in kbit/s	ITU-T G.997.1 Section 7.3.2.1.1	RW
6	Maximum Data Rate	maximum net data rate desired by the operator in kbit/s	ITU-T G.997.1 Section 7.3.2.1.3	RW
7	Minimum Data Rate in low power state	minimum net data rate desired by the operator during the low power state (L1/L2)	ITU-T G.997.1 Section 7.3.2.1.5	RW
8	Maximum Interleaving Delay	maximum one-way interleaving delay, coded in ms (2 – 63) or with special value (no boundaries, fast channel)	ITU-T G.997.1 Section 7.3.2.2	RW
9	Actual interleaving Delay	Value in milliseconds which corresponds to inter leaver setting.	ITU-T G.997.1 section 7.5.2.3	R

Table 1: Access Port Parameters

[1] Read operation is possible in the Access Port Discovery use case. Write operation is possible in the Access Port Configuration use case.

7.2.2 Access Port Configuration Parameters

The table below summarizes the different parameters that are configurable by the BNG using the Layer 2 Control Mechanism. The table lists the different parameters that are described throughout the Technical Report, with a reference to the corresponding section.

Parameter	Reference
Layer 1 parameters	
DSL configuration profile name (i.e reference to a pre-configured DSL profile in the element management system)	section 6.2
Minimum Data Rate	section 7.2.1 (ITU-T G.997.1 Section 7.3.2.1.1)
Maximum Data Rate	section 7.2.1 (ITU-T G.997.1 Section 7.3.2.1.3)
Minimum Data Rate in low power state	section 7.2.1 (ITU-T G.997.1 Section 7.3.2.1.5)
Maximum Interleaving Delay	section 7.2.1 (ITU-T G.997.1 Section 7.3.2.2)
AdminStatus (blocked / released)	section 7.2.2
Layer 2 parameters	
Encapsulation type	R-68
ATM VPI/VCI and QoS parameters (for ATM/DSL only)	
Upstream policing	section 6.2
Rate control	section 6.2
Ethernet (802.1p) queue mapping and scheduling	section 6.2
Port association to a unicast VLAN	
Port association to a multicast VLAN	section 9.4.1, R-38
Ethernet/IP parameters	
Access Control List	section 7.2.2
Source MAC address filter	section 7.2.2
Destination MAC address filter	section 7.2.2
Source IP address filter	section 7.2.2
Multicast Access Control List	section 7.2.4
Max Simultaneous Streams	section 7.2.4

Table 2: Access Port Configuration Parameters Configurable by the BNG (within the scope of this Technical Report)

For the layer 1 parameters, Access Port Configuration could be done in a number of ways:

- Configure discrete DSL parameters
- Configure the DSL profile name (i.e. a reference to a pre-configured DSL profile)
- Configure the entire DSL profile

For each access port, the BNG must be able to set the AdminStatus. This is a parameter of the Port Configuration Mechanism and can be used in order to block a suspicious port after a security attack.

AdminStatus:

- Blocked
- Released

For security purposes, access control lists must include:

- Source MAC address filter
  - Allowing access from specific devices (i.e. MAC address)
  - Denying access from a specific MAC address
- Destination MAC address filter
  - Allowing access to specific destinations
  - Denying access to specific destinations
- Source IP address filter
  - Allowing access from a specific IP address
  - Denying access from a specific IP address

7.2.3 OAM Parameters

General Loopback Format

Using OAM capabilities triggered by the Layer 2 Control Mechanism is described in chapter 6.3. OAM functions and their related parameters are standardized in ITU-T Recommendations I.361 and I.610. The following parameter set describes the F5 End-to-End Loopback cell:

Cell format UNI:	ITU-T I.361, ITU-T I.610
GFC (Generic Flow Control)	GFC = 0000
VPI (Virtual Path Identifier):	VPI = e.g. 1
VCI (Virtual Channel Identifier)	VCI = e.g 32
PTI (Payload Type Indication):	PTI = 101: F5 OAM End-to-End
CLP (Cell Loss Priority):	CLP = 0/1

Access Node

Besides the general OAM format, the Access Node needs to calculate a timer value, which defines a window for receiving all responses to the OAM Loopback cells that have been sent towards the RG. In the case of ATM based OAM, this timer value is equal to the number of end-to-end F5 OAM Loopback cells to be sent, multiplied by the F5 loopback timeout (i.e. 5 seconds per the ITU-T I.610 standard).

The Access Node also needs to determine the difference between the number of F5 end-to-end OAM Loopback cells sent and the number of Loopback cells received within a certain period of time. The Access Node compares this value with a configurable threshold value, in order to determine whether or not connectivity to the RG is acceptable. It then sends a Layer 2 Control message towards the BNG containing the result.

Cell format UNI:	ITU-T I.361, ITU-T I.610
GFC (Generic Flow Control)	GFC = 0000
VPI (Virtual Path Identifier):	VPI = e.g. 1
VCI (Virtual Channel Identifier)	VCI = e.g. 32
PTI (Payload Type Indication):	PTI = 101: F5 OAM End-to-End
CLP (Cell Loss Priority):	CLP = 0

Number of cells to be sent to the RG, triggered by a Layer 2 Control command: e.g. 32
Access Node OAM Loopback reply receiving window: e.g. > 5 sec * 32.
Threshold (received LB cells): e.g. 20

BNG

The BNG triggers the Access Node to send end-to-end OAM Loopback cells on a DSL port and ATM PVC. Like the Access Node, the BNG uses a timer value which defines a window for receiving a response from the Access Node. Also the BNG needs to be able to interpret the test result received from the Access Node (see next section).

Timer Value “receiving window – Access Node”: e.g. > 5sec. * 32 sec.

7.2.3.1 L2C OAM Test Result

The BNG sends a trigger message towards the Access Node. The Access Node itself responds with a Port Configuration Response message. This message provides the status of the Access Port as well as error status information. See also Table 3.

For proper operation of this use case, the error information needs to be independent of the layer 2 technology used. These messages are sent from the Access Node to the BNG, to inform about the current status and the result of the test in case the OAM operation fails.

Error status information
Specified access line does not exists
DSL line status showtime
DSL line status idle
DSL line status silent
DSL line status training
Loopback test timed out (If the threshold of successful received LB cells is not met.)
Access Node IWF not available

Table 3: OAM Test Result Elements

7.2.4 Multicast Parameters

For each access port, a list of multicast groups/streams can be configured at the AN to specify which groups/streams are allowed/not allowed to be sent on that port:

Access Circuit	**Multicast Group Address / prefix mask**	**Multicast Source Address / prefix mask**	**ACL Attribute**
ACI1	224.x.y.z/32	a.b.c.d/29	>Allowed
	224.x1.y1.z1/24	a1.b1.c1.d1/29	>Not Allowed
ACI2	…		

Table 4: Basic ACL Structure Example

The Multicast Group Address is the IP address of the video channel.
The Multicast Source Address is the IP address of the video server. This field is only applicable when SSM is used. In the case of ASM this field is not relevant

The Access Port (DSL line) can be identified using the Agent Circuit ID sub-option added to a DHCP or PPPoE message, and may include layer 2 information for identifying a particular ATM PVC or Ethernet VLAN on that port.

In addition, for each access port, the actual number of multicast streams can be checked at each zapping request received from a specific port.

Access Circuit	Max Simultaneous Streams
ACI1	e.g. 4
ACI2	e.g. 2
…	

Table 5: ACL with Max Simultaneous Streams

An entry is created for each customer (identified by **ACI**) that is entitled to receive multicast streams.

8 Coexistence with Element Management Systems

Network operators normally have a Network Management Centre (NMC) to manage their access network. Configuration of transmission parameters and reporting of OAM Information is usually via an Element Management System (EMS). Usually an EMS communicates with the network elements over an IP based DCN (data communication network). A common protocol for exchanging management information between EMS and network elements in transmission networks is SNMP. The management information is described in a Management Information Base (MIB).

Since the mechanism introduced with Layer 2 Control also performs element management functions, there is a need to define an appropriate means to ensure peaceful 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.

The following are general requirements for supporting multiple managers:

- **Configuration prioritization** – When two managers configure the same parameters of the same network element there must be a method to determine which of them has priority over the other in the context of the specific parameters involved;
- **Configuration integrity** – When two managers concurrently execute a configuration action the result might be an impaired configuration. When that occurs, the configuration might include a mixture of details, partially configured by the first manager and partially by the second manager. A mechanism is required that maintains configuration integrity in the presence of multiple concurrent configuration actions taking place;
- **Managers' awareness of actual configuration** – Two functions are required:
    - A mechanism for the Access Node to determine that a configuration action is completed.
    - A mechanism that, upon completing a configuration action, triggers notification messages from the Access Node to all involved element management systems and BNG managers about changes performed by one of them.

9 Requirements

9.1 General Requirements

The control channel between BNG and Access Node uses the same physical network- and routing resources as that used for customer traffic. This means that the connection is an in-band connection between the involved network elements. Therefore there is no need for an additional physical interface to establish a Layer 2 Control Channel.

The use cases described within this Technical Report require the use of a control protocol between the Access Node and the BNG. This Technical Report does not specify the protocol itself, but lists the high-level protocol requirements that must be met by the actual implementation.

R-01 The Layer 2 Control Protocol implementation MUST be based on the IETF ANCP protocol specification, defined in draft-ietf-ancp-protocol (version 04 at the time of writing this Technical Report).

9.1.1 Transportation principles for DSL aggregation

The Layer 2 Control Mechanism is intended to support both ATM and Ethernet based DSL aggregation networks. Other aggregation methods are beyond the scope of this Technical Report.

R-02 If ATM interfaces are used, encapsulation according to RFC2684 (routed) MUST be supported.

R-03 If Ethernet interfaces are used, encapsulation according to RFC894 MUST be supported.

9.1.1.1 ATM Aggregation Networks

In the case of an ATM access/aggregation network, a typical practice is to send the Layer 2 Control Messages over a dedicated Permanent Virtual Circuit (PVC) configured between the AN and the BNG. This ATM PVCs would then be given a high priority so that the ATM cells carrying the Layer 2 Control Messages are not lost in the event of congestion. It is not recommended to transport the Layer 2 Control Messages within the Virtual Path (VP) that also carries the customer connections, if that VP is configured with a best effort QoS class (e.g. Unspecified Bit Rate (UBR)). The PVCs of multiple Layer 2 Control Adjacencies can be routed into a VP that is given a high priority and runs across the aggregation network. This requires the presence of a Virtual Circuit (VC) cross-connect in the aggregation node that terminates the VP.

9.1.1.2 Ethernet Aggregation Networks

In the case of an Ethernet access/aggregation network, a typical practice is to send the Layer 2 Control Messages over a dedicated Ethernet Virtual LAN (VLAN) using a separate VLAN identifier (VLAN ID). This can be achieved using a different VLAN ID for each Access Node, or, in networks with many Access Nodes and a high degree of

aggregation, one Customer VLAN (C-VLAN) per Access Node and one Service VLAN (S-VLAN) for the Layer 2 Control Adjacencies of all Access Nodes. The traffic should be given a high priority (e.g. by using a high Class of Service (CoS) value) so that the Ethernet frames carrying the Layer 2 Control Messages are not lost in the event of congestion.
Note that these methods for transporting Layer 2 Control Messages are typical examples; they do not rule out other methods that achieve the same behavior.

9.1.2 Layer 2 Control Adjacency Requirements

R-04 The Control Protocol MUST support an adjacency protocol in order to automatically synchronize its operational state (as defined in the Adjacency definition in Section 2.3) between its peers, to agree on which version of the protocol to use, to discover the identity of its peers, and detect when they change.

R-05 The Control Protocol MUST include a mechanism to automatically detect adjacency loss.

R-06 A loss of the Layer 2 Control Adjacency MUST NOT affect subscriber connectivity.

R-07 If the Layer 2 Control Adjacency is lost, it MUST result in deterministic behavior on all network elements involved.

R-08 The Control Protocol MUST support a mechanism to synchronize access port configuration and status information between L2C peers as part of establishing or recovering the Layer 2 Control Adjacency between L2C peers.

9.2 High-Level Protocol Requirements

The following section defines a list of requirements that must be achieved by the Control Protocol itself, or by underlying protocols (e.g. a transport layer).

Functional Requirements

R-09 The Control Protocol MUST address all the use cases described in this Technical Report.

R-10 The Control Protocol MUST be general-purpose and extensible enough to support additional use cases (including the use of Access Nodes other than a DSLAM, e.g. OLT for Passive Optical Networks).

R-11 The Control Protocol MUST allow for the definition of additional protocol information elements by third-party organizations such as the Broadband Forum.

R-12 The Control Protocol interactions MUST be reliable.

R-13 The Control Protocol MUST support ”request/response” transaction-based interactions for the BNG to communicate control decisions to the Access Node,

or for the BNG to request information from the Access Node. The network elements MUST remain in a known stable state, irrespective of whether or not the transaction is successful.

In the case where the BNG wants to communicate a multiplicity of independent control decisions to the Access Node, the transaction (and notion of atomicity) applies to the individual control decisions. This avoids having to roll back all control decisions. Similarly, if the BNG wants to request multiple independent information elements from the Access Node, the notion of transaction applies to the individual information elements.

R-14 The Control Protocol MUST support sending information reports from Access Nodes, having up to several thousands of Access Ports, in real-time.

R-15 The protocol MUST be scalable enough to allow a given BNG to control at least 5000 Access Nodes.

R-16 The implementation of the Control Protocol in the BNG and Access Nodes MUST support an element management interface. This MUST allow the retrieving of statistics and alarms (e.g. via SNMP) about the operation of the Control Protocol, as well as initiating OAM operations and retrieving corresponding results.

R-17 The Control Protocol MUST support a means to handle the sending/receiving of a large burst of messages efficiently.

R-18 The Control Protocol MUST support configuring or modifying parameters associated with a particular Access Node.

R-19 The Control protocol MUST be capable of providing multicast Access Control List (ACL) information to Access Loops on an Access Node.

R-20 The Control Protocol MUST support the configuration of the maximum number of multicast groups/streams allowed to be received concurrently per Circuit ID.

R-21 The Control Protocol MUST be capable of blocking and unblocking all traffic on a specific Access Loop using the Port Configuration Mechanism.

R-22 The Control Protocol MUST be capable of configuring ACLs by the Port Configuration Mechanism. For example, such a list may include source MAC addresses and destination MAC address in order to allow/deny access to/from specific destinations.

Protocol Design Requirements

R-23 The Control Protocol MUST be simple and lightweight enough to allow an implementation on Access Nodes with limited resources (e.g. CPU and memory).

R-24 The Control Protocol MUST have an Adjacency establishment sequence to inform each peer about the protocol version and control capabilities supported (Access Node, BNG) and negotiate a common subset.

R-25 The Control Protocol MUST provide versioning support in order to allow different protocol versions to operate in the network at the same time (independently).

R-26 The Control Protocol MUST provide a "shutdown" sequence to inform its peer that the system is gracefully shutting down.

R-27 The Control Protocol MUST include a "report" model for the Access Node to spontaneously communicate to the BNG changes of states.

9.3 Redundancy

R-28 The Layer 2 Control Mechanism MUST support 1:1 BNG redundancy, using cold standby.

R-29 The Layer 2 Control Mechanism SHOULD support 1+1 BNG redundancy, using warm or hot standby

R-30 The Access Node SHOULD be able to establish and maintain a Layer 2 Control Adjacency to redundant BNGs simultaneously, and exchange Layer 2 Control state information in order to synchronize the Layer 2 Control state between these BNGs.

9.4 Access Node Requirements

9.4.1 General Architecture

The Layer 2 Control Mechanism is defined by means of a dedicated Layer 2 Control relation between the Access Node (AN) and the BNG. If one service provider has multiple physical BNG devices which represent one logical device (single edge architecture) one Access Node can be connected to more than one BNG. Therefore the physical Access Node needs to be split into virtual Access Nodes each having its own Layer 2 Control reporting and/or enforcement function.

R-31 An Access Node as a physical device can be split into logical partitions. Each partition may have its independent BNG. The Access Node MUST support at least 2 partitions. The Access Node SHOULD support 8 partitions.

R-32 One partition consists of a group of one or more DSL ports. Each physical DSL port of an Access Node MUST be assigned to only one partition.

R-33 Each AN partition MUST have a separate Layer 2 Control Adjacency to a BNG

R-34 Each AN partition MUST be able to enforce access of the controllers to their designated partitions.

R-35 When the Access Node supports IGMP processing, the AN MUST support ACL configuration using the Control Protocol.

R-36 When used as a node capable of multicast flow replication, the AN MUST be able to report the instantaneous status related to multicast flows currently replicated by the AN.

R-37 The AN MUST be able to report membership information for a particular multicast flow (i.e. Any Source Multicast (*,G) group or Source Specific Multicast (S,G) group), whenever the BNG requests it to the AN through the Layer 2 Control Mechanism.

R-38 The Access Node MUST support dynamically creating and deleting the association between an access port and a set of multicast VLANs, on receipt of an L2C message containing this mapping.

R-39 The Access Node MUST support OAM Loopback function according ITU-T I.610.

R-40 The Access Node MUST be able to be triggered by the Layer 2 Control Mechanism to send F5 end-to-end OAM Loopback cells on a given Access Port.

R-41 The Access Node MUST be able to receive looped F5 end-to-end OAM Loopback cells and to report the result using the Layer 2 Control Mechanism.

R-42 The Access Node MUST be able to determine the difference between the number of F5 end-to-end OAM Loopback cells sent and the number of Loopback cells received within a certain period of time.

R-43 The Access Node MUST be able to compare the value derived in R-42 with a configurable threshold value, in order to determine whether or not connectivity to the RG is acceptable.

R-44 The Access Node MUST send a Port Configuration Response Message declaring connectivity to the RG to be either acceptable or not, according to the determination made in R-43.

R-45 The Access Node MUST send port status information and error message elements reporting error conditions towards the BNG according to Table 3.

9.4.2 Layer 2 Control Channel Attributes

The Layer 2 Control Channel is a bidirectional IP communication interface between the controller function (in the BNG) and the reporting/enforcement function (in the Access Node). It is assumed that this interface is configured (rather than discovered) on the Access Node and the BNG.

Depending on the network topology, the Access Node can be located in a street cabinet or a central office. If an Access Node in a street cabinet installation is connected to a BNG, all user and Layer 2 Control traffic can use the same physical link. Usually, remote Access Nodes are aggregated by an aggregation network and connected to the BNG. Certain connection attributes must be supported:

R-46 The Layer 2 Control Channel MUST be able to run in-band together with the data traffic.

R-47 The Layer 2 Control Channel MUST be terminated at the Access Node (in case of cascading, the closest AN to the User Interface).

R-48 The Access Node MUST process Layer 2 Control transactions in real-time.

R-49 The Access Node SHOULD mark Layer 2 Control Messages with a high priority (e.g. VBRrt for ATM cells, p-bit 6 or 7 for Ethernet packets)

R-50 If ATM interfaces are used then any VPI and VCI value MUST be able to be used for the purpose of supporting the Layer 2 Control Channel.

R-51 If Ethernet interfaces are used then any C-VID and S-VID MUST be able to be used for the purpose of supporting the Layer 2 Control Channel.

9.4.3 Capability Negotiation Failure

R-52 In case the Access Node and BNG cannot agree on a common set of capabilities, the Access Node MUST report this to network management.

9.4.4 Adjacency Status Reporting / Synchronization

R-53 The Access Node MUST support generating an alarm to a network/element manager upon loss or malfunctioning of the Layer 2 Control adjacency with the BNG.

R-54 The Access Node MUST be able to automatically resynchronize access port configuration and status with the BNG upon re-establishing the Layer 2 Control Adjacency.

R-55 The Access Node MUST support a mechanism for forced re-synchronization of access port configuration and status information exchanged in L2C without impacting the Layer 2 Control Adjacency.

R-56 It is possible that multiple state changes happen on an Access Port while the Adjacency is down. When the Adjacency is re-established, the Access Node SHOULD send only the most recent state information of that access port to the BNG.

9.4.5 Identification

R-57 To identify the Access Node within a control domain the identifier must be unique. To identify the Access Node and the access port, a unique identifier is required per control domain. This identifier MUST be in line with the addressing scheme principles specified in Section 3.9.3/TR-101.

R-58 To allow for correlation in the BNG, the AN MUST use the same ACI format for identifying the AN and access port in L2C messages, PPPoE and DHCP messages.

9.4.6 Message Handling

R-59 The Access Node MUST be able to insert the Access Loop characteristics in the Port Status Report messages sent to the BNG.

R-60 The Access Node SHOULD be able to wait to send a Port Status Report message until the characteristics of the access port are stable for a minimum time period. This avoids sending multiple Port Status Report messages in case of several consecutive changes in that time period (e.g. due to DSL resync). In the case where the Access Node performs this process, then such a time period MUST be configurable.

R-61 The Access Node MUST send a Port Status Report message to the BNG each time the Access Port attributes change above a threshold value during the time the RG is active. This threshold SHOULD be configurable.

Note: R-61 should be considered in conjunction with R-60. In other words, R-61 only considers those changes above the configured thresholds, where the characteristics of the access port are stable.

R-62 It may happen that a DSL line becomes unstable and continues to switch between Port Up and Port Down states for a certain time period. In this case, the Access Node SHOULD inform the BNG that the line is unstable. The time period to conclude that the DSL line is unstable SHOULD be configurable. Informing the BNG about the unstable line can be done by means of a Port Status Report message.

Note: Once the instability has disappeared and the access port reaches a stable state, another Port Status Report message may be sent, as described in R-60 and R-61.

9.4.7 Parameter Control

Layer 2 Control is not designed to replace an Element Manager managing the Access Node. There are parameters in the Access Node, such as the DSL Noise Margin and DSL Power Spectral Densities (PSD), which are not allowed to be changed via the L2C Mechanism, but only via the Element Manager. This has to be ensured and protected by the Access Node.

When using the Layer 2 Control Mechanism for Access Port Configuration, the element management system needs to configure which parameters may or may not be modified using the L2C Mechanism. Furthermore, for those parameters that may be modified using the L2C Mechanism, the element management system needs to specify the default values to be used when an Access Node comes up after node recovery.

R-63 When Access Port Configuration via the Layer 2 Control Mechanism is required, the element management system MUST configure on the Access Node which parameter set(s) may be changed/controlled using the Layer 2 Control Mechanism.

9.5 BNG Requirements

9.5.1 General Architecture

R-64 The BNG MUST support the L2C Mechanism.

R-65 The BNG MUST establish L2C Adjacencies only with authorized L2C peers.

R-66 The BNG MUST support the capability to simultaneously run the Control Protocol with multiple Access Nodes in a network.

R-67 The BNG MUST be able to establish a Layer 2 Control Adjacency to a particular partition on an Access Node and control the Access Loops belonging to such a partition.

R-68 The BNG MUST support learning Access Port attributes from its peer Access Node partitions via the Layer 2 Control Mechanism, and share such information with AAA/policy servers.

R-69 The BNG MUST be able to use the actual net data rate and layer 1 and layer 2 encapsulation overhead information, sent by the AN via the Layer 2 Control Mechanism, as an input to the Hierarchical Scheduling process.

R-70 The BNG SHOULD support reducing or disabling the shaping limit used in the Hierarchical Scheduling process (cf.R-69), according to per-subscriber authorization data retrieved from a AAA or Policy Server.

R-71 The BNG MUST support reporting of Access Port attributes learned via the Layer 2 Control Mechanism to a AAA server using Broadband Forum RADIUS VSAs defined in TR-101 [2]. The DSL line attributes are defined in Table 3 of TR-101. In addition to those attributes, the following two additional attributes are relevant to the Layer 2 Control Mechanism:

- DSL Type: Defines the type of transmission system in use, amongst a list of well-known DSL technologies.
- DSL line state: The state of the DSL line (showtime, idle, silent).

R-72 The BNG MUST support configuring or deleting parameters associated with a particular Access Port on an Access Node, triggered by the AAA process.

R-73 The BNG SHOULD support dynamically configuring and re-configuring discrete service parameters for Access Ports that are controlled by the BNG. The configurable service parameters for Access Ports could be driven by local configuration on the BNG or by a policy server.

R-74 The BNG SHOULD support triggering an AN via the L2C Mechanism to execute local OAM procedures on a PVC on an Access Port that is controlled by the BNG. If the BNG supports this capability, then it MUST also support the following:

- The BNG MUST identify the Access Port on which OAM procedures need to be executed by specifying an ACI in the Request Message to the AN.

- The BNG MUST support processing and reporting of the remote OAM results learned via the L2C Mechanism.

R-75 As part of the parameters conveyed within the OAM message to the AN, the BNG SHOULD send the list of test parameters pertinent to the OAM procedure. In the case of ATM based OAM, the set of test parameters includes the number of loopbacks to be performed on the Access Port and the timeout value for the overall test. In case no test parameters are conveyed, the AN and BNG MUST use default and/or appropriately computed values (see Section 7.2.3).

R-76 After issuing an OAM request, the BNG MUST consider the request to have failed if no response is received after a certain period of time. The timeout value MUST be either the one sent within the OAM message to the AN, or the computed timeout value when no parameter was sent (see Section 7.2.3).

R-77 The BNG MUST treat subscriber session state independently from any Layer 2 Control Adjacency state. The BNG MUST NOT bring down the PPP/DCHP sessions just because the Layer 2 Control Adjacency goes down.

R-78 The BNG SHOULD internally treat L2C traffic in a timely and scalable fashion.

R-79 The BNG SHOULD support protection of L2C communication to an Access Node in the case of line card failure.

R-80 The BNG MUST be capable of using the L2 Control Mechanism to configure multicast ACLs on Access Ports on an Access Node.

R-81 The BNG MUST be capable of configuring the Access Node with the 'maximum number of multicast streams' allowed to be received concurrently per Access Port.

R-82 The BNG MUST be able to request the cessation of the delivery of a multicast group on a specified Access Port on an Access Node, using the L2 Control Mechanism.

R-83 The BNG MUST support the ability to send an L2C message towards the AN, specifying the mapping of the Access Port's ACI to the set of retail ISP multicast VLANs associated with the Access Port.

R-84 The BNG MUST be able to send an L2C message to the AN, removing any mapping between that Access Port's ACI and retail ISP multicast VLAN(s).

R-85 The BNG must support querying the AN via the L2C Mechanism to obtain information on what Access Ports are currently receiving a given multicast flow

R-86 The BNG must support querying the AN via the L2C Mechanism to obtain information on what multicast flows are currently being sent on a specific Access Port

R-87 The BNG must support querying the AN via the L2C Mechanism to obtain information on what multicast flows are currently replicated on each of the Access Ports

9.5.2 Layer 2 Control Channel Attributes

R-88 The BNG MUST mark L2C packets as high priority (e.g. appropriately set DSCP, Ethernet priority bits or ATM CLP bit) such that the aggregation network between the BNG and the AN can prioritize L2C packets over user traffic in case of congestion.

9.5.3 Capability Negotiation Failure

R-89 The BNG MUST only commence L2C information exchange and state synchronization with the AN when there is a non-empty common set of capabilities with that AN.

R-90 In case the BNG and Access Node cannot agree on a common set of capabilities, as part of the Layer 2 Control capability negotiation procedure, the BNG MUST report this to network management.

9.5.4 Adjacency Status Reporting / Synchronization

R-91 The BNG MUST support generating an alarm to a network/element manager upon loss or malfunctioning of the Layer 2 Control Adjacency with the Access Node.

R-92 The BNG MUST be able to automatically resynchronize Access Port configuration and status with the Access Node upon re-establishing the Layer 2 Control Adjacency.

R-93 The BNG SHOULD support a mechanism for forced re-synchronization of Access Port configuration and status information exchanged in L2C without impacting the Layer 2 Control Adjacency.

9.5.5 Identification

R-94 The BNG MUST support correlating L2C Messages pertaining to a given Access Port with subscriber session(s) over that port. This correlation MUST be achieved by either:

- Matching an ACI inserted by the AN in L2C Messages with corresponding ACI value received in subscriber signaling (e.g. PPPoE and DHCP) messages as inserted by the AN. The format of ACI is defined in TR-101 [2]
- Matching an ACI inserted by the AN in L2C Messages with an ACI value locally configured for a static subscriber on the BNG.

9.5.6 Message Handling

R-95 The BNG MUST protect its resources from misbehaving L2C peers.

9.5.7 Wholesale Model

R-96 In the case of wholesale access, network provider's BNG SHOULD support reporting of Access Port attributes learned from AN via the L2C Mechanism (or values derived from such attributes), to a retail provider's network gateway owning the corresponding subscriber(s).

R-97 The BNG when acting as a LAC MUST communicate generic Access Port related information to the LNS in a timely fashion.

R-98 The BNG when acting as a LAC SHOULD asynchronously notify the LNS of updates to generic Access Port related information.

R-99 In the case of L2TP wholesale, the BNG MUST support a proxy architecture that gives different providers conditional access to dedicated L2C resources on an Access Node.

R-100 In the case of L2TP wholesale, the intermediate function in the BNG as defined in R-99 MUST support a mapping function between (physical) Access Port identifiers used in the access network and (logical) Access Port identifiers used towards the LNS.

9.6 Management Related Requirements

R-101 It MUST be possible to configure the following parameters on the Access Node and the BNG:

- Parameters related to the Control Channel transport method: these include the VPI/VCI and transport characteristics (e.g. VBR-rt) for ATM networks or the C-VLAN ID and S-VLAN ID and p-bit marking for Ethernet networks;
- Parameters related to the Control Channel itself: these include the IP address of the IP interface on the Access Node and the BNG.

R-102 When the operational status of the Layer 2 Control Channel is changed (up>down, down>up) a linkdown/linkup trap SHOULD be sent towards the element management system. This requirement applies to both the AN and the BNG.

R-103 The Access Node MUST be able to use SNMP to associate individual Access Ports with specific Layer 2 Control Channel instances.

R-104 The Access Node MUST notify the element management system of L2C configuration changes in a timely manner.

R-105 The Access Node MUST provide a mechanism that allows the concurrent access on the same resource from several managers (element management system via SNMP, BNG via L2C). In the case of concurrent changes, a mechanism must exist to resolve which change is applied first.

9.7 Security Related Requirements

The following security requirements are recommended for the deployment of the L2C Mechanism within an intra-provider network. These requirements apply to the design of the L2C Mechanism rather than its protocol implementation.

R-106 The L2C Mechanism MUST provide mutual authentication between Access Node and BNG.

R-107 The L2C Mechanism MUST allow authorization to take place at the BNG and the Access Node.

R-108 The L2C Mechanism MUST be robust against denial of service attacks.

R-109 The L2C Mechanism SHOULD offer confidentiality protection using message encryption.

R-110 The L2C Mechanism SHOULD distinguish the control messages from the data.

R-111 The integrity of the L2C interactions MUST be ensured using either integrity with a separate protocol (e.g. IPSec) or by designing message integrity into the protocol.

R-112 The Access Node MUST NOT allow the sending of Layer 2 Control Messages towards the customer premises.

From an academic point of view, all traditional methods of providing security and the resulting requirements may be of interest. But from a service providers' point of view, assuming the presence of a relatively secure environment, not all threat scenarios might be applicable to such a network. For example the Man-in-the-Middle attack is a well-known kind of attack, but for a wired access network, which is a protected domain and separated from third party access, it seems rather unlikely that a Man-in the-Middle attack will occur between an Access Node and a BNG.

Only in the case of network deployments that are inter-provider does it seem appropriate that the L2C Mechanism also offers means for replay protection of messages as well as data origin authentication.

Appendix I: Zero-touch Provisioning

This appendix provides information on a zero-touch provisioning process that enables the Access Node to retrieve a DSL port configuration profile the very first time a subscriber connects to the network, i.e. without the profile data being pre-configured on the Access Node. The described behavior can be considered an extension of the concepts defined in Section 6.2 Access Port Configuration. Some of the details of such a zero-approach are not spelled out here, and are considered for further study.

Overview

The operation of the DSL port starts in a basic configuration, using a basic, pre-configured DSL configuration profile that takes into account specific parameters (e.g. the E-side electrical length (ESEL) parameter, which is dependent on the physical conditions and location of the Access Node). This profile enables simple access to the BNG for authentication only.

The first time the subscriber is successfully authenticated, the BNG collects user data and customer-specific product data, and creates a new DSL configuration profile to be used for future connectivity. This profile is either generated automatically or updated if a previous profile present on the BNG). The name of the profile is communicated via the Layer 2 Control Channel towards the Access Node.

The Access Node then retrieves the data associated with this profile by contacting a server (e.g. a AAA or Policy Server) that holds this information. To do this, the Access Node sends a request to the BNG, which in turn retrieves the information from the server and sends the profile data back to the Access Node. The details of this mechanism are not specified here. Once the Access Node has retrieved the profile data, it applies the profile on the DSL line, leading to the DSL line to resynchronize and the new profile to be activated.

When using this zero-touch approach, some form of coordination is required between the server holding the profile names and profile data, and the Access Node Element Management System (EMS). As mentioned in R-63 in section 9.4.7, the EMS configures the Access Node such that the profile data can be changed by the BNG using the Layer 2 Control Mechanism. The EMS also needs to be made aware once the new DSL configuration profile is installed on the Access Port. The details related to these interactions are not addressed here.

Port Configuration Flows

1. The DSL port synchronizes with a basic profile; the DSLAM informs the BNG that the port is up.
2. The customer on this port contacts the BNG for authentication and sets up a service session, e.g. a PPP session.

3. With a successful authentication, the AAA server provides the name of the DSL configuration profile to be applied by the Access Node on that Access Port, say profile 'abc' according to subscriber authentication.
4. The BNG sends the new profile name 'abc' to the DSLAM.
5. If the DSLAM does not have the detailed profile data available for profile 'abc', it has to request the data from a server. It does so by sending a request to the BNG. The BNG retrieves the profile data from a server (e.g. AAA or Policy Server) and sends the data for profile 'abc' to the DSLAM.
6. When the DSLAM receives profile 'abc', it applies this profile on the Access Port, which is resynchronizes according to profile 'abc'. The DSLAM then sends a Port Up message to the BNG.
7. By identifying the subscriber, the server may provide to the BNG additional parameters to be configured on the subscriber's port, e.g. VLAN ID.
8. The BNG configures these parameters on the Access Port on the DSLAM.
9. The customer is able to use the service.

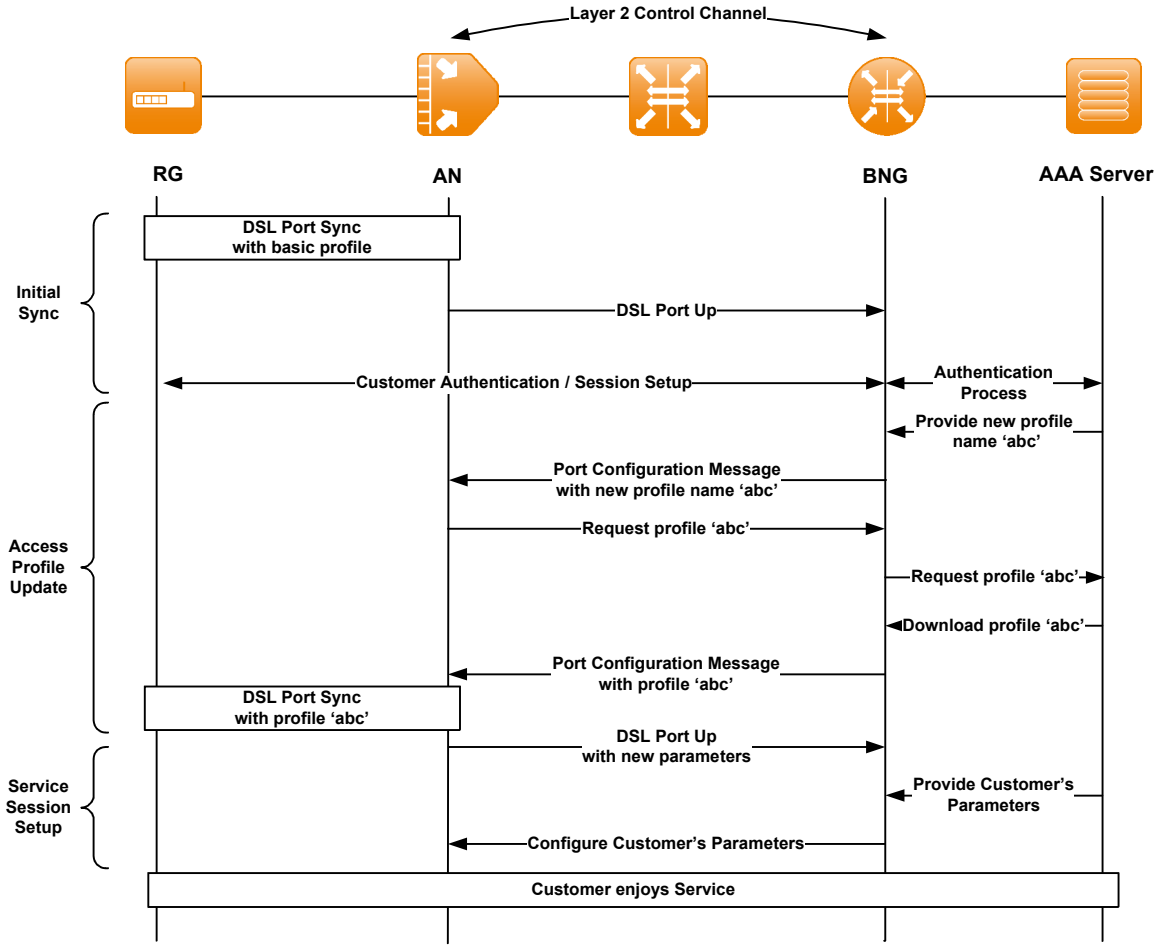

Figure 17: Access Port Configuration Flow

End of Broadband Forum Technical Report TR-147

