Internet Engineering Task Force (IETF)
Request for Comments: 7256
Updates: 6320
Category: Standards Track
ISSN: 2070-1721

F. Le Faucheur
R. Maglione
Cisco
T. Taylor
Huawei

July 2014

Multicast Control Extensions for the Access Node Control Protocol (ANCP)

Abstract

This document specifies the extensions to the Access Node Control Protocol (ANCP) (RFC 6320) required for support of the multicast use cases defined in the Access Node Control Protocol framework document (RFC 5851) and one additional use case described in this document. These use cases are organized into the following ANCP capabilities:

- multicast replication initiated by the Network Access Server (NAS);
- conditional access and admission control with white and black lists;
- conditional access and admission control with grey lists;
- bandwidth delegation; and
- committed bandwidth reporting.

These capabilities may be combined according to the rules given in this specification.

This document updates RFC 6320 by assigning capability type 3 to a capability specified in this document and by changing the starting point for IANA allocation of result codes determined by IETF Consensus from 0x100 to 0x64.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.
Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc7256.

Table of Contents

1. Introduction 5
   1.1. A Note on Scope 7
2. Terminology 7
3. Multicast Use Cases 7
   3.1. NAS-Initiated Multicast Replication Control Use Case 8
      3.1.1. Goals 8
      3.1.2. Message Flow 9
   3.2. Conditional Access and Admission Control Use Case 9
      3.2.1. Goals 9
      3.2.2. Message Flow 10
   3.3. Multicast Flow Reporting Use Case 11
      3.3.1. Goals 11
      3.3.2. Message Flow 11
   3.4. Committed Bandwidth Reporting Use Case 11
      3.4.1. Goals 11
      3.4.2. Message Flow 12
4. ANCP Messages 13
   4.1. Provisioning Message 13

4.1.1. Sender Behavior 14
4.1.2. Receiver Behavior 14
4.2. Port Management Message 15
4.2.1. Sender Behavior 16
4.2.2. Receiver Behavior 16
4.3. Multicast Replication Control Message 17
4.3.1. Sender Behavior 21
4.3.2. Receiver Behavior 21
4.4. Multicast Admission Control Message 24
4.4.1. Sender Behavior 25
4.4.2. Receiver Behavior 26
4.5. Bandwidth Reallocation Request Message 27
4.5.1. Sender Behavior 28
4.5.2. Receiver Behavior 28
4.6. Bandwidth Transfer Message 31
4.6.1. Sender Behavior 32
4.6.2. Receiver Behavior 32
4.7. Delegated Bandwidth Query Request Message 34
4.7.1. Sender Behavior 34
4.7.2. Receiver Behavior 34
4.8. Delegated Bandwidth Query Response Message 34
4.8.1. Sender Behavior 35
4.8.2. Receiver Behavior 35
4.9. Multicast Flow Query Request and Response Messages 36
4.9.1. Sender Behavior 36
4.9.2. Receiver Behavior 37
4.10. Committed Bandwidth Report Message 38
4.10.1. Sender Behavior 38
4.10.2. Receiver Behavior 39
5. ANCP TLVs For Multicast 39
5.1. Multicast-Service-Profile TLV 39
5.2. Multicast-Service-Profile-Name TLV 41
5.3. List-Action TLV 41
5.4. Sequence-Number TLV 44
5.5. Bandwidth-Allocation TLV 45
5.6. White-List-CAC TLV 45
5.7. MRepCtl-CAC TLV 46
5.8. Bandwidth-Request TLV 46
5.9. Request-Source-IP TLV 47
5.10. Request-Source-MAC TLV 48
5.11. Request-Source-Device-Id TLV 48
5.12. Multicast-Flow TLV 49
5.13. Report-Buffering-Time TLV 50
5.14. Committed-Bandwidth TLV 51
6. Multicast Capabilities 51
6.1. Required Protocol Support 52
6.1.1. Protocol Requirements for NAS-Initiated Multicast Replication 52

6.1.2. Protocol Requirements for Committed Multicast Bandwidth Reporting 54
6.1.3. Protocol Requirements for Conditional Access and Admission Control with White and Black Lists 55
6.1.4. Protocol Requirements for Conditional Access and Admission Control with Grey Lists 56
6.1.5. Protocol Requirements for Bandwidth Delegation 57
6.2. Capability-Specific Procedures for Providing Multicast Service 57
6.2.1. Procedures for NAS-Initiated Multicast Replication 58
6.2.2. Procedures for Committed Bandwidth Reporting 58
6.2.3. Procedures for Conditional Access and Admission Control with Black and White Lists 59
6.2.4. Procedures for Conditional Access and Admission Control with Grey Lists 61
6.2.5. Procedures for Bandwidth Delegation 63
6.3. Combinations of Multicast Capabilities 64
6.3.1. Combination of Conditional Access and Admission Control with White and Black Lists and Conditional Access and Admission Control with Grey Lists 64
6.3.2. Combination of Conditional Access and Admission Control with Bandwidth Delegation 65
6.3.3. Combination of NAS-Initiated Replication with Other Capabilities 65
6.3.4. Combinations of Committed Bandwidth Reporting with Other Multicast Capabilities 66
7. Miscellaneous Considerations 66
7.1. Report Buffering Considerations 66
7.2. Congestion Considerations 67
8. Security Considerations 67
9. IANA Considerations 69
10. Acknowledgements 72
11. References 73
11.1. Normative References 73
11.2. Informative References 73
Appendix A. Example of Messages and Message Flows 75
A.1. Provisioning Phase 75
A.2. Handling Grey-Listed Flows 81
A.3. Handling White-Listed Flows 87
A.4. Handling of Black-Listed Join Requests 92
A.5. Handling of Requests to Join and Leave the On-Line Game 92
A.6. Example Flow for Multicast Flow Reporting 95

1. Introduction

[RFC5851] defines a framework and requirements for an Access Node (AN) control mechanism between a Network Access Server (NAS) and an Access Node (e.g., a Digital Subscriber Line Access Multiplexer (DSLAM)) in a multi-service reference architecture in order to perform QoS-related, service-related, and subscriber-related operations. [RFC6320] specifies a protocol for Access Node Control in broadband networks in line with this framework.

[RFC6320] supports, specifically for DSL access, three use cases defined in [RFC5851]: the Topology Discovery use case, the Line Configuration use case, and the Remote Connectivity Test use case. However, it does not support the multicast use cases defined in [RFC5851]. The present document specifies the extensions to the Access Node Control Protocol required for support of these multicast use cases. In addition, it supports the Committed Bandwidth Reporting use case, described below. In terms of ANCP, these use cases are organized into five capabilities:

- NAS-initiated multicast replication;
- conditional access and admission control with white and black lists;
- conditional access and admission control with grey lists;
- bandwidth delegation; and
- committed bandwidth reporting.

NAS-initiated multicast replication assumes that multicast join and leave requests are terminated on the NAS or that the NAS receives requests to establish multicast sessions through other means (e.g., application-level signaling). The NAS sends commands to the AN to start or stop replication of specific multicast flows on specific subscriber ports. This use case is described briefly in the next-to-last paragraph of Section 3.4 of [RFC5851].

Conditional access is described in Section 3.4.1 of [RFC5851]. Section 3.4.2.2 of [RFC5851] mentions a way in which conditional access can be combined with admission control to allow best-effort multicast flows, and Section 3.4.2.3 points out the necessary conditions for using both conditional access and admission control.

In the case of "conditional access and admission control with white and black lists", multicast join and leave requests are terminated at the AN and accepted or ignored in accordance with the direction

provided by white and black lists, respectively. The white and black lists are provisioned per port at startup time and may be modified thereafter. The NAS may combine conditional access with admission control of white-listed flows by appropriate provisioning.

Conditional access and admission control with grey lists is similar to conditional access and admission control with white lists, except that before accepting any request matching a grey list entry, the AN sends a request to the NAS for permission to replicate the flow. Again, the NAS can enable admission control of grey-listed flows at the AN.

Bandwidth delegation is described in Section 3.4.2.1 of [RFC5851]. It allows flexible sharing of total video bandwidth on an access line between the AN and the NAS. One application of such bandwidth sharing is where the AN does multicast admission control, while the NAS or Policy Server does unicast admission control. In that case, bandwidth delegation allows dynamic sharing of bandwidth between unicast and multicast video traffic on each access line.

Committed bandwidth reporting is described in Section 3.4. The AN reports the amount of multicast bandwidth it has granted to a given access line each time that value changes. These reports may be buffered for a NAS-provisionable interval so that reports for multiple access lines can be bundled into the same message.

The formal specification of the behaviors associated with each of these capabilities, singly and in combination, is given in Section 6.

In addition to the multicast service processing behavior just sketched, the definition of each capability includes support for the multicast accounting and reporting services described in Section 3.4.3 of [RFC5851]. Because of this common content and because of other protocol overlaps between the different capabilities, the protocol descriptions for the multicast extensions specified in this document are merged into a single non-redundant narrative. Tables in Section 6 then indicate the specific sub-sections of the protocol description that have to be implemented to support each capability.

This document updates RFC 6320 by assigning capability type 3 to the NAS-initiated multicast replication capability and by changing the starting point for IANA allocation of result codes determined by IETF Consensus from 0x100 to 0x64.

1.1. A Note on Scope

The requirements in [RFC5851] were formulated with the IPTV application in mind. Two basic assumptions underlie the use case descriptions:

- that the Home Gateway operates in bridged mode, and
- that multicast signaling uses IGMP ([RFC2236] [RFC3376]) or Multicast Listener Discovery (MLD) [RFC3810] rather than PIM [RFC4601].

Without the first assumption the AN may lose sight of individual subscriber devices making requests for multicast service. This has a very minor effect on the capabilities described below but prevents the application of per-device policies at the NAS. Changing the second assumption would require that, in applications where the AN is responsible for snooping IGMP and MLD, it now also monitors for PIM signaling. The capabilities described in the present document do not depend explicitly on what type of multicast signaling is used, but the multiple phases of PIM setup could add complexity to their implementation.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

This document uses the terms "connection admission control" ("CAC" or simply "admission control") and "conditional access" as they are used in [RFC5851].

The expression "delegated bandwidth" is used as a shorter way of saying: "the total amount of video bandwidth delegated to the AN for multicast admission control".

3. Multicast Use Cases

Quoting from [RFC5851]:

> ... the Access Node, aggregation node(s), and the NAS must all be involved in the multicast replication process. This prevents several copies of the same stream from being sent within the access/aggregation network. In case of an Ethernet-based access/aggregation network, this may, for example, be achieved by means of IGMP snooping or IGMP proxy in the Access Node and aggregation node(s).

By introducing IGMP processing in the access/aggregation nodes, the multicast replication process is now divided between the NAS, the aggregation node(s), and Access Nodes. In order to ensure backward compatibility with the ATM-based model, the NAS, aggregation node, and Access Node need to behave as a single logical device. This logical device must have exactly the same functionality as the NAS in the ATM access/aggregation network. The Access Node Control Mechanism can be used to make sure that this logical/functional equivalence is achieved by exchanging the necessary information between the Access Node and the NAS.

[RFC5851] describes the use cases for ANCP associated with such multicast operations and identifies the associated ANCP requirements. This section describes a subset of these use cases as background to facilitate reading of this document, but the reader is referred to [RFC5851] for a more exhaustive description of the ANCP multicast use cases. Detailed example message flows can also be found in Appendix A.

In the diagrams below, participation of the Home Gateway is optional, depending on whether it is operating in bridged or routed mode. Note that devices behind the Home Gateway may require the Home Gateway to operate in routed mode to ensure that they can obtain access to non-IPTV multicast services.

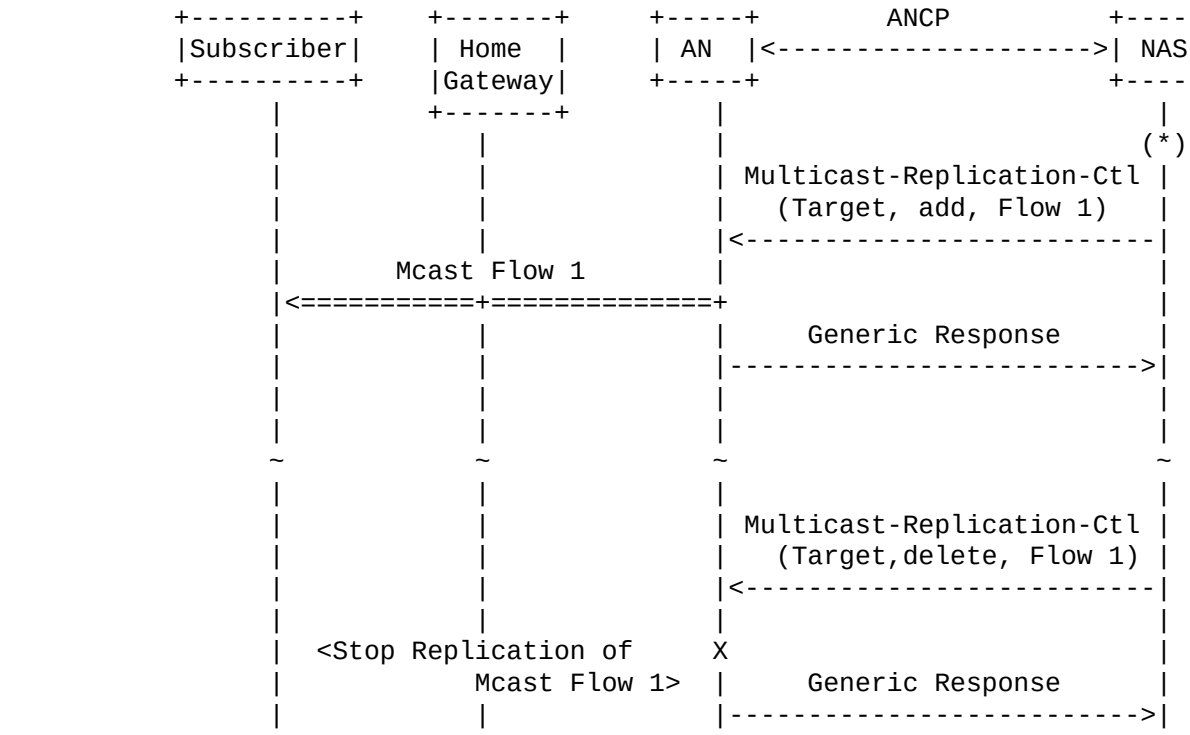
3.1. NAS-Initiated Multicast Replication Control Use Case

3.1.1. Goals

One option for multicast handling is for the subscriber to communicate the join/leave information to the NAS. This can be done, for instance, by terminating all subscriber IGMP ([RFC3376]) or MLD ([RFC2710] [RFC3810]) signaling on the NAS. Another example could be a subscriber using some form of application-level signaling, which is redirected to the NAS. In any case, this option is transparent to the access and aggregation network. In this scenario, the NAS uses ANCP to create and remove replication state in the AN for efficient multicast replication. Thus, the NAS only sends a single copy of the multicast stream towards the AN, which, in turn, performs replication to multiple subscribers as instructed by the NAS via ANCP. The NAS performs conditional access and admission control when processing multicast join requests and only creates replication state in the AN if admission succeeds.

3.1.2. Message Flow

With the NAS-initiated use case, a Multicast Replication Control message is sent by the NAS to the AN with a directive to either join or leave one (or more) multicast flow(s). In the example message flow, the AN uses a Generic Response message to convey the outcome of the directive. Figure 1 illustrates such an ANCP message exchange as well as the associated AN behavior.



(*) The NAS may optionally seek direction from an external Authorization/Policy Server before admitting the flow.

Figure 1: NAS-Initiated Multicast Replication Control

3.2. Conditional Access and Admission Control Use Case

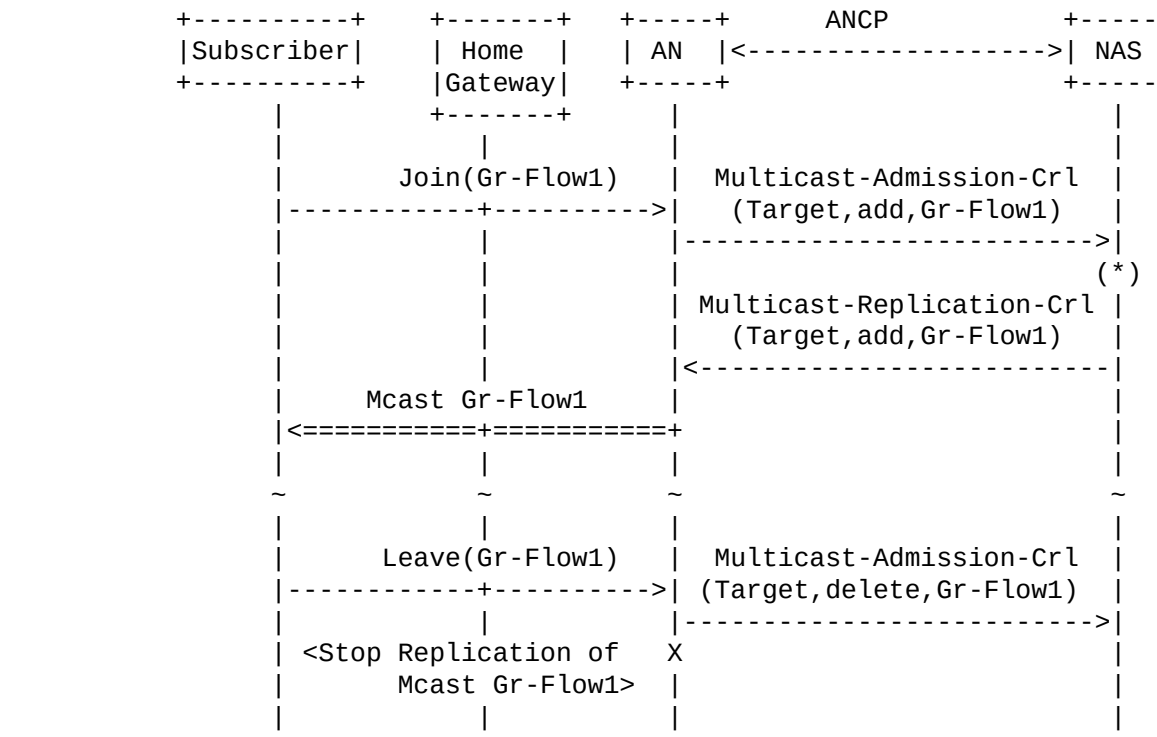
3.2.1. Goals

One option for multicast handling is for the access/aggregation nodes to participate in IGMP/MLD processing (e.g., via IGMP/MLD snooping). In this scenario, on detecting a join/leave request from an end user for a multicast flow (in the grey list), the AN uses ANCP to request a conditional access and admission control decision from the NAS. In turn, after conditional access and admission control checks, the NAS

uses ANCP to instruct the AN to change the replication states accordingly.

3.2.2. Message Flow

For support of the conditional access and admission control use case, on detection of an IGMP/MLD join request, the AN sends a Multicast Admission Control message to the NAS to request a conditional access and admission control check. In the case of a positive outcome, the NAS sends a Multicast Replication Control message to the AN with a directive to replicate the multicast flow to the corresponding user. Similarly, on detection of an IGMP/MLD leave, a Multicast Admission Control message is sent by the AN to the NAS to keep the NAS aware of user departure for the flow. This message flow is illustrated in Figure 2.



Gr-Flow1: a multicast flow matching the grey list for that port

(*) The NAS may optionally seek direction from an external Authorization/Policy Server before admitting the flow.

Figure 2: Multicast Conditional Access and Admission Control

3.3. Multicast Flow Reporting Use Case

3.3.1. Goals

The multicast flow reporting use case allows the NAS to asynchronously query the AN to obtain an instantaneous status report related to multicast flows currently replicated by the AN.

3.3.2. Message Flow

The NAS sends a Multicast Flow Query Request message to the AN in order to query the AN about information such as which multicast flows are currently active on a given AN port or which ports are currently replicating a given multicast flow. The AN conveys the requested information to the NAS in a Multicast Flow Query Response message. This message flow is illustrated in Figure 3.

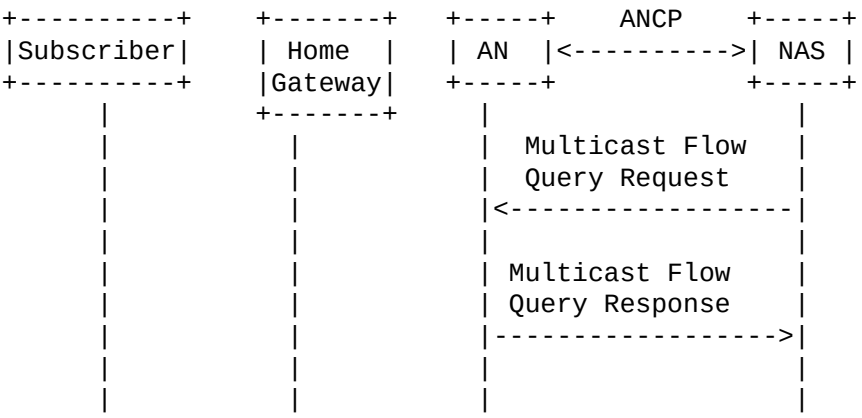


Figure 3: Multicast Flow Reporting

3.4. Committed Bandwidth Reporting Use Case

3.4.1. Goals

The committed bandwidth reporting use case allows the NAS to maintain current awareness of how much multicast bandwidth the AN has committed to a given access line, so that the NAS can adjust its forwarding scheduler to ensure the associated QoS. Note that this involves a finer level of detail than provided by bandwidth delegation, since the amount of delegated bandwidth is an upper limit on the amount of bandwidth committed rather than an actual value. To reduce the volume of messaging, reports from the AN may be buffered so that one message reports on changes for multiple access lines.

3.4.2. Message Flow

The message flow associated with this use case is shown in Figure 4. The figure assumes that a non-zero buffering interval was previously provisioned on the AN.

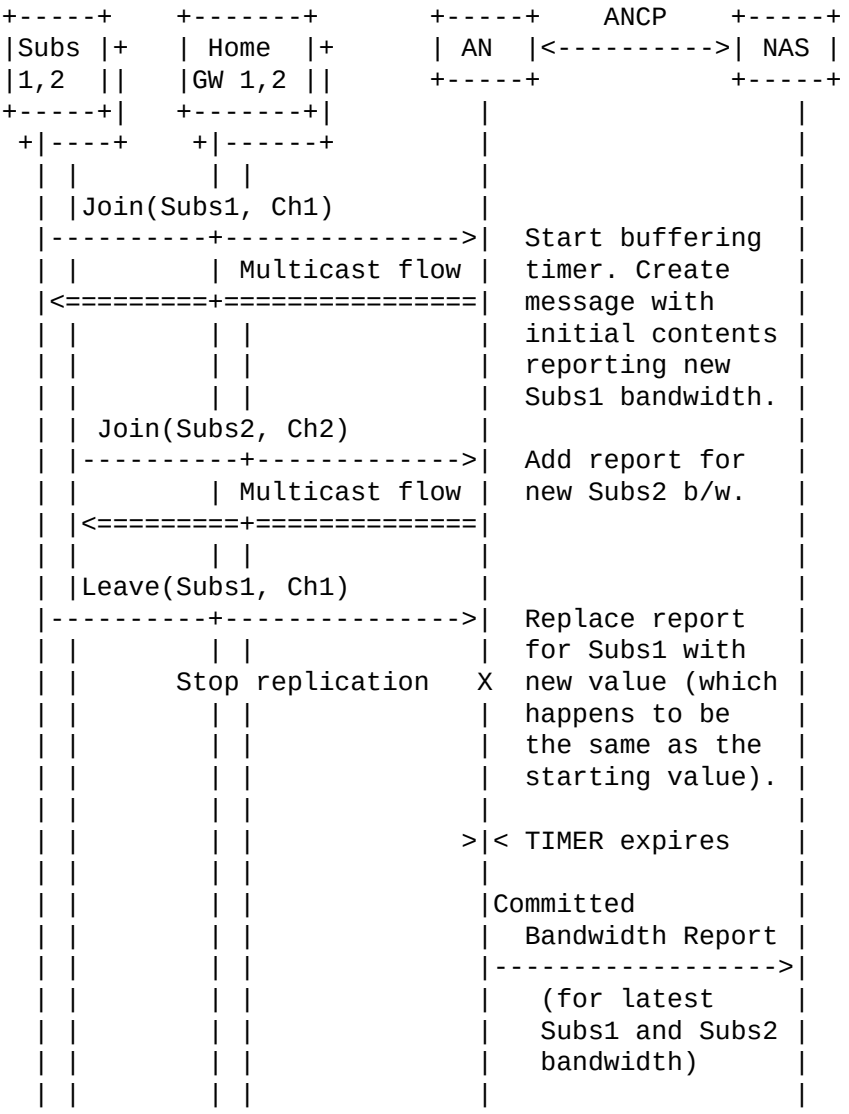


Figure 4: Message Flow for Committed Bandwidth Reporting

4. ANCP Messages

This section defines new ANCP messages and new usage of existing ANCP messages as well as procedures associated with the use of these messages.

Unless stated otherwise, receivers MUST ignore message contents that are not supported by the set of capabilities negotiated between the NAS and the Access Node.

4.1. Provisioning Message

Section 4.1 of [RFC6320] defines the Provisioning message that is sent by the NAS to the AN to provision information in the AN.

The present document specifies that the Provisioning message MAY be used by the NAS to provision multicast-related information (e.g., multicast service profiles). The ANCP Provisioning message payload MAY contain:

- one or more instances of the Multicast-Service-Profile TLV. The Multicast-Service-Profile TLV is defined in the present document in Section 5.1. Each instance of the Multicast-Service-Profile TLV contains a multicast service profile name and one or more list actions. A list action consists of an action (add, delete, replace), a list type (white, black, or grey), and list content (multicast source and group addresses).

- an instance of the White-List-CAC TLV. The White-List-CAC TLV is defined in Section 5.6. If present, this TLV indicates that the AN is required to do admission control before replicating white-listed flows.

- an instance of the MRepCtl-CAC TLV. The MRepCtl-CAC TLV is defined in Section 5.7. If present, this TLV indicates that the AN is required to do admission control before replicating flows specified in Multicast Replication Control messages.

- an instance of the Report-Buffering-Time TLV. The Report-Buffering-Time TLV is defined in Section 5.13. If present, this TLV indicates Committed Bandwidth Report messages should be buffered for the amount of time given by the TLV before being transmitted to the NAS.

See Section 6 for information on which multicast capabilities require support of these TLVs in the Provisioning message.

4.1.1. Sender Behavior

When directed by the Policy Server or by management action, the NAS sends the Provisioning message to initially provision or to update the white, black, and/or grey multicast channel lists associated with a set of named multicast service profiles or to direct the AN to perform admission control for specific classes of flows.

To provision or update a multicast service profile, the NAS MUST include within the message one or more instances of the Multicast-Service-Profile TLV specifying the content to be provisioned or updated. The NAS MUST NOT include any list type (white, black, or grey) that is not supported by the set of multicast capabilities negotiated between the NAS and the AN. The NAS MUST NOT use the Provisioning message to send instances of the Multicast-Service-Profile TLV to the AN unless the Multicast-Service-Profile TLV is supported by the set of multicast capabilities negotiated between the NAS and the AN.

To require admission control to be performed at the AN on white-listed flows, the NAS MUST include a copy of the White-List-CAC TLV in the Provisioning message. The White-List-CAC TLV MUST NOT be provided unless the negotiated set of capabilities includes conditional access and admission control with white and black lists.

To require admission control to be performed at the AN on grey-listed flows or on NAS-initiated flows, the NAS MUST include a copy of the MRepCtl-CAC TLV in the Provisioning message. The MRepCtl-CAC TLV MUST NOT be provided unless the negotiated set of capabilities includes NAS-initiated multicast replication or conditional access and admission control with grey lists.

To require buffering of Committed Bandwidth Report messages so that reports for multiple access lines can be included in the same message, the NAS MUST include a copy of the Report-Buffering-Time TLV containing a non-zero time value in a Provisioning message sent to the AN. The Report-Buffering-Time TLV MUST NOT be provided unless the negotiated set of capabilities includes committed bandwidth reporting.

4.1.2. Receiver Behavior

The receiving AN provisions/updates the white, black, and/or grey lists associated with the multicast service profile names contained in the Multicast-Service-Profile TLV instances within the message according to the contents of the associated List-Action TLVs. The AN MUST process List-Action TLVs in the order in which they appear within the message. In keeping with the general rule stated in

Section 4, the AN MUST ignore instances of the List-Action TLV referring to any list type (white, black, or grey) that is not supported by the set of multicast capabilities negotiated between the NAS and the AN.

When a new multicast service profile is identified by a Multicast-Service-Profile TLV, the initial state of all lists associated with that profile according to the negotiated set of multicast capabilities is empty until changed by the contents of Multicast-Service-Profile TLVs.

The receipt of a Provisioning message containing updates to an existing multicast service profile subsequent to startup will cause the AN to review the status of active flows on all ports to which that profile has been assigned. For further details, see Section 6.

If the White-List-CAC and/or MRepCtl-CAC TLV is present in the Provisioning message and the respective associated capabilities have been negotiated, the AN prepares (or continues) to do admission control on the indicated class(es) of flow. If one or both of these TLVs was present in an earlier Provisioning message but is absent in the latest message received, the AN ceases to do admission control on the indicated class(es) of flow.

The buffering time specified in an instance of the Report-Buffering-Time TLV will not be applied until the current accumulation process of Committed Bandwidth Report messages finishes.

As indicated in [RFC6320], the AN MUST NOT reply to the Provisioning message if it processed it successfully. If an error prevents successful processing of the message content, the AN MUST return a Generic Response message as defined in [RFC6320], containing a Status-Info TLV with the appropriate content describing the error. For this purpose, the presence of a list type in a Multicast-Service-Profile TLV, which was ignored because it was not supported by the negotiated set of capabilities, is not considered to be an error.

4.2. Port Management Message

As specified in [RFC6320], the NAS may send DSL line configuration information to the AN (ANCP-based DSL line configuration use case) using ANCP Port Management messages. See Section 7.3 of [RFC6320] for the format of the Port Management message in that usage.

This document specifies that the Port Management message MAY be used to convey either or both of the following TLVs:

- Multicast-Service-Profile-Name TLV (defined in Section 5.2). This TLV associates a Multicast Service Profile with the access line specified by the extension block and, in the case of white and black lists, delegates conditional access to the AN for the specified access line and channels.

- Bandwidth-Allocation TLV (defined in Section 5.5). This TLV specifies the total multicast bandwidth available to the AN for admission control at the access line.

When the Port Management message is used for this purpose:

- the Function field in the Port Management message MUST be set to 8, "Configure Connection Service Data".

- the message MUST include TLV(s) to identify the access line concerned. If the access line is a DSL loop, the line-identifying TLV(s) MUST be as specified in Section 5.1.2 of [RFC6320]. For non-DSL access lines, the appropriate alternative line-identifying TLV(s) MUST be present. Line configuration data other than the two TLVs listed in the previous paragraph MAY be present.

4.2.1. Sender Behavior

The NAS sends the Port Management message at startup time to initialize parameters associated with the access line specified in the message and with the multicast capabilities negotiated between the NAS and the AN. The NAS MAY send additional Port Management messages subsequent to startup, to update or, in the case of the Bandwidth-Allocation TLV, reset these parameters. If the NAS includes a Multicast-Service-Profile-Name TLV in the Port Management message, the name MUST match a profile name provided in a Multicast-Service-Profile TLV in a prior Provisioning message. The NAS MUST NOT include a TLV unless it is supported by the set of multicast capabilities negotiated between the NAS and the AN. See Section 6 for further information.

4.2.2. Receiver Behavior

If the Port Management message contains a Multicast-Service-Profile-Name TLV, the AN associates the named profile with the specified access line. This association replaces any previous association. That is, a given access line is associated with at most one multicast service profile. The replacement of one multicast service profile with another will cause the AN to review the status of all active flows on the target port. For further details see Section 6.

If the Port Management message contains a Bandwidth-Allocation TLV, the AN adopts this as the current value of its total multicast bandwidth limit for the target port. If the AN has already committed multicast bandwidth exceeding the amount given in the Bandwidth-Allocation TLV, the AN SHOULD NOT discontinue any multicast streams in order to bring bandwidth down to within the new limit, unless such action is required by local policy. However, the AN MUST NOT admit new multicast streams that are subject to admission control until it can do so within the limit specified by the Bandwidth-Allocation TLV.

If the Port Management request cannot be processed due to error and the Result field of the request is Nack (0x1) or AckAll (0x2), the AN SHOULD add a Status-Info TLV to the Extension Value field in its reply if this will provide useful information beyond what is provided by the Result Code value returned in the response header. In particular, if the name within the Multicast-Service-Profile-Name TLV does not match a profile name given in a prior Provisioning message, the AN SHOULD return a reply where the Result Code field in the header indicates 0x55, "Invalid TLV contents", the Error Message field in the Status-Info TLV contains the text "Multicast profile name not provisioned", and the Status-Info TLV contains a copy of the Multicast-Service-Profile-Name TLV.

4.3. Multicast Replication Control Message

This section defines a new message called the Multicast Replication Control message. The Multicast Replication Control message is sent by the NAS to the AN with one or more directives to add (join) or delete (leave) a multicast flow on a target object identified in the content of the message.

The Message Type for the Multicast Replication Control message is 144.

The ANCP Multicast Replication Control message payload contains the following TLVs:

- Target TLV: The Target TLV is defined in Section 4.3 of [RFC6320]. It MUST appear once and only once. It is encoded as specified in [RFC6320] or extensions and identifies the AN port subject to the request for admission or release.

- Command TLV: The Command TLV is defined in Section 4.4 of [RFC6320]. It MUST be present. It MAY appear multiple times.

As [RFC6320] indicates, the contents of the Command Info field within the Command TLV are specific to the message in which the TLV occurs. For the Multicast Replication Control message, these contents consist of:

- a Command Code field;
- an Accounting field; and
- an instance of the Multicast-Flow TLV.

Figure 5 illustrates the complete Command TLV with the contents specific to the Multicast Replication Control message.

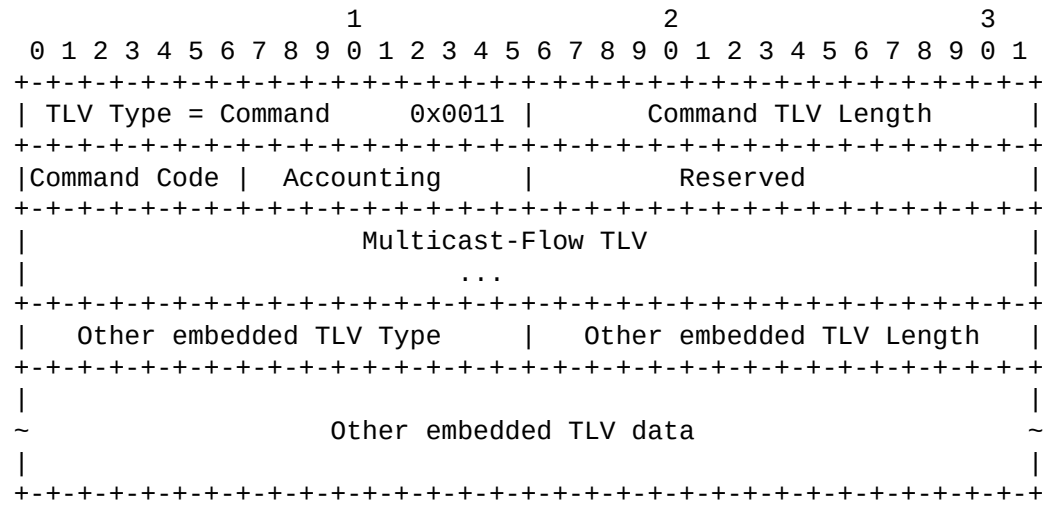


Figure 5: Contents of the Command TLV in the Multicast Replication Control Message

- Command Code: One of the following command directives:

  1 "Add"

  2 "Delete"

  3 "Delete All"

  4 "Admission Control Reject"

  5 "Conditional Access Reject"

  6 "Admission Control and Conditional Access Reject"

  Directives 4 through 6 are used as described in Section 4.4.2.

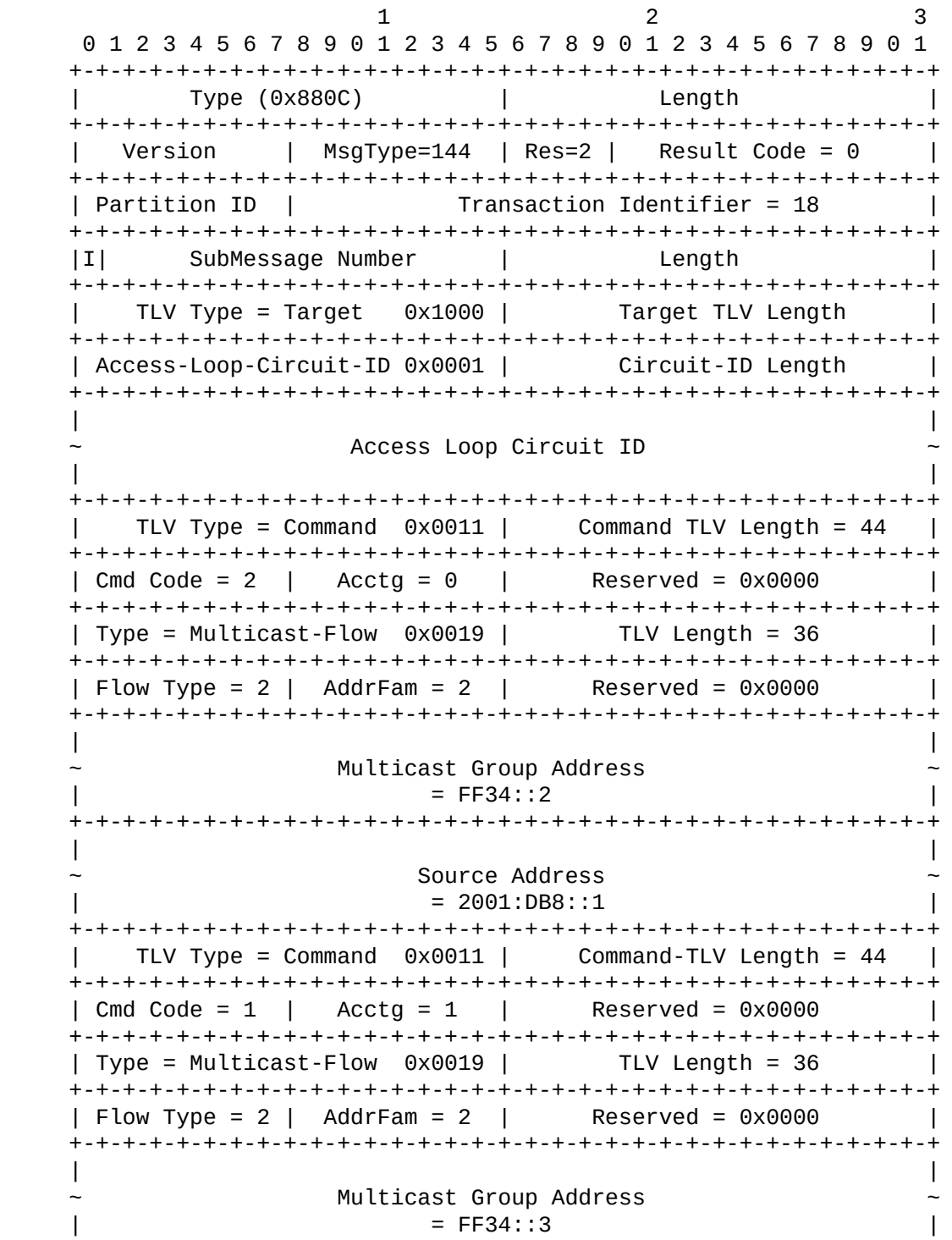
- Accounting: Meaningful only when the Command Code is "Add" (1). In that case, 0 indicates flow accounting is disabled, and 1 indicates that octet accounting for the flow is requested. The sender MUST set the Accounting field to 0, and the receiver MUST ignore the Accounting field for other Command Code values.

- Reserved: Reserved for future use. MUST be set to zeroes by the sender and ignored by the receiver.

- Multicast-Flow TLV: An instance of the Multicast-Flow TLV (Section 5.12) specifying the flow to be added or deleted. The Multicast-Flow TLV is omitted if the Command Code has value "Delete All" (3).

- Other embedded TLV data: No other embedded TLVs are currently specified within the Multicast Replication Control message and Command TLV. However, see the description of the Multicast Admission Control message (Section 4.4). Unrecognized embedded TLVs SHOULD be silently discarded.

The figure below is an example of a Multicast Replication Control message that would result in a swap from multicast Source-Specific Multicast (SSM) flows 2001:DB8::1, FF34::2 to 2001:DB8::2, FF34::3 on the target identified by the Access Loop Circuit ID:


0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Type (0x880C)
Length
Version
MsgType=144
Res=2
Result Code = 0
Partition ID
Transaction Identifier = 18
I
SubMessage Number
Length
TLV Type = Target 0x1000
Target TLV Length
Access-Loop-Circuit-ID 0x0001
Circuit-ID Length
Access Loop Circuit ID
TLV Type = Command 0x0011
Command TLV Length = 44
Cmd Code = 2
Acctg = 0
Reserved = 0x0000
Type = Multicast-Flow 0x0019
TLV Length = 36
Flow Type = 2
AddrFam = 2
Reserved = 0x0000
Multicast Group Address
= FF34::2
Source Address
= 2001:DB8::1
TLV Type = Command 0x0011
Command-TLV Length = 44
Cmd Code = 1
Acctg = 1
Reserved = 0x0000
Type = Multicast-Flow 0x0019
TLV Length = 36
Flow Type = 2
AddrFam = 2
Reserved = 0x0000
Multicast Group Address
= FF34::3

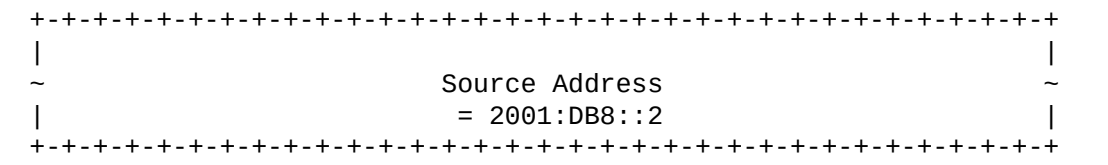


Figure 6: Example Change of Source Flow Using Multicast Replication Control Message

4.3.1. Sender Behavior

The NAS MAY issue a Multicast Replication Control message to the AN to convey one or more directives to add (join) or delete (leave) one or more multicast flows.

The NAS MAY send this message on its own initiative to support the NAS-initiated multicast control use case presented in [RFC5851] and summarized in Section 3.1. In that case, the NAS MUST set the Result field to AckAll (0x2) or Nack (0x1) according to its requirements.

The NAS MAY also send this message in response to a Multicast Admission Control message (defined in Section 4.4) received from the AN to support the conditional access and admission control use case presented in [RFC5851] and summarized in Section 3.2. In that case, the NAS MUST set the Result field to Nack (0x1).

In either case, the sender MUST populate the Result Code field with the value 0 and the ANCP Transaction Identifier field with a unique value, as described in Section 3.6.1.6 of [RFC6320].

Each Multicast Replication Control message MUST contain one or more commands, each encapsulated in its own Command TLV. The sender MUST use a separate Command TLV for each distinct multicast flow.

When the order of processing of two commands does not matter, the commands MUST be transmitted in separate Multicast Replication Control messages.

4.3.2. Receiver Behavior

When successive commands (in the same or different messages) relate to the same target and multicast flow, the state of each feature controlled or affected by attributes received in the Multicast Replication Control message SHALL be as set by the last command or message referring to that target and flow and containing the controlling attribute. As an example, successive Multicast Replication Control messages containing add commands for a given port and flow but differing only in the Accounting field update the state

of the accounting feature to what is set in the final command received, but all other features are unaffected by the second message.

If more than one Command TLV is present in a Multicast Replication Control message, the AN MUST act on the commands in the order in which they are presented in the message. The AN SHALL assign a sequence number to each command in a given Multicast Replication Control message, starting from 1 for the first command.

If a Command TLV adds one or more flows and the AN is performing admission control for Multicast Replication Control messages, then the AN MUST perform admission control before replicating the flows. If the admission control check fails, the AN MUST treat the failure as an error as described below. The appropriate Result Code value for the response is 0x13 "Out of resources".

If the AN processes the complete Multicast Replication Control message successfully and the Result field of the Multicast Replication Control message was set to AckAll (0x2), the AN MUST respond with a Generic Response message where the Result field is set to Success (0x3), the Result Code field is set to 0, and the Transaction Identifier field is copied from the Multicast Replication Control message. The body of the response MAY be empty or MAY be copied from the Multicast Replication Control message.

If the AN processes the complete Multicast Replication Control message successfully and the Result field of the Multicast Replication Control message was set to Nack (0x1), the AN MUST NOT respond to the message.

The processing/execution of multiple commands contained in a single Multicast Replication Control message MUST be interrupted at the first error encountered and the remaining commands in the Multicast Replication Control message discarded. Similarly, if a given command specifies multiple Single-Source Multicast (SSM) flows and an error occurs, processing MUST be interrupted at that point, and the remainder of the Command TLV discarded.

If the AN detects an error in a received Multicast Replication Control message and the Result field in that message was set to Nack (0x1) or AckAll(0x2), the AN MUST generate a Generic Response message providing error information to the NAS. This specification identifies the following new Result Code values beyond those specified in [RFC6320], which MAY be used in a Generic Response sent in reply to a Multicast Replication Control message:

0x64 Command error.

Where detected: ANCP agent at the AN.

Further description: an invalid command code has been received.

Required additional information in the message: see below.

Target: ANCP agent at the NAS.

Action RECOMMENDED for the receiving ANCP agent: Report the error to the control application with an indication of the erroneous information associated with the invalid TLV(s).

0x65 Invalid flow address.

Where detected: ANCP agent at the AN.

Further description: either inconsistent flow address information has been provided or the address family is unsupported.

Required additional information in the message: see below.

Target: ANCP agent at the NAS.

Action RECOMMENDED for the receiving ANCP agent: Report the error to the control application with an indication of the erroneous information associated with the invalid TLV(s).

0x66 Multicast flow does not exist.

Where detected: control application at the AN.

Further description: the NAS has attempted to delete a flow that is not active on the given access line.

Required additional information in the message: see below.

Target: control application at the NAS.

Action RECOMMENDED for the receiving ANCP agent: report the error to the control application with an indication of the erroneous information associated with the invalid TLV(s).

A Generic Response message responding to the Multicast Replication Control message and containing one of the above Result Code values MUST include a Status-Info TLV, which includes one or two embedded TLVs as follows:

- a Sequence-Number TLV as described in Section 5.4, giving the sequence number of the failed command, MUST be included; and

- the failed Command TLV itself SHOULD be included.

  Note: The Error Message field of the Status-Info TLV MAY be used to report more details than implied by the Result Code value in the message header. For example, the Result Code value could be 0x65, and the Error Message field could contain the text: "Source address present for ASM flow".

4.4. Multicast Admission Control Message

This section defines a new message called the Multicast Admission Control message. The Multicast Admission Control message is sent by the AN to the NAS to request admission of a multicast flow, or to notify of the removal of a multicast flow, for a given target.

The Message Type for the Multicast Admission Control message is 145.

The ANCP Multicast Admission Control message payload contains two TLVs:

- Target TLV: The Target TLV is defined in [RFC6320]. It MUST appear once and only once in the Multicast Admission Control message. It is encoded as specified in [RFC6320] or extensions and identifies the AN port subject to the request for admission or release.

- Command TLV: The Command TLV is defined in [RFC6320]. It MUST be present. If it appears more than once, only the first instance is considered meaningful in the present version of this specification, and the other instances are ignored.

  Note: In the future, the specification of the Multicast Admission Control message may be extended to allow transport of more than a single directive (e.g., to carry both a leave from one group and a join to another group for the same target). It is expected that this would support a similar notion of strict sequenced processing as currently defined for handling multiple directives in the Multicast Replication Control message whereby all directives following the first directive that cannot be executed are not

executed either. When the strict sequenced processing of the directives is not required, the directives are distributed across separate messages.

The Command TLV has the same contents as were described above for the Multicast Replication Control message, with the following additions:

- A Request-Source-IP TLV MAY be appended to the Command TLV as an additional embedded TLV.
- Similarly, a Request-Source-MAC TLV MAY be appended to the Command TLV as an additional embedded TLV.
- Finally and preferably, a Request-Source-Device-Id TLV MAY be appended to the Command TLV as an additional embedded TLV.

Note that the Command TLV length includes the length of any embedded TLVs, including the embedded TLV headers.

4.4.1. Sender Behavior

The AN sending the Multicast Admission Control message MUST set the Result field to Ignore (0x0).

The AN MUST populate the ANCP Transaction Identifier field with a unique value, as described in Section 3.6.1.6 of [RFC6320].

The AN MUST encode the Command TLV as specified in Section 4.3 with the following additional rules:

- The Accounting field MUST be set to 0.
- The Command Code field MUST be set to "Add" (1) when the message conveys a join request, to "Delete" (2) when the message conveys a leave, and to "Delete All" (3) when the message conveys a leave of all channels (on the target).
- The Multicast-Flow TLV within the Command TLV identifies the multicast flow subject to the request for admission or release. When the Command Code is 3, the Multicast-Flow TLV is omitted.
- The Request-Source-IP embedded TLV MAY be included by the AN to convey the IP address of the sender of the join/leave message (e.g., IGMP/MLD join/leave) that triggered the AN to include the corresponding Command TLV in the Multicast Admission Control message. If it appears more than once, only the first instance is considered meaningful, and the other instances are ignored.

- The Request-Source-MAC embedded TLV MAY be included by the AN to convey the Media Access Control (MAC) address of the sender of the join/leave message (e.g., IGMP/MLD join/leave) that triggered the AN to include the corresponding Command TLV in the Multicast Admission Control message. If it appears more than once, only the first instance is considered meaningful, and the other instances are ignored.

- As a third alternative, the Request-Source-Device-Id embedded TLV MAY be included by the AN to convey a local identifier of the sender of the join/leave message (e.g., IGMP/MLD join/leave) that triggered the AN to include the corresponding Command TLV in the Multicast Admission Control message. If it appears more than once, only the first instance is considered meaningful, and the other instances are ignored.

The inclusion of Request-Source-IP or Request-Source-MAC in the Multicast Admission Control message is typically done to allow the application of policies applicable to specific devices within the customer's network. However, transmission of either of these fields beyond the AN introduces potential privacy issues. Instead of transmitting either of these identifiers, it is RECOMMENDED that the AN map the required identifier to a local value known to the AN and Authentication, Authorization, and Accounting (AAA) but not to the NAS, as discussed in Section 8. The local identifier is transmitted using the Request-Source-Device-Id TLV.

4.4.2. Receiver Behavior

On receipt of a Multicast Admission Control message:

- The NAS MUST ignore the Result field.

- If the directive in the Multicast Admission Control message is "Delete" (2) or "Delete All" (3) and is processed correctly by the NAS, the NAS MUST NOT generate any ANCP message in response to the Multicast Admission Control message.

- If the directive in the Multicast Admission Control message is "Add" (1) and is accepted by the NAS, the NAS MUST generate a Multicast Replication Control message in response to the Multicast Admission Control message. The Multicast Replication Control message:

  * MUST contain a Result set to Nack (0x1);

  * MUST contain a Transaction ID with a unique value, as described in Section 3.6.1.6 of [RFC6320]; and

  * MUST contain the directive as accepted by the NAS. The NAS MAY modify the Accounting field if flow accounting is required.

- If the directive in the Multicast Admission Control message is "Add" (1) and is processed correctly but not accepted by the NAS (i.e., it does not pass the conditional access and admission control check), the NAS MAY generate a Multicast Replication Control message in response to the Multicast Admission Control message. This optional message can be used by the AN to maintain statistics about admission control rejections. When used in this situation, the Multicast Replication Control message:

  * MUST contain a Result set to 0x0;

  * MUST contain a Transaction ID with a unique value, as described in Section 3.6.1.6 of [RFC6320]; and

  * MUST contain the directive rejected by the NAS (i.e., Target TLV and Command TLV) but with a Command Code set to "Admission Control Reject" (4), "Conditional Access Reject" (5), or "Admission Control and Conditional Access Reject" (6) as applicable.

- If the Multicast Admission Control message cannot be processed correctly by the NAS (e.g., the message is malformed, the multicast flow does not exist, etc.), the NAS MUST generate a Generic Response message (defined in Section 4.2 of [RFC6320]) with appropriate content indicating the reason for the failure.

4.5. Bandwidth Reallocation Request Message

The Bandwidth Reallocation Request message is used when the bandwidth delegation capability is included in the negotiated set. It MAY be sent either by the NAS or by the AN to request an adjustment in the amount of delegated bandwidth. It will be sent by the NAS typically to reduce the multicast bandwidth allocated to the AN in order for the NAS to satisfy a request to add one or more flows. Conversely, the AN will send a Bandwidth Reallocation Request message to obtain additional bandwidth to satisfy a request to add a multicast channel. In each case, the requestor has a minimum requirement for additional bandwidth and MAY ask for additional bandwidth beyond this amount (e.g., to handle anticipated future requests).

The Bandwidth Reallocation Request message contains two TLVs:

- the Target TLV (Section 4.3 of [RFC6320] or an extension), specifying a single access line; and

- the Bandwidth-Request TLV (Section 5.8), specifying the required and preferred amounts of delegated bandwidth.

The Message Type for the Bandwidth Reallocation Request message is 146.

4.5.1. Sender Behavior

The Result field in the header of the Bandwidth Reallocation Request message is not used, and the sender MUST set it to Ignore (0x0).

The bandwidth values in the Bandwidth-Request TLV are expressed in terms of total multicast bandwidth allocated to the AN.

> Note: The choice of "total bandwidth" rather than "incremental bandwidth" was made so that it would be easier for the AN and NAS to keep their respective views of the current amount of delegated bandwidth synchronized.

Because the values are totals rather than desired increments/decrements, the relationship between the required amount and the preferred amount will differ depending on whether the Bandwidth Reallocation Request message is issued by the NAS or the AN.

- If the NAS is making the request, the preferred amount MUST be less than or equal to the required amount. The required amount MUST be less than the current amount of delegated bandwidth.

- If the AN is making the request, the preferred amount MUST be greater than or equal to the required amount. The required amount MUST be greater than the current amount of delegated bandwidth.

4.5.2. Receiver Behavior

When the peer receives a valid Bandwidth Reallocation Request message, it SHOULD determine whether it can satisfy the request from its existing allocation of unused video bandwidth. If it decides that it can reallocate bandwidth to the peer, it MAY choose to return any amount between the required and the preferred amounts indicated in the Bandwidth Reallocation Request message.

The peer MUST return a Bandwidth Transfer message (Section 4.6) indicating its decision. If the request is met, the Result field of the Bandwidth Transfer message MUST be set to Success (0x3), the Result Code field MUST be set to 0x000, and the Bandwidth-Allocation TLV (Section 5.5) MUST contain the new value of total multicast bandwidth. This new value MUST lie between the required and preferred values, inclusive, from the request message. If the

request is not met, the Result field of the Bandwidth Transfer message MUST be set to Failure (0x4), the Result Code field MUST be set to 0, and the Bandwidth-Allocation TLV MUST contain the value of the currently allocated amount of delegated bandwidth as the responder views it.

The following cases indicate that the sender holds a different view of the amount of delegated bandwidth from the receiver:

- The NAS receives a request where the required amount is less than its view of the current amount of delegated bandwidth.

- The AN receives a request where the required amount is greater than its view of the current amount of delegated bandwidth.

If one of these cases occurs, the receiver, with one exception, MUST send a Bandwidth Transfer message indicating Success.

- If the NAS received the request, the allocated amount in the NAS's response MUST be at least equal to the NAS's view of the current amount of delegated bandwidth.

- If the AN received the request, the allocated amount in the AN's response MUST be no greater than the AN's view of the current amount of delegated bandwidth.

The exception is when the NAS receives a request while it has a request of its own outstanding. Handling of that case is described below.

> Note: While the cases just described are an error condition, the success response achieves a graceful recovery.

To avoid deadlock due to race conditions, the following rules MUST be applied:

a. If the NAS receives a Bandwidth Reallocation Request message while it has a Bandwidth Reallocation Request message of its own outstanding for the same access line, the NAS MUST provide an immediate failure response to the request from the AN, with a Result Code value set to 0x68 "Inconsistent views of delegated bandwidth amount" or 0x69 "Bandwidth request conflict" as applicable. (See below for more information).

b. If the AN receives a Bandwidth Reallocation Request message while it has a Bandwidth Reallocation Request message of its own outstanding for the same access line, the AN MUST release any bandwidth it has already committed to an outstanding join request

while it is awaiting a response from the NAS. It MUST decide upon and send its response to the NAS taking the released bandwidth into account.

If the receiver is unable to process the Bandwidth Reallocation Request message due to an error, then the receiver MUST return a Bandwidth Transfer message where:

- the Result field is set to Failure (0x4),
- the Result Code field is set appropriately to indicate the type of error that was detected,
- the Bandwidth-Allocation TLV contains the value of the current amount of delegated bandwidth as the responder views it, and
- a Status-Info TLV MAY follow the Bandwidth-Allocation TLV giving further information about the error.

This specification provides three new Result Code values applicable specifically to the contents of the Bandwidth-Request TLV. These Result Code values by their nature MUST only be used when the error is being reported in a Bandwidth Transfer message rather than a Generic Response message.

0x67 Invalid preferred bandwidth amount.

Where detected: control application at the receiver of the Bandwidth Reallocation Request message.

Further description: the preferred and required amounts of bandwidth in the TLV do not have the numerical relationship described above.

Required additional information in the message: as described above.

Target: control application at the sender of the Bandwidth Reallocation Request message.

Action RECOMMENDED for the receiving ANCP agent: report the error to the control application with the returned value of the Bandwidth-Allocation TLV. See also Section 4.6.2.2.

0x68 Inconsistent views of delegated bandwidth amount.

Where detected: control application at the NAS.

Further description: the NAS has an outstanding Bandwidth Reallocation Request, so it is rejecting a similar request from the AN. In the AN request, the required amount was less than the NAS's view of the current amount of delegated bandwidth.

Required additional information in the message: as described above.

Target: control application at the AN.

Action RECOMMENDED for the receiving ANCP agent: report the error to the AN control application with the returned value of the Bandwidth-Allocation TLV. See also Section 4.6.2.2.

0x69 Bandwidth request conflict.

Where detected: control application at the NAS.

Further description: the NAS has an outstanding Bandwidth Reallocation Request, so it is rejecting a similar, valid request from the AN.

Required additional information in the message: as described above.

Target: control application at the AN.

Action RECOMMENDED for the receiving ANCP agent: report the error to the AN control application with the returned value of the Bandwidth-Allocation TLV. See also Section 4.6.2.2.

4.6. Bandwidth Transfer Message

The Bandwidth Transfer message is used to transfer video bandwidth from the sender to the peer for a specific access line. This message MAY be sent either from the AN or from the NAS. As described in the previous section, it is the required response to a valid Bandwidth Reallocation Request message.

The Bandwidth Transfer message MAY also be used to transfer bandwidth autonomously from one peer to another. One example of this usage is to release bandwidth borrowed earlier by means of the Bandwidth

Reallocation Request message. When the message is used in this way, the Result field in the Bandwidth Transfer message MUST be set to Ignore (0x0).

Note: This allows the receiver to distinguish between an autonomous transfer and a response to a previous Bandwidth Reallocation Request message, for purposes of validation.

The Message Type for the Bandwidth Transfer message is 147. The Bandwidth Transfer message contains the following TLVs:

- the Target TLV, designating the access line concerned;
- an instance of the Bandwidth-Allocation TLV (Section 5.5). The bandwidth value in the Bandwidth-Allocation TLV is the new amount of delegated bandwidth allocated to the target.

4.6.1. Sender Behavior

When sending a Bandwidth Transfer message where the Result value is Ignore (0x0) or Success (0x3), the following relationships MUST hold:

- If the message is sent by the NAS, the bandwidth value in the Bandwidth-Allocation TLV MUST be greater than or equal to the sender's view of the current amount of delegated bandwidth for the access line concerned.
- If the message is sent by the AN, the bandwidth value in the Bandwidth-Allocation TLV MUST be less than or equal to the sender's view of the current amount of delegated bandwidth for the access line concerned.

Further sender behavior is specified above, in Section 4.5.2.

4.6.2. Receiver Behavior

4.6.2.1. Behavior of the NAS

If the amount of delegated bandwidth provided in the Bandwidth-Allocation TLV is not greater than the NAS's view of the current amount of delegated bandwidth, the NAS MUST update its view of the current amount of delegated bandwidth to the amount indicated in the Bandwidth Transfer message. This is required regardless of whether the Result field of that message indicates Success or Failure.

If the amount of delegated bandwidth provided in the Bandwidth-Allocation TLV is greater than the NAS's view of the current amount of delegated bandwidth, the NAS MAY accept the given value as its new

value of delegated bandwidth. Alternatively, the NAS MAY force the AN to modify its view of the amount of delegated bandwidth to that held by the NAS by sending a Port Management message for the target access line concerned that contains a Bandwidth-Allocation TLV with a value equal to the amount of delegated bandwidth the NAS wishes to enforce.

4.6.2.2. Behavior of the AN

If the amount of delegated bandwidth provided in the Bandwidth-Allocation TLV of the Bandwidth Transfer message differs from the AN's view of the current amount of delegated bandwidth, the AN MUST update its view of the current amount of delegated bandwidth to the amount indicated in the Bandwidth Transfer message. This is required with the exception of a Bandwidth Transfer message with a Result field equal to Failure (0x4) and a Result Code field equal to 0x68 "Inconsistent views of delegated bandwidth amount" or 0x69 "Bandwidth request conflict". If Result Code value 0x68 is received, the AN MUST issue a Delegated Bandwidth Query Request message to determine the NAS's current view of the amount of delegated bandwidth. The AN MUST update its own view based on the value returned in the Delegated Bandwidth Query Response message. If Result Code value 0x69 is received, the AN SHOULD carry out this procedure unless it can account for the discrepancy as a result of a transfer of bandwidth to the NAS that was carried out just before the incoming Bandwidth Transfer message was processed.

> Note: The two Result Code values indicate a race condition where the AN may have just completed a transfer of bandwidth to the NAS. As a result, the value given in the Bandwidth Transfer message may be outdated, and the AN needs to query the NAS to find its latest view. The procedure assumes that ordering is preserved between the Bandwidth Transfer message sent by the AN in response to the NAS's request and the subsequent Delegated Bandwidth Query Request message.

If the AN has already committed multicast bandwidth exceeding the amount given in the Bandwidth-Allocation TLV, the AN SHOULD NOT discontinue any multicast streams in order to bring bandwidth down to within the new limit, unless such action is required by local policy. However, the AN MUST NOT admit new multicast streams that are subject to admission control until it can do so within the limit specified by the Bandwidth-Allocation TLV. As specified in Section 6.2.5.2, the AN MAY attempt to correct the situation by sending a request to the NAS for an increased allocation of delegated bandwidth using the Bandwidth Reallocation Request message.

4.7. Delegated Bandwidth Query Request Message

The Message Type for the Delegated Bandwidth Query Request (and Response) messages is 148.

The Delegated Bandwidth Query Request message MAY be sent either by the NAS or by the AN to retrieve the peer's view of the amount of delegated bandwidth. The request contains one TLV:

- a Target TLV designating the access line for which the information is requested.

4.7.1. Sender Behavior

The sender MUST set the Result field in the header of the Delegated Bandwidth Query Request message to AckAll (0x2). The Result Code value MUST be set to 0. The sender MUST populate the ANCP Transaction Identifier field with a unique value, as described in Section 3.6.1.6 of [RFC6320].

4.7.2. Receiver Behavior

If the AN or NAS receives a valid Delegated Bandwidth Query Request message, it MUST respond with a Delegated Bandwidth Query Response message. The Result field in the header of the response MUST be set to Success (0x3). The Result Code field MUST be set to 0. The Transaction Identifier field MUST be copied from the request message. The body of the response MUST contain the Target TLV, copied from the request message. Finally, the body of the response MUST contain a Bandwidth-Allocation TLV, containing the current amount of delegated bandwidth from the point of view of the receiver of the request.

If the contents of the Delegated Bandwidth Query Request message are in error, the receiver MUST return a Delegated Bandwidth Query Response message with the Result field in the header set to Failure (0x3). The Result Code field MUST be set to the value that indicates the nature of the error (e.g., 0x500 "One or more of the specified ports do not exist"). The Transaction Identifier field MUST be copied from the request. The body of the response MUST contain the Target TLV copied from the request. This MAY be followed by a Status-Info TLV giving further information about the error.

4.8. Delegated Bandwidth Query Response Message

The Delegated Bandwidth Query Response message is sent in reply to a Delegated Bandwidth Query Request message. The response to a valid request contains two TLVs:

- the Target TLV, copied from the request; and
- a Bandwidth-Allocation TLV, giving the responder's view of the current amount of multicast bandwidth delegated to the AN.

The Message Type for the Delegated Bandwidth Query Response message is 148.

4.8.1. Sender Behavior

Sender behavior for the Delegated Bandwidth Query Response message is specified in Section 4.7.2.

4.8.2. Receiver Behavior

If the Delegated Bandwidth Query Response message indicates Success (0x3), the actions described in Sections 4.8.2.1 and 4.8.2.2 apply.

4.8.2.1. Behavior at the NAS

If the amount of delegated bandwidth provided in the Bandwidth-Allocation TLV is less than the NAS's view of the current amount of delegated bandwidth, the NAS MUST update its view of the current amount of delegated bandwidth to the amount indicated in the Delegated Bandwidth Query Response message.

If the amount of delegated bandwidth provided in the Bandwidth-Allocation TLV is greater than the NAS's view of the current amount of delegated bandwidth, the NAS MAY accept the given value as its new value of delegated bandwidth. Alternatively, the NAS MAY force the AN to modify its view of the amount of delegated bandwidth to that held by the NAS by sending a Port Management message for the target access line concerned that contains a Bandwidth-Allocation TLV with a value equal to the amount of delegated bandwidth the NAS wishes to enforce.

4.8.2.2. Behavior at the AN

The AN SHOULD accept the value returned in the Bandwidth-Allocation TLV of the Delegated Bandwidth Query Response message as the correct value of the current amount of delegated bandwidth. If the AN has already committed multicast bandwidth exceeding the amount given in the Bandwidth-Allocation TLV, the AN SHOULD NOT discontinue any multicast streams in order to bring bandwidth down to within the new limit, unless such action is required by local policy. However, the AN MUST NOT admit new multicast streams that are subject to admission control until it can do so within the limit specified by the Bandwidth-Allocation TLV. As specified in Section 6.2.5.2, the AN

MAY attempt to correct the situation by sending a request to the NAS for an increased allocation of delegated bandwidth using the Bandwidth Reallocation Request message.

> Note: A race condition is possible where the AN sends a query, the NAS requests more bandwidth, then receives and responds to the query, and then receives the Bandwidth Transfer message responding to its request. It is up to the AN to take appropriate action in this case. The best action appears to be not to act on the result of the first query but to repeat the query after sending the Bandwidth Transfer message. Similar considerations apply to a race between queries from both sides.

4.9. Multicast Flow Query Request and Response Messages

This section defines two new messages called the Multicast Flow Query Request and Multicast Flow Query Response. The Multicast Flow Query Request message is sent by the NAS to request information about the multicast flows that are active on the AN. The Multicast Flow Query Response message is sent in response by the AN to provide the requested information to the NAS.

The Message Type for the Multicast Flow Query Request and Multicast Flow Query Response messages is 149.

The contents of the Multicast Flow Query Request and Multicast Flow Query Response messages depend on the nature of the query, as described below.

4.9.1. Sender Behavior

The sender of a Multicast Flow Query Request message MUST set the Result field to AckAll (0x2). The Result Code field MUST be set to 0x000. The sender MUST populate the ANCP Transaction Identifier field with a unique value, as described in Section 3.6.1.6 of [RFC6320].

The Multicast Flow Query Request message MAY be used by the NAS to retrieve:

- the AN's view of which multicast flows are currently active on a specified set of access ports; or
- the AN's view of the access ports on which a specified set of multicast flows are currently active; or
- the AN's view of all the multicast flows currently active on each access port of the AN.

To retrieve the AN's view of which multicast flows are currently active on a given port of the AN, the NAS MUST include a Target TLV in the Multicast Flow Query Request payload identifying that port. The Target TLV is encoded as specified in [RFC6320].

To retrieve the AN's view of the ports currently receiving a given multicast flow, the NAS MUST include a Multicast-Flow TLV in the Multicast Flow Query Request payload identifying that flow. The Multicast-Flow TLV is encoded as specified in Section 5.12.

The NAS MAY include multiple Target TLVs or multiple Multicast-Flow TLVs in the Multicast Flow Query Request message but MUST NOT include both Target and Multicast-Flow TLVs in the same message.

To retrieve the AN's view of all of the multicast flows currently active on each port of the AN, the NAS MUST send a Multicast Flow Query Request message that does not contain any instance of the Target TLV or the Multicast-Flow TLV.

4.9.2. Receiver Behavior

The AN MUST respond to a Multicast Flow Query Request message that has a valid format and a valid content with a Multicast Flow Query Response message. The Result field in the response MUST be set to Success (0x3). The Result Code field MUST be set to 0. The Transaction Identifier field MUST be copied from the request.

If the Multicast Flow Query Request contains one (or more) Target TLVs, the AN MUST include, for each of these Target TLVs, the following set of TLVs:

- Target TLV. This MUST be identical to the Target TLV in the received Multicast Flow Query Request message.

- Multicast-Flow TLV(s). The Multicast-Flow TLV MUST appear once per multicast flow that is currently active on the AN port identified in the preceding Target TLV.

The Target TLVs MUST appear in the response from the AN in the same order as in the query from the NAS.

If the Multicast Flow Query Request message contains one (or more) Multicast-Flow TLVs, the AN MUST include, for each of these Multicast-Flow TLVs, the following set of TLVs:

- Multicast-Flow TLV. This MUST be identical to the Multicast-Flow TLV in the received Multicast Flow Query Request message.

- Target TLV(s). The Target TLV MUST appear once per AN port on which the multicast flow identified in the preceding Multicast-Flow TLV is active.

The Multicast-Flow TLVs MUST appear in the response from the AN in the same order as in the query from the NAS.

If the Multicast Flow Query Request message contains no Target TLV and no Multicast Flow TLV, the AN MUST include, for each AN port currently receiving multicast flow(s), the following set of TLVs:

- Target TLV. This MUST identify one AN port.

- Multicast-Flow TLV(s). The Multicast-Flow TLV MUST appear once per Multicast Flow that is currently active on the AN port identified in the preceding Target TLV.

If the contents of the Multicast Flow Query Request message are in error, the AN MUST reply with a Multicast Flow Query Response message with the Result field set to Failure (0x4) and the Result Code field set to indicate the nature of the error. If the request contained multiple instances of the Target TLV or the Multicast-Flow TLV and one of these is in error, the response message MUST contain the results for the preceding instances of the TLV as if there had been no error. These successful results MUST be followed by the TLV in error, copied from the request. The AN MUST NOT do further processing of the request. The AN MAY add a Status-Info TLV to provide further information on the nature of the error.

4.10. Committed Bandwidth Report Message

This section describes the Committed Bandwidth Report message, which is sent from the AN to the NAS to report the most recent amount of multicast bandwidth usage committed to one or more access lines.

The Message Type for the Committed Bandwidth Report message is 150.

The Committed Bandwidth Report message contains one or more instances of the Committed-Bandwidth TLV, as described in Section 5.14.

4.10.1. Sender Behavior

The sender of a Committed Bandwidth Report message MUST set the Result field to Ignore (0x0). The Result Code field MUST be set to 0x000. The sender MUST populate the ANCP Transaction Identifier field with a unique value, as described in Section 3.6.1.6 of [RFC6320].

Each instance of the Committed-Bandwidth TLV included in the message MUST identify an access line for which the amount of committed multicast bandwidth has changed since the previous Committed Bandwidth Report message was sent and MUST report the latest amount of multicast bandwidth committed to that line. There MUST be only one instance of the Committed-Bandwidth TLV present in the message for any given access line. The message MUST include an instance of the Committed-Bandwidth TLV for every access line for which committed multicast bandwidth has changed since the previous Committed Bandwidth Report message was sent.

Further behavior at the AN is specified in Section 6.2.2.

4.10.2. Receiver Behavior

The usage of the contents of a Committed Bandwidth Report message received by the NAS is implementation-dependent. One example is that the NAS uses the reports of multicast bandwidth commitments to adjust its forwarding scheduler operation to provide the intended level of QoS.

The NAS MUST NOT reply to a valid Committed Bandwidth Report message. The NAS MAY send a Generic Response message indicating the nature of any errors detected in a Committed Bandwidth Report message that it has received.

5. ANCP TLVs For Multicast

This section defines new ANCP TLVs for the control of multicast flows.

5.1. Multicast-Service-Profile TLV

This document defines the new Multicast-Service-Profile TLV.

The Multicast-Service-Profile TLV MAY be included in a Provisioning message as specified in Section 4.1.

The Multicast-Service-Profile TLV is illustrated in Figure 7. It consists of a TLV header encapsulating a single instance of the Multicast-Service-Profile-Name TLV and one or more instances of the List-Action TLV.

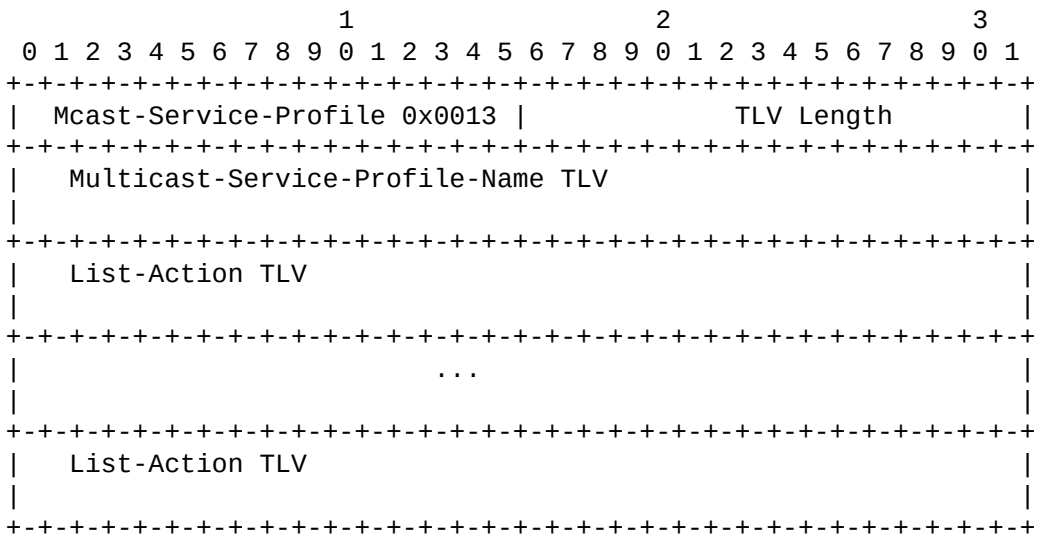


Figure 7: Multicast-Service-Profile TLV

The Multicast-Service-Profile TLV has the following fields:

- TLV Type: 0x0013
- TLV Length: determined by the contents following the TLV header.
- Multicast-Service-Profile-Name TLV: described in Section 5.2. The Multicast-Service-Profile-Name TLV MUST contain an identifier that is unique over all profiles provisioned to the same AN partition. This identifier will be used to refer to the profile when activating it for a given target within a Port Management message (see Section 4.2).
- List-Action TLV: described in Section 5.3. The List-Action TLV(s) provide the content of a newly defined multicast service profile or modify the existing content. If more than one List-Action TLV is present, the order of the TLVs may be significant, since List-Action TLVs are processed in the order in which they appear.

5.2. Multicast-Service-Profile-Name TLV

The Multicast-Service-Profile-Name TLV carries the identifier of a multicast service profile provisioned on the AN. It is illustrated in Figure 8.

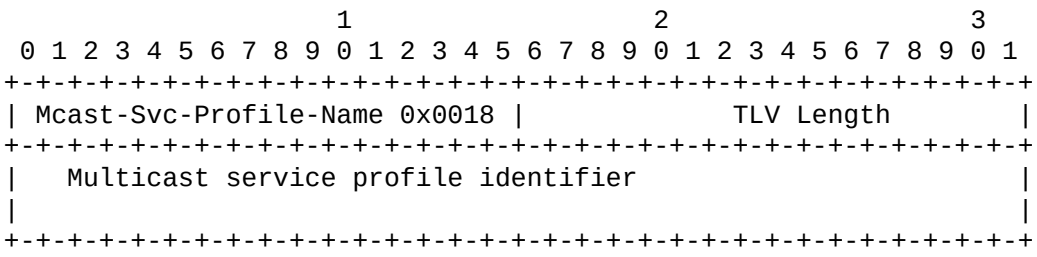


Figure 8: Multicast-Service-Profile-Name TLV

The Multicast-Service-Profile-Name TLV has the following fields:

- TLV Type: 0x0018
- TLV Length: up to 255 octets.
- Multicast service profile identifier: an opaque sequence of octets identifying a specific multicast service profile.

  Note: The identifier could have the form of human-readable text or an arbitrary binary value, depending on the operator's practices.

5.3. List-Action TLV

The List-Action TLV identifies multicast flows to be added to or removed from a list of white-, black-, or grey-listed flows. It is meaningful only in association with a Multicast-Service-Profile-Name TLV identifying the profile to which the List-Action TLV applies. Such an association can be achieved by placing both TLVs in the same base message payload or as embedded TLVs of another TLV such as the Multicast-Service-Profile TLV. The List-Action TLV is shown in Figure 9.

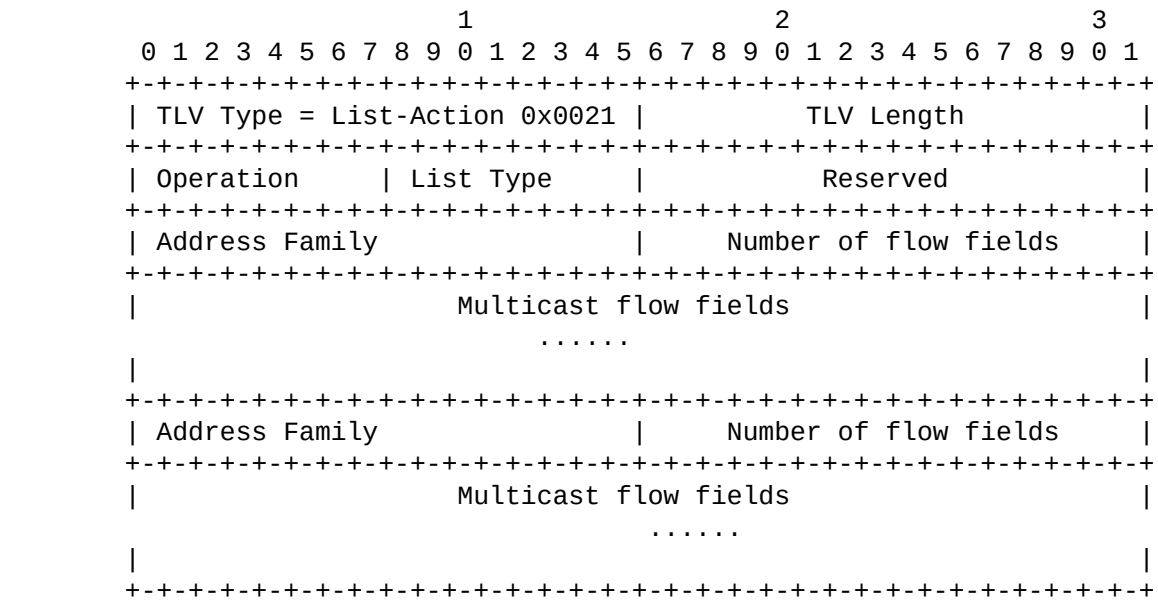


Figure 9: List-Action TLV

The List-Action TLV contains the following fields:

- TLV Type: 0x0021

- TLV Length: length of the subsequent contents.

- Operation: operation to be performed upon the white, black, or grey list identified by the List Type field within the profile identified by the associated Multicast-Service-Profile-Name embedded TLV. The possible values are:

  - 1 "Add": the multicast flow fields are to be added to the list.

  - 2 "Delete": the multicast flow fields are to be removed from the list. Each multicast flow field in the List-Action MUST match exactly an existing entry in the list concerned. Thus, to remove part of the range provided by a wildcarded list entry, it is necessary to remove the entire entry and add back the remaining partial range(s).

  - 3 "Replace": the multicast flow fields replace the existing contents of the list.

- List Type: the list type being modified by this List-Action TLV. The possible values are 1 "White", 2 "Black", or 3 "Grey".

- Reserved: a sender MUST set this field to zeroes. A receiver MUST ignore the contents of this field.

- Address Family: the IP version of the set of multicast flow fields that follow, encoded according to [PIMreg]. Possible values are 1 "IPv4" or 2 "IPv6". Either an IPv4 list or an IPv6 list or both MAY be present in the List-Action TLV.

- Number of flow fields: the number of multicast flow fields of the given address family that follows.

- Multicast flow field: a field identifying one or more multicast flows. It consists of an 8-bit group address prefix length, an 8-bit source address prefix length, a group prefix of 0-16 octets, and a source prefix of 0-16 octets, as shown in Figure 10.

Each multicast flow field refers either to a Source-Specific Multicast (SSM) channel or to an Any-Source Multicast (ASM) group. The scope of the designation may be broadened to multiple channels or groups through use of prefix length values smaller than the total address length for the given address family. Multicast flow fields MUST be placed consecutively within the embedded TLV without intervening padding except to round out individual addresses to the nearest octet boundary.

A multicast flow field consists of two single-octet prefix lengths followed by zero to two prefix values as shown in Figure 10:

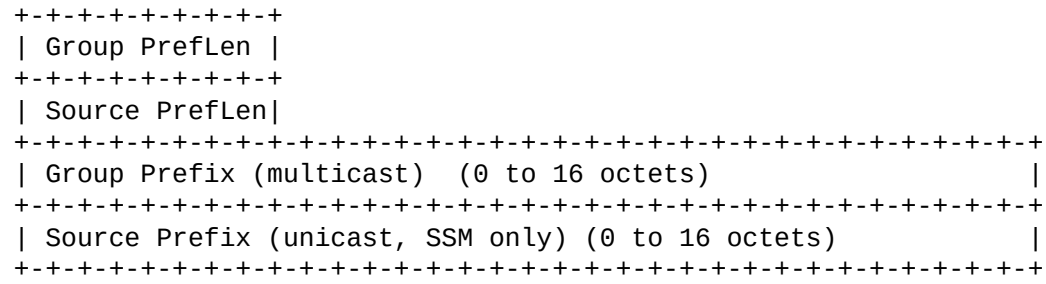


Figure 10: Organization of a Single Multicast Flow Field

The prefix length has its usual meaning. It is the number of most-significant bits specified within the corresponding prefix. The prefix length MAY vary from 0 to 32 in the IPv4 sub-list and from 0 to 128 in the IPv6 sub-list.

A value of 0 for either the Group PrefLen (prefix length) or the Source PrefLen indicates that any value of the corresponding address will match (wildcard). If the value 0 is provided for a particular prefix length, the corresponding prefix MUST be omitted from the field contents.

The length of a Source or Group Prefix field is equal to (PrefLen + 7)/8 octets, truncated to the nearest integer. Unused bits at the end of the prefix MUST be set to zeroes.

5.4. Sequence-Number TLV

The Sequence-Number TLV conveys a sequence number of some sort. The specific meaning of the sequence number is message-specific. Within this specification, the Sequence-Number TLV is used as an embedded TLV in a Status-Info TLV in a Generic Response message reporting a failed command in a Multicast Replication Control or Multicast Admission Request message. It identifies the sequence number within the message of the command that failed.

The Sequence-Number TLV has the format shown in Figure 11.

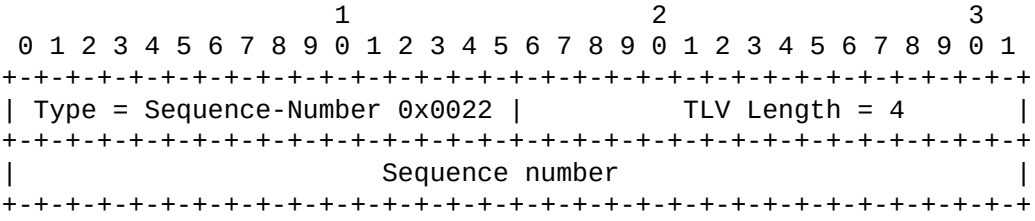


Figure 11: Sequence-Number TLV

The Sequence-Number TLV has the following fields:

- TLV Type: 0x0022
- TLV Length: 4
- Sequence number: the sequence number of a specific entity within a series, where numbering starts from 1 for the first entity in the series. Represented as a 32-bit binary number, most significant bit first.

5.5. Bandwidth-Allocation TLV

The Bandwidth-Allocation TLV is used to indicate the total amount of video bandwidth delegated to the AN for multicast admission control for a given access line, in kilobits per second. The TLV has the format shown in Figure 12.

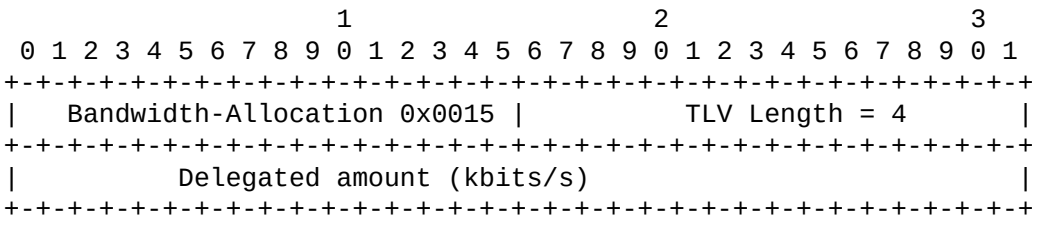


Figure 12: Bandwidth-Allocation TLV

The Bandwidth-Allocation TLV has the following fields:

- TLV Type: 0x0015
- TLV Length: 4
- Delegated amount: the bandwidth amount delegated to the AN for admission of multicast video on a given port, kilobits per second. Represented as a 32-bit binary value, most significant bit first.

5.6. White-List-CAC TLV

The White-List-CAC TLV is used to indicate that the NAS wishes the AN to do admission control for white-listed flows. Details on when the White-List-CAC TLV may be provisioned are specified in Section 6. The White-List-CAC TLV is illustrated in Figure 13.

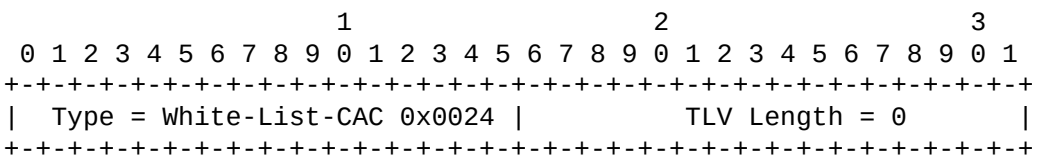


Figure 13: White-List-CAC TLV

The White-List-CAC TLV contains the following fields:

- TLV Type: 0x0024
- TLV Length: 0, since the TLV contains no data other than the TLV header.

5.7. MRepCtl-CAC TLV

The MRepCtl-CAC TLV is used to indicate that the NAS wishes the AN to do admission control for flows added by the Multicast Replication Control message. Details on when the MRepCtl-CAC TLV may be provisioned are specified in Section 6. The MRepCtl-CAC TLV is illustrated in Figure 14.

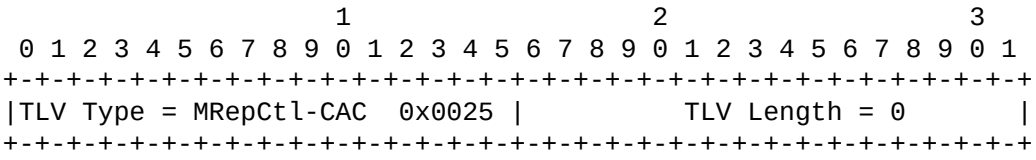


Figure 14: MRepCtl-CAC TLV

The MRepCtl-CAC TLV contains the following fields:

- TLV Type: 0x0025
- TLV Length: 0, since the TLV contains no data other than the TLV header.

5.8. Bandwidth-Request TLV

The Bandwidth-Request TLV is used to request an adjustment of the total amount of video bandwidth allocated to the AN for multicast admission control for a given line. The "Required amount" field indicates the minimum adjustment required to meet the request. The "Preferred amount" field indicates the adjustment the requestor would prefer to have, if possible. Section 4.5 discusses the required relationships between the "Required amount", "Preferred amount", and current values of total bandwidth allocated to the AN.

The Bandwidth-Request TLV has the format shown in Figure 15.

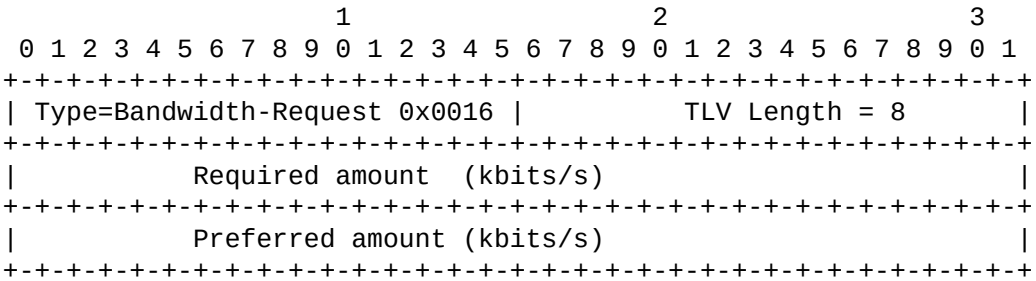


Figure 15: Bandwidth-Request TLV

The Bandwidth-Request TLV has the following fields:

- TLV Type: 0x0016
- TLV Length: 8 octets
- Required amount: the minimum or maximum amount, depending on whether the sender is the AN or the NAS respectively, of delegated video bandwidth that is being requested, in kilobits per second. Represented as a 32-bit binary value, most significant bit first.
- Preferred amount: the preferred amount of delegated video bandwidth that is being requested, in kilobits per second. Represented as a 32-bit binary value, most significant bit first.

5.9. Request-Source-IP TLV

The Request-Source-IP TLV provides the IP address of the entity that originated a specific request to join or leave a multicast channel. The TLV is illustrated in Figure 16.

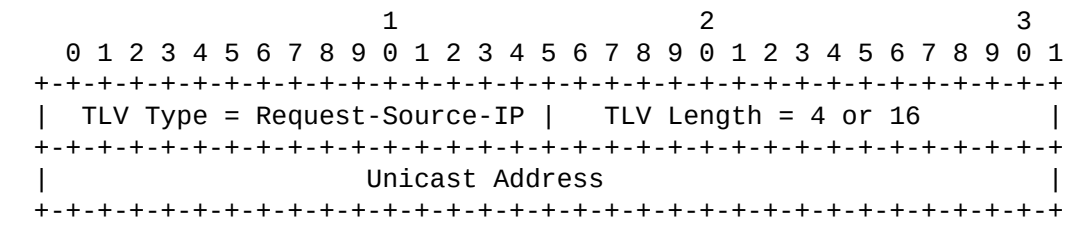


Figure 16: Request-Source-IP TLV

The Request-Source-IP TLV contains the following fields:

- TLV Type: 0x0092
- TLV Length: 4 for an IPv4 address or 16 for an IPv6 address.
- Unicast address: IP address of the source of a multicast flow join request, in network byte order.

5.10. Request-Source-MAC TLV

The Request-Source-MAC TLV provides the MAC address of the entity that originated a specific request to join or leave a multicast channel. The TLV is illustrated in Figure 17.

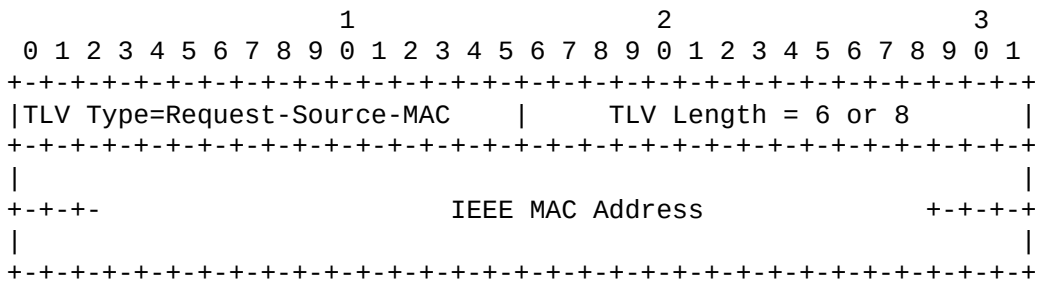


Figure 17: Request-Source-MAC TLV

The Request-Source-MAC TLV contains the following fields:

- TLV Type: 0x0093.
- TLV Length: either 6 octets (MAC-48 or EUI-48) or 8 octets (EUI-64).
- IEEE MAC Address: MAC address of the device originating the request to join a multicast flow. Within the address, bytes and bits, respectively, shall be ordered from most to least significant, consistent with [IEEE48] for MAC-48 and EUI-48 and with [IEEE64] for EUI-64.

  Note: EUI-48 and EUI-64 are registered trademarks of the IEEE.

5.11. Request-Source-Device-Id TLV

The Request-Source-Device-Id TLV provides a local identifier of the entity that originated a specific request to join or leave a multicast channel. The TLV is illustrated in Figure 18.

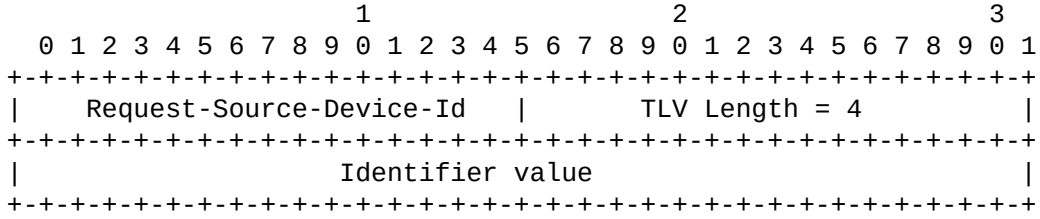


Figure 18: Request-Source-Device-Id TLV

The Request-Source-Device-Id TLV contains the following fields:

- TLV Type: 0x0096.
- TLV Length: 4
- Identifier value: local device identifier value, known to the AN and AAA. Given that the scope of the identifier is a single customer network, 32 bits is a more-than-sufficient numbering space.

5.12. Multicast-Flow TLV

IGMPv3 [RFC3376] and MLDv2 [RFC3810] allow multicast listeners to specify multiple source addresses for the same multicast group. Similarly, the Multicast-Flow TLV specifies a multicast flow in terms of its multicast group address and, if applicable, one or more unicast source addresses. The Multicast-Flow TLV is illustrated in Figure 19.

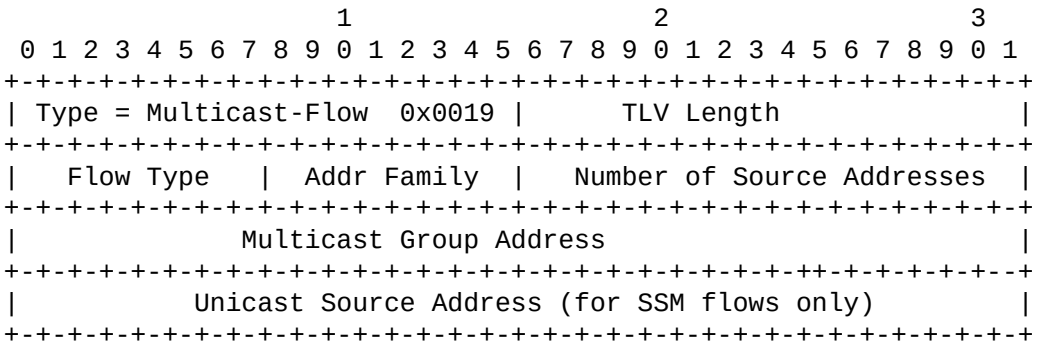


Figure 19: Multicast-Flow TLV

The Multicast-Flow TLV has the following fields:

- TLV Type: 0x0019
- TLV Length: ranges from a minimum of 8 (for an ASM IPv4 flow) upwards. Total length is 4 + 4*(Number of Source Addresses +1) for IPv4 or 4 + 16*(Number of Source Addresses + 1) for IPv6.
- Flow Type: 1 "Any-Source Multicast (ASM)", 2 "Source-Specific Multicast (SSM)".
- Addr Family: address family of the multicast source and group addresses, encoded in accordance with the IANA "PIM Address Family" registry ([PIMreg]). 1 indicates IPv4; 2 indicates IPv6.

- Number of Source Addresses: 0 for ASM, 1 or more for SSM.

- Multicast Group Address: a multicast group address within the given address family. The group address MUST always be present.

- Unicast Source Address: unicast address within the given address family. If the Flow Type is "ASM" (1), a source address MUST NOT be present. If the Flow Type is "SSM" (2), the number of source addresses given by the Number of Source Addresses field MUST be present.

The full versions of IGMPv3 and MLDv2 support both INCLUDE and EXCLUDE modes for specifying the desired sources for SSM flows. The Multicast-Flow TLV supports INCLUDE mode only. [RFC5790] (Lightweight IGMPv3 and MLDv2) provides guidance on converting EXCLUDE mode IGMP/MLD records to INCLUDE mode for the Multicast-Flow TLV.

5.13. Report-Buffering-Time TLV

The Report-Buffering-Time TLV provides the time for which a Committed Bandwidth Report message must be held with the intention of accumulating multiple reports of changed committed multicast bandwidth in one report, to reduce the volume of messages sent to the NAS. For further information see Section 6.2.2. The TLV is illustrated in Figure 20.

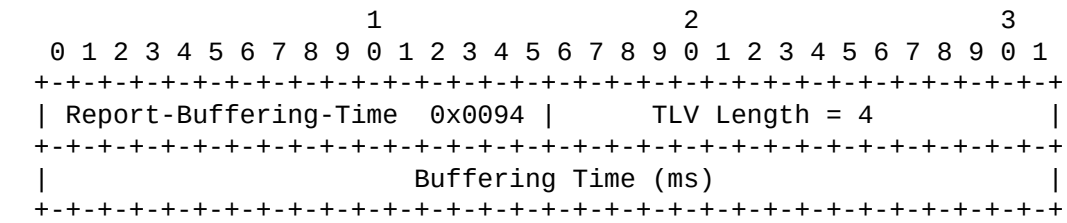


Figure 20: Report-Buffering-Time TLV

The Report-Buffering-Time TLV contains the following fields:

- TLV Type: 0x0094

- TLV Length: 4 octets

- Buffering Time is a 32-bit unsigned integer containing a time value in milliseconds (ms).

5.14. Committed-Bandwidth TLV

The Committed-Bandwidth TLV identifies an access line and provides the current amount of multicast bandwidth that the AN has committed to it. The TLV is illustrated in Figure 21.

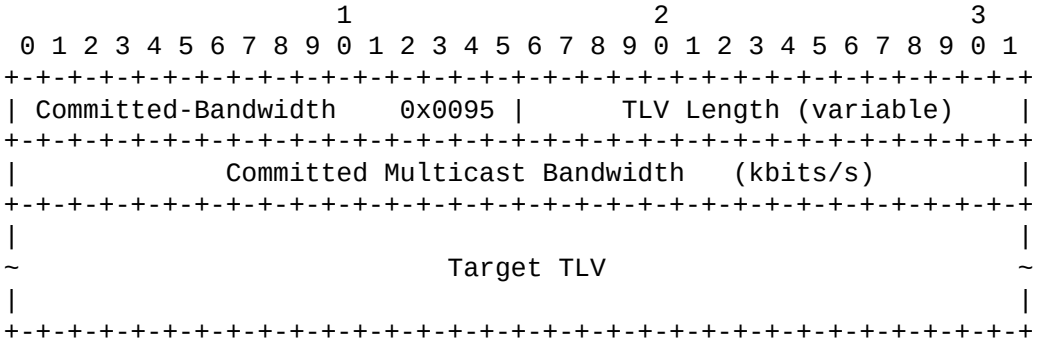


Figure 21: Committed-Bandwidth TLV

The Committed-Bandwidth TLV contains the following fields:

- TLV Type: 0x0095
- TLV Length: 4 octets plus the length of the Target TLV, including its header and any padding.
- Committed Multicast Bandwidth: a 32-bit unsigned integer providing a bandwidth amount in kbits/s.
- Target TLV: identifies the access line to which this amount of multicast bandwidth is currently committed.

6. Multicast Capabilities

Section 3.5 of [RFC6320] defines a capability negotiation mechanism as well as a number of capabilities. This section defines five new capabilities in support of different modes of multicast operation:

- NAS-initiated multicast replication (capability type 3);
- committed bandwidth reporting (capability type 5);
- conditional access and admission control with white and black lists (capability type 6);

- conditional access and admission control with grey lists (capability type 7); and

- bandwidth delegation (capability type 8).

The "Capability Data" field within the Capability TLV for all of these capabilities is empty. All of these capabilities are independent of the access technology.

The remainder of this section consists of three sub-sections. Section 6.1 specifies the protocol elements that must be implemented in order to support each capability. Section 6.2 specifies the procedures that apply to each capability on its own. Section 6.3 specifies how the capabilities interact if more than one multicast capability is included in the set of capabilities negotiated between the AN and the NAS.

6.1. Required Protocol Support

This section specifies the protocol elements that MUST be implemented to support each of the five multicast capabilities. Support of multiple multicast capabilities requires implementation of the union of the sets of protocol elements applying to each of the individual capabilities in the supported set.

In addition to the elements listed below, implementation of the Target TLV (Section 4.3 of [RFC6320]) is REQUIRED for all of the capabilities specified in this document.

6.1.1. Protocol Requirements for NAS-Initiated Multicast Replication

Table 1 specifies the protocol elements within Section 4 and Section 5 that MUST be implemented to support the NAS-initiated multicast replication capability. Additionally, implementation of the Multicast Replication Control message requires implementation of the Command TLV (Section 4.4 of [RFC6320] with additional details in Section 4.3 of this document).

Reference	Protocol Element
Section 4.1	Provisioning message with MRepCtl-CAC TLV
Section 4.2	Port Management message with Bandwidth-Allocation TLV
Section 4.3	Multicast Replication Control message
Section 4.9	Multicast Flow Query Request and Response messages
Section 5.4	Sequence Number TLV
Section 5.5	Bandwidth-Allocation TLV
Section 5.7	MRepCtl-CAC TLV
Section 5.12	Multicast-Flow TLV

Table 1: Protocol Requirements for NAS-Initiated Multicast Replication

6.1.2. Protocol Requirements for Committed Multicast Bandwidth Reporting

Table 2 specifies the protocol elements within Section 4 and Section 5 that MUST be implemented to support the committed multicast bandwidth reporting capability.

Reference	Protocol Element
Section 4.1	Provisioning message with Report-Buffering-Time TLV
Section 4.10	Committed Bandwidth Report message
Section 4.9	Multicast Flow Query Request and Response messages
Section 5.13	Report-Buffering-Timer TLV
Section 5.14	Committed-Bandwidth TLV
Section 5.12	Multicast-Flow TLV

Table 2: Protocol Requirements for Committed Multicast Bandwidth Reporting

6.1.3. Protocol Requirements for Conditional Access and Admission Control with White and Black Lists

Table 3 specifies the protocol elements within Section 4 and Section 5 that MUST be implemented to support the conditional access and admission control with white and black lists multicast capability.

Reference	Protocol Element
Section 4.1	Provisioning message with Multicast-Service-Profile TLV, white and black lists only, and White-List-CAC TLV
Section 4.2	Port Management message with Multicast-Service-Profile-Name and Bandwidth-Allocation TLVs
Section 4.9	Multicast Flow Query Request and Response messages
Section 5.1	Multicast-Service-Profile TLV
Section 5.2	Multicast-Service-Profile-Name TLV
Section 5.3	List-Action TLV, white and black lists only
Section 5.5	Bandwidth-Allocation TLV
Section 5.6	White-List-CAC TLV
Section 5.12	Multicast-Flow TLV

Table 3: Protocol Requirements for Conditional Access and Admission Control with White and Black Lists

6.1.4. Protocol Requirements for Conditional Access and Admission Control with Grey Lists

Table 4 specifies the protocol elements within Section 4 and Section 5 that MUST be implemented to support the conditional access and admission control with grey lists multicast capability. Additionally, implementation of the Multicast Replication Control message requires implementation of the Command TLV (Section 4.4 of [RFC6320] with additional details in Section 4.3 of this document).

Reference	Protocol Element
Section 4.1	Provisioning message with Multicast-Service-Profile TLV, grey lists only, and MRepCtl-CAC TLV
Section 4.2	Port Management message with Multicast-Service-Profile-Name and Bandwidth-Allocation TLVs
Section 4.3	Multicast Replication Control message
Section 4.4	Multicast Admission Control message
Section 4.9	Multicast Flow Query Request and Response messages
Section 5.1	Multicast-Service-Profile TLV, grey lists only
Section 5.2	Multicast-Service-Profile-Name TLV
Section 5.3	List-Action TLV, grey lists only
Section 5.4	Sequence Number TLV
Section 5.5	Bandwidth-Allocation TLV
Section 5.7	MRepCtl-CAC TLV
Section 5.9	Request-Source-IP TLV
Section 5.10	Request-Source-MAC TLV
Section 5.11	Request-Source-Device-Id TLV
Section 5.12	Multicast-Flow TLV

Table 4: Protocol Requirements for Conditional Access and Admission Control with Grey Lists

6.1.5. Protocol Requirements for Bandwidth Delegation

Table 5 specifies the protocol elements within Section 4 and Section 5 that MUST be implemented to support the bandwidth delegation capability.

Reference	Protocol Element
Section 4.2	Port Management message with Bandwidth-Allocation TLV
Section 4.5	Bandwidth Reallocation Request message
Section 4.6	Bandwidth Transfer message
Section 4.7	Delegated Bandwidth Query Request message
Section 4.8	Delegated Bandwidth Query Response message
Section 4.9	Multicast Flow Query Request and Response messages
Section 5.5	Bandwidth-Allocation TLV
Section 5.8	Bandwidth-Request TLV
Section 5.12	Multicast-Flow TLV

Table 5: Protocol Requirements for Bandwidth Delegation

6.2. Capability-Specific Procedures for Providing Multicast Service

This section describes multicast service procedures for each capability as if it were the only multicast capability within the negotiated set. Procedures involving combinations of multicast capabilities are described in Section 6.3.

The use of the Multicast Flow Query Request and Response messages to determine the association between multicast flows and ports is common to all multicast capabilities. No additional text is required here, beyond that already given in Section 4.9 to describe the use of those messages.

6.2.1. Procedures for NAS-Initiated Multicast Replication

NAS-initiated multicast replication may be negotiated to support a mode of operation where IGMP/MLD requests are terminated on the NAS. Alternatively, it may be negotiated to allow the NAS to respond to requests sent by other means (e.g., through application signaling) that require the replication of multicast channels to a given access line.

6.2.1.1. Provisioning

The NAS MAY perform admission control for NAS-initiated replication. In this case, it MUST NOT include the MRepCtl-CAC TLV in a Provisioning message sent to the AN. Alternatively, the NAS MAY enable admission control at the AN for NAS-initiated multicast replication. To do this, it MUST include the MRepCtl-CAC TLV in a Provisioning message sent to the AN, and it MUST also include a Bandwidth-Allocation TLV in a Port Management message for each access line.

6.2.1.2. Multicast Service Procedures

The procedures associated with NAS-initiated multicast replication are straightforward. To initiate replication, the NAS MUST send a Multicast Replication Control message to the AN, containing one or more commands adding flows, as described in Section 4.3.1. To terminate replication, the NAS MUST send a Multicast Replication Control message where the commands delete instead of adding the flows. The AN acts upon these messages as specified in Section 4.3.2.

6.2.2. Procedures for Committed Bandwidth Reporting

Committed bandwidth reporting may be negotiated if the NAS requires current knowledge of the amount of multicast bandwidth committed to each access line and cannot obtain this information by other means.

6.2.2.1. Provisioning

The default buffering time when committed bandwidth reporting is enabled is zero (immediate reporting). To change this, the NAS MAY send an instance of the Report-Buffering-Time TLV containing a non-zero time value to the AN in a Provisioning message. If the NAS subsequently wishes to change the buffering time again, it MAY do so in another Provisioning message.

6.2.2.2. Multicast Service Procedures

If the buffering time for committed bandwidth reporting is zero, the AN MUST send a Committed Bandwidth Report message to the NAS each time the amount of multicast bandwidth committed to any access line under its control changes.

If a non-zero value is provided in the Report-Buffering-Time TLV, the AN is in one of two states at any given moment: not-buffering or buffering. The AN enters buffering state if it is in not-buffering state and the multicast bandwidth amount committed to some access line changes. It leaves buffering state when the AN sends a Committed Bandwidth Report message.

Upon entry to the buffering state, the AN MUST start a buffering timer and create a Committed Bandwidth Report message containing a Committed-Bandwidth TLV for the triggering access line, but it MUST NOT send it. If a multicast bandwidth change occurs for another access line, the AN MUST add a new Committed-Bandwidth TLV to the message for that additional line. If a multicast bandwidth change occurs for a line for which a Committed-Bandwidth TLV is already present in the buffered report, the AN MUST update the corresponding Committed-Bandwidth TLV to contain the new bandwidth value rather than adding another Committed-Bandwidth TLV for the same access line.

The buffering timer expires after the period provided by the Report-Buffering-Time TLV. When it expires, the AN MUST send the Committed Bandwidth Report message that it has been accumulating to the NAS. Exceptionally, the AN MAY choose to send the message before the timer expires, in which case it MUST clear the buffering timer when the message is sent. In either case, the AN enters the not-buffering state as a result.

> Note: Report buffering implies that NAS reaction to changes in multicast bandwidth usage is delayed by the amount of the buffering period. The choice of buffering period must take this into consideration.

6.2.3. Procedures for Conditional Access and Admission Control with Black and White Lists

6.2.3.1. Provisioning

The NAS provisions named multicast service profiles containing white and black lists on the AN using the Provisioning message containing one or more Multicast-Service-Profile TLVs. The NAS MAY update the contents of these profiles from time to time as required by sending

additional Provisioning messages with Multicast-Service-Profile TLVs containing incremental modifications to the existing white and black lists or replacements for them.

The NAS assigns a specific multicast service profile to an individual access line using the Port Management message containing a Multicast-Service-Profile-Name TLV. The NAS MAY change the multicast service profile for a given access line at any time by sending a Port Management message identifying a new multicast service profile.

The NAS MAY choose to enable admission control at the AN for white-listed flows. To do this, it MUST send a Provisioning message as described in Section 4.1, which includes the White-List-CAC TLV, and it MUST provide a multicast bandwidth allocation for each access line by including a Bandwidth-Allocation TLV in a Port Management message.

6.2.3.2. Multicast Service Procedures

The conditional access and admission control with white and black lists capability assumes that IGMP/MLD requests are terminated on the AN. When the AN receives a join request, it MUST check to see whether the requested flow is white-listed or black-listed as described below. Requests for black-listed flows MUST be discarded. If the NAS has enabled admission control on the AN as described in the previous section, but a white-listed flow would cause the amount of committed multicast bandwidth to exceed the provisioned limit, the request MUST be discarded. The AN replicates flows passing these checks to the access line.

To determine if a requested flow is white-listed, the AN searches for a best match to the flow in the applicable multicast service profile. Matching is done on the prefixes specified in the profile, ignoring the address bits of lower order than those in the prefix.

If the requested multicast flow matches multiple lists associated with the access line, then the most specific match will be considered by the AN. If the most specific match occurs in multiple lists, the black list entry takes precedence over the white list. In this context, the most specific match is defined as:

- first, most specific match (longest prefix length) on the multicast group address (i.e., on G of <S,G>), and
- then, most specific match (longest prefix length) on the unicast source address (i.e., on S of <S,G>).

If the requested multicast flow is not part of any list, the join message SHOULD be discarded by the AN. This default behavior can easily be changed by means of a "catch-all" statement in the white list. For instance, adding (<S=*,G=*>) in the white List would make the default behavior to accept join messages for a multicast flow that has no other match on any list.

When the AN receives a leave request, it terminates replication of the multicast flow.

If the AN receives a Provisioning message that updates an existing multicast service profile, the AN MUST review the status of active flows on all ports to which the updated profile is currently assigned. Similarly, if a Port Management message assigns a new multicast service profile to a given port, the AN MUST review all active flows on that port. If the most specific match for any flow is a black list entry, the flow MUST be terminated immediately. If any of the remaining flows do not match an entry in the white list, they also MUST be terminated immediately. White-listed flows MUST be allowed to continue.

6.2.4. Procedures for Conditional Access and Admission Control with Grey Lists

6.2.4.1. Provisioning

The NAS provisions named multicast service profiles containing grey lists on the AN using the Provisioning message containing one or more Multicast-Service-Profile TLVs. The NAS MAY update the contents of these profiles from time to time as required by sending additional Provisioning messages with Multicast-Service-Profile TLVs containing incremental modifications to the existing grey lists or replacements for them.

The NAS assigns a specific multicast service profile to an individual access line using the Port Management message containing a Multicast-Service-Profile-Name TLV. The NAS MAY change profiles on the line by sending a subsequent Port Management message identifying a new profile.

The NAS MAY perform admission control for grey-listed flows. In that case, the NAS MUST NOT include the MRepCtl-CAC TLV in a Provisioning message sent to the AN. Alternatively, the NAS MAY enable admission control at the AN for grey-listed flows. To do this, it MUST include the MRepCtl-CAC TLV in a Provisioning message sent to the AN and MUST also provide a Bandwidth-Allocation TLV in a Port Management message for each access line.

6.2.4.2. Multicast Service Procedures

The conditional access and admission control with grey lists capability assumes that IGMP/MLD requests are terminated on the AN. When the AN receives a join request, it MUST determine whether there is a match to the requested flow in the grey list of the multicast service profile provisioned against the given access line. If there is no match, the request is discarded. Otherwise, the AN MUST send a Multicast Admission Control message to the NAS with content identifying the access line and the multicast flow to be added. As indicated in Section 4.4, the AN MAY add information identifying the requesting device.

If the NAS decides to enable the flow, it MUST send a Multicast Replication Control message to the AN to replicate the flow to the access line with the Result field set to Nack (0x1), as described in Section 4.3.1.

When the AN receives the Multicast Replication Control message, it performs admission control if that has been enabled as described in the previous section. If admitting the flow would cause the committed multicast bandwidth at the access line to exceed the provisioned limit, the AN reports an error to the NAS as described in Section 4.3.2. Otherwise, it replicates the multicast flow as requested.

If the NAS decides not to permit the flow, it MAY send a Multicast Replication Control message in response to the Multicast Admission Control message to allow the AN to update its internal records. The content of this message is described in Section 4.4.2.

When the AN receives a leave request, it MUST terminate replication of the flow to the access line. It MUST then send a Multicast Admission Control message to the NAS indicating the deletion. The NAS updates its internal records but MUST NOT respond to the message.

If the AN receives a Provisioning message that updates an existing multicast service profile, the AN MUST review the status of active flows on all ports to which the updated profile has been assigned. Similarly, if the AN receives a Port Management message that assigns a new profile to a given port, the AN MUST review all active flows on that port. In either case, if any flow does not match an entry in the grey list, it MUST be terminated immediately.

6.2.5. Procedures for Bandwidth Delegation

6.2.5.1. Provisioning

The NAS SHOULD provision an initial amount of delegated multicast bandwidth for each access line using the Port Management message containing the Bandwidth-Allocation TLV.

> Note: If it fails to do so and a value has not been provisioned on the AN by other means, the AN will be forced to request a bandwidth allocation as soon as it receives a join request.

The NAS MAY, at any time, force an update of the amount of delegated bandwidth by the same means.

6.2.5.2. Multicast Service Procedures

The bandwidth delegation capability assumes that IGMP/MLD requests are terminated on the AN. When the AN receives a join request, it checks whether it has sufficient remaining uncommitted multicast bandwidth on the access line to accommodate the new multicast flow. If not, it MAY send a request to the NAS for an increased allocation of delegated bandwidth using the Bandwidth Reallocation Request message. The NAS MUST return a Bandwidth Transfer message indicating whether it has granted the request and, if so, the new amount of delegated bandwidth.

If the AN has sufficient uncommitted multicast capacity to admit the request, either originally or as the result of a successful request to the NAS, it replicates the requested flow to the access line. Otherwise, it discards the request.

When the AN receives a leave request for an active flow, it ceases replication.

The NAS or AN MAY, at some point, detect that their respective views of the amount of delegated bandwidth are inconsistent. If so, they can recover using procedures described in Sections 4.5 and 4.6. As a further aid to synchronization, either the NAS or the AN MAY from time to time check the peer's view of the amount of delegated bandwidth using the Delegated Bandwidth Query message.

The NAS or AN MAY, at any time, release bandwidth to the peer using an autonomous Bandwidth Transfer message. The contents of this message are described in Section 4.6.

6.3. Combinations of Multicast Capabilities

6.3.1. Combination of Conditional Access and Admission Control with White and Black Lists and Conditional Access and Admission Control with Grey Lists

If conditional access and admission control with white and black lists is combined with conditional access and admission control with grey lists, provisioning of the multicast service profiles is as described in Section 6.2.3.1 except that multicast service profiles will also include grey lists. Admission control is enabled independently on the AN for white lists by including the White-List-CAC TLV in the Provisioning message and for grey lists by including the MRepCtl-CAC TLV in the Provisioning message. The Bandwidth-Allocation TLV provisions an amount that applies to both white- and grey-listed flows if admission control is enabled for both.

With regard to multicast service procedures, one point of difference from the individual capabilities must be noted. This is an interaction during the profile matching procedure. The AN MUST seek the best match among multiple lists as described in Section 6.2.3.2. However, if there are multiple matches of equal precision, the order of priority is black list first, grey list second, and white list last.

Once profile matching has been completed, processing of a join request is as described in Section 6.2.3.2 for white- or black-listed flows or Section 6.2.4.2 for grey-listed flows. Requests that do not match any list SHOULD be discarded.

When the AN receives a leave request, it MUST terminate replication of the flow to the access line. If the flow was grey-listed, the AN MUST then send a Multicast Admission Control message to the NAS indicating the deletion.

If the AN receives a Provisioning message that updates an existing multicast service profile, the AN MUST review the status of active flows on all ports to which the updated profile is currently assigned. Similarly, if a Port Management message assigns a new multicast service profile to a given port, the AN MUST review all active flows on that port. If any flow has its most specific match in a black list entry, it MUST be terminated immediately. If any of the remaining flows do not match an entry in the white or grey list, they MUST also be terminated immediately. Finally, if any remaining flows were originally admitted because they were white-listed but after the change they are grey-listed, the AN MUST generate a Multicast Flow Query Response message autonomously as if it were responding to a Multicast Flow Query Request message, listing all

such flows. These flows MUST be allowed to continue until the NAS or the subscriber terminates them. Flows with their most specific match in the white list MUST be allowed to continue.

The autonomously generated Multicast Flow Query Response message MUST be formatted as if it were a successful response to a request containing no Target and no Multicast-Flow TLV, as described in Section 4.9.2, with the exception that the Transaction Identifier field MUST be set to all zeroes.

> Note: The procedures in the previous paragraphs imply that the AN has to retain a memory of whether an admitted flow was white-listed or grey-listed at the time of its admission/readmission.

6.3.2. Combination of Conditional Access and Admission Control with Bandwidth Delegation

The provisioning and bandwidth management procedures of Section 6.2.5 apply in addition to the procedures in Sections 6.2.3, 6.2.4, or 6.3.1 as applicable. Conditional access follows the rules given in those sections in terms of matching flows against white and black and/or grey lists. When admission control is enabled at the AN, the amount of bandwidth used by the AN is negotiable as described in Section 6.2.5.2.

6.3.3. Combination of NAS-Initiated Replication with Other Capabilities

NAS-initiated multicast replication can coexist with the other capabilities, but some means must exist to prevent double replication of flows. The simplest way to do this is to terminate all IGMP/MLD requests on the AN, so that NAS-initiated multicast replication is stimulated only by signaling through other channels. Other arrangements are possible but need not be discussed here.

Assuming the necessary separation of responsibilities, the only point of interaction between NAS-initiated multicast replication and the other multicast capabilities is in the area of admission control. Specifically, if the AN is to do admission control for flows added by Multicast Replication Control messages, regardless of whether they are part of NAS-initiated replication or grey list multicast service processing, the NAS includes the MRepCtl-CAC TLV in a Provisioning message and the Bandwidth-Allocation TLV in a Port Management message. If, instead, the NAS will do admission control for flows added by Multicast Replication Control messages, regardless of whether they are part of NAS-initiated replication or grey list multicast service processing, it does not send the MRepCtl-CAC TLV in

a Provisioning message to the AN. The NAS can independently enable admission control for white flows on the AN by including the White-List-CAC TLV in the Provisioning message.

6.3.4. Combinations of Committed Bandwidth Reporting with Other Multicast Capabilities

Committed bandwidth reporting can take place independently of other multicast capabilities that have been negotiated. However, some combinations do not make sense because of redundancy. In particular, the NAS obtains the same information that committed bandwidth reporting gives if the only other capabilities operating are NAS-initiated replication and/or conditional access and admission control with grey lists.

7. Miscellaneous Considerations

This section deals with two sets of considerations. "Report Buffering Considerations" considers requirements for configuration in support of some of the committed bandwidth reporting capability. "Congestion Considerations" is a warning to implementors about the possibility of control-plane congestion, with suggestions for mitigation.

7.1. Report Buffering Considerations

The committed bandwidth reporting capability allows the provisioning of a report buffering period to reduce the number of messages the AN passes to the NAS. An appropriate value for this period, if buffering is allowed at all, depends first on the effect of delay in reporting bandwidth changes and secondly on the rate at which bandwidth changes are expected to occur.

Let us assume, in the first instance, that a delay in adjusting hierarchical scheduling at the NAS causes additional bandwidth demand to be served momentarily on a best-effort basis, introducing the possibility of jitter and, more crucially, packet loss. Appendix IV of ITU-T Recommendation G.1080 [ITU-T_G.1080] indicates that the maximum tolerable duration of a loss episode is less than 16 ms. This would more likely apply in the middle of a program rather than when it was starting up but at least gives an (extremely conservative) order of magnitude for setting the buffering period.

The next question is whether enough messaging is likely to be generated that multiple bandwidth changes would be observed within such an interval. Let us consider a reasonable example in a DSL environment, where during the busiest hour of the day subscribers start watching at the rate of one program per subscriber per hour.

Typically, because of program scheduling, the new channel requests might be concentrated within a three-minute period, giving an effective request rate of 1/(3 minutes * 60 seconds * 1000 ms/second) * 16 ms = 0.00009 requests per buffering interval of 16 ms. With these figures, an AN serving 10,000 subscribers will report an average of 0.9 bandwidth changes per 16 ms buffering interval. It appears that buffering is worthwhile only for larger-scale deployments.

Note that simple replacement of one channel with another -- channel surfing -- does not require reporting or adjustment at the NAS end.

7.2. Congestion Considerations

Implementors must beware of the possibility that a single channel-surfing subscriber could generate enough control messaging to overload the AN or the messaging channel between the AN and the NAS. The implementation problem is to strike the right balance between minimizing the processing of requests that have been overtaken by subsequent events and meeting requirements for what is termed "channel zapping delay". Nominally, such a requirement is to be found in Section 8.1 of [ITU-T_G.1080], but unfortunately no quantitative value was available at the time of publication of this document. Implementors will therefore have to base their work on discussions with customers until standardized requirements become available. (It is possible that regional bodies or more specialized bodies have overtaken the ITU-T in this regard.)

A typical strategy for minimizing the work associated with request processing includes deliberate buffering of join requests for a short period in case matching Release requests are detected, followed by discard of both requests. More generally, processing of requests from individual subscribers may be rate limited, and the global rate of messaging to the NAS can also be limited. If the AN gets overloaded, deliberate dropping of stale requests can be implemented, for some definitions of "stale".

8. Security Considerations

The security considerations of ANCP are discussed in [RFC6320] and in [RFC5713]. Multicast does not, in principle, introduce any new security considerations, although it does increase the attractiveness of ANCP as a means of denial of service (e.g., through direction of multicast streams onto the target) or theft of service.

As mentioned in Section 4.4, the inclusion of the Request-Source-MAC TLV or Request-Source-IP TLV in the Multicast Admission Control message presents privacy issues. An attacker able to get access to

the contents of this message would, like the content provider, be able to track consumption of multicast content to the individual device and potentially to individual persons if they are associated with particular devices. To make the connection between devices and individuals, the attacker needs to get information from sources other than ANCP, of course, but let us assume that this has happened.

The protection specified for ANCP in [RFC6320] will apply to the transmission of the Multicast Admission Control message across the access network to the NAS. Hence, the attacker's potential points of access are between the subscriber and the AN, at the AN and at the NAS. Moreover, if the MAC or IP address are transmitted onwards from the NAS to AAA in a request for policy, that whole onward path has to be examined for vulnerability.

The question is how many of these potential points of attack can be eliminated through operational practice. The segment from the subscriber through the AN itself seems out of the scope of this discussion -- protection of this segment is basic to subscriber privacy in any event and likely a business requirement. The segment from the AN to the NAS is covered by the basic ANCP protection specified in [RFC6320]. This leaves the NAS and the path between the NAS and AAA for consideration.

The operator can eliminate the path between the NAS and AAA as a point where the attacker can access per-device information by downloading per-device policy to the NAS for all identified user devices for the particular subscriber. The NAS then selects the applicable policy based on the particular device identifier it has received. This is as opposed to the NAS sending the identifier of the device in question to AAA and getting policy just for that device.

The alternative is to protect the path between the NAS and AAA. If Diameter is used as the AAA protocol, Section 2.2 of [RFC6733] mandates use of IPsec, TLS/TCP, or DTLS/SCTP for that purpose. If RADIUS is used, the operator should deploy TLS transport as specified in [RFC6614].

This leaves the NAS itself as a point of attack. In theory, the NAS could be eliminated if the AN remapped the requesting MAC or IP address to an identifier known to itself and AAA but not the NAS. This would require local configuration on the AN, which may be possible under some circumstances. The Request-Source-Device-Id TLV specified in Section 5.11 is available to transmit such an identifier in place of the Request-Source-MAC TLV or Request-Source-IP TLV.

9. IANA Considerations

This document defines the following additional values within the "ANCP Message Types" registry:

Message Type	Message Name	Reference
144	Multicast Replication Control	RFC 7256
145	Multicast Admission Control	RFC 7256
146	Bandwidth Reallocation Request	RFC 7256
147	Bandwidth Transfer	RFC 7256
148	Delegated Bandwidth Query	RFC 7256
149	Multicast Flow Query	RFC 7256
150	Committed Bandwidth Report	RFC 7256

This document defines the following additional values for the "ANCP Result Codes" registry. In support of these assignments, IANA has changed the lower limit of 0x100 specified by [RFC6320] for assignments by IETF Consensus to 0x64.

Result Code	One-Line Description	Reference
0x64	Command error.	RFC 7256
0x65	Invalid flow address.	RFC 7256
0x66	Multicast flow does not exist.	RFC 7256
0x67	Invalid preferred bandwidth amount.	RFC 7256
0x68	Inconsistent views of delegated bandwidth amount.	RFC 7256
0x69	Bandwidth request conflict.	RFC 7256

This document defines the following additional values for the "ANCP Command Codes" registry:

Command Code Value	Command Code Directive Name	Reference
1	Add	RFC 7256
2	Delete	RFC 7256
3	Delete All	RFC 7256
4	Admission Control Reject	RFC 7256
5	Conditional Access Reject	RFC 7256
6	Admission Control and Conditional Access Reject	RFC 7256

This document defines the following additional values within the "ANCP TLV Types" registry:

Type Code	TLV Name	Reference
0x0013	Multicast-Service-Profile	RFC 7256
0x0015	Bandwidth-Allocation	RFC 7256
0x0016	Bandwidth-Request	RFC 7256
0x0018	Multicast-Service-Profile-Name	RFC 7256
0x0019	Multicast-Flow	RFC 7256
0x0021	List-Action	RFC 7256
0x0022	Sequence-Number	RFC 7256
0x0024	White-List-CAC	RFC 7256
0x0025	MRepCtl-CAC	RFC 7256
0x0092	Request-Source-IP	RFC 7256
0x0093	Request-Source-MAC	RFC 7256
0x0094	Report-Buffering-Time	RFC 7256
0x0095	Committed-Bandwidth	RFC 7256
0x0096	Request-Source-Device-Id	RFC 7256

This document defines the following additional values for the "ANCP Capability Types" registry:

Value	Capability Type Name	Tech Type	Capability Data?	Reference
3	NAS-Initiated Multicast Replication	0	No	RFC 7256
5	Committed Bandwidth Reporting	0	No	RFC 7256
6	Conditional Access and Admission Control with White and Black Lists	0	No	RFC 7256
7	Conditional Access and Admission Control with Grey Lists	0	No	RFC 7256
8	Bandwidth Delegation	0	No	RFC 7256

10. Acknowledgements

The authors would like to acknowledge Wojciech Dec for providing useful input to this document, Robert Rennison for his help in shaping the definition of the Multicast-Service-Profile TLV, Shridhar Rao for his comments and suggestions, and Aniruddha A for his proposal that formed the base of the Multicast Flow Reporting solution. Philippe Champagne, Sanjay Wadhwa, and Stefaan De Cnodder provided substantial contributions on the solution for the NAS-initiated multicast control use case. Kristian Poscic provided the committed bandwidth reporting use case.

Thanks to the Document Shepherd, Matthew Bocci, and Area Director, Ted Lemon, for points raised by their reviews following Working Group Last Call.

Further thanks to Dacheng Zhang, Mehmet Ersue, and Christer Holmberg for their reviews on behalf of the Security, Operations, and Gen-Art directorates. Dacheng’s comments led to changes at several points in the document, while Mehmet’s led to creation of the Miscellaneous Considerations section. Finally, thanks to Brian Haberman for stimulating a review of the architectural assumptions and their relationship to the ability of user devices to obtain access to non-IPTV multicast services. This also led to changes in the document.

11. References

11.1. Normative References

[PIMreg] IANA, "Protocol Independent Multicast (PIM) Parameters", <http://www.iana.org/assignments/pim-parameters>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2710] Deering, S., Fenner, W., and B. Haberman, "Multicast Listener Discovery (MLD) for IPv6", RFC 2710, October 1999.

[RFC3376] Cain, B., Deering, S., Kouvelas, I., Fenner, B., and A. Thyagarajan, "Internet Group Management Protocol, Version 3", RFC 3376, October 2002.

[RFC3810] Vida, R. and L. Costa, "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, June 2004.

[RFC5790] Liu, H., Cao, W., and H. Asaeda, "Lightweight Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Version 2 (MLDv2) Protocols", RFC 5790, February 2010.

[RFC6320] Wadhwa, S., Moisand, J., Haag, T., Voigt, N., and T. Taylor, "Protocol for Access Node Control Mechanism in Broadband Networks", RFC 6320, October 2011.

11.2. Informative References

[IEEE48] IEEE, "Guidelines for 48-Bit Global Identifier", <http://standards.ieee.org/regauth/oui/tutorials/EUI48.html>.

[IEEE64] IEEE, "Guidelines for 64-Bit Global Identifier", <http://standards.ieee.org/regauth/oui/tutorials/EUI64.html>.

[ITU-T_G.1080] ITU-T, "Quality of experience requirements for IPTV services", ITU-T Recommendation G.1080, December 2008.

[RFC2236] Fenner, W., "Internet Group Management Protocol, Version 2", RFC 2236, November 1997.

[RFC4601] Fenner, B., Handley, M., Holbrook, H., and I. Kouvelas, "Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)", RFC 4601, August 2006.

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

[RFC5851] Ooghe, S., Voigt, N., Platnic, M., Haag, T., and S. Wadhwa, "Framework and Requirements for an Access Node Control Mechanism in Broadband Multi-Service Networks", RFC 5851, May 2010.

[RFC6614] Winter, S., McCauley, M., Venaas, S., and K. Wierenga, "Transport Layer Security (TLS) Encryption for RADIUS", RFC 6614, May 2012.

[RFC6733] Fajardo, V., Arkko, J., Loughney, J., and G. Zorn, "Diameter Base Protocol", RFC 6733, October 2012.

Appendix A. Example of Messages and Message Flows

This appendix provides an example in which most of the possible message flows for multicast control are illustrated. This appendix is for informational purposes only. In case of discrepancy with text in the body of this document, the text in the body of the document is to be considered as the normative text.

Assume the following, for a given access port:

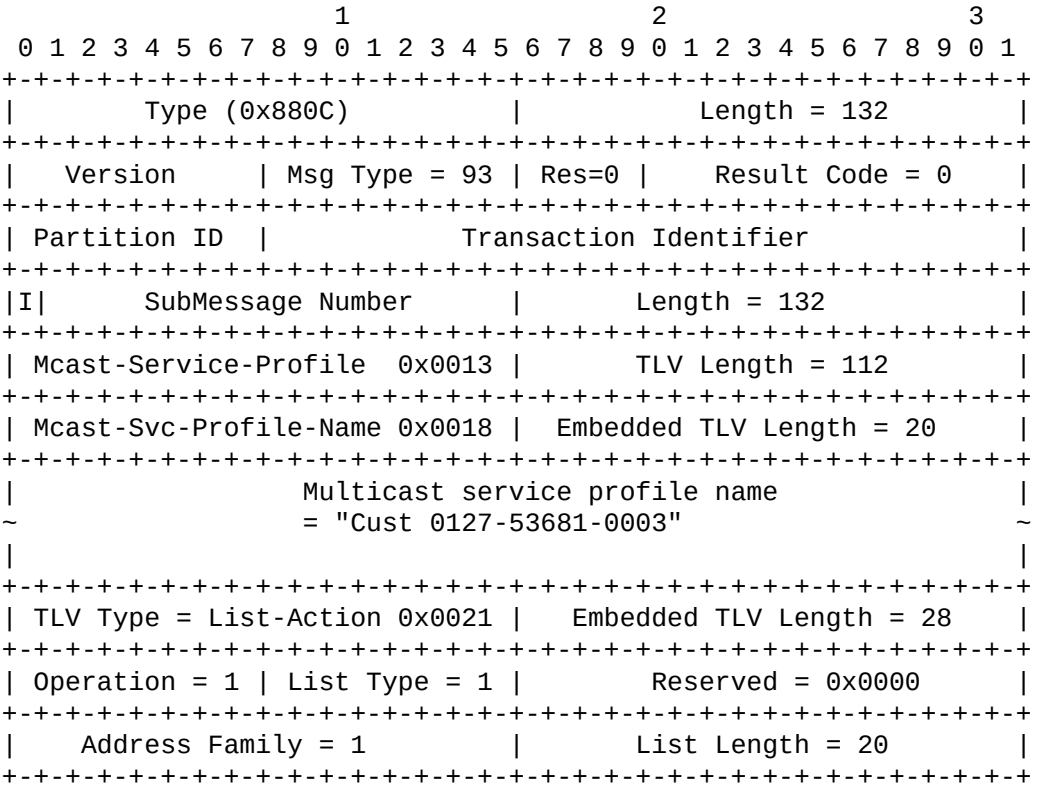
- The basic subscribed service is white-listed. The AN will be responsible for admission control for this service.
- Some premium services are available, but requests for these services must be referred to the Policy Server for proper credit processing. For this reason, they are grey-listed. The NAS will be responsible for admission control for these services.
- The subscriber has asked that certain services be blocked so that his children cannot view them. These services are black-listed.
- All of the above services are Source-Specific Multicast (SSM). In addition, by means that bypass the AN, the subscriber can signal intent to join an on-line game service that is Any-Source Multicast (ASM). The NAS is responsible for admission control for this service.
- Bandwidth delegation is, in effect, to share video bandwidth between the AN and the NAS.

The stated conditions require the use of four of the five capabilities specified in this memo.

A.1. Provisioning Phase

Assume that capability negotiation has been completed between the AN and NAS and that the set of negotiated capabilities includes the following four multicast capabilities: NAS-initiated multicast replication, conditional access and admission control with white and black lists, conditional access and admission control with grey lists, and bandwidth delegation. At this point, the NAS can provision the service profiles on the AN and enable admission control at the AN for white-listed flows. To do this, the NAS sends the AN a Provisioning message containing this information. An example message providing the profile for our assumed subscriber is shown in Figure 22. The message has the following contents:

- Message Type is 93.
- The Result and Result Code fields in the header are set to zeroes, as specified [RFC6320].
- A Transaction Identifier is assigned by the NAS.
- The Multicast-Service-Profile TLV (of which typically there would be multiple instances) contains a Multicast-Service-Profile-Name TLV (with a length of 20 octets assumed for the example) and three List-Action TLVs, one each for the white, grey, and black lists within the profile. The white list flows come in two sets of group addresses: 233.252.0.0/29, coming from a server at 192.0.2.15, and 233.252.0.32/29, coming from a server at 192.0.2.16. The grey-listed flows are in the band 233.252.0.64/29, coming from a server at 192.0.2.21. Finally, the black list flows are two individual flows that happen to overlap with the grey list band: 233.252.0.65 and 233.252.0.69, also with source 192.0.2.21.
- The White-List-CAC TLV indicates that the AN does admission control on white-listed flows.



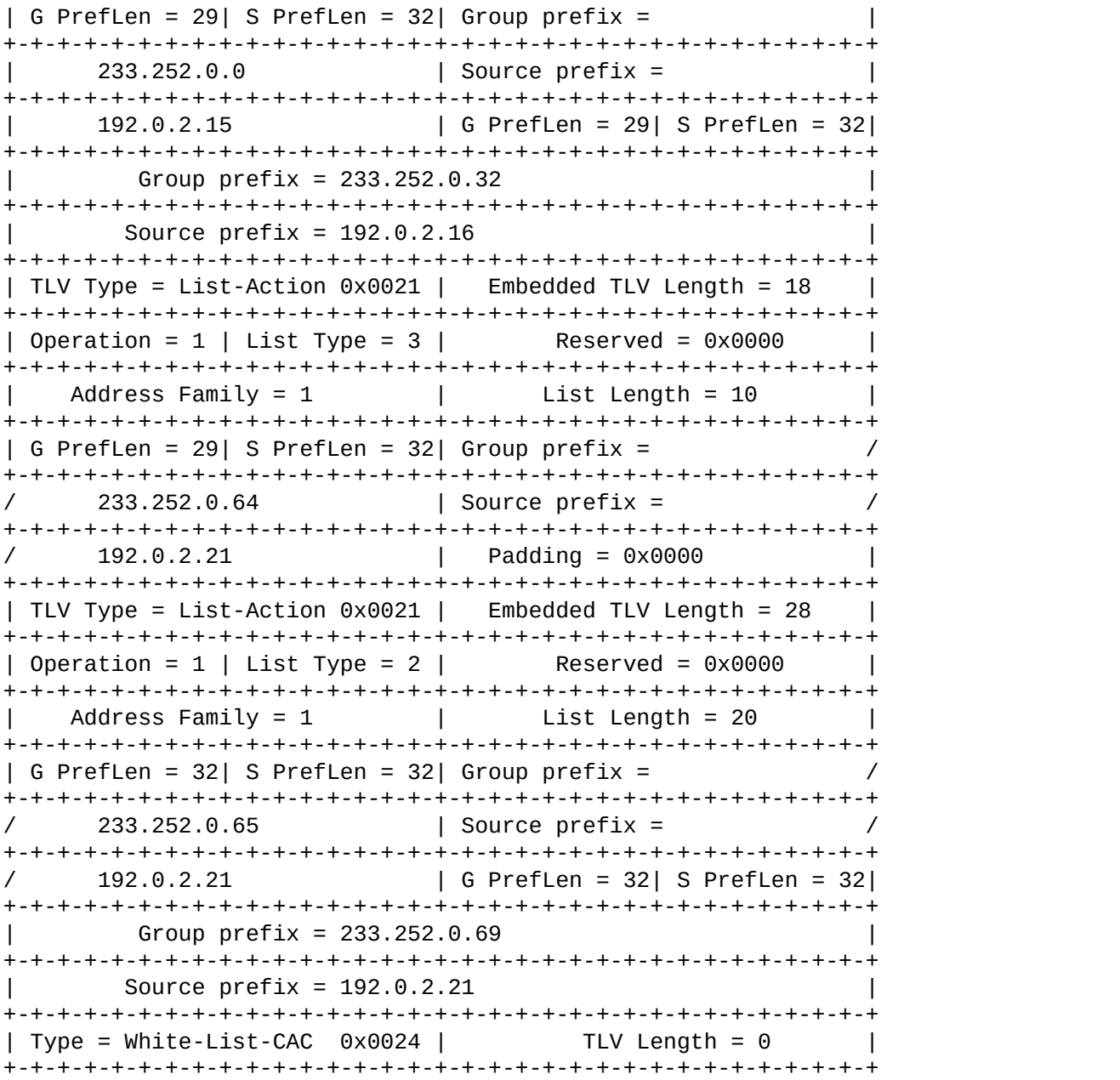
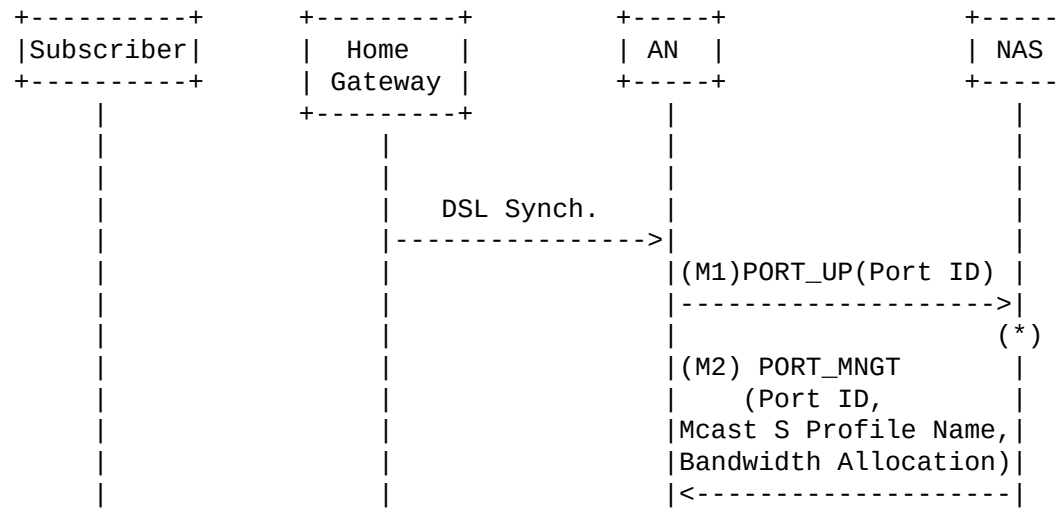


Figure 22: Example Provisioning Message

Note that the padding after the middle List-Action TLV is counted as part of the length of the Multicast-Service-Profile TLV but is not included in the length of that List-Action TLV. Note also that the Length field in the message header, unlike those in the TLVs, includes the message header itself, as required by [RFC6320].

Finally, note that the Provisioning message does not include a MRepCtl-CAC TLV since in our example admission control for grey-listed flows and for NAS-initiated replication is performed by the NAS.

As soon as the AN port comes up, the AN sends an ANCP PORT_UP message to the NAS specifying the Access Loop Circuit ID. The NAS replies with an ANCP Port Management message that, together with the other parameters, includes the multicast service profile name to be associated to that port along with the initial amount of delegated bandwidth. The corresponding message flow is illustrated in Figure 23.



(*) The NAS may optionally seek direction from an external Authorization/Policy Server

Figure 23: Configuring an AN Port with Multicast Service Profile ID and Delegated Bandwidth Amount

The Port Management message will typically contain other TLVs, but our example (Figure 24) just shows the Target, Multicast-Service-Profile-Name, and Bandwidth-Allocation TLVs. The Target TLV identifies the subscriber line, the Multicast-Service-Profile-Name TLV is identical to the one contained in the Provisioning message, and the Bandwidth-Allocation TLV provides just enough bandwidth (2000 kbits/s) for one channel to start with.

The following fields in the Port Management message header are shown with specific values either as directed by the base protocol document or for the sake of our example:

- Message Type is 32.
- Result is set to Nack (0x1) for this example.
- Result Code is 0.
- A Transaction Identifier is assigned by the NAS.
- Port is set to 0.
- Event Sequence Number, the R flag and the other bits marked x, Duration, the Event Flags, and the Flow Control Flags are all irrelevant for this function and are set to 0.
- Function is set to "Configure Connection Service Data" (8).
- X-Function is set to 0.
- Tech Type is "DSL" (5).
- Block lengths are calculated assuming a Circuit-Id length of 4 in our example. Recall that the example Multicast-Service-Profile-Name TLV length is 20.

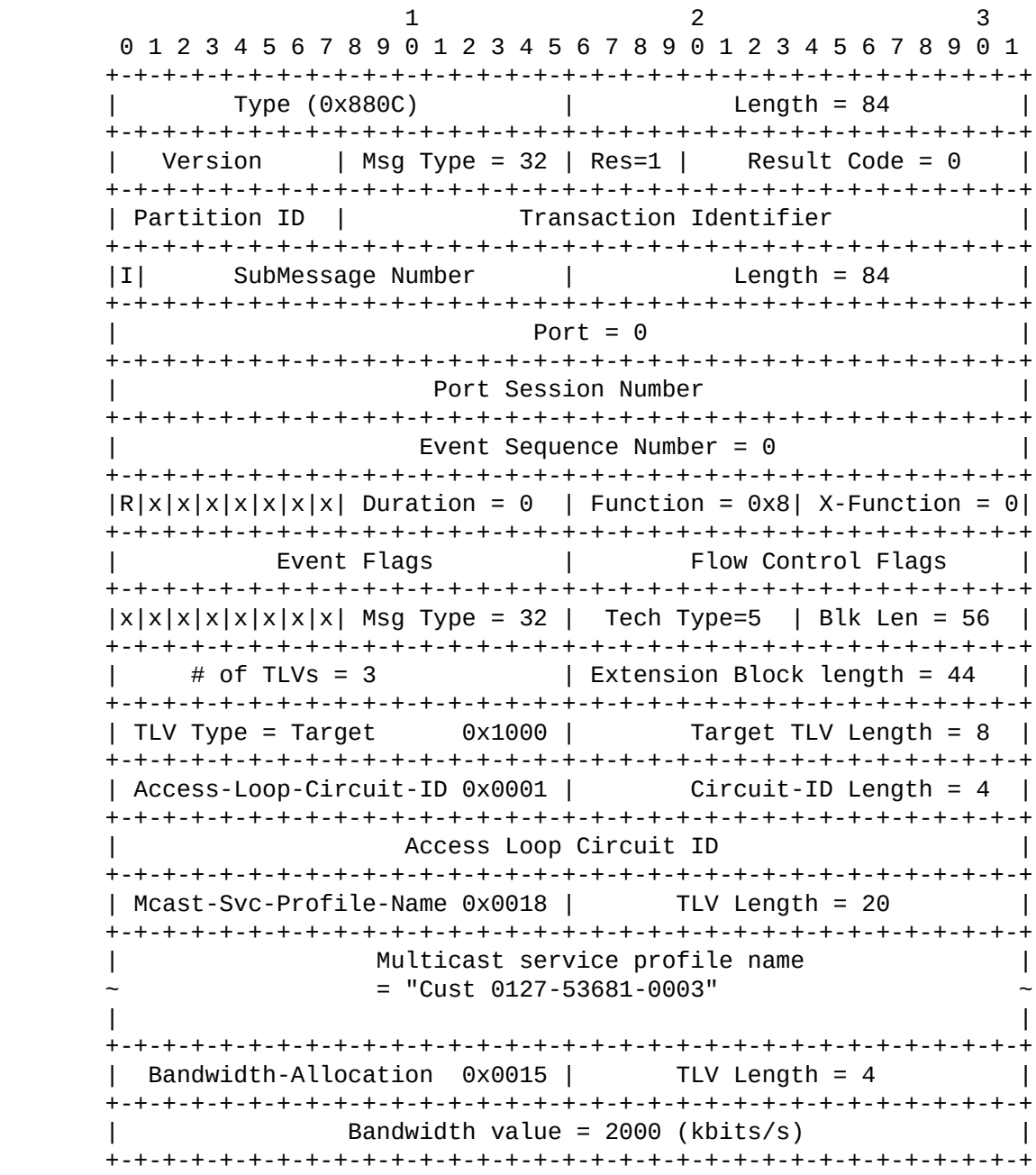
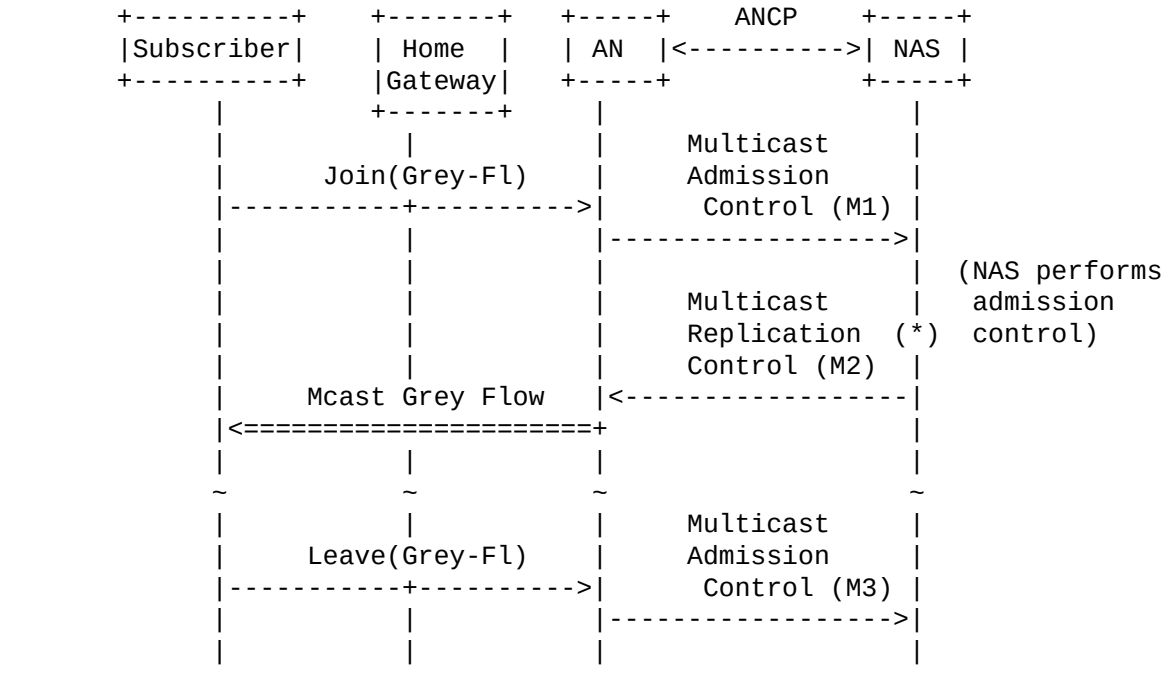


Figure 24: Example Port Management Message

A.2. Handling Grey-Listed Flows

Suppose now that the subscriber chooses to watch the premium channel characterized by source 192.0.2.21, group 233.252.0.67. Upon receiving the join request, the AN matches it against the multicast service profile for the port and determines that it is a grey-listed flow. Figure 25 illustrates the resulting ANCP message flow for the case of a simple join and leave, when admission control for grey-listed flows is not activated on the AN.

To start the flow, the AN sends a Multicast Admission Control message (M1) to the NAS. The NAS decides whether the flow can be admitted, applying both policy and bandwidth criteria. It returns its decision (positive in this example) in a Multicast Replication Control message (M2). Later, when the subscriber leaves the flow, the AN informs the NAS by sending another Multicast Admission Control message.



Grey-Fl: multicast flow matching an entry in grey list

(*) The NAS may optionally seek direction from an external Authorization/Policy Server.

Figure 25: Successful Join/Leave Operations, Grey-Listed Flow

The Multicast Admission Control message M1 contains:

- an ANCP Header with:
  - Message Type is 145;
  - Result = Ignore (0x0); and
  - a Transaction Identifier assigned by the AN.
- a Target TLV identifying the AN Port
- a Command TLV containing:
  - Command Code = "Add" (1);
  - Accounting = "No" (0);
  - a Multicast-Flow embedded TLV indicating the multicast flow for which the AN received the IGMP join: flow type "SSM" (2), address family "IPv4" (1), Group address = 233.252.0.67, Source Address = 192.0.2.21; and
  - a Request-Source-Device-Id embedded TLV containing the IGMP join source local device identifier value 5.

The Multicast Admission Control message M1 is illustrated in Figure 26:

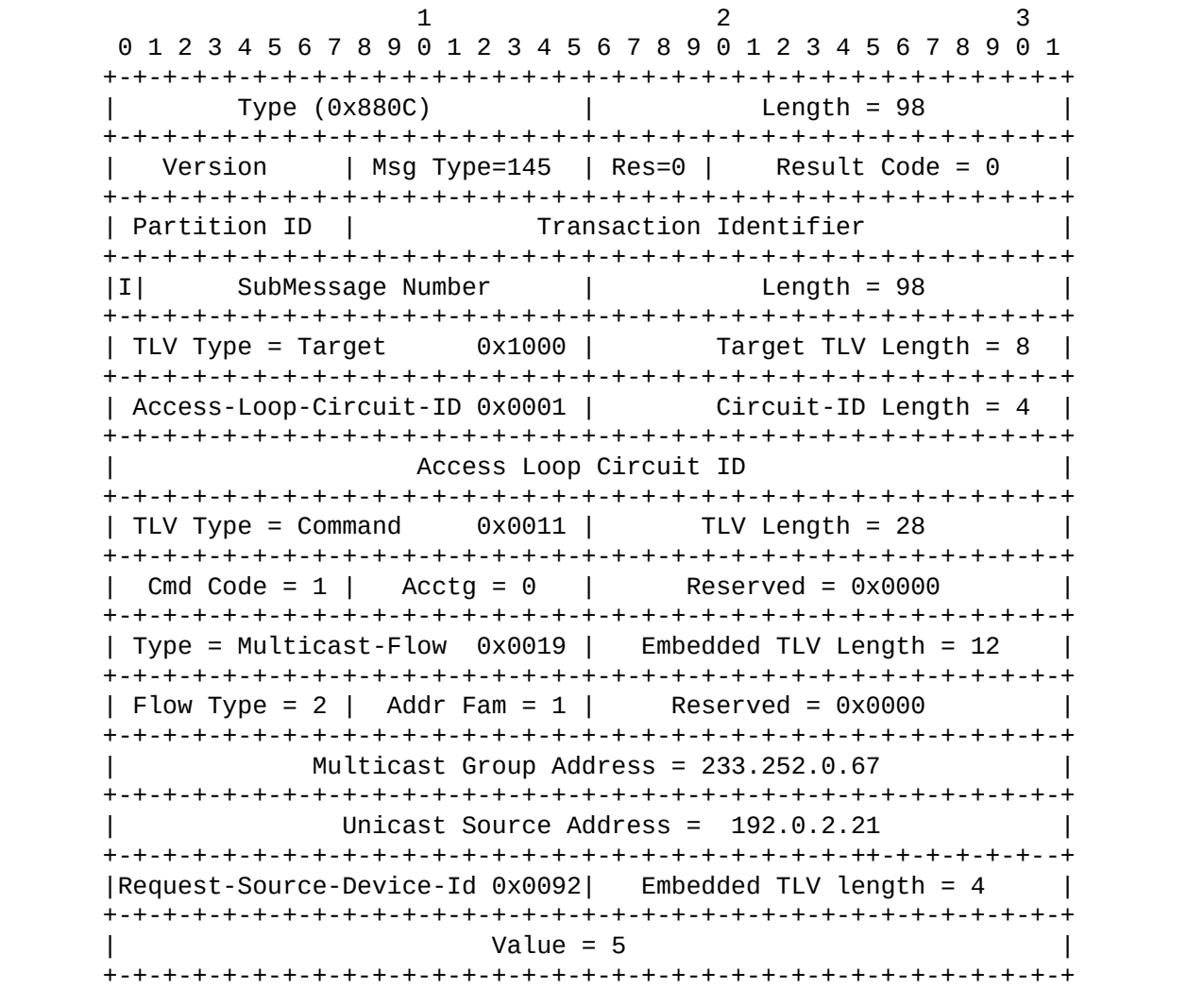


Figure 26: Multicast Admission Control Message Seeking to Add a Flow

The Multicast Replication Control message M2 contains:

o an ANCP Header with:

  * Message Type = "Multicast Replication Control" (144);

  * Result= 0x1 (Nack); and

  * a Transaction Identifier assigned by the NAS;

- a Target TLV identifying the AN Port
- a Command TLV containing:
  - Command Code = "Add" (1);
  - Accounting = "Yes" (1), since in our example the operator wants accounting on this flow; and
  - a Multicast-Flow embedded TLV indicating the multicast flow that the NAS is admitting for this access line: flow type "SSM" (2), address family "IPv4" (1), Group address = 233.252.0.67, Source Address = 192.0.2.21.

The Multicast Admission Control message M2 is illustrated in Figure 27.

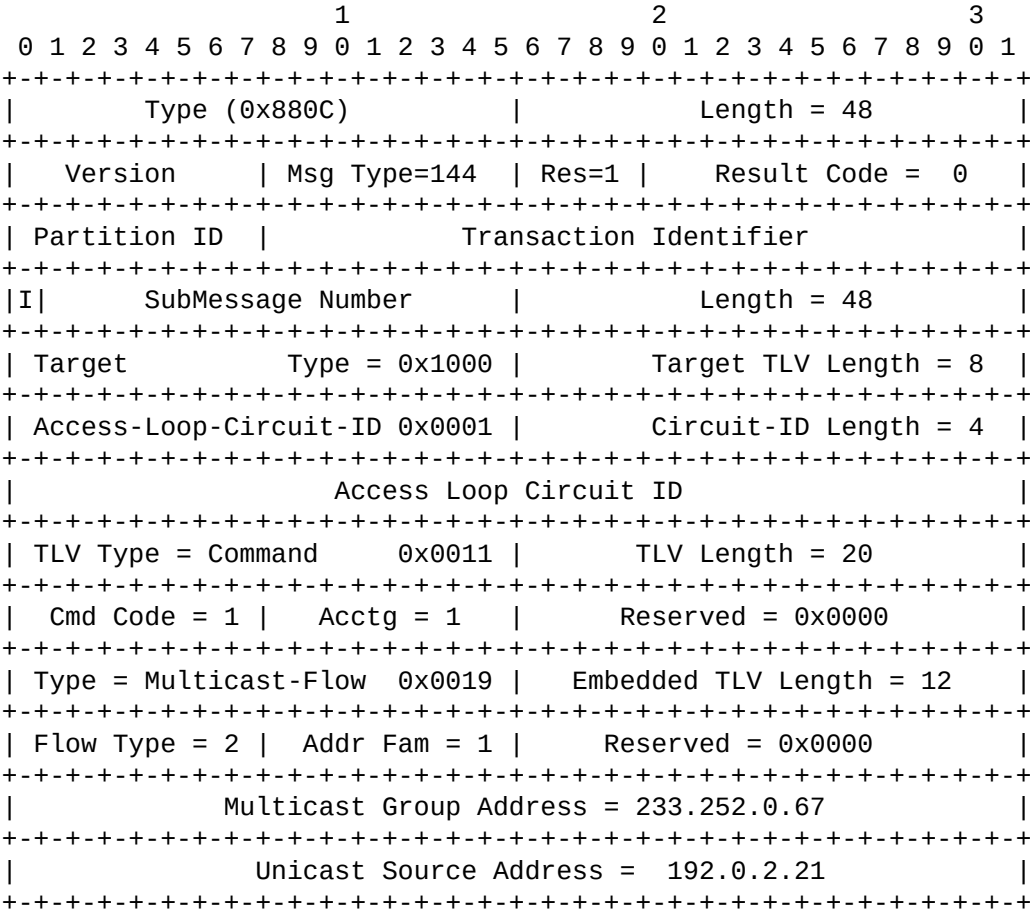


Figure 27: Multicast Replication Control Message Admitting a Flow

The Multicast Admission Control message M3 advising the NAS that the flow has been terminated contains:

- an ANCP Header with:
  - Message Type is 145;
  - Result = Ignore (0x0); and
  - a Transaction Identifier assigned by the AN.
- a Target TLV identifying the access line
- a Command TLV containing:
  - a Command Code = "Delete" (2);
  - Accounting = "No" (0);
  - a Multicast-Flow embedded TLV indicating the multicast flow for which the AN received the IGMP leave: flow type "SSM" (2), address family "IPv4" (1), Group address = 233.252.0.67, Source Address = 192.0.2.21; and
  - a Request-Source-Device-Id embedded TLV containing the IGMP leave request source, the device identified by the local value 5.

The Multicast Admission Control message M3 is illustrated in Figure 28.

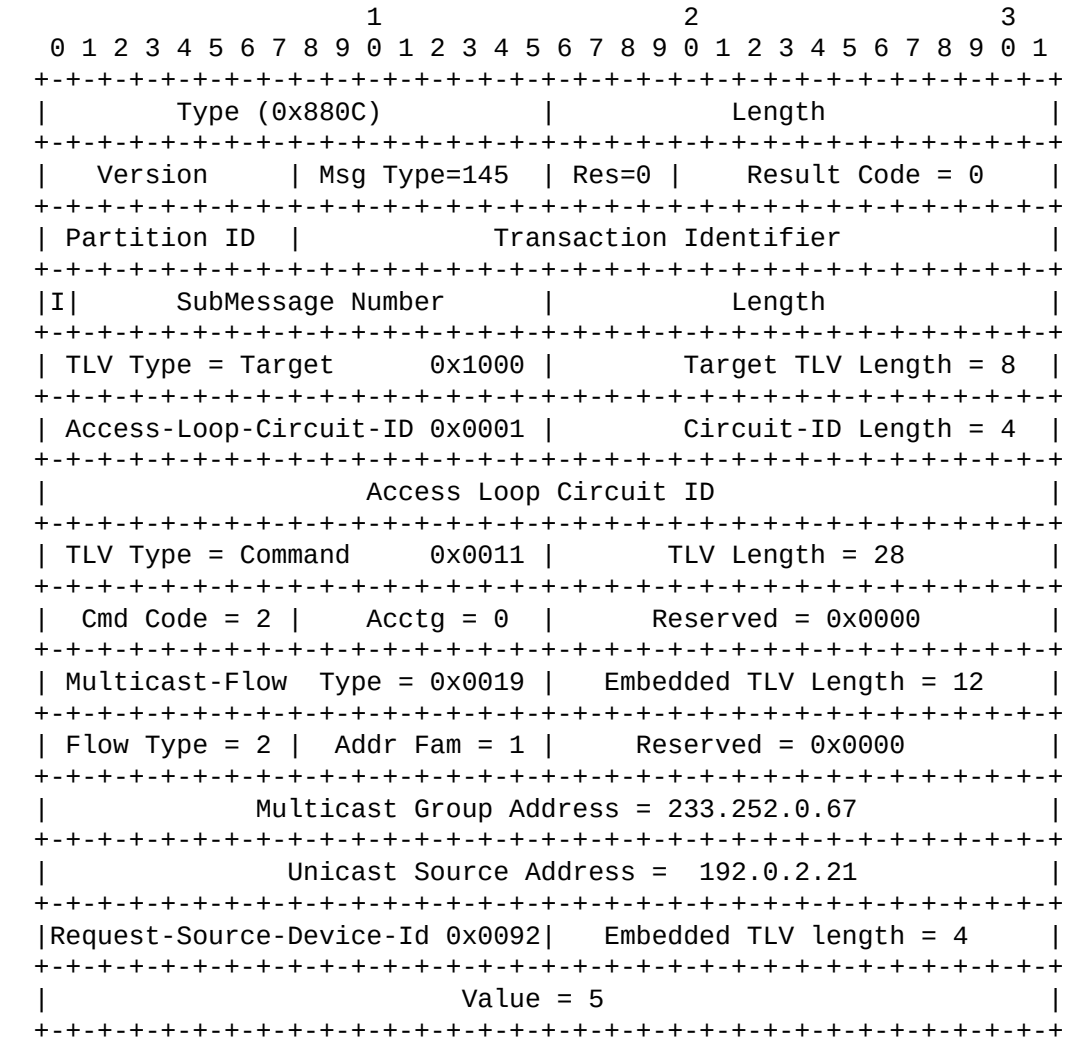


Figure 28: Multicast Admission Control Message Signaling Flow Termination

A.3. Handling White-Listed Flows

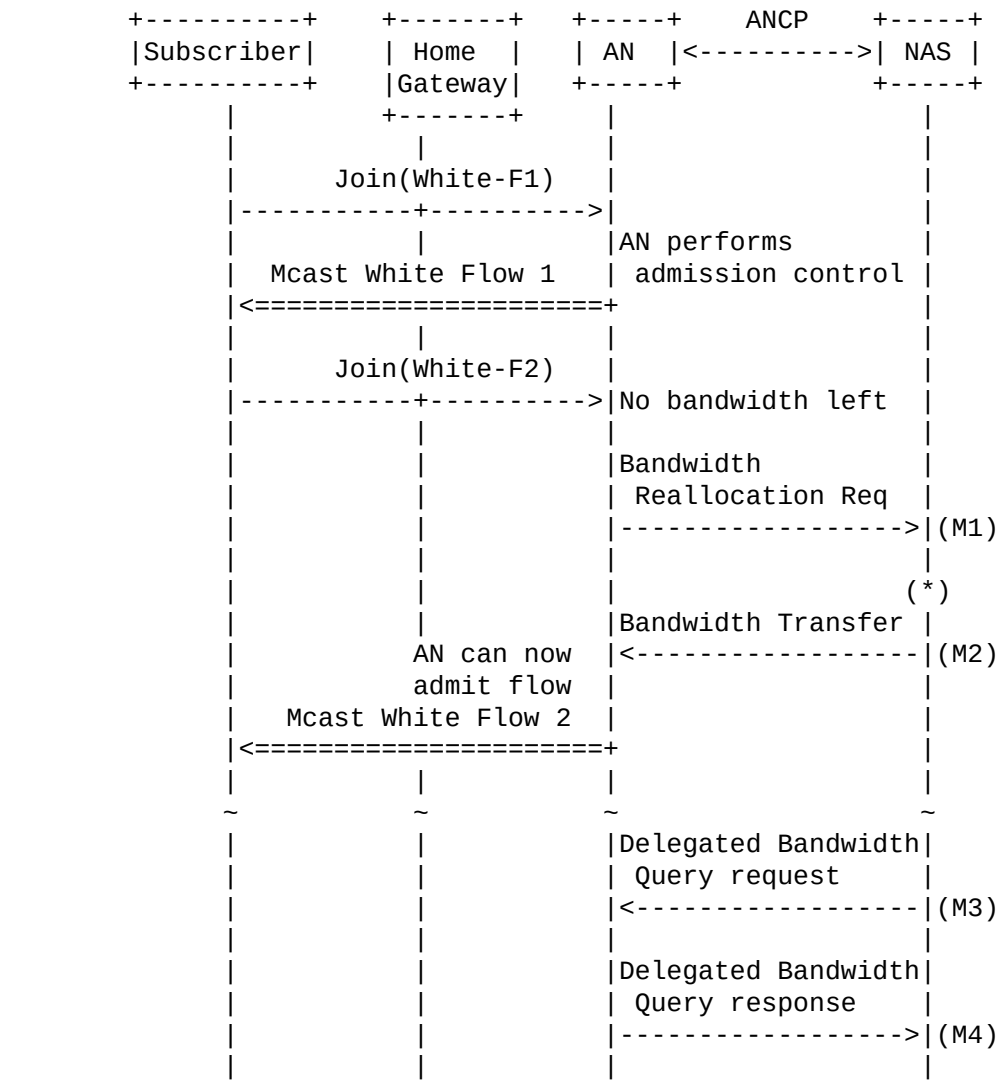
The NAS has enabled white list admission control on the AN, and the bandwidth delegation capability has been negotiated. White-listed flows in themselves require no messages to the NAS, either upon admission or upon termination, but the AN may request an increase in the amount of delegated bandwidth if it needs the increase to admit a flow.

Consider an example where the AN has already admitted one white-listed flow, thereby using up the initially provisioned amount of delegated bandwidth (2000 kbits/s). A request is received to join a new flow in the white list range. The AN chooses to send a Bandwidth Reallocation Request message to the NAS, requesting that the delegated bandwidth allocation be increased to 4000 kbits/s at a minimum and preferably to 6000 kbits/s.

In our example, the NAS is managing bandwidth tightly, as witnessed by its minimal initial allocation of just enough for one flow. It is willing to provide the minimum additional amount only and therefore returns a Bandwidth Transfer message where the delegated bandwidth value is given as 4000 kbits/s. With this amount, the AN is able to admit the second white-listed flow. The AN could send a similar Bandwidth Transfer message back to the NAS bringing the delegated bandwidth amount back down to 2000 kbits/s when one of the flows is terminated, but this shows nothing new and is omitted.

As one more point of illustration, suppose that the NAS chooses to audit the current amount of delegated bandwidth to ensure it is synchronized with the AN. It sends a Delegated Bandwidth Query Request message to the AN and receives a Delegated Bandwidth Query Response message with the current allocation as the AN sees it.

The complete message flow is shown in Figure 29.



(*) The NAS may optionally seek direction from an external Authorization/Policy Server.

Figure 29: Successful Join/Leave Operations, White-Listed Flow

The Bandwidth Reallocation Request message (M1) is shown in Figure 30. The contents require little explanation. The Message Type for the Bandwidth Reallocation Request is 146. The Result field is set to Ignore (0x0). Besides the Target TLV, the message has one other TLV, the Bandwidth-Request, with a TLV Type of 0x0016. The TLV contains Required Amount and Preferred Amount fields, set to 4000 and 6000 kbits/s respectively.

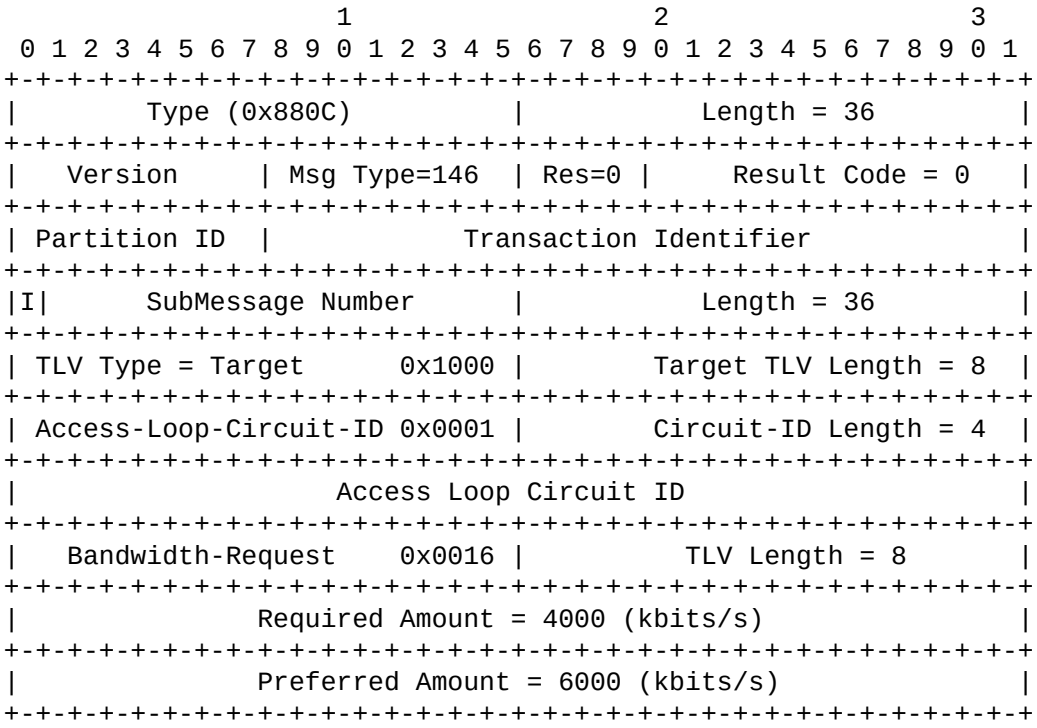


Figure 30: Bandwidth Reallocation Request Message

The Bandwidth Transfer message (M2) is shown in Figure 31. Again, the contents are easily understood. The Message Type for the Bandwidth Transfer message is 147. The Result field is set to Success (0x3). The message contains the Target TLV and the Bandwidth-Allocation TLV. The latter has a TLV Type of 0x0015 and contains a Delegated Amount field, set to 4000 kbits/s.

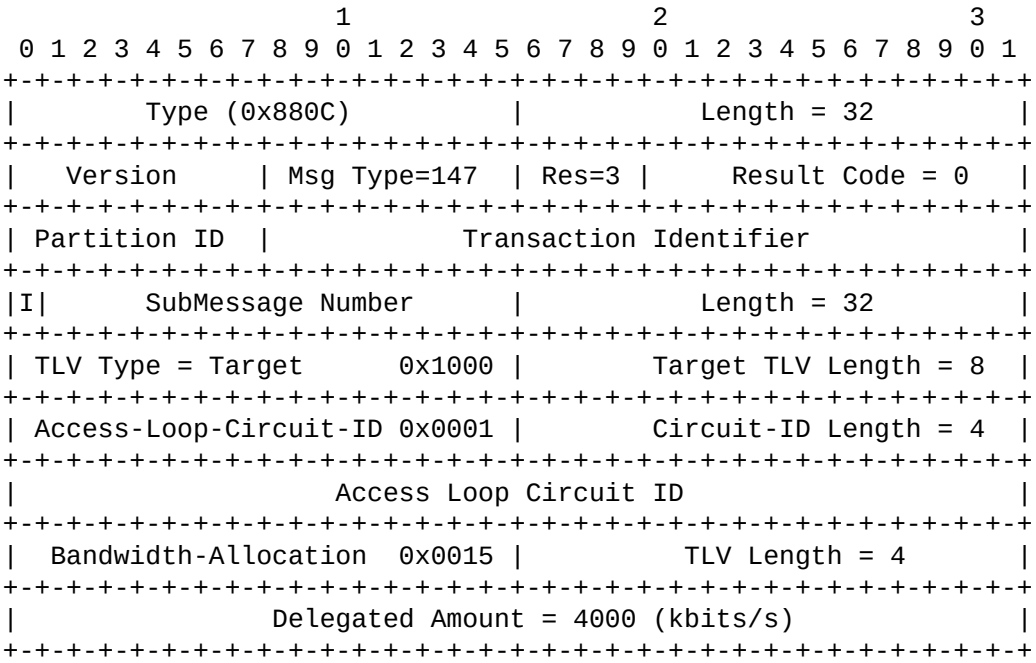


Figure 31: NAS Response, Bandwidth Transfer Message

The Delegated Bandwidth Query Request message (M3) is shown in Figure 32. The Message Type for the Delegated Bandwidth Query request message is 148. The Result field is set to AckAll (0x2). The message contains the Target TLV only.

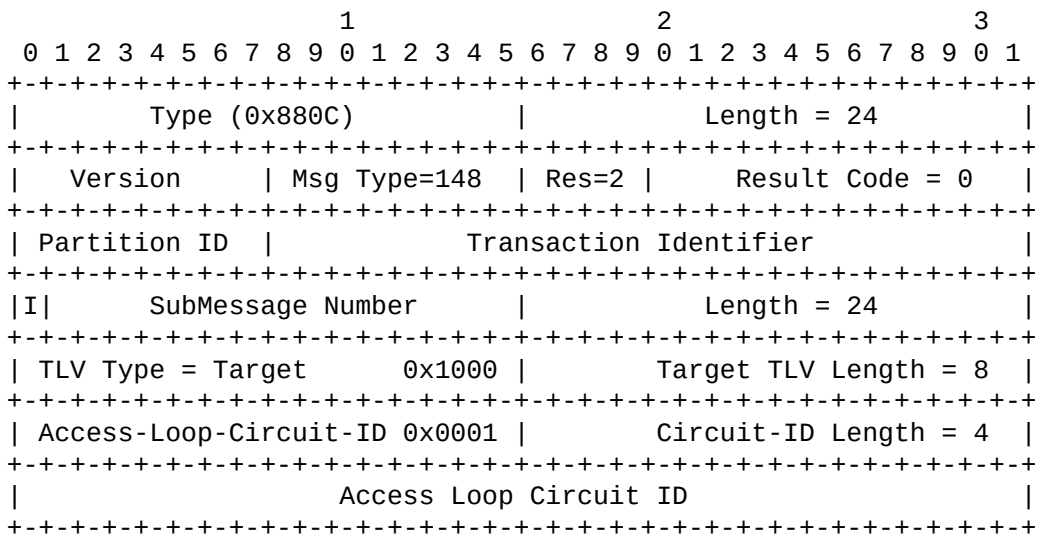


Figure 32: Delegated Bandwidth Query Request Message

Finally, the Delegated Bandwidth Query Response message (M4) is shown in Figure 33. The Message Type for the Delegated Bandwidth Query response message is 148. The Result field is set to Success (0x3). The message contains the Target TLV and the Bandwidth-Allocation TLV with the Delegated Amount field set to 4000 kbits/s.

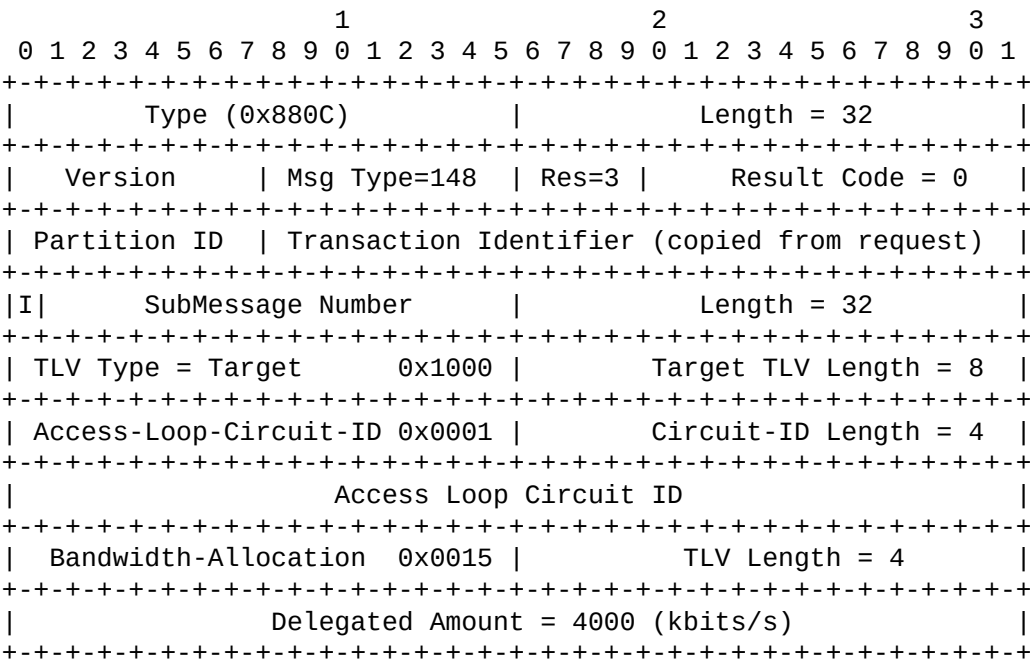


Figure 33: Delegated Bandwidth Query Response Message

A.4. Handling of Black-Listed Join Requests

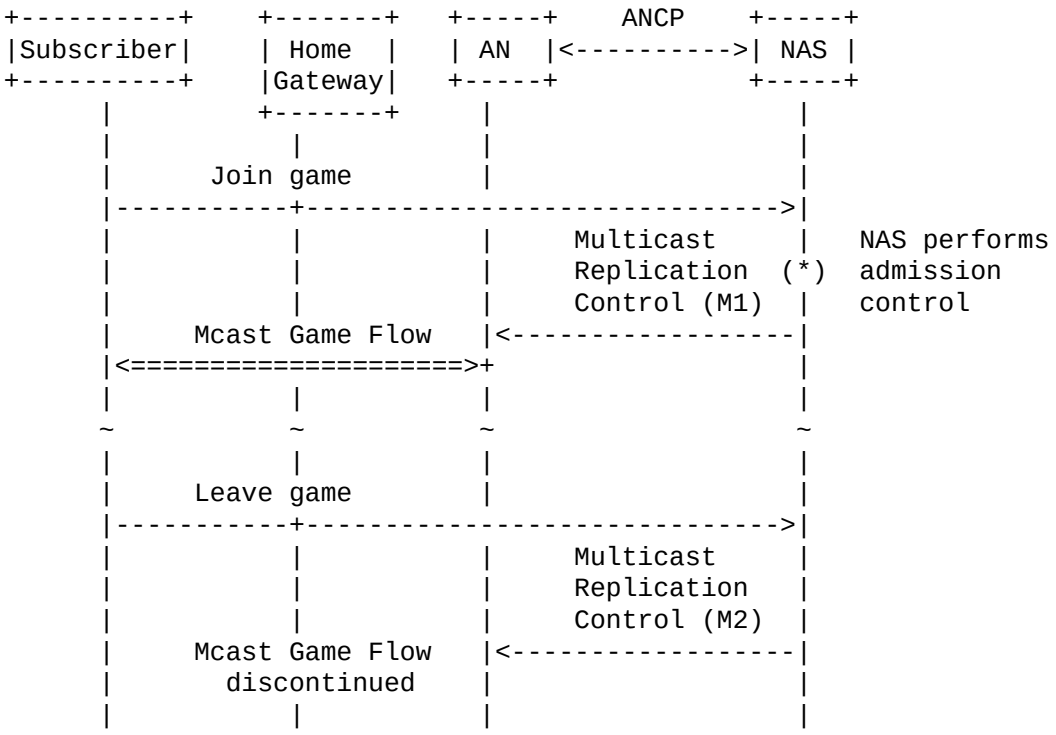
This section introduces no new messages, since requests for flows in the black list are simply ignored. The one thing to point out is the overlap in our example between the set of flows in the grey list and the flows in the black list. This does not create any ambiguity, since not only does the black list have priority for equally good matches, but also the black list entries are more specific (group prefix lengths of 32 versus 29 in the grey list) than the grey list flow prefixes.

A.5. Handling of Requests to Join and Leave the On-Line Game

The final class of multicast control actions in our example allows the subscriber to enter and leave the on-line game. As described at the beginning of this example, the game uses Any-Source Multicast (ASM). Subscriber signaling bypasses the AN, going directly to the NAS (e.g., through a web interface).

When the subscriber requests to join the game, the NAS (after applying policy and bandwidth checks) sends a Multicast Replication Control message to the AN to enable the flow on the port concerned. The AN knows not to apply admission control, since it has not received an MRepCtl-CAC TLV in the Provisioning message. When the subscriber leaves, the NAS sends another Multicast Replication Control message to delete the flow. This message sequence is shown in Figure 34.

It is possible that the NAS finds that there is not enough bandwidth available to accommodate the subscriber's request. In this case, the NAS could send a Bandwidth Reallocation Request message to the AN, asking it to release some of the bandwidth delegated to it. This is not shown in the present example, since the messages are the same as those already presented with the exception that the Preferred Amount in the request will be *less than* or equal to the Required amount, rather than *greater than* or equal to it.



(*) The NAS may optionally seek direction from an external Authorization/Policy Server.

Figure 34: NAS-Initiated Flows for On-Line Gaming

The Multicast Replication Control message (M1) in Figure 35 looks like the message in Figure 27 with two exceptions. The first is that the NAS has the option to set the Result field to AckAll (0x02) if it needs positive reassurance that the flow has been enabled. This was not done here to save having to depict a response differing only in the Result field. The larger difference in this example is that the flow description in the Multicast-Flow embedded TLV is that of an ASM multicast group (Flow Type = 1) with IPv4 (1) group address 233.252.0.100.

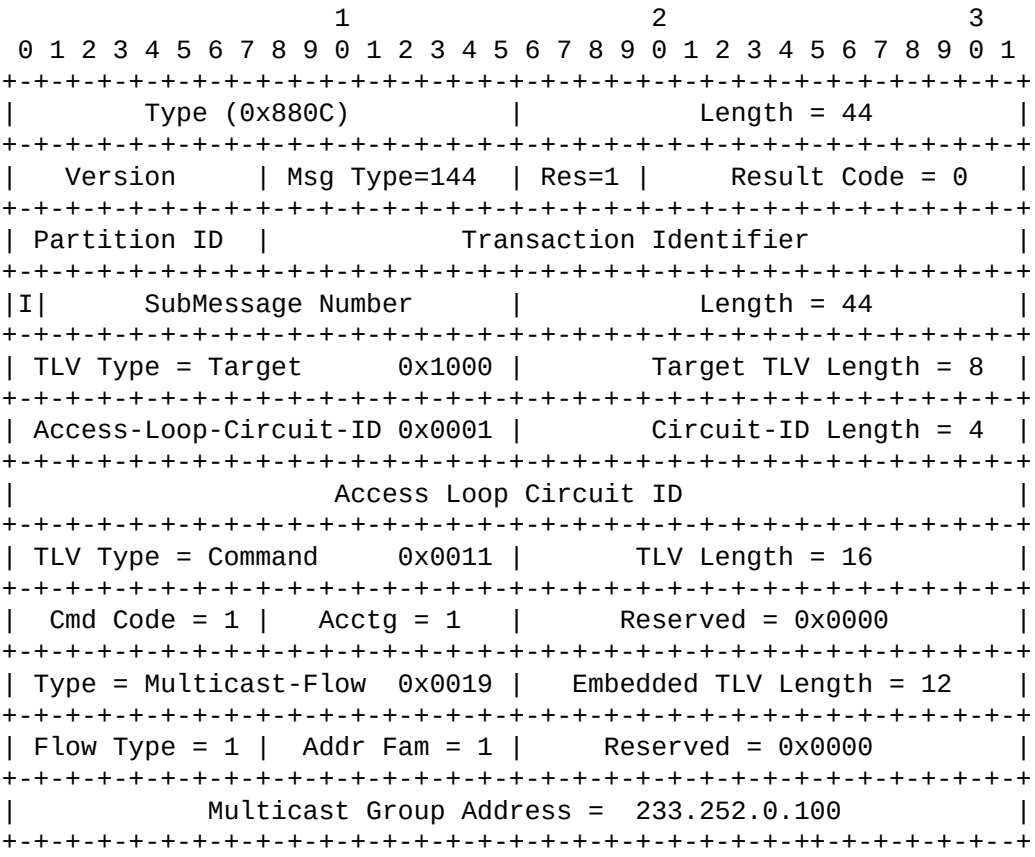


Figure 35: Enabling the Subscriber to Join an On-Line Game

Message M2 terminating the flow when the subscriber leaves the game looks the same as the message in Figure 35 with two exceptions: the Command Code becomes "Delete" (2), and Accounting is set to "No" (0) to turn off flow accounting. Of course, the Transaction Identifier values will differ between the two messages.

A.6. Example Flow for Multicast Flow Reporting

The example in this section is independent of the example in the preceding sections.

Figure 36 illustrates a message flow in a case where the NAS queries the AN about which multicast flows are active on port 10, port 11, and port 20 of the AN.

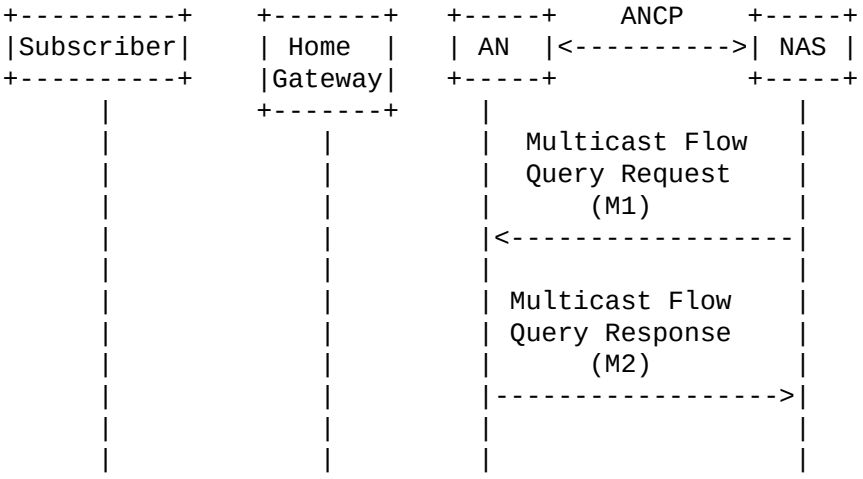


Figure 36: Per-Port Multicast Flow Reporting

The Multicast Flow Query Request message (M1) is illustrated in Figure 37. The Message Type is 149. The Result field is set to AckAll (0x2). Three Target TLVs are present, identifying port 10, port 20, and port 11, respectively.

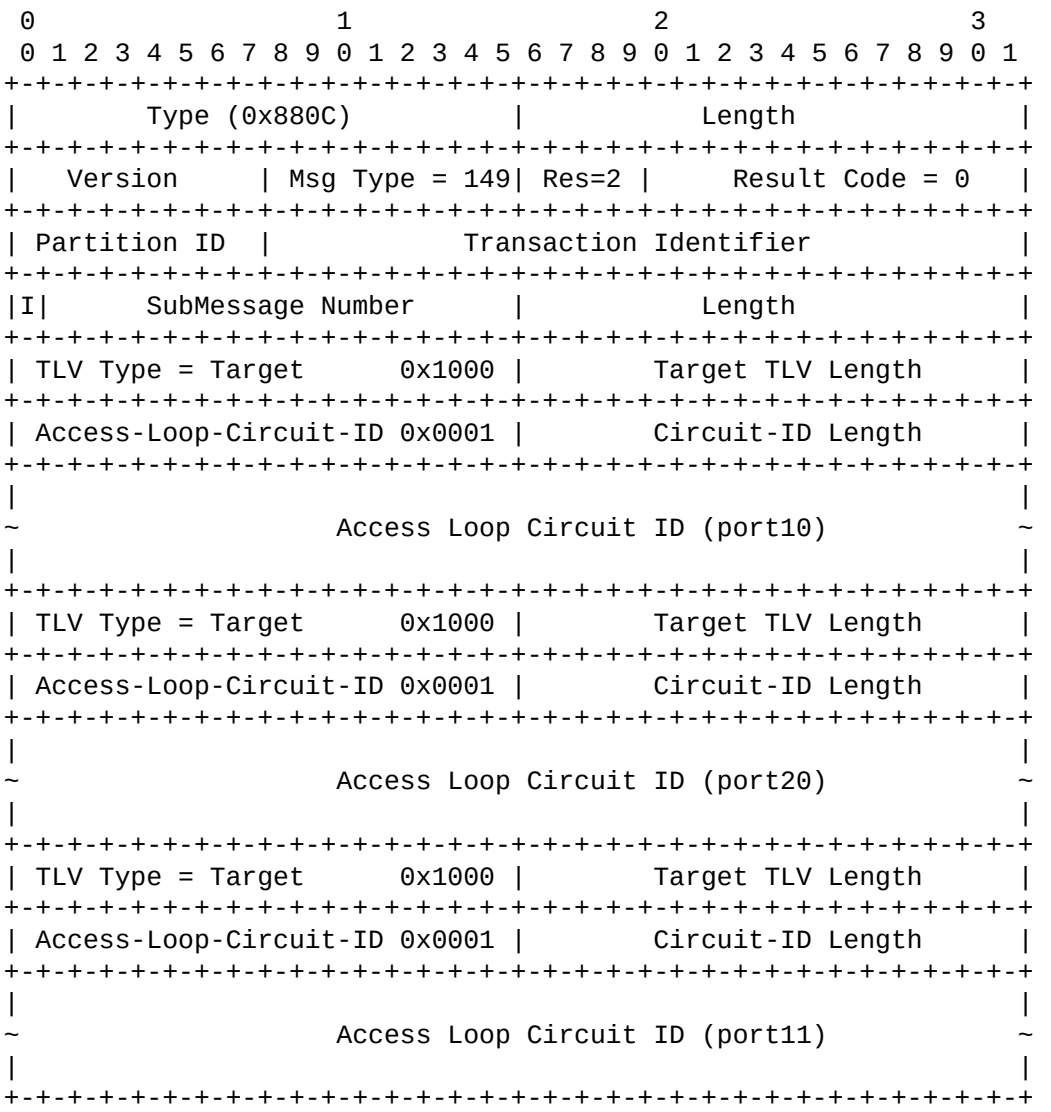
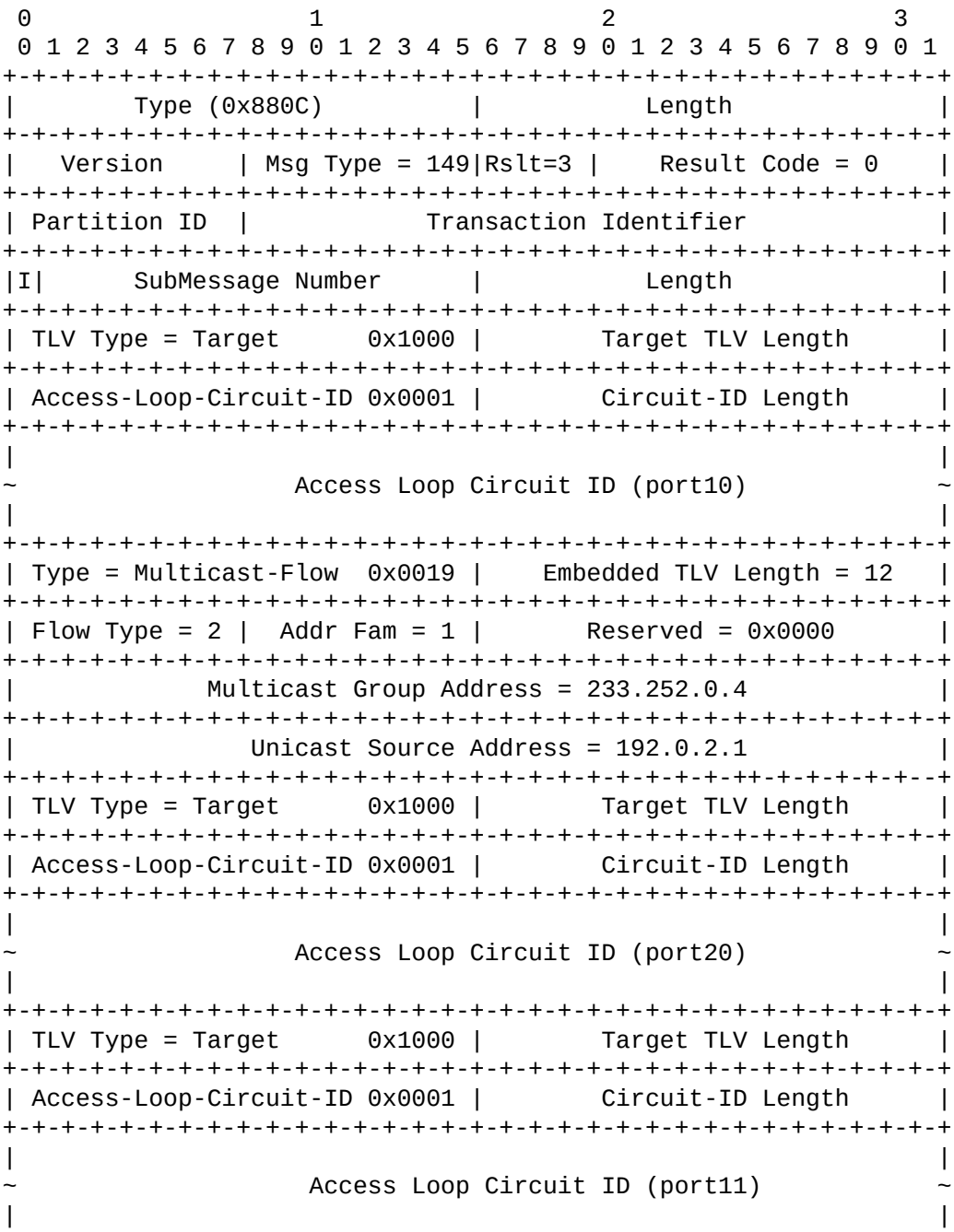


Figure 37: Multicast Flow Query Request Message for Per-Port Multicast Flow Reporting

The Multicast Flow Query Response message (M2) is illustrated in Figure 38. It indicates that there is one active multicast flow [(192.0.2.1, 233.252.0.4)] on port 10, no active multicast flow on port 20, and two active multicast flows [(192.0.2.1, 233.252.0.4) and (192.0.2.2, 233.252.0.10)] on port 11.



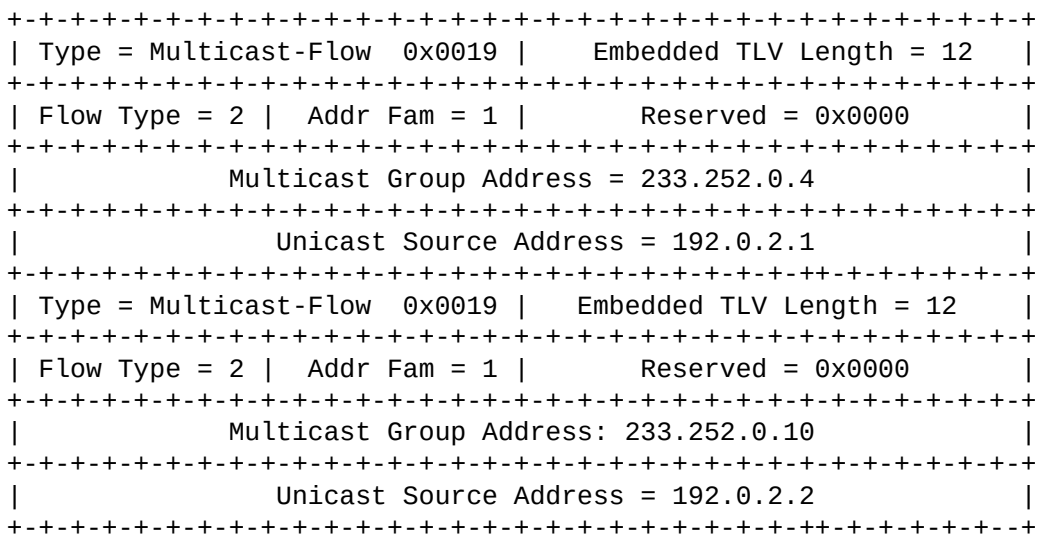


Figure 38: Multicast Flow Query Response Message for Per-Port Multicast Flow Reporting

Authors' Addresses

Francois Le Faucheur
Cisco Systems
45 Allee des Ormes
Mougins 06250
France

Phone: +33 4 97 23 26 19
EMail: flefauch@cisco.com

Roberta Maglione
Cisco Systems
181 Bay Street
Toronto, ON M5J 2T3
Canada

EMail: robmgl@cisco.com

Tom Taylor
Huawei Technologies
Ottawa
Canada

EMail: tom.taylor.stds@gmail.com