DSL Forum

Working Text
WT-147
Draft
Version 1.6

Layer 2 Control Mechanism For Broadband Multi-Service Architectures

13 June 2007

Produced by
Architecture and Transport Working Group

Editors:
Norbert Voigt, Nokia Siemens Networks
Sven Ooghe, Alcatel-Lucent
Michel Platnic, ECI Telecom

Chairs:
David Allan, Nortel Networks
David Thorne, British Telecom

Notice

The DSL Forum is a non-profit corporation organized to create guidelines for DSL network system development and deployment. This Working Text is a draft, and has not been approved by members of the Forum. Even if approved, this document is not binding on the DSL Forum, any of its members, or any developer or service provider. The document is subject to change. This document is protected by copyright by the DSL Forum and is for use by DSL Forum members only. Advance written permission by the DSL Forum is required for distribution of this document in its entirety or in portions outside the DSL Forum.

Version History

Version Number	Version Date	Version Editor	Changes
1.0	27 February 2006	Norbert Voigt, Siemens Sven Ooghe, Alcatel Michel Platnic, ECI	First draft
1.1	17 March 2006	Norbert Voigt, Siemens Sven Ooghe, Alcatel Michel Platnic, ECI	Revised according agreed scope.
1.2	29 September 2006	Norbert Voigt, Siemens Sven Ooghe, Alcatel Michel Platnic, ECI	Incorporated DSL2006.325.01 and DSL2006.324.02 + some agreed revisions
1.3	6 October 2006	Norbert Voigt, Siemens Sven Ooghe, Alcatel Michel Platnic, ECI	Updated according to Athens minutes: 701, 345/547, 712, 749, 714, 654, 731. Added definitions and checked consistency of terminology. Structured BNG subchapter similar to AN subchapter.
1.4	1 February 2007	Norbert Voigt, Siemens Sven Ooghe, Alcatel-Lucent Michel Platnic, ECI	Incorporated DSL2006.875.01+ updates of this contribution according to Atlanta minutes
1.5	26 April 2007	Norbert Voigt, Siemens Sven Ooghe, Alcatel-Lucent Michel Platnic, ECI	Updated according to Vancouver minutes, DSL2007.056, 059, 068, 069, 093, 125
1.6	13 June 2007	Norbert Voigt, Nokia Siemens Networks Sven Ooghe, Alcatel-Lucent Michel Platnic, ECI	Updated by DSL2007.300.01 according to minutes, of conference call on June 13th.

Technical comments or questions about this document should be directed to:

Editors: Norbert Voigt
Siemensallee 1
17489 Greifswald, Germany
Tel: +49 3834 555 771
E-Mail: norbert.voigt@nsn.com

Sven Ooghe
Copernicuslaan 50
2018 Antwerpen, Belgium
Tel: + 32 3 240 4226
E-Mail: sven.ooghe@alcatel-lucent.be

Michel Platnic
30 Hasivim Street
49517 Petakh Tikva, Israel
Tel: + 972 3 926 85 35
E-Mail: michel.platnic@ecitele.com

Table of Contents

List of Figures

Summary

In a Working Text document, this element is optional. However, it MUST be provided by the editor and agreed by the Working Group prior to approval of the Working Text.

DSL Forum Working Text WT-147
Layer 2 Control Mechanism
For Broadband Multi-Service Architecture

1 Purpose

NOTE – This document 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.

The purpose of this document 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 will ensure the transmission of the information does not need to go through distinct element managers but rather using a direct device-device communication. This allows for performing access link related operations within those network elements, while avoiding impact on the existing OSS systems.

2 Scope

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

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

This document 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 the information for e.g. QoS purposes;
- Configuration of service parameters on selected access ports. This may include physical layer service parameters (e.g. DSL sync 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 case of ATM-Ethernet interworking (cf. TR-101), or Ethernet OAM in case of an end-to-end Ethernet network;
- Communicating multicast related information between a BNG and an Access Node in order to allow, for example, centralized policy control.

2.1 Definitions

This Working Text 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. 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 northbound 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. Beyond aggregation, it is also an injection point for policy management and IP QoS in the access network.

BNG IP Edge Router where bandwidth and QoS policies may be applied.

Further, it uses the following terms:

Actual Data Rate Within this document 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 rate in L1 and L2 states.

Net Data Rate Within this document the term is used as defined by ITU-T G.993.2, cf. Table 5-1 and Figure K-10, i.e. the portion of the total data rate that can be used to transmit user information (e.g. ATM cells or Ethernet frames). It excludes overhead that pertains to the physical transmission mechanism (e.g. trellis coding in case of DSL).

Line Rate Within this document 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. Within this document only Layer 2 Control Mechanism is used, respectively its abbreviation.

Layer 2 Control Mechanism
A method for multiple network scenarios with an extensible communication scheme that conveys status and control information between one or more ANs 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), active (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.

NOTE – WT-147v1.4 contained a few occurrences of "Layer 2 Control Session". These have been renamed to "Layer 2 Control Adjacencies.

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

2.2 Abbreviations

This Working Text defines the following abbreviations:

ACI	Access Circuit Identifier
ACL	Access Control List
AN	Access Node
BNG	Broadband Network Gateway
BRAS	Broadband Remote Access Server
L2C	Layer 2 Control

2.3 Conventions

In this document, several words are used to signify the requirements of the specification. These words are often capitalized.

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.

3 References

No normative references are included in this document.

or:

The following DSL Forum Technical Reports and other references contain provisions, which, through reference in this text, constitute provisions of this Technical Report. At the time of publication, the editions indicated were valid. All Technical Reports and other 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 Technical Report and other references listed below. A list of the currently valid DSL Forum Technical Reports is published at www.dslforum.org.

NOTE – The reference to a document within this Technical Report does not give it, as a stand-alone document, the status of a Technical Report.

[1] DSL Forum TR-059 (September 2003), *DSL Evolution - Architecture Requirements for the Support of QoS-Enabled IP Services*.

[2] DSL Forum TR-101 (May 2006), *Migration to Ethernet-Based DSL Aggregation*.

4 Introduction

DSL technology is widely deployed for Broadband Access for Next Generation Networks. Several documents like DSL-Forum TR-058, DSL-Forum TR-059 and DSL Forum TR-101 describe possible architectures for these access networks.
In the scope of these specifications is the delivery of voice, video and data services.
The framework defined by this document is targeted at DSL-based access (either by means of ATM/DSL or as Ethernet/DSL).

Traditional architectures require permanent virtual circuit(s) per subscriber. Such virtual circuit is configured on layer 2 and terminated at the first layer 3 device (e.g. BRAS). Beside the data plane, the models define the architectures for element, network and service management. But due to organizational boundaries between departments operating the local loop, departments operating the ATM network, and departments operating the IP network interworking at the management plane is not always possible.
Besides, 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 service control is required, which implies a tighter coordination between Network Nodes (e.g. Access Nodes and BNG), without burdening the OSS layer with unpractical expectations. The following sub-sections will provide examples of such need.

4.1 Access Port Discovery

TR-059 identified various queuing/scheduling mechanisms to avoid congestion in the access network while dealing with multiple flows with distinct QoS requirements. Such mechanisms require that a BNG (e.g. a BRAS) gains knowledge about the access network with the various links being used and their respective rates. Some of the information required is somewhat dynamic in nature (e.g. DSL sync rate), hence cannot come from a provisioning and/or inventory management OSS system. Especially, when the subscriber line is operated in Rate Adaptive Mode (RAM) it is very important to enforce consistency of such data.

TR-101 defines the migration to Ethernet-based aggregation networks. Thus, there is no longer a “logical circuit” or “logical path” terminated on the layer 3 device (e.g. BNG), as a representation of the subscriber local loop. That creates in turn some challenges to properly configure the BNG and its hierarchical scheduler.

Dynamic and automated discovery of the access network links addresses these issues. The control plane allows the Access Node (e.g. DSLAM) to communicate to the BNG the characteristics of the access links and any corresponding updates as well as information about general Access Node capabilities.

4.2 Access Port Configuration

DSL Configuration

Following dynamic line identification (subscriber local loop) as assisted by the mechanism described in the previous sub-section (Access Port Discovery), the BNG then query a subscriber management OSS system (e.g. RADIUS server) to retrieve subscriber authorization data (service profiles, AKA user entitlement). Most of such service mechanisms are typically enforced by the BNG itself, but there are a few cases where it is useful to push such service parameter to the Access Node for local execution of a mechanism (e.g. DSL related) on the corresponding subscriber line.
Besides the configuration of physical layer service parameter the use case also comprises network layer service parameters, e.g. 802.1p scheduling configuration on the access link.

Ethernet/IP Configuration

When deploying multiple services through DSL access, it is necessary to provide different QoS levels for the different services. Additionally, services such as VoIP with real-time performance requirements require necessary end-to-end QoS strategies.
Using the Layer 2 Control Mechanism the QoS issue between BNG and Access Node can be resolved by conveying QoS attributes from the BNG to the Access Node.
Using such an approach simplifies the OSS infrastructure for service management, allowing to fully centralizing subscriber-related service data (e.g. RADIUS server back-end) and avoiding complex cross-organization B2B interactions.

4.3 Layer 2 OAM

Traditionally, ATM circuits are point-to-point connections between BNG and DSLAM/RG. In order to test the connectivity on layer 2, appropriate OAM functionality is used for operation and troubleshooting. By migrating to Ethernet-based aggregation networks (as defined by TR-101), ATM OAM functionality is not applicable.
In such a mixed Ethernet and ATM access network (including the local loop), operators requesting to keep the same ways to test and troubleshoot connectivity. Corresponding control plane functions must be envisioned. Considering existing ATM architecture an end-to-end OAM loopback is performed between the edge devices (BRAS and RG) of the broadband access network. To reach consistency in operation of a broadband access network an appropriate functionality must be implemented. A Layer 2 Control Mechanism between BNG and Access Node can close the gap which currently occurs by migrating to Ethernet, until appropriate native Ethernet OAM standard mechanisms are ratified.

From an operator's point of view and once Ethernet technology is used between the BNG and the RG similar end-to-end OAM mechanisms are desired as used to be applied by ATM OAM. Unfortunately there is no comparable data structure for Ethernet-based Access Nodes because the OAM mechanisms based on IEEE802.3ah or IEEE802.1ag are still being discussed. When Ethernet-based VDSL2 access is present, a port status test triggered by the BNG EMS and conveyed via Layer 2 Control Mechanism could be seen as workaround (cf. figure 27 of TR-101).

NOTE – Contributions on details of such a use case are solicited.

4.4 Multicast

With the rise of supporting IPTV services in a resource efficient way, multicast services are getting increasingly important. This especially holds for an Ethernet-based access/aggregation architecture. In such a model, typically IGMP is 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. DSLAM, Ethernet aggregation switch). In such a context it needs to be seen if and how the Layer 2 Control Mechanism applies to such multicast-based applications. 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.

5 General Architecture Aspects

In this section first the concept of the Layer 2 Control Mechanism is described. Then, the reference architecture is described where the Layer 2 Control Mechanism 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 5-1. 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 throughout this document.

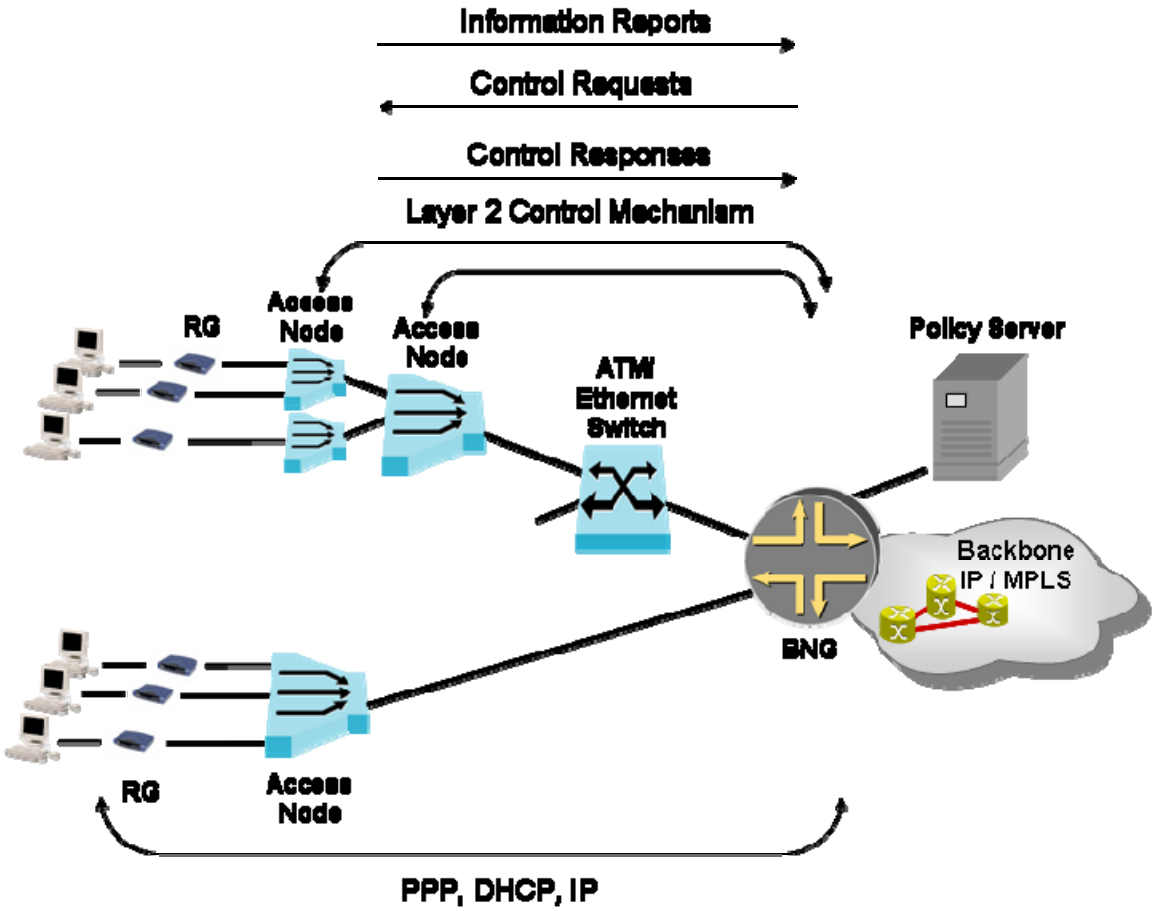


Figure 5-1: Layer 2 Control Mechanism

From a functional perspective, 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 and/or enforcement** function: the reporting function is used to convey status information to the controller function that requires the information for executing local functions. An example of this is the transmission of an access loop rate from an Access Node to a BNG tasked with shaping traffic to that rate. The enforcement function is contacted by the controller function to trigger a local action. An example of this 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 & 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 to address transition issues.

The messages in this document are described in an abstract way, independent from any actual protocol mapping. The actual protocol specification is out of scope of this document, but there are certain characteristics of the protocol required such as to simplify specification, implementation, debugging & troubleshooting, but also to be easily extensible in order to support additional use cases. This is discussed in a chapter 9.1.

5.2 Reference Architecture

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

- In 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 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 new access and aggregation technology for triple play services, the primary focus throughout this document 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 5-2.

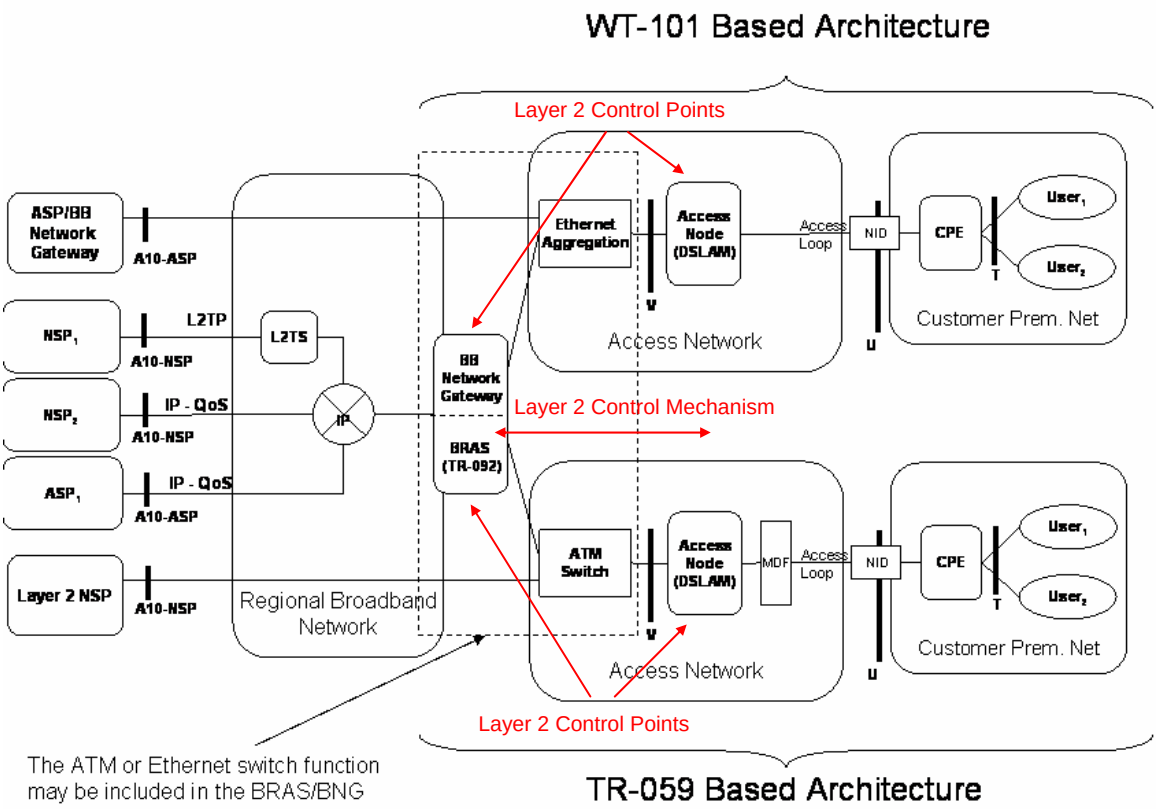


Figure 5-2: TR-059 and TR-101 Network Architecture for DSL Aggregation with Layer 2 Control Mechanism

5.2.1 The Routing Gateway (RG)

The requirements of the Routing Gateway are consistent with those detailed in TR-068 and TR-101.

5.2.2 The U interface

The U reference point is defined as the interface between the Access Network and the CPN. Encapsulation protocols and transport scenarios are described inTR-059 and TR-101.

5.2.3 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 allow them to inter-work with a common aggregation network technology. For example, an access node can support ADSL2+, VDSL2 and BPON 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 or both functions are performed at the same time.

The framework defined by this document is targeted at DSL-based access (either by means of ATM/DSL or as Ethernet/DSL). However, the framework shall be open to non-DSL technologies, like PON, FTTx and WiMAX. But this is not in scope of this document.

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

5.2.4 Access Node Deployment Options

NOTE – This section should describe how the Layer 2 Control Mechanism is to be used with Subtending Access Nodes. In such architecture, a "higher" level Access Node could proxy Layer 2 Control Messages to the "lower" Access Nodes, which terminates the messages. Contributions on the details of such a scheme are solicited.

5.2.5 The V Interface

Encapsulation protocols and transport scenarios described inTR-059 and TR-101.

5.2.6 Aggregation Network

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

5.2.7 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). 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 document.
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 existing management mechanisms remain operational as before.

Specifically when using the Layer 2 Control Mechanism for performing a *configuration* action on a network element, one gets confronted with 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. Conflicts therefore need to be avoided.

Also, when using the Layer 2 Control Mechanism for performing a *reporting* action, there is a possibility to integrate this with a Subscriber policy system that keeps track of the different subscriber related parameters (e.g. access loop bitrate).

NOTE – Contributions on these aspects are solicited.

5.3.1 Port Addressing Scheme

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

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 DSL ports. This allows the access loop 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 loop 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 TR-101.

This document 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 on the specific interworking function present in the Access Node. In some cases, no PPPoE or DHCP session may be present, while the port addressing would still be desirable.

5.4 Multicast Architecture

NOTE – Some text describing the Multicast architecture needed here.
. Contributions dslf2006.691 and dslf2006.726 on such aspects were presented, accepted for living list and need to be consolidated.

5.5 Security Aspects

Potential attacks would probably be directed to the access network in order to:

- disrupt the communication of individual subscribers, a large fraction of subscribers or within the access network itself,
- gain own profit (e.g., by modifying the QoS settings), or
- intercept subscribers-related data.

Thus, the L2C Mechanism needs to consider means to protect messages against eavesdropping, modification, injection and replay while in transit. Furthermore, it is important to prevent Access Nodes and BNGs from Denial of Service Attacks in order to protect own resources like bandwidth, processing power. In general, any impersonation has to be avoided.

In the following, potential attacks are explained in detail:

Message Modification involves integrity violations, modifying messages. Reordering, delaying, dropping, injecting, truncating, or any other modification of messages might be possible actions.

Replaying of Signaling Messages involves eavesdropping and collecting of messages first. Messages are 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 happens when a large number of messages are transmitted by a probably 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 who is able to capture all traversed 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 for traffic analysis or replay attacks. The gathered information about the network can later be used to gain unauthorized access or to alter own QoS settings.

6 Use Cases for Layer 2 Control Mechanism

6.1 Access Port Discovery

6.1.1 Overview and Motivation

In networks that use a BNG performing advanced functions like hierarchical scheduling, as required by TR-101 (same requirement exists in TR-059 for the BRAS), the BNG needs to have an accurate view of the Access Node and its line characteristics.

Line discovery function allows the BNG to perform these advanced functions without having to depend on an error-prone & possibly complex integration with an OSS system. Such a function also allows the BNG to communicate back to the Access Node service & subscriber-related line configuration parameters, alleviating the need for OSS integration with the Access Node for subscriber-related data.

In case the data rate on the subscriber line or any other link that was discovered in the access network is modified, it then maybe necessary to control and check all elements along the data path (BNG and Access Node) from which the bandwidth was discovered, 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 should be informed.

Communicating Access Loop attributes is specifically important in case the rate of the Access Loop changes overtime. 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 after the DSL sync rate has become stable.
Additionally, during the time the RG is active, data rate changes can occur due to environmental conditions (the DSL Access Loop can get "out of sync" and can retrain to a lower value, or the DSL Access Loop could use Seamless Rate Adaptation making the actual data rate fluctuate while the line is active). In this case, the Access Node sends an additional Information Report to the BNG each time the Access Loop attributes changes above a threshold value.

The use case may actually include more information than link identification and corresponding data rates, such as Interleaving Delay or Minimum and Maximum attainable rates. A more complete list of such DSL parameters can be found in Table 3 of TR-101.

6.1.2 Control Interactions

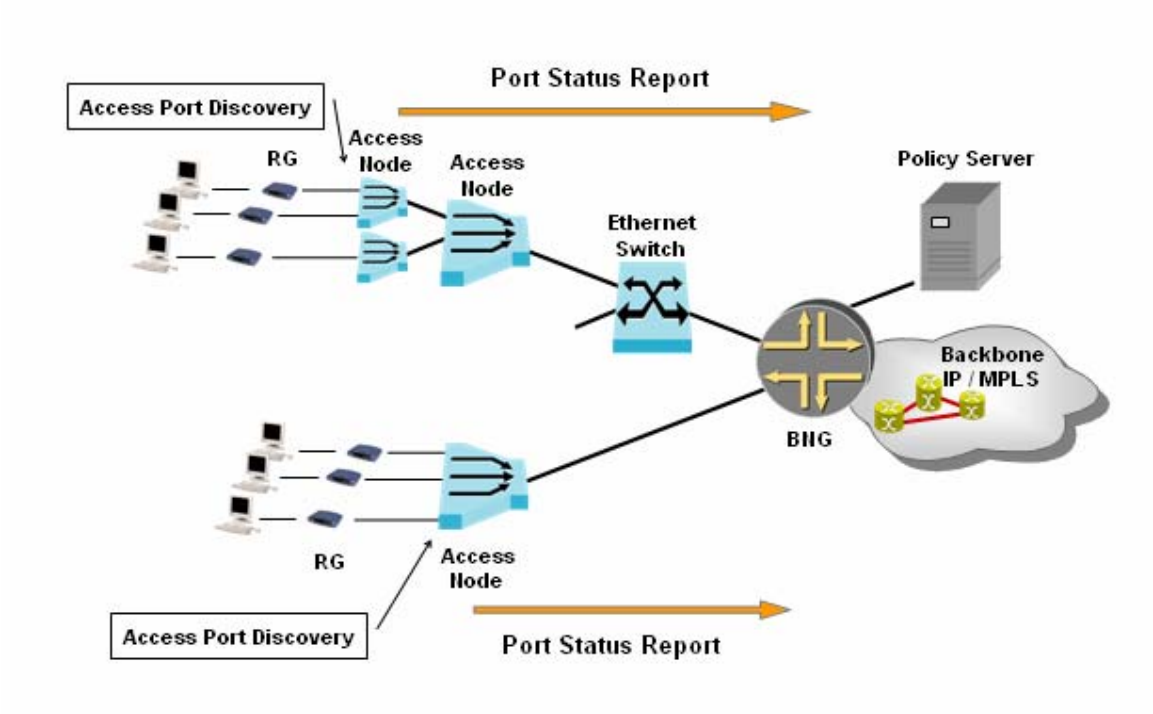


Figure 6-1: Access Port Discovery

To allow the BNG to dynamically adapt his schedulers, the Access Node informs the BNG with a Report Message when a new link is discovered or when the data rate on one of its links changes (e.g. the data rate on the subscriber line, i.e. sync rate). 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 parameters discovered are:

- Independent of layer 2 at U-interface
- Independent of layer 2 at V-interface

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 (rate) of the DSL local loop (sync rate)
- The identification and speed (rate) of the RT/Access Node link (when relevant)

The BNG can adjust downstream shaping to current subscriber line rate, and more generally re-configure the appropriate nodes of its hierarchical scheduler (support of advanced capabilities according. to TR-101).

Note: It is expected that Remote Terminals will implement such a Layer 2 Control Mechanism, and that “master” Access Nodes should be aware of RT DSL local loops and RT/Access Node

links on their behalf. The details of this functionally are, though, for future study. Contributions on such aspects are solicited.

6.2 Access Port Configuration

6.2.1 Overview and Motivation

DSL Configuration

Subscriber line rates are typically configured in a static way. If a subscriber wants to change its line rate, this requires an OPEX intensive reconfiguration of the line configuration via the network operator, possibly implying a business-to-business transaction between an ISP and an Access Provider. The defined Layer 2 Control Mechanism supports a more flexible approach for supporting "bandwidth on demand".

More generally, several service/subscriber DSL parameters (e.g. rate, inter-leaving delay) can benefit from such flexible approach to enable a "service on demand" model.

Ethernet/IP Configuration

The ETSI TISPAN NGN architecture describes session admission control functionality by means of a Resource and Admission Control Sub-System (RACS). The RACS enables the operator to configure admission control and set the respective bearer service policies. It provides the means for value-added services to obtain network resources that are necessary to offer services to the end-user.
QoS attributes of the Access Node can be configured via the L2C Mechanism by sending the information from the BNG to the Access Node.

It may be possible that a Subscriber wants to change its Access Loop rate, but that the Layer 2 Control adjacency is down. In such a case, the BNG will not be able to request the configuration change on the Access Node. The BNG should then report this failure to the OSS system, which could use application specific signaling to notify the Subscriber of the fact that the change could not be performed at this time.

6.2.2 Control Interactions

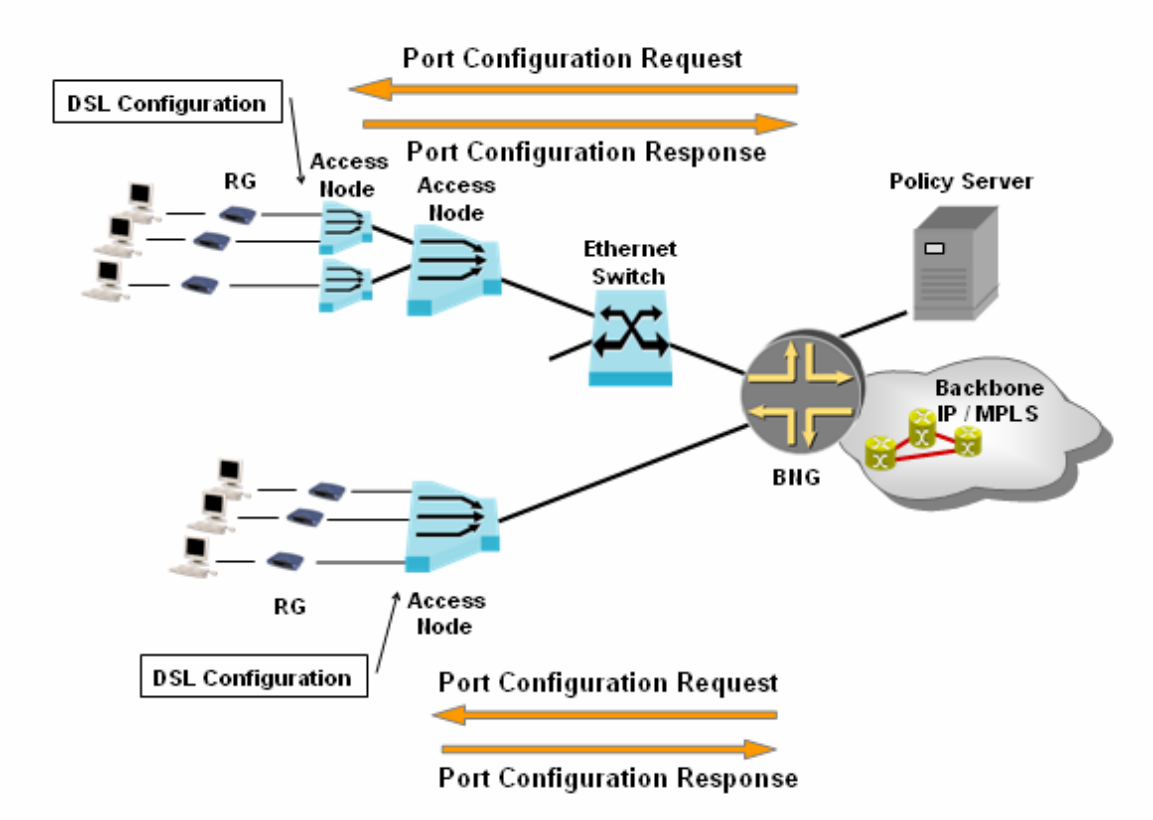


Figure 6-2: DSL Configuration

One way to change line parameters is by using profiles. These profiles (DSL profiles for different services) are pre-configured by the EMS managing 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 information reporting a new subscriber line, the BNG may send line configuration information (e.g. reference to a DSL profile) to the Access Node using a Port Configuration Request Messages. The BNG may get such line configuration data from a policy server (e.g. RADIUS). The BNG may update the line configuration due to a subscriber service change (e.g. triggered by the policy server).

The line configuration parameters are:
- Independent of layer 2 at U-interface,
- Independent of layer 2 at V-interface.

Example of sequence:
- BNG is informed by a policy server, e.g. via COPS about requested bandwidth
- BNG instructs Access Node to configure for example the line rate for a specific port
- Access Node configures line rate and informs BNG about new line rate

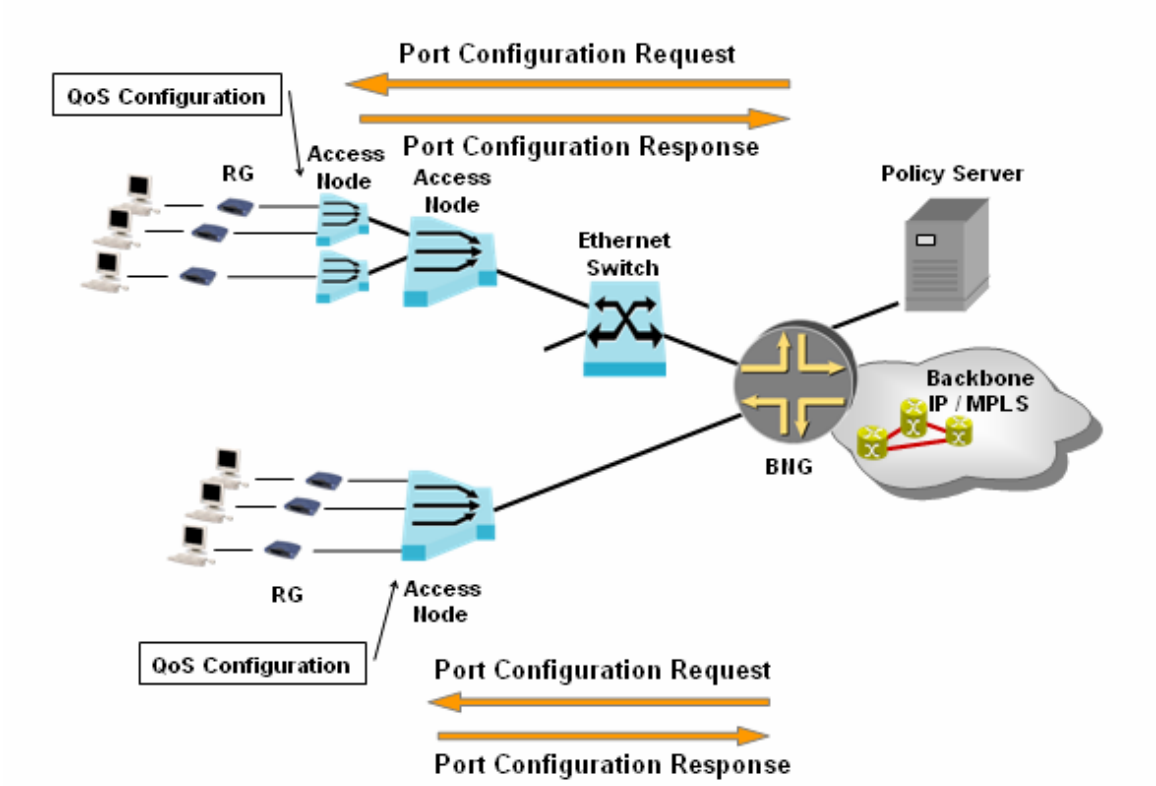


Figure 6-3: Ethernet/IP Configuration

Triggered by the subscriber's access request, the BNG authenticates the subscriber by using Radius or DHCP service. Then the BNG retrieves QoS policy information per subscriber and service from the 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.
A Port Configuration Response is sent by the Access Node to the BNG, which may notify about the configured QoS attributes.
When the subscriber terminates the service, BNG detects the service termination and notifies Access Node to release network resource and the QoS policy enforcement.

QoS Policy Configuration is

- Independent on Layer 2 at U-Interface
- Ethernet on Layer 2 at V-Interface

Sequence example:

- BNG can convey QoS attributes to the Access Node
- Access Node informs BNG about configuration result
- Access Node can release network resources dynamically

6.3 Layer 2 OAM

6.3.1 Overview and Motivation

DSL access is commonly used as a virtual leased line connection between RG and BNG. Most of existing trouble tickets are related to RG problems, so L2 OAM is primarily required to check whether the subscriber line is working correctly. In order to achieve this, the following basic requirements are to be met:

1. End to end visibility on L2 between BNG and RG (with or without a PPP or DHCP session being established)
2. Unique point to point connection between RG and BNG within layer 2 for addressing customer connection(s)
3. Use of a default Loop Back ID when addressing the connection endpoint at the RG, combined with connection ID which assigns the virtual connection between RG and BNG. This provides a unique addressing scheme for DSL connections between RG and BRAS
   (e.g. administering the RG's MAC addresses is to complex for operation in a mass market environment due to the fact that various RG's could be connected to the open U-interface)

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.
Ethernet uses a destination based forwarding paradigm whereby the destination MAC address needs to be known to verify Ethernet layer connectivity. An Ethernet loopback would verify integrity via successfully 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).
As long as there is ATM end-to-end between BNG and 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 PVC/PVP assignment. Therefore the loopback endpoint can be addressed by one default loopback location ID which is equal to all endpoints. That simplifies the operation because no administration of different subscriber specific loopback IDs is needed.

Once Ethernet technology is used between the BNG and the Access Node this end-to-end ATM OAM test can't be used, and Ethernet OAM should be used. Unfortunately there is no comparable data structure for Ethernet-based DSLAMs because the OAM mechanisms based on IEEE802.3ah or IEEE802.1ag is still being discussed. When Ethernet-based DSL access technology is present, a port status test triggered by the BNG's EMS and conveyed via a Layer 2 Control Mechanism is seen as a workaround.

6.3.2 Control Interactions

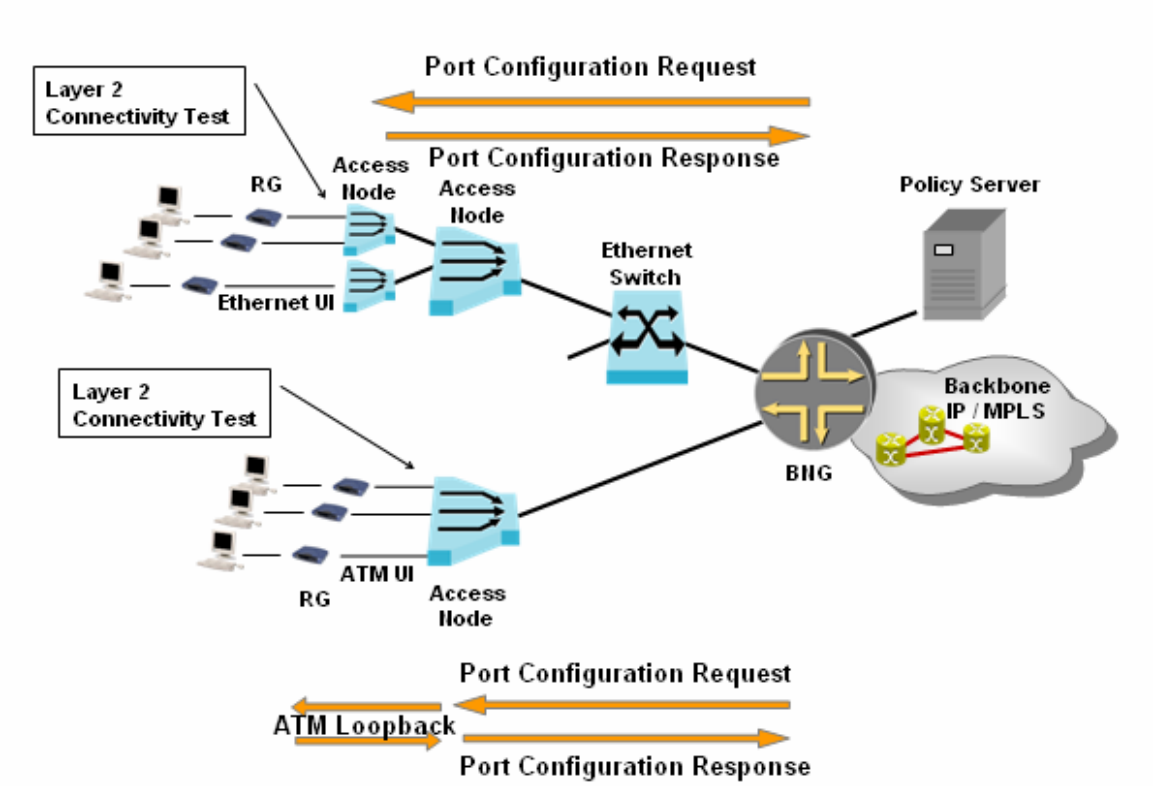


Figure 6-4: Layer 2 OAM

Triggered by a local management interface, the BNG can initiate a loop test between Access Node and DSL modem via a Layer 2 Control operation. A Port Configuration Request is sent to the Access Node, which triggers on the subscriber line (local loop) either an ATM F5 loopback test in case of ATM U-Interface or a port synchronization and admin test in case of Ethernet U-Interface. A Port Configuration Response is sent by the Access Node to the BNG, which may report results via a local management interface. Thus, the connectivity between BNG and DSL modem (RG) can be monitored by a single trigger event.

As described in chapter 6.3.1, new deployment scenarios support Ethernet transport layer end-to-end and while using RGs that do not support any loopback test capability, the Access Node may terminate the BNG's Port Configuration Request and rely on the subscriber synchronization state to answer the request.

Layer 2 connectivity test

- Supports both Ethernet and ATM Layer 2 at U-Interface
- Supports Ethernet at V-Interface
- Is irrelevant for ATM at V-Interface

Example of sequence:

- BNG can initiate ATM (or Ethernet) local loop test
- Access Node sends ATM F4/F5 OAM loopback cell in case of ATM over DSL or Access Node sends equivalent loopback frame in case of Ethernet over DSL to show DSL connectivity
- Access Node informs BNG about test result

6.4 Multicast

6.4.1 Overview and Motivation

NOTE– The first part of this paragraph could be inspired by DSL2007.056.01 – text to be proposed.

For enabling multicast at an Access Node port, an Access Control List (ACL) must be provided per AN port. The ACL must contain customer multicast related information in order to provide the end-customer permission to join dedicated IP multicast groups.

The ACL allows a network provider to authorize or deny the access of specific multicast content to a customer.

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

Entitlement information residing within the AN should be consulted at each channel request prior to delivering the stream to the Access Port.

Following are the two qualitative criteria that must be checked by AN while receiving a channel request:
Is the customer entitled to receive any multicast content?
Is the customer entitled to receive the specific multicast content he requested?

In addition, a quantitative criterion must be checked for compliancy:
Is the customer exceeding the maximum number of authorized simultaneous channels he is entitled to receive?

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

ACL Population

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

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 case of static information used to populate the ACL, the 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. 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 in 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.

6.4.2 Control Interactions

NOTE: Text and figure needed for this part.

7 Message Descriptions and Information Flows for L2C

7.1 Message Description

The following message types may exist to facilitate the exchange of this control information

1) A Boot Request Message sent by BNG or Access Node
2) A Boot Response Message
3) A Port Configuration Request Message sent by the BNG to Access Node
4) A Port Configuration Response Message that is sent in reply by the Access Node
5) A Port Status Report Message 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 may contain at least the following parameters

- <Sequence Number>
- <Holding Time>
- <Device Type>
- <Port Characteristics Capable>
- <OAM Capable>
- <Port Configuration Capable>
- <Multicast Capable>

The receiver, to foresee future extensions, must ignore unknown capabilities.

7.1.2 Boot Response Message

The Boot Response Message may contain at least the following parameters

- <Sequence Number>
- <Holding Time>
- <Device Type>
- <Port Characteristics Capable (Y/N)>
- <OAM Capable (Y/N)>
- <Port Configuration Capable (Y/N)>
- <Multicast Capable (Y/N)>

7.1.3 Access 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 are communicated

The operation is intended to be transactional in nature (performed in an atomic way; in case of failure, no change occurred on the Access Node side).
The following parameters may 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)>
- <Line Configuration Parameters | Optional>

- <OAM Test Parameters | Optional>
- <Multicast Information | Optional>

7.1.4 Access Port Configuration Response Message

An Access Node sends the Port Configuration Response Message to a BNG in reply to a Port Configuration Request Message destined to it.
The parameters of this message may include:

- <Subscriber ID>
- <Sequence No>
- <Line ID | Optional>
- <Configuration Result | Optional>
- <OAM Test Results | Optional>

While awaiting the response of a Configuration Request Message, the BNG may retransmit the requests after a certain amount of time. If no response is received after that time, the BNG should consider that the operation has failed.

7.1.5 Access Port Status Report Message

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

- After a DSL entering a stable link status (idle, silent or showtime)
- After recovery of the communication channel
- When one or more of the configured line parameters are administratively modified

The message may contain some of the following parameters:

- <Sequence No>
- <Subscriber ID | Optional>
- <DSL Parameter | 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 such link. In the case of the subscriber line, this is actually the sync rate of the DSL line. The DSL parameters above are exemplified. A more complete list can be found in Table 3 of TR-101.

7.2 Information Flows

7.2.1 Access Port Discovery

For the synchronization of a digital subscriber line, the given main parameters which are decisive, other than the current interference level, are the different DSL bitrates (actual, minimum, attainable, at low power state) upstream and downstream, and the interleaving delays (actual and maximum) upstream and downstream.
DSL as a transmission method offers two operating modes, in which digital subscriber lines can be operated.
The principles are valid for ATM-based as well as for Ethernet-based Access Nodes.
The Access Node queries the current state of the synchronization of the DSL line and sends this to the BNG. Thereupon, with the interaction with RADIUS, the setting of the BNG shapers can take place, which limits the data traffic in the downstream direction in such a manner, that no more cell loss occurs in the Access Node.
In practice the shaper is adjusted in the BNG to the maximum range of the DSL line. If the distance between Access Node and RG synchronizes itself to a smaller data rate, data packets are buffered in the Access Node and with memory overflow are rejected. Traffic, which is completed with TCP/IP, is transferred without significant data loss, since the TCP protocol contains appropriate safeguard mechanisms.
If traffic is transferred with UDP, data loss can occur if no Layer 5-7 safeguard mechanisms are used. Rejected cells/frames and the associated IP packages are then not recognized and this leads to impairments of the connection. Without Rate Adaptive Mode, data will be buffered individually according to the connection within the BNG and only whole frames will be rejected. In contrast to this, the Access Node works on an Ethernet level.

A remedy here is the realization of a control channel, which queries the current state of the synchronization of the DSL line and sends this to the BNG. Thereupon, with the interaction with RADIUS, the setting of the BNG shapers can take place, which limits the data traffic in the downstream direction in such a manner, that no more cell loss occurs in the Access Node.

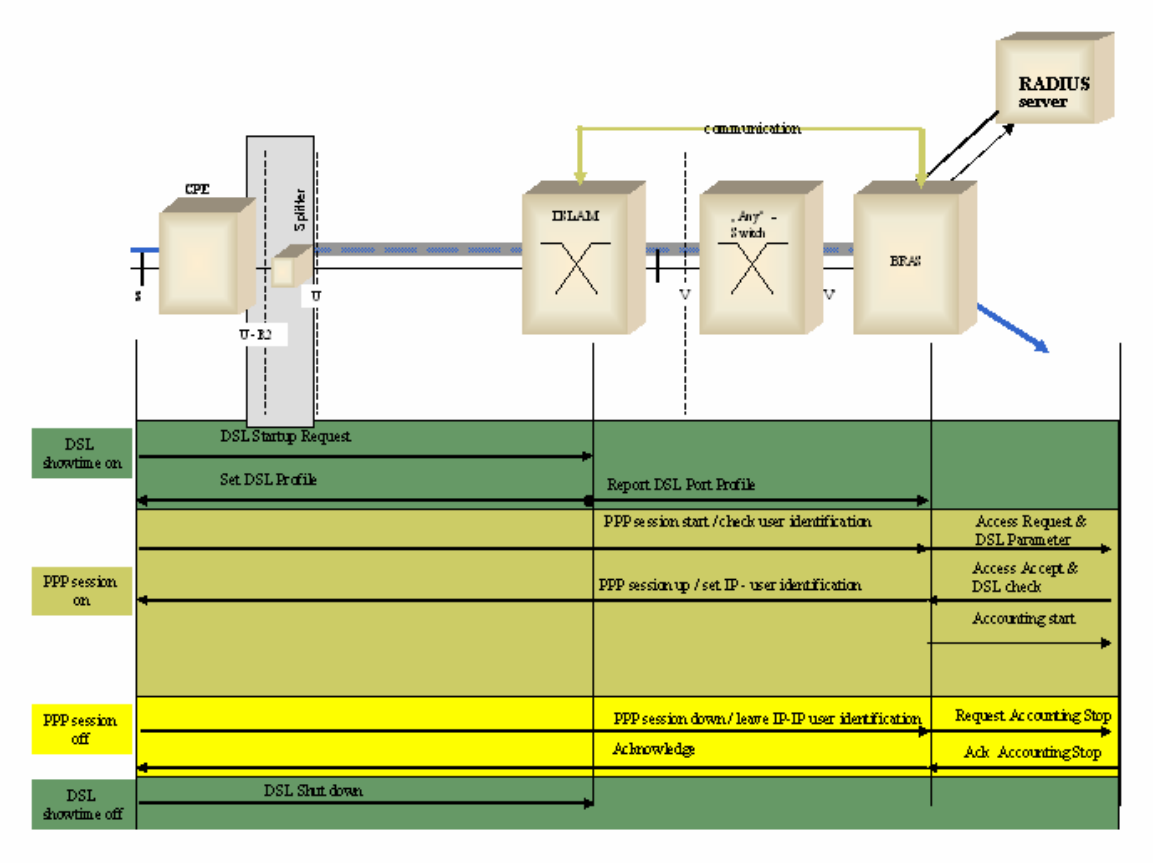


Figure 7-1: Access Port Discovery

7.2.2 Access Port Configuration

Call for contributions.
TBD

7.2.3 Layer 2 OAM

Referring to TR-101, chapter 7.4 describing requirements for an interworking in the Access Node, the following information flows show the interworking using Layer 2 Control Messages.

If Ethernet technology is to be used between BNG and Access Node, then the ATM OAM test function can no longer be used. This missing functionality on Ethernet-Basis will be made available again with the procedure described here, using the control channel.
Comparable with the ATM end-to-end Loopback function, an end-to-end connection check possibility is likewise realized with this extension. Since however – by Ethernet in the aggregation platform – this end-to-end view is lost, the control takes place in two stages. The accessibility between Access Node and BNG is guaranteed using the Layer 2 Control Mechanism.

Triggered by the BNG's EMS, the interworking function (IWF) in the Access Node will insert an ATM F5 Loopback cell at the respective DSL-Port of the Access Node. The answer of the RG is evaluated at the DSL-Port and the appropriate result is sent by a Layer 2 Control Message to BNG which passes the result to the EMS accordingly.

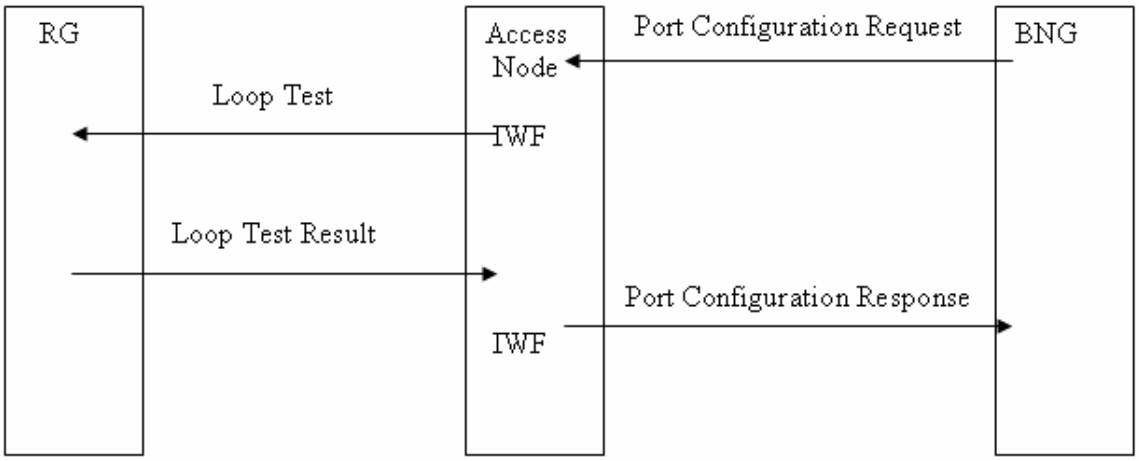


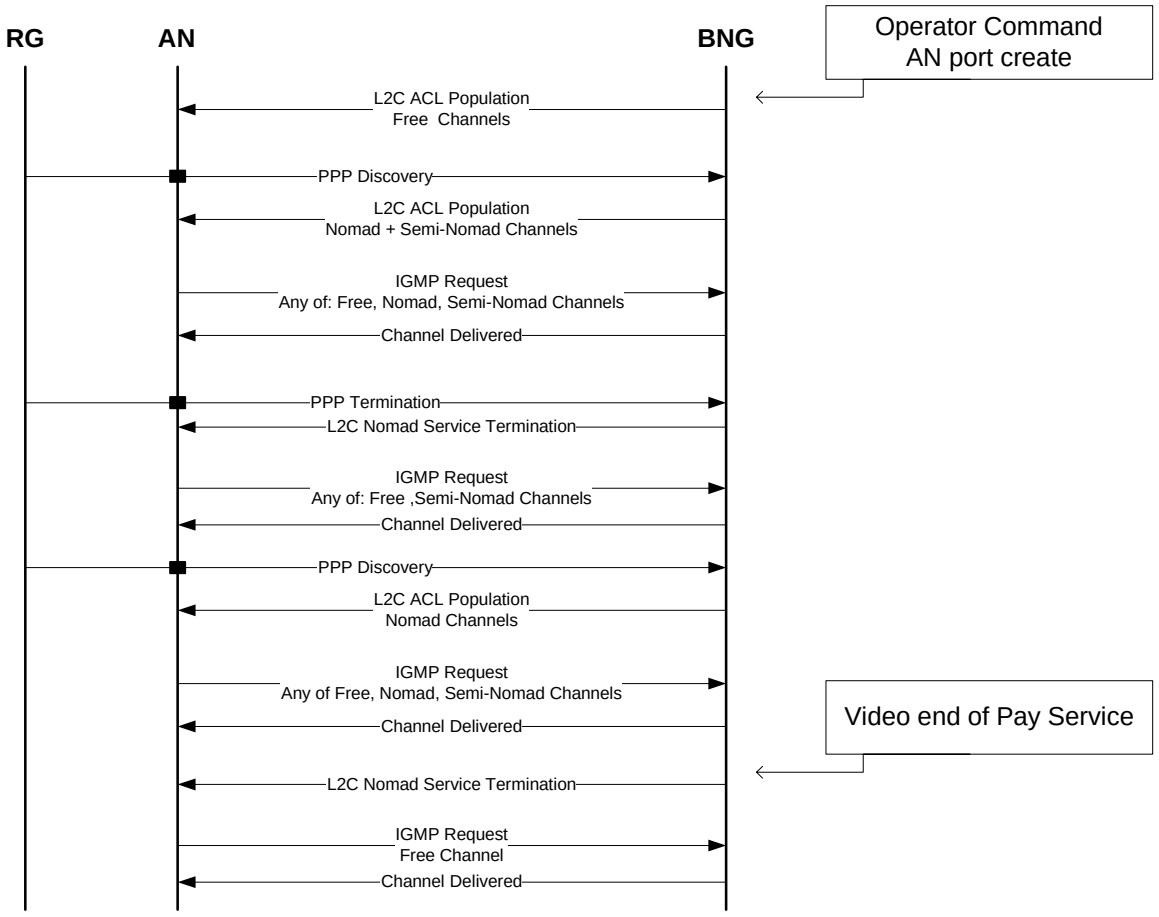
Figure 7-2: OAM with L2C triggered Loop Test

Using Ethernet between BNG and RG and assuming the RG is incapable of any loopback test or just in case the MAC address of the RG is unknown or has a bad value, a workaround is needed for testing the DSL port as long as there is no OAM mechanism based on IEEE802.3ah or IEEE802.1ag.
Also in this case the BNG can, triggered by the local management interface, initiate a loop test or a port synchronization test via Layer 2 Control operation.
A sufficient keep-alive mechanism between the BNG and the Access Node provides monitoring of the Layer 2 Control Adjacency which gives connectivity information.

7.2.4 Multicast

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, i.e. downstream.



7.3 Message Parameters

7.3.1 Access Port Discovery - xDSL Parameter

The complete set of access loop characteristics that is to be conveyed using the Access Port Discovery use case is listed in the following table:

Pos.	Message Type	Information	Reference
1	DSL Type: ADSL Transmission System	Which DSL type is in use (e.g. ADSL1, ADSL2, SDSL, ADSL2+, VDSL, VDSL2…) This parameter defines the transmission system in use	Not described ITU-T G.997.1 Section 7.5.1.1
2	DSL Port State	Port up (showtime)/ port down (idle or silent)	ITU-T G.997.1 Section 7.5.1.5
3	Actual data rate Up- and Downstream	Actual data rate upstream and downstream of a synchronized	ITU-T G.997.1 Section 7.5.2.1

		DSL port	
4	Attainable Data Rate Up- and Downstream	Maximum data rate which can be achieved.	ITU-T G.997.1 Section 7.5.1.19 and 7.5.1.20
5	Minimum Data Rate	minimum data rate desired by the operator in kbit/s (up/down)	ITU-T G.997.1 Section 7.3.2.1.1
6	Maximum Data Rate	maximum data rate desired by the operator in kbit/s. (up/down)	ITU-T G.997.1 Section 7.3.2.1.3
7	Minimum Data Rate in low power state	minimum data rate desired by the operator during the low power state (L1/L2).	ITU-T G.997.1 Section 7.3.2.1.5
8	Maximum Interleaving Delay	maximum one-way interleaving delay	ITU-T G.997.1 Section 7.3.2.2
9	Actual interleaving Delay	Value in milliseconds which corresponds to inter leaver setting.	ITU-T G.997.1 section 7.5.2.3

Table 1: Access Port parameters

Note: As required in R-54, the parameters described in the above table may have some additional attributes.

7.3.2 Access Port Configuration Parameter

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

AdminStatus:
* Blocked
* Released

For security purposes, access control list shall 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.

7.3.3 OAM Parameter

TBD

7.3.4 Multicast Parameter

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

[1] Not allowed
don't allow this stream to be sent on the access port, i.e. the Access Node will discard IGMP reports from the subscriber with the indicated group IP address.

[2] Allowed
allow this stream to be sent on the access port, i.e. the Access Node will accept IGMP reports from the subscriber with the indicated group IP address and install replication state.

Access Circuit	Multicast Group Address	Multicast Source Address	ACL Attribute
ACI1	224.x.y.z	a.b.c.d	>Allowed
	224.x1.y1.z1	a1.b1.c1.d1	>Not Allowed
ACI2	...		

Figure 3 Basic ACL structure

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 applicable when IGMPv3 SSM is used. Otherwise, (e.g. when IGMPv2 serves as the zapping protocol) 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 must be checked at each zapping request received from a specific port.

Access Circuit	Max Simultaneous Streams

ACI1	e.g. 4
ACI2	e.g. 2
...	

Figure 4: ACL with Max Simultaneous Streams

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

The 'maximum simultaneous streams' defines the maximum number of multicast streams that can be active simultaneously across a Access Circuit. It must be possible to indicate whether or not this object is used in the decision making process.

8 Interworking with Element Management Systems

Network operators are usually running a Network Control Center (NCC) to control their access network. Configuration of transmission parameters and reporting of OAM Information is done with Element Management Systems (EMS). Usually an EMS communicates with the network elements over an IP based DCN (data communication network) and handles the management of the whole 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 need to define proper means to ensure the coexistence with the existing management system. Especially, when configuration changes are performed, there is the challenge of supporting multiple managers for the same network element at the same time.

NOTE - A section should be provided regarding the specific case of the ACLs.
In case of partial updates of ACLs, management system should be synchronized.

NOTE – Contributions on these aspects are solicited.

9 Requirements

9.1 General Requirements

The control channel between BNG and Access Node uses the same physical network- and routing resources as the customer payload. This means that the connection is an inband 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 the document require the use of a control protocol between the Access Node and the BNG. This document does not specify the protocol

itself, but lists the high level protocol requirements that must be met by the actual implementation.

The IETF ANCP working group is in the process of developing the Access Node Control Protocol (ANCP) that meets the requirements listed in this document. The protocol is based on GSMPv3 [RFC 3292] and included the necessary extensions to cover the described use cases.
In the naming convention of the IETF, the BNG has the role of the controller and the Access Node represents the controlled switch.

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 recommendation.

R-01 The Layer 2 Control Mechanism MUST be defined in a way that is independent of the underlying layer 2 transport technology. Specifically, the Layer 2 Control Mechanism MUST support transmission over an ATM as well as over an Ethernet aggregation network.

R-02 The Control Protocol MUST be mapped on top of the IP network layer.

R-03 If ATM interfaces are used, encapsulation according to RFC2684 routed MUST be supported.

R-04 If Ethernet interfaces are used, encapsulation according to RFC894 MUST be supported.

9.1.1.1 ATM aggregation networks

In 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. These 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 discouraged to route the Layer 2 Control Messages within the VP that also carries the customer connections, if that VP is configured with a best effort QoS class (e.g. Unspecified Bitrate (UBR)). The PVCs of multiple Layer 2 Control Adjacencies can be routed into a Virtual Path (VP) that is given a high priority and runs across the aggregation network. This requires the presence of a VC cross-connect in the aggregation node that terminates the VP.

9.1.1.2 Ethernet aggregation networks

In 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 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-05 The Control Protocol MUST support an adjacency protocol in order to automatically synchronize states 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-06 The Control Protocol SHOULD include a "keep-alive" mechanism to automatically detect adjacency loss.

R-07 A loss of the Layer 2 Control Adjacency MUST NOT affect subscriber connectivity and element operation.

R-08 If the Layer 2 Control Adjacency is lost, it MUST NOT lead to undefined states on the network elements.

R-09 The Layer 2 Control Adjacency MUST be designed such that loss or malfunction of the adjacency is automatically detected by its peers

R-10 The Control Protocol MUST be able to recover from loss of the Layer 2 Control Adjacency (e.g. due to link or node failure) and automatically resynchronize state upon re-establishing the Layer 2 Control Adjacency.

9.2 High-Level Protocol Requirements

This 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-11 The Control Protocol MUST address all use cases described in this document, and be general-purpose and extensible enough to foresee additional use cases (including the use of other Access Nodes than Access Node, e.g. OLT for Passive Optical Networks).

R-12 The Control Protocol MUST be flexible enough to accommodate the various technologies that can be used in an access network and in the Access Node.

R-13 The Control Protocol MUST be an open protocol, either an existing protocol endorsed by an appropriate standard body (e.g. IETF) or a new protocol which will be submitted for standardization to an appropriate standard body. It must be possible for the DSL Forum to define additional protocol information elements.

R-14 The Control Protocol interactions MUST be reliable.

R-15 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. Transactions MUST be atomic, i.e. they are either fully completed, or rolled-back to the previous state.

In case the BNG wants to communicate a bulk 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 a bulk of independent information elements from the Access Node, the notion of transaction applies to the individual information elements.

R-16 The Control Protocol MUST be able to recover from access network connectivity disruption and automatically resynchronize (see also R-10 in section 9.1.2).

R-17 The Control Protocol MUST allow fast-paced transactions in order to provide real time transactions of a fully populated Access Node to the BNG.

R-18 In large-scale networks Access Nodes are provisioned but not always fully populated. Therefore the protocol MUST be scalable enough to allow a given BNG to control at least 5000 of Access Nodes.

R-19 The Control Protocol SHOULD minimize sources of configuration mismatch, help automation of the overall operation of the systems involved (Access Nodes and BNG) and be easy to troubleshoot.

R-20 The implementation of the Control Protocol in the BNG and Access Nodes MUST be manageable via an element management interface. This MUST allow to retrieve statistics and alarms (e.g. via SNMP) about the operation of the Control Protocol, as well as initiate OAM operations and retrieve corresponding results.

R-21 The Control Protocol SHOULD support a means to handle sending/receiving a large burst of messages efficiently (e.g. using “message bundling”).

R-22 The control protocol MUST be capable of providing multicast Access Control List (ACL) information to access loops on an Access Node. The ACL must contain customer multicast related information in order to provide the end-customer permission to join dedicated IP multicast groups.

R-23 The Control Protocol MUST support the configuration of the ‘maximum number of multicast groups/streams’ allowed to be received concurrently per Circuit ID.

R-24 The Control Protocol MUST support partial updates of the ACLs.

R-25 The Control Protocol MUST be capable of providing opening and closing a specific access loop by the Port Configuration Mechanism.

R-26 The Control Protocol MUST be capable of configuring access control lists 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

There might be variations on the chosen approach which would achieve similar purposes.

R-27 The Control Protocol MUST be simple and lightweight enough to allow an implementation on Access Nodes with limited control plane resources (e.g. CPU and memory).

R-28 The Control Protocol SHOULD have a "boot" sequence allowing to inform the peer about control capabilities supported by the two peers (Access Node, BNG) and negotiate a common subset (see also R-05). This sequence SHOULD be such that a system supporting the Control Protocol would automatically recognize when its peer doesn't support it at all.

NOTE - Foresee future evolutions while keeping upward compatibility (step-by-step transition from existing deployments).

R-29 The Control Protocol SHOULD include a "keep-alive" mechanism to automatically detect loss of connectivity on the access network or failure of the peer node (see also R-06).

R-30 The Control Protocol SHOULD provide a "shutdown" sequence allowing to inform the peer that the system is gracefully shutting down.

R-31 The Control Protocol SHOULD include a "report" model for the Access Node to spontaneously communicate to the BNG changes of states.

R-32 The Control Protocol MUST provide a means for the Access Node and the BNG to perform capability negotiation and negotiate a common subset.

R-33 The access loop characteristics information MUST be conveyed with a loop characteristics field structured with type-length-value sub-fields used by the protocol implementing the Layer 2 Control Mechanism. Sync data rate values MUST be encoded as 32-bit binary values, describing the rate in kbps. Interleaving delays MUST be encoded as 32-bit binary values, describing the delay in milliseconds. The complete set of sub-options is listed in table 1.

9.3 Access Node Requirements

9.3.1 General Architecture

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

R-34 An Access Node as physical device can be split in logical partitions. Each partition MAY have its independent BNG. Therefore the Access Node MUST support at least 2 partitions. The Access Node SHOULD support 8 partitions.

R-35 One partition is grouped of several DSL ports. Each physical DSL port of an Access Node MUST be assigned uniquely to one partition.

R-36 Each AN partition MUST have a separate Layer 2 Control Adjacency to a BNG and SHOULD be able to enforce access control on the controllers to only designated partitions being bound to one controller.

R-37 The Access Node SHOULD be able to work with redundant controllers.

R-38 When the Access Node supports IGMP processing, the AN MUST support per Circuit ID an Access Control List (ACL) indicating the multicast groups/streams that are allowed resp. not allowed to be sent to that port.

R-39 When the Access Node supports IGMP processing, the AN MUST support ACL configuration using the Control Protocol.

R-40 The Access Node MUST be able to control the maximum number of multicast streams that is allowed to be received concurrently per Access Circuit.

9.3.2 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.

Dependent on network topology the Access Node can be located in street cabinet or central office installation. If an Access Node in street cabinet installation is connected to a BNG all user and layer 2 control data 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-41 The Layer 2 Control Channel SHOULD use the same facilities as the ones used for the data traffic.

R-42 The Layer 2 Control Channel MUST be terminated at the Access Node (in case of cascading, the closest AN to the User Interface).

R-43 The Access Node MUST NOT support the capability to configure sending Layer 2 Control Messages towards the customer premises.

R-44 The Access Node SHOULD process Layer 2 Control transactions in a timely fashion.

R-45 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) in order for the packets not to be dropped in case of congestion.

R-46 If ATM interfaces are used VPI as well as VCI value MUST be configurable in the full range.

R-47 If Ethernet interfaces are used, C-Tag as well as S-Tag MUST be configurable in the full range.

9.3.3 Capability Negotiation Failure

R-48 In case the Access Node and BNG cannot agree on a common set of capabilities, as part of the Layer 2 Control capability negotiation procedure, the Access Node MUST report this to network management.

9.3.4 Adjacency Status Reporting

R-49 The Access Node SHOULD support generating an alarm to a network/element manager upon loss or malfunctioning of the Layer 2 Control adjacency with the BNG.

9.3.5 Identification

R-50 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 of TR-101.

R-51 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.

9.3.6 Message Handling

R-52 The Access Node MUST be able to insert the access loop characteristics in the Information Report messages sent to the BNG.

R-53 The Access Node SHOULD dampen notifications related to line attributes or line state.

9.3.7 Parameter Control

Naturally 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 EMS needs to configure on the Access Node 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 EMS needs to specify the default values to be used when an Access Node comes up after node recovery.

R-54 When Access Port Configuration via the Layer 2 Control Mechanism is required, the EMS MUST configure on the Access Node which parameter set(s) may be changed/controlled using the Layer 2 Control Mechanism.

NOTE – TBD what is configurable

9.4 BNG Requirements

9.4.1 General Architecture

R-55 The BNG MUST support the L2C Mechanism.

R-56 The BNG MUST only communicate with authorized L2C peers.

R-57 The BNG MUST support the capability to simultaneously run the Control Protocol with multiple access nodes in a network.

R-58 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-59 The BNG MUST support learning of access loop attributes, from its peer access node partitions via the Layer 2 Control Mechanism, and share such information with AAA/policy servers.

R-60 The BNG MUST support shaping traffic directed towards a particular local-loop to not exceed the DSL sync rate learnt from the AN via the Layer 2 Control Mechanism.

R-61 The BNG SHOULD support a reduction or disabling of such shaping limit, derived from Policy/Radius per-subscriber authorization data.

R-62 The BNG MUST support reporting of access loop attributes learned via the Layer 2 Control Mechanism to a Radius server using DSL-Forum Radius VSAs defined in [2]. The DSL access loop attributes are defined in Table 3 in [2]. In addition to the attributes defined in [2], 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)

NOTE –work out the RADIUS VSA encoding for the above additional two information elements.

R-63 The BNG MUST correlate layer 2 configuration data with the RADIUS authorization process and related subscriber data.

R-64 The BNG SHOULD support shaping traffic directed towards a particular access loop to include layer-1 and layer-2 encapsulation overhead information received for a specific access loop from the AN via the L2C Mechanism.

R-65 The BNG SHOULD support dynamically configuring and re-configuring discrete service parameters for access loops that are controlled by the BNG. The configurable service parameters for access loops could be driven by local configuration on the BNG or by a radius/policy server.

[Editor's Note: Call for contribution, since the use case of the requirement above is not yet described.]

R-66 The BNG SHOULD support triggering an AN via the L2C Mechanism to execute local OAM procedures on an access loop that is controlled by the BNG. If the BNG supports this capability, then it MUST further support the following:

- The BNG MUST identify the access loop on which OAM procedures need to be executed by specifying an ACI in the Request Message to the AN.
- The BNG SHOULD support processing and reporting of the remote OAM results learned via the L2C Mechanism.

R-67 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. The AN will then execute the OAM procedure on the specified access loop according to the specified parameters. In case no test parameters are conveyed, the AN and BNG MUST use default and/or appropriately computed values.

R-68 After issuing an OAM request, the BNG will consider the request to have failed if no response is received after a certain period of time. The timeout value SHOULD be either the one sent within the OAM message to the AN, or the computed timeout value when no parameter was sent.

The exact set of test parameters mentioned above depends on the particular OAM procedure executed on the access loop. An example of a set of test parameters is the number of loopbacks to be performed on the access loop and the timeout value for the overall test. In this case, and assuming an ATM based access loop, the default value for the timeout parameter would be equal to the number of F5 loopbacks to be performed, multiplied by the F5 loopback timeout (i.e. 5 seconds per the ITU-T I.610 standard).

R-69 The BNG MUST treat subscriber session state independently from any Layer2 Control Adjacency state. The BNG MUST NOT bring down the PPP/DCHP sessions just because the Layer 2 Control Adjacency goes down.

R-70 The BNG SHOULD internally treat L2C traffic in a timely and scalable fashion.

R-71 The BNG SHOULD support protection of L2C communication to an access node in case of line card failure.

R-72 When the BNG is used in conjunction with an Access Node supporting IGMP processing, the BNG MUST be capable of configuring the Access Node with which multicast groups/streams are allowed resp. not allowed to be sent to a particular Access Circuit.

R-73 The BNG MUST be capable of using the L2 Control Mechanism to configure multicast ACLs on access loops on an Access Node.

R-74 The BNG MUST be capable of configuring the Access Node with the 'maximum number of multicast streams' allowed to be received concurrently per Access Circuit.

R-75 The BNG MUST be able to request the cessation of the delivery of a multicast group on a specified access loop on an Access Node, using the L2 Control Mechanism.

9.4.2 Layer 2 Control Channel Attributes

R-76 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.

9.4.3 Capability Negotiation Failure

R-77 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-78 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.

9.4.4 Adjacency Status Reporting

R-79 The BNG SHOULD support generating an alarm to a network/element manager upon loss or malfunctioning of the Layer 2 Control adjacency with the Access Node.

9.4.5 Identification

R-80 The BNG MUST support correlating L2C Messages pertaining to a given access loop with subscriber session(s) over that access loop. 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 [2]
- Matching an ACI inserted by the AN in L2C Messages with an ACI value locally configured for a static subscriber on the BNG.

9.4.6 Message Handling

R-81 The BNG SHOULD protect its resources from misbehaved L2C peers by providing a mechanism to dampen information related to an access node partition.

9.4.7 Wholesale Model

R-82 In case of wholesale access, network provider's BNG SHOULD support reporting of access loop 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-83 The BNG when acting as a LAC MUST communicate generic access line related information to the LNS in a timely fashion.

R-84 The BNG when acting as a LAC MAY asynchronously notify the LNS of updates to generic access line related information.

R-85 In 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.

9.5 AAA Server Requirements

TBD
call for contributions

9.6 Management Related Requirements

R-86 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-87 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 EMS. This requirement applies to both the AN and the BNG.

R-88 The Access Node MUST provide the possibility using SNMP to associate individual DSL lines with specific Layer 2 Control Channel instances.

R-89 The Access Node MUST notify the EMS in a timely manner of L2C configuration changes.

R-90 The Access Node MUST provide a mechanism that allows the concurrent access on the same resource from several managers (EMS via SNMP, BNG via L2C). Only one manager may perform a change at a certain time.

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-91 The L2C Mechanism MUST provide mutual authentication between Access Node and BNG.

R-92 The L2C Mechanism MUST allow authorization to take place at the BNG and the Access Node.

R-93 The L2C Mechanism MUST be robust against denial of service attacks.

R-94 The L2C Mechanism SHOULD offer confidentiality protection using message encryption.

R-95 The L2C Mechanism SHOULD distinguish the control messages from the data.

R-96 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-97 For security purposes, the Layer 2 Control Messages sent over the channel MUST NOT be sent towards the customer premises.

From an academical point of view, all methods of traditional security considerations and the resulting requirements should be reflected on. But from service providers' point of view, who relies on a relatively secured 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, it seems appropriate that the L2C Mechanism also offers means for replay protection of messages as well as to offer data origin authentication.