

Network Working Group  
Internet-Draft  
Intended status: Standards Track  
Expires: February 25, 2011

S. Wadhwa  
J. Moisand  
Juniper Networks  
T. Haag  
Deutsche Telekom  
N. Voigt  
Nokia Siemens Networks  
T. Taylor, Ed.  
Huawei Technologies  
August 24, 2010

Protocol for Access Node Control Mechanism in Broadband Networks  
draft-ietf-ancp-protocol-12

Abstract

This document describes the Access Node Control Protocol (ANCP). ANCP operates 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. Use cases for ANCP are documented in RFC 5851. As well as describing the base ANCP protocol, this document specifies capabilities for Digital Subscriber Line (DSL) topology discovery, line configuration, and line testing. The design of ANCP anticipates the specification in other documents of extensions to the protocol to support additional ANCP protocol capabilities covering other use cases and other technologies.

ANCP is based on GSMPv3 (RFC 3292), but with many modifications and extensions, to the point that the two protocols are not interoperable.

Status of this Memo

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

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

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

This Internet-Draft will expire on February 25, 2011.

#### Copyright Notice

Copyright (c) 2010 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10, 2008. The person(s) controlling the copyright in some of this material may not have granted the IETF Trust the right to allow modifications of such material outside the IETF Standards Process. Without obtaining an adequate license from the person(s) controlling the copyright in such materials, this document may not be modified outside the IETF Standards Process, and derivative works of it may not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.

## Table of Contents

1. Specification Requirements . . . . .	5
2. Introduction . . . . .	5
2.1. Terminology . . . . .	6
3. Broadband Access Aggregation . . . . .	7
3.1. ATM-based broadband aggregation . . . . .	7
3.2. Ethernet-based broadband aggregation . . . . .	9
4. Access Node Control Protocol -- General Aspects . . . . .	9
4.1. Protocol Version . . . . .	11
4.2. ANCP Transport . . . . .	11
4.3. Encoding of Text Fields . . . . .	12
4.4. Treatment of Reserved and Unused Fields . . . . .	12
4.5. Use of the GSMPv3 Adjacency Protocol . . . . .	12
4.5.1. ANCP Adjacency Message Format . . . . .	13
4.5.2. ANCP Adjacency Procedures . . . . .	15
4.6. ANCP General Message Formats . . . . .	17
4.6.1. The ANCP Message Header . . . . .	17
4.6.2. The ANCP Message Body . . . . .	20
5. ANCP Capabilities For Digital Subscriber Lines (DSL) . . . . .	22
5.1. Overview . . . . .	22
5.1.1. ATM-Specific Considerations . . . . .	22
5.1.2. Ethernet-Specific Considerations . . . . .	23
5.2. ANCP Based DSL Topology Discovery . . . . .	24
5.2.1. Goals . . . . .	24
5.2.2. Message Flow . . . . .	24
5.2.3. Specification of the ANCP DSL Topology Discovery Capability . . . . .	25
5.3. ANCP based DSL Line Configuration . . . . .	40
5.3.1. Goals . . . . .	40
5.3.2. Message Flow . . . . .	40
5.3.3. Specification of the ANCP DSL Line Configuration Capability . . . . .	42
5.4. ANCP Based DSL Line Testing Capability . . . . .	46
5.4.1. Message Flow . . . . .	46
5.4.2. Specification of the ANCP DSL Line Testing Capability . . . . .	47
6. Additional ANCP Messages and TLVs . . . . .	51
6.1. Additional Messages and General Messaging Principles . . . . .	51
6.1.1. General Principles for the Design of ANCP Messages . . . . .	51
6.1.2. Provisioning Message . . . . .	52
6.1.3. Generic Response Message . . . . .	53
6.2. TLVs For General Use . . . . .	54
6.2.1. Target TLV . . . . .	54
6.2.2. Command TLV . . . . .	55
6.2.3. Status-Info TLV . . . . .	56
7. IANA Considerations . . . . .	57
7.1. Summary . . . . .	57

7.2. IANA Actions . . . . .	58
8. Security Considerations . . . . .	62
9. Acknowledgements . . . . .	62
10. References . . . . .	62
10.1. Normative References . . . . .	62
10.2. Informative References . . . . .	63
Authors' Addresses . . . . .	64

## 1. Specification Requirements

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].

## 2. Introduction

This draft defines a new protocol, the Access Node Control Protocol (ANCP), to realize a control plane between a service-oriented layer 3 edge device (the Network Access Server, NAS) and a layer 2 Access Node (e.g., Digital Subscriber Line Access Module, DSLAM) in order to perform QoS-related, service-related and subscriber-related operations. The protocol specification takes GSMPv3 [RFC3292] as a starting point and specifies modifications and extensions to GSMPv3 to achieve ANCP requirements. Although ANCP is based on GSMPv3, the two protocols are not interoperable.

This specification assumes ANCP transport over TCP/IP. TCP encapsulation for ANCP is as defined for GSMPv3 in [RFC3293]. ANCP encapsulation directly over Ethernet and ATM as defined for GSMPv3 in [RFC3293] is not considered.

ANCP uses a subset of GSMPv3 messages, message content, and procedures to implement currently defined use cases. Additional ANCP messages, message content, and procedures are specified in this document and may also be specified in other documents extending ANCP.

The organization of this document is as follows:

- o The next sub-section introduces some terminology that will be useful in understanding the rest of the document.
- o Section 3 provides a description of the access networks within which ANCP will typically be deployed.
- o Section 4 specifies generally applicable aspects of the ANCP protocol.
- o Section 5 describes and specifies the ANCP implementation of three capabilities applicable to the control of DSL access technology: topology discovery, line configuration, and line testing (OAM).
- o Section 6 provides a set of specifications expected to be useful when defining extensions to the base protocol.

- o Section 7 is the IANA Considerations section. Some codepoints are added to existing GSMPv3 registries set up by [RFC3292], but a number of new ANCP-specific registries are also defined.
- o Section 8 addresses security considerations relating to ANCP, with heavy reliance on [RFC5713].

RFC Editor's Note: the following paragraph should be deleted upon publication.

At the time of writing of this specification some implementations of the ANCP protocol based on pre-standards drafts are already available. These early-draft implementations use protocol version/sub-version 3.1. The standard ANCP protocol will use version/sub-version 3.2 Adopting a new sub-version value provides a way to disambiguate the two protocols and provides support for running a pre-standard and a standards compliant ANCP implementation on any given ANCP node. The mechanism used to identify the protocol version/sub-version is part of the adjacency negotiation process and it is described in detail in Section 4.5. NOTE: this mechanism does not guarantee backwards compatibility of the published ANCP specification with those early-draft implementations.

## 2.1. Terminology

**Access Node (AN):** Network device, usually located at a service provider central office or street cabinet that terminates access (local) loop connections from subscribers. In case the access loop is a Digital Subscriber Line (DSL), the Access Node provides DSL signal termination, and is referred to as a DSL Access Multiplexer (DSLAM).

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

**Home Gateway (HGW):** Network element that connects subscriber devices to the Access Node and the access network. In the case of DSL, the Home Gateway is a DSL network termination that may operate either as a layer 2 bridge or as a layer 3 router. In the latter case, such a device is also referred to as a Routing Gateway (RG).

**Net Data Rate:** portion of the total data rate of the DSL line that can be used to transmit actual user information (e.g. ATM cells of Ethernet frames). It excludes overhead that pertains to the physical transmission mechanism (e.g. trellis coding in case of

DSL). This is defined in section 3.39 of ITU-T G.993.2.

DSL line (synch) rate: the total data rate of the DSL line, including the overhead attributable to the physical transmission mechanism.

DSL multi-pair bonding: method for bonding (or aggregating) multiple xDSL lines into a single bi-directional logical link, henceforth referred to in this draft as "DSL bonded circuit". DSL "multi-pair" bonding allows an operator to combine the data rates on two or more copper pairs, and deliver the aggregate data rate to a single customer. ITU-T recommendations G.998.1 and G.998.2 respectively describe ATM and Ethernet based multi-pair bonding.

Type-Length-Value (TLV): a data structure consisting of a sixteen-bit type field, a sixteen-bit length field, and a variable-length value field padded to the nearest 32-bit word boundary, as described in Section 4.6.2. The value field of a TLV can contain other TLVs. An IANA registry is maintained for values of the ANCP TLV Type field.

ANCP Protocol Capability: A detailed specification of ANCP messages, message content, and procedures required to implement a specific use case or set of use cases. ANCP capabilities may be specific to one access technology or technology independent. The set of capabilities applicable to a given ANCP session are negotiated during session startup.

ANCP session (also called an adjacency): A session between a NAS and an Access Node, beginning with the initiation of the transport connection by the AN, passing through adjacency negotiation, discovery and provisioning stages, and continuing with service control and possible OAM operations until the transport connection is terminated. There may be more than one ANCP session active between the NAS and a given AN due to partitioning.

### 3. Broadband Access Aggregation

#### 3.1. ATM-based broadband aggregation

The end to end DSL network consists of network service provider (NSP) and application service provider (ASP) networks, regional/access network, and customer premises network. Figure 1 shows ATM broadband access network components.

The regional/access network consists of the regional network, Network Access Server (NAS), and the access network as shown in Figure 1.

Its primary function is to provide end-to-end transport between the customer premises and the NSP or ASP.

The Access Node terminates the DSL signal. It may be in the form of a DSLAM in the central office, or a remote DSLAM, or a Remote Access Multiplexer (RAM). The Access Node is the first point in the network where traffic on multiple DSL lines will be aggregated onto a single network.

The NAS performs multiple functions in the network. The NAS is the aggregation point for subscriber traffic. It provides aggregation capabilities (e.g. IP, PPP, ATM) between the Regional/Access Network and the NSP or ASP. These include traditional ATM-based offerings and newer, more native IP-based services. This includes support for Point-to-Point Protocol over ATM (PPPoA) and PPP over Ethernet (PPPoE), as well as direct IP services encapsulated over an appropriate layer 2 transport.

Beyond aggregation, the NAS is also the injection point for policy management and IP QoS in the regional/access networks. To allow IP QoS support over an existing non-IP-aware layer 2 access network without using multiple layer 2 QoS classes, a mechanism based on hierarchical scheduling is used. This mechanism, defined in [TR\_059], preserves IP QoS over the ATM network between the NAS and the routing gateway (RG) at the edge of the subscriber network, by carefully controlling downstream traffic in the NAS, so that significant queuing and congestion does not occur further down the ATM network. This is achieved by using a diffserv-aware hierarchical scheduler in the NAS that will account for downstream trunk bandwidths and DSL synch rates.

[RFC5851] provides detailed definition and functions of each network element in the broadband reference architecture.



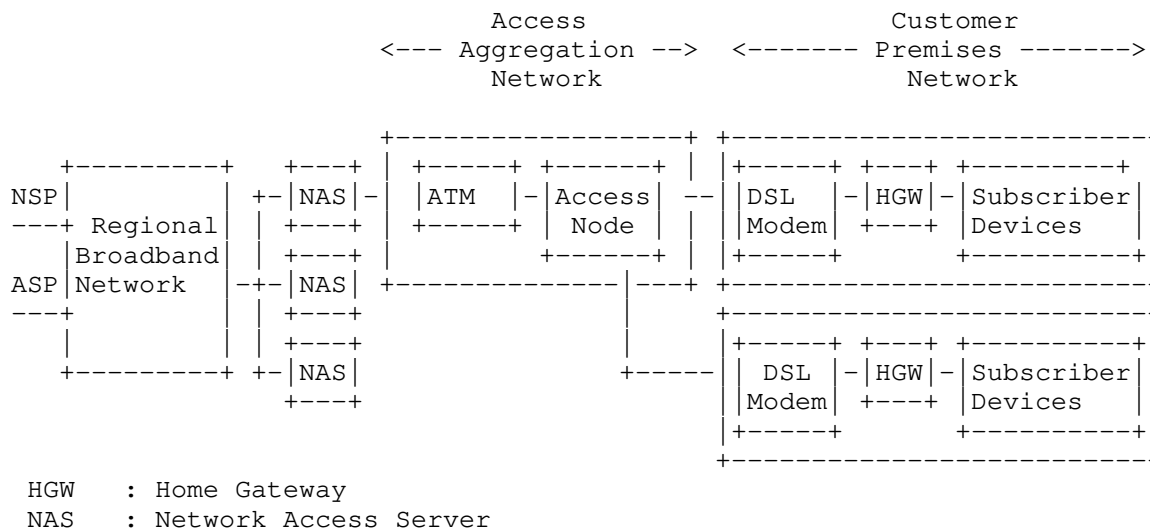


Figure 1: ATM Broadband Aggregation Topology

### 3.2. Ethernet-based broadband aggregation

The Ethernet aggregation network architecture builds on the Ethernet bridging/switching concepts defined in IEEE 802. The Ethernet aggregation network provides traffic aggregation, class of service distinction, and customer separation and traceability. VLAN tagging defined in IEEE 802.1Q and being enhanced by IEEE 802.1ad is used as standard virtualization mechanism in the Ethernet aggregation network. The aggregation devices are "provider edge bridges" defined in IEEE 802.ad.

Stacked VLAN tags provide one possible way to create equivalent of "virtual paths" and "virtual circuits" in the aggregation network. The "outer" vlan can be used to create a form of "virtual path" between a given DSLAM and a given NAS. "Inner" VLAN tags create a form of "virtual circuit" on a per DSL line basis. This is the 1:1 VLAN allocation model. An alternative model is to bridge sessions from multiple subscribers behind a DSLAM into a single VLAN in the aggregation network. This is the N:1 VLAN allocation model. Architectural and topological models of an Ethernet aggregation network in context of DSL aggregation are defined in [TR\_101].

#### 4. Access Node Control Protocol -- General Aspects

This section specifies aspects of the Access Node Control Protocol

(ANCP) that are generally applicable. As indicated above, ANCP is derived from GSMPv3 [RFC3292]. Reference to [RFC3292] is made where this is applicable, but ANCP introduces numerous modifications and extensions to the basic GSMPv3 protocol. Moreover, ANCP uses only a subset of the messages, message contents, and procedures defined for GSMPv3.

The following are the only GSMPv3 [RFC3292] messages that are currently used by ANCP.

#### Event Messages

- \* Port UP Message
- \* Port DOWN Message

These messages are used by the ANCP "DSL topology discovery" capability.

**Port Management Messages** These messages are used by the ANCP "DSL line configuration" and ANCP "DSL line testing" capabilities.

**Adjacency Protocol Messages** These messages are used to bring up a protocol adjacency between a NAS and an AN.

ANCP modifies and extends some basic GSMPv3 procedures. These modifications and extensions are summarized below, and described in more detail in the succeeding sections.

- o ANCP provides support for a capability negotiation mechanism between ANCP peers by extending the GSMPv3 adjacency protocol. This mechanism and corresponding adjacency message extensions are defined in section Section 4.5.
- o The TCP connection establishment procedure in ANCP deviates slightly from connection establishment in GSMPv3 as specified in [RFC3293]. This is described in section Section 4.2.
- o ANCP adds content to GSMPv3 messages in the form of additional fixed fields and Type-Length-Value (TLV) structures. TLVs also provide flexibility to both GSMPv3 and ANCP-specific messages because their order in the message and whether or not specific TLVs are present can vary from one message instance to the next.

#### 4.1. Protocol Version

GSMPv3 messages contain an 8-bit protocol version field. As described below, ANCP subdivides this into two 4-bit sub-fields, for version and sub-version. Implementations of this version of the ANCP specification MUST set the version sub-field to 3 and the sub-version sub-field to 1. That is, the hexadecimal representation of the value of the complete protocol version field MUST be 0x31.

RFC EDITOR'S NOTE: please change the value of sub-version in the above paragraph to 2 (respectively a version field value of 0x32) in the published specification. For an explanation see the Introduction above.

#### 4.2. ANCP Transport

This document specifies the use of TCP/IP for transport of ANCP messages. Other specifications may introduce additional transports in the future.

In the case of ATM access, a separate PVC (control channel) capable of transporting IP may be configured between NAS and the AN for ANCP messages.

In the case of an Ethernet access/aggregation network, a typical practice is to send the Access Node Control Protocol messages over a dedicated Ethernet virtual LAN (VLAN) using a separate VLAN identifier (VLAN ID).

When transported over TCP, ANCP messages MUST use the encapsulation specified for GSMPv3 messages carried over TCP in [RFC3293]. This encapsulation consists of a four-byte header field prepended to the ANCP message as shown in Figure 2.

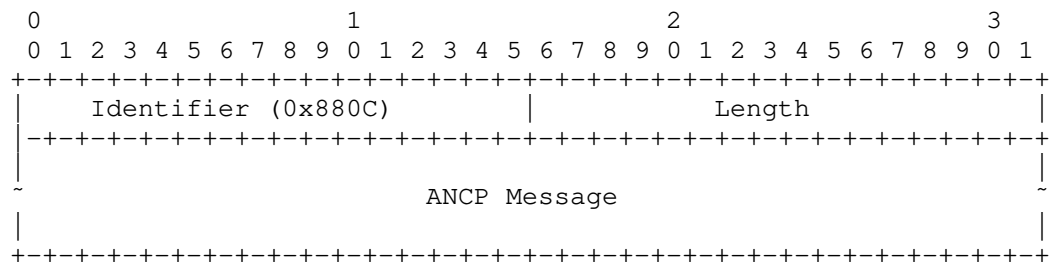


Figure 2: Encapsulation of ANCP Messages Over TCP/IP

The fields of the encapsulating header are as follows:

**Identifier:** This 2-byte field identifies a GSMP or ANCP message. The type code for GSMP and ANCP messages is 0x880C (i.e., the same as GSMP's Ethertype).

**Length:** This 2-byte unsigned integer indicates the total length of the ANCP message. It does not include the 4-byte encapsulating header.

The Access Node MUST initiate the TCP session to the NAS. This is a deviation from [RFC3293], which requires the controller to initiate the TCP connection to the switch.

This is necessary to avoid static provisioning on the NAS for all the ANs that are being served by the NAS. It is easier to configure a given AN with the single IP address of the NAS that serves the AN.

The NAS MUST listen for incoming connections from the Access Nodes. Port 6068 is used for TCP connection.

In the event of an ANCP transport protocol failure, all pending ANCP messages destined to the disconnected recipient SHOULD be discarded until the transport connection is re-established.

#### 4.3. Encoding of Text Fields

In ANCP, all text fields use UTF-8 encoding [RFC3629]. Note that US ASCII characters have the same representation when coded as UTF-8 as they do when coded according to [US\_ASCII].

#### 4.4. Treatment of Reserved and Unused Fields

ANCP messages contain a number of fields that are unused or reserved. Some fields are always unused (typically because they were inherited from GSMPv3 but are not useful in the ANCP context. Others are unused in the current specification, but are provided for flexibility in future extensions to ANCP. Both reserved and unused fields MUST be set to zeroes by the sender and MUST be ignored by the receiver.

Unused bits in a flag field are shown in figures as 'x'. The above requirement (sender set to zero, receiver ignore) applies to such unused bits.

#### 4.5. Use of the GSMPv3 Adjacency Protocol

Section 11 of [RFC3292] defines the GSMPv3 adjacency protocol. ANCP reuses the GSMPv3 adjacency protocol to synchronize the NAS and Access Nodes and maintain the ANCP session. After the TCP connection

is established, adjacency protocol messages MUST be exchanged as specified in Section 11 of [RFC3292], subject to the additional specifications of this section. ANCP messages other than adjacency protocol messages MUST NOT be sent until the adjacency protocol has achieved synchronization.

#### 4.5.1. ANCP Adjacency Message Format

The GSMPv3 adjacency message format defined in Section 11 of [RFC3292] is modified and extended for ANCP as shown in Figure 3 below. The 8-bit "version" field in the GSMPv3 adjacency protocol messages is modified to carry the ANCP version (four bits) and sub-version (four bits). See Section 4.1 for the values to set for version and sub-version for the present version of this specification. In addition to the modification of the version field, ANCP adds several new fields. These are described below the figure.

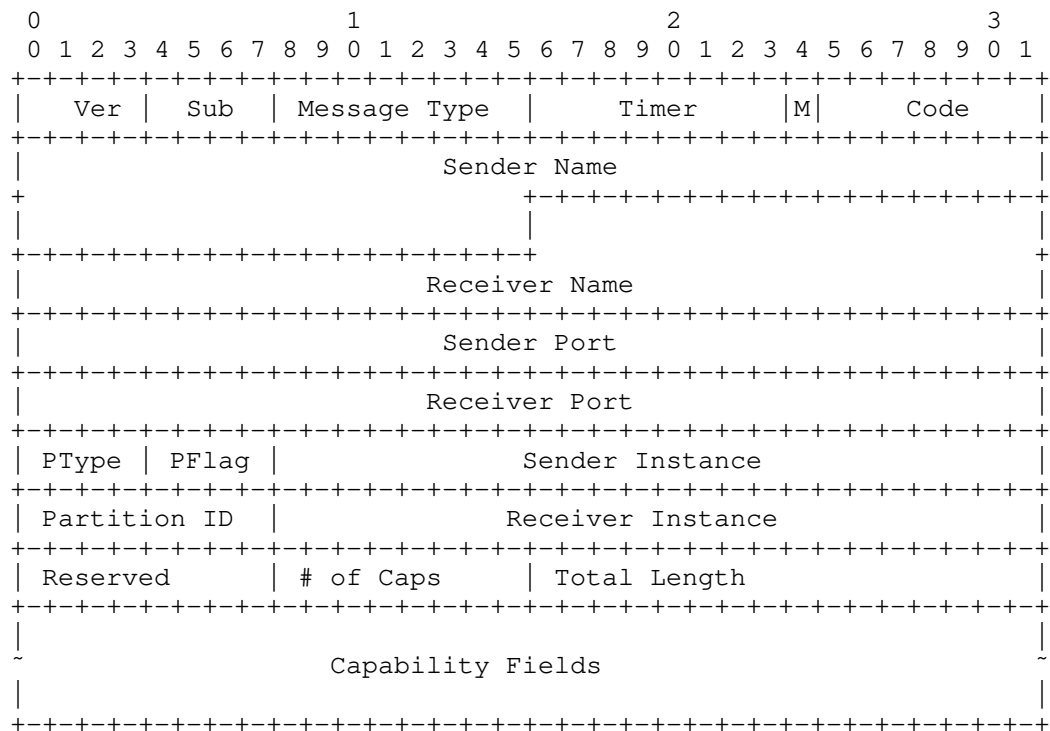


Figure 3

The fields added by ANCP are as follows:

Reserved: reserved for use by a future version of this specification.

Note: this was the Tech Type field in pre-standard versions of ANCP, but was determined to be unnecessary.

# of Caps: indicates the number of capability fields that follow.

Total Length: indicates the total number of bytes occupied by the capability fields that follow.

Capability Fields: Each capability field indicates one ANCP capability supported by the sender of the adjacency message. Negotiation of a common set of capabilities to be supported within the ANCP session is described in Section 4.5.2. The detailed format of a capability field is described below.

The format of a capability field is shown in Figure 4:

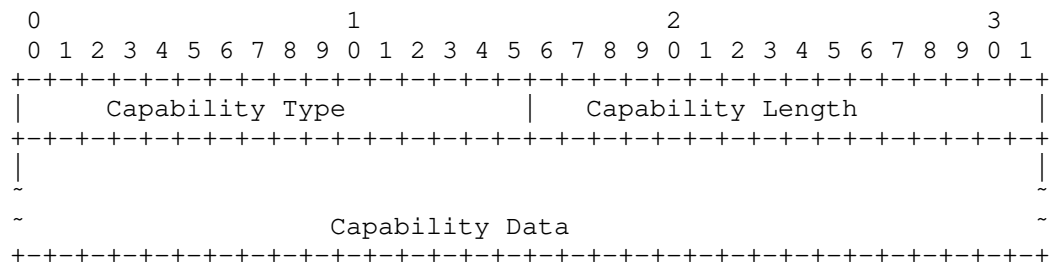


Figure 4: Capability Field

The sub-fields of this structure are as follows:

Capability Type: indicates the specific capability supported. An IANA registry exists for values of this sub-field. The values specified by this document are listed below.

Capability Length: the number of bytes of data contained in the Capability Data sub-field, excluding padding. If the definition of a particular capability includes no capability data, the value of the Capability Length sub-field is zero.

Capability Data: contains data associated with the capability as specified for that capability. If the definition of a particular capability includes no capability data, the Capability Data sub-field is absent (has zero length). Otherwise, the Capability Data sub-field MUST be padded with zeroes as required to terminate on a

4-byte word boundary. The possibility of specifying capability data provides the flexibility to advertise more than the mere presence or absence of a capability if needed.

The following capabilities are defined for ANCP as applied to DSL access:

- o Capability Type : DSL Topology Discovery = 0x01

Access technology: DSL

Length (in bytes) : 0

Capability Data : NULL

For the detailed protocol specification of this capability see Section 5.2.

- o Capability Type : DSL Line Configuration = 0x02

Access technology: DSL

Length (in bytes) : 0

Capability Data : NULL

For the detailed protocol specification of this capability see Section 5.3.

- o Capability Type : DSL Line Testing = 0x04

Access technology: DSL

Length (in bytes) : 0

Capability Data : NULL

For the detailed protocol specification of this capability see Section 5.4.

#### 4.5.2. ANCP Adjacency Procedures

The NAS MUST set the M-flag in the SYN message (signifying it is the master). Once the adjacency is established, periodic adjacency messages (type ACK) MUST be exchanged. The default for the ACK interval to be advertised in the adjacency messages is 25 seconds for ANCP. The actual value SHOULD be configurable and is an implementation choice. It is RECOMMENDED that both ends specify the

same timer value; to achieve this, each end SHOULD compare the timer value in the first adjacency message it receives with its own preferred value and agree to use the higher of the two values. That is, the node that receives a higher timer value than its own SHOULD reply in its subsequent adjacency messages (such as SYNACK, ACK) with the higher timer value.

In the adjacency protocol the version and sub-version fields are used for version negotiation. The version negotiation is performed before synchronisation is achieved. In a SYN message the version/sub-version fields always contain the highest version understood by the sender. A receiver receiving a SYN message with a version/sub-version higher than it understands MUST silently discard that message. A receiver receiving a SYN message with a version/sub-version within the range of versions that it understands MUST reply with a SYNACK with the version/sub-version from the received SYN in its ANCP version/sub-version fields. This defines the version/sub-version of the ANCP protocol to be used while the adjacency remains synchronised. All other ANCP messages within the session MUST use the agreed version in the version/sub-version fields.

The semantics and suggested values for the Code, Sender Name, Receiver Name, Sender Instance, and Receiver Instance fields are as defined in Section 11 of [RFC3292]. The Sender Port, and Receiver Port SHOULD be set to 0 by both ends. The pType field SHOULD be set to 0 (No Partition). The pFlag SHOULD be set to 1 (New Adjacency).

If the adjacency times out on either end, due to not receiving an adjacency message for a duration of (3 \* Timer value), where the timer value is specified in the adjacency message, all the state received from the ANCP neighbor SHOULD be cleaned up, and the TCP connection SHOULD be closed. The NAS MUST continue to listen for new connection requests. The AN MUST try to re-establish the TCP connection and both sides MUST attempt to re-establish the adjacency.

The handling defined above will need some modifications when ANCP graceful restart procedures are defined. These procedures will be defined in a separate document.

Both the NAS and the Access Node MUST advertise supported capabilities in the adjacency messages they send. The same message MAY advertise capabilities for any mixture of access technologies. If a received adjacency message indicates no support for a capability that is supported by the receiving device, it MUST turn off the capability locally and MUST send an updated adjacency message with the corresponding capability field omitted to match the received capability set. This process will eventually result in both sides



agreeing on the maximal common set of supported capabilities. The adjacency MUST NOT come up if that common set is empty.

After initial synchronization, if at any time a capability mismatch is detected, the adjacency MUST be brought down (RSTACK MUST be generated by the device detecting the mismatch), and synchronization MUST be re-attempted.

#### 4.6. ANCP General Message Formats

This section describes the general format of ANCP messages other than the adjacency messages.

The GSMPv3 general message format, used by all GSMP messages other than adjacency protocol messages, is defined in Section 3.1.1 of GSMPv3 [RFC3292]. ANCP modifies this base GSMPv3 message format as shown in Figure 5.

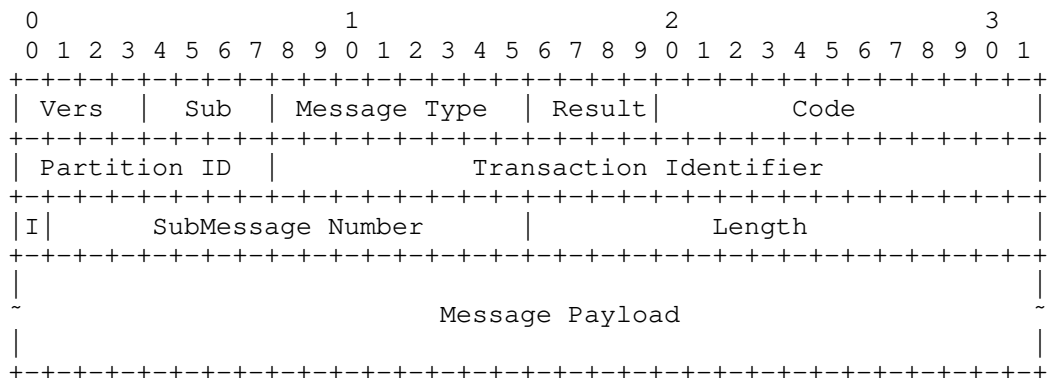


Figure 5: ANCP General Message Format

#### 4.6.1. The ANCP Message Header

The immediately visible differences from GSMPv3 are the subdivision of the Version field into version and sub-version, and the reallocation of space between Result and Code to enlarge the range for Code. The 8-bit version field in the base GSMPv3 message header is split into two 4 bit fields for carrying the version and a sub-version of the ANCP protocol. The Result field in the message header has been modified to be 4 bits long, and the Code field to be 12 bits long.

A complete explanation of the header fields is as follows:

**Version and Sub-version:** The version of the ANCP protocol that was agreed for the session during adjacency negotiation. For the values that must be placed into these fields, see Section 4.1.

**Message Type:** The ANCP message type. Message type values are registered in a common GSMPv3/ANCP IANA registry.

**Result:** The Result field is derived from GSMPv3 [RFC3292]. Ignore (0x0) is a new value added by ANCP. The remaining Result values below are a subset of those defined for GSMPv3. GSMPv3 expected the sender of a request to choose between NACK (0x1) and AckAll (0x2) according to its needs. ANCP specifies what Result value each request should have. Responses indicate either Success (0x3) or Failure (0x4) as the case may be.

**Ignore:** Res = 0x0 - Ignore this field on receipt and follow the procedures specified for the received message type.

**Nack:** Res = 0x1 - Result code indicating that no response is expected to the message other than in cases of failure caused during the processing of the message contents or of the contained directive(s).

**AckAll:** Res = 0x2 - Result code indicating that a response to the message is requested in all cases.

**Success:** Res = 0x3 - Set in a response message by the receiver of a request to indicate successful execution of all directives in the corresponding request message.

**Failure:** Res = 0x4 - Set in a response message by the receiver of a request to indicate either that there was an error in the content of the request message or that one or more directives in the corresponding request could not be executed successfully.

**Code:** This field gives further information concerning the result in a response message. It is mostly used to pass an error code in a failure response but can also be used to give further information in a success response message or an event message. In a request message, the Code field is not used and MUST be set to zero.

ANCP implementations MAY use any of the Code values specified in the IANA registry "Global Switch Management Protocol version 3 (GSMPv3) Failure Response Message Name Space" if they appear applicable. In particular, the values:

- 2 Invalid request message (i.e., a properly formed message which violates the protocol through its timing or direction of transmission)
- 4 One or more of the specified ports do not exist
- 6 One or more of the specified ports are down
- 7 Invalid Partition ID
- 19 Out of resources (e.g. memory exhausted, etc.)
- 30 The limit on the maximum number of point-to-multipoint connections that the switch can support has been reached
- 31 The limit on the maximum number of branches that the specified point-to-multipoint connection can support has been reached

may unfortunately apply to ANCP usage, where "Port" is interpreted to mean an access line or a Target as defined in Section 6.2.1.

Instead of the value:

- 3 The specified request is not implemented on this switch
- specified by [RFC3292], this specification defines a new value:
- 81 Request message type not implemented

This value MAY be sent in a failure response from either the AN or the NAS. This specification also defines the additional values:

- 82 Transaction identifier out of sequence
- 83 Malformed message
- 84 TLV or value not supported by negotiated capability set

ANCP extensions defining new code values SHOULD use the range 256 (0x100) through 511 (0x1FF) for this purpose.

The range of values from 256 to 4095 is reserved for IETF use.

Partition ID: This field is a 8 bit number which signifies a partition on the AN.

The AN and NAS may agree on the partition ID using one of the

following possible options:

- 1 - The partition ID may be configured on the AN and learned by the NAS in the adjacency message;
- 2 - The partition ID may be statically configured on the NAS as part of configuring the neighbor information.

**Transaction ID:** 24-bit field set by the sender of a request message to associate a response message with the original request message. Unless otherwise specified for a given message type, the Transaction ID in request messages MUST be set to a value in the range (1,  $2^{24} - 1$ ). When used in this manner, the Transaction ID sequencing MUST be maintained independently for each ANCP adjacency and per message type. Furthermore, it SHOULD be incremented linearly for each new message of the given type, cycling back to 1 after running the full range. Each Transaction ID sequence SHOULD be reinitialized to a random non-zero value when an adjacency is negotiated. For event messages, the Transaction ID SHOULD be set to zero.

Unless otherwise specified, the default behaviour for all ANCP responses is that the value of the Transaction ID MUST be copied from the corresponding request message.

**I flag and SubMessage Number:** An ANCP implementation SHOULD set the I Flag and subMessage Number fields to 1 to signify no fragmentation.

**Length:** Length of the ANCP message including its header fields and defined ANCP message body.

#### 4.6.2. The ANCP Message Body

The detailed contents of the message payload portion of a given ANCP message may vary with the capability in the context of which it is being used. However, the general format consists of zero or more fixed fields, followed by a variable amount of data in the form of Type-Length-Value (TLV) data structures.

The general format of a TLV is shown in Figure 6:

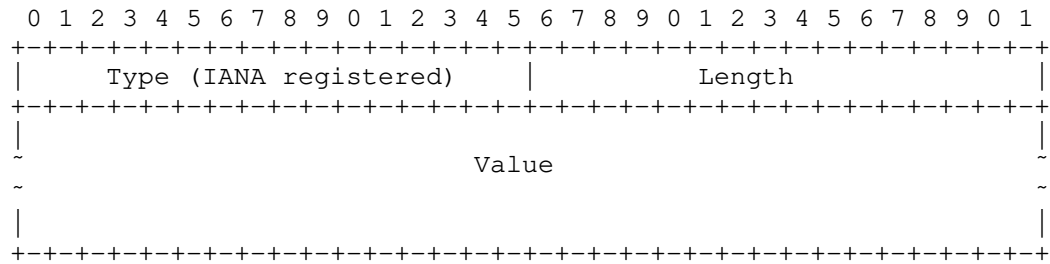


Figure 6: General TLV Format

The fields of a TLV are defined as follows:

**Type:** The TLV Type is a 16-bit unsigned value identifying the TLV type and nature of its contents. An IANA registry has been established for ANCP TLV Type codes.

**Length:** The number of bytes of data in the Value field of the TLV, excluding any padding required to bring this TLV to a 4-byte word boundary (see "Value" below). If a TLV contains other TLVs, any padding in the contained TLVs **MUST** be included in the value of Length.

If the TLV contains another TLV followed by other data, the outer TLV will not be properly parsable unless Length is set as indicated; if the interior padding is omitted from Length, as many bytes of data at the end of the outer TLV will be missed. If the outer TLV contains another TLV as its final field it requires no padding of its own (since the contained TLV including padding ends on a 4-byte boundary). In this case the issue is one of consistency rather than parsability, since the padding of that final TLV could be omitted from Length without loss of data.

Depending on the specification of the TLV, the value of Length may be zero, a constant for all instances of the TLV, or a varying quantity.

**Value** The actual data carried by the TLV, if any. The value field in each TLV **MUST** be padded with zeroes as required to align with a 4-byte word boundary. The Value field of a TLV may include fixed fields and/or other TLVs.

Unless otherwise specified, TLVs **MAY** be added to a message in any order. If the recipient of a message does not understand a particular TLV, it **MUST** silently ignore it.

A number of TLVs are specified in the remainder of this document.

## 5. ANCP Capabilities For Digital Subscriber Lines (DSL)

### 5.1. Overview

DSL is a widely deployed access technology for Broadband Access for Next Generation Networks. Specifications such as [TR\_059], [TR\_058], and [TR\_092] describe possible architectures for these access networks. The scope of these specifications includes the delivery of voice, video, and data services.

When deploying value-added services across DSL access networks, special attention is required to assure quality of service and service control, which implies a tighter coordination between network elements in the broadband access network without burdening the OSS layer.

This document specifies basic ANCP capabilities for use specifically in controlling Access Nodes serving DSL access (Tech Type = 0x05). The same ANs could be serving other access technologies (e.g. Metro-Ethernet, Passive Optical Networking, WiMax), in which case the AN will also have to support the corresponding other-technology-specific capabilities. These additional capabilities are not specified here, but may be specified in other documents.

The DSL capabilities specified in this section are:

**DSL Topology Discovery:** Dynamic discovery of access topology and DSL line attributes by the NAS, to support tight QoS control in the access network.

**DSL Line Configuration:** Pushing subscriber and service data retrieved by the NAS from an OSS system (e.g., RADIUS server) to the Access Nodes, to simplify OSS infrastructure for service management.

**DSL Line Testing:** NAS controlled, on-demand access- line test capability (rudimentary end-to-end OAM).

#### 5.1.1. ATM-Specific Considerations

Topology discovery and line configuration involve the DSL line attributes. For ATM based access networks, the DSL line on the DSLAM is identified by the port and PVP/PVC corresponding to the subscriber. The DSLAMs are connected to the NAS via an ATM access aggregation network. Since, the DSLAM (Access Node) is not directly

connected to the NAS, the NAS needs a mechanism to learn the DSL line identifier (more generally referred to as "access loop circuit ID") corresponding to a subscriber. The access loop circuit ID has no local significance on the NAS. The ANCP messages for topology discovery and line configuration carry opaque Access-Loop-Circuit-ID values which have only local significance on the DSLAMs.

The access loop circuit identifier can be carried as a UTF-8-encoded string in the ANCP messages. This allows ANCP to be decoupled from the specifics of the underlying access technology being controlled. On the other hand, this requires a NAS mechanism by which each such identifier can be correlated to the context of an aggregation-network-facing IP interface (corresponding to the subscriber) on the NAS. This will typically require local configuration of such IP interfaces, or of the underlying ATM interfaces.

#### 5.1.2. Ethernet-Specific Considerations

One possible way of approaching the use of Ethernet technology in the access aggregation network is to recreate the equivalent of Virtual Paths (VPs) and Virtual Circuits (VCs) by using stacked Virtual LAN tags. As an example, one can use an "outer" VLAN to create a form of "virtual path" between a given DSLAM and a given NAS, and then use "inner" VLAN tags to create a form of "virtual circuit" on a per DSL line basis. In this case, VLAN tags conveyed in topology discovery and line configuration messages will allow unique identification of the DSL line in a straightforward manner, assuming the VLAN tags are not translated in some way by the aggregation network, and are unique across physical ports.

However, some carriers do not wish to use this "connection oriented" approach. Therefore, an alternative model is to bridge sessions from multiple subscribers behind a DSLAM to a single VLAN in the aggregation network. This is the N:1 model. In this model, or in the case where user traffic is sent untagged, the Access Node needs to insert the exact identity of the DSL line in the topology discovery and line configuration messages, and then have a mechanism by which this can be correlated to the context of an aggregation-network-facing IP interface (for the subscriber) on the NAS. This can either be based on local configuration on the NAS, or on the fact that a DSLAM (Access Node) typically inserts the access loop circuit ID in subscriber signaling messages relayed to the NAS (i.e. DHCP or PPPoE discovery messages).

Section 5.2.3.3 defines TLVs to represent the "access loop circuit ID".

## 5.2. ANCP Based DSL Topology Discovery

### 5.2.1. Goals

[TR\_059] discusses various queuing/scheduling mechanisms to avoid congestion in the access network while dealing with multiple flows with distinct QoS requirements. Such mechanisms require that the NAS gains knowledge about the topology of the access network, the various links being used and their respective net data rates. Some of the information required is somewhat dynamic in nature (e.g. DSL sync rate, and therefore also the net data rate), hence cannot come from a provisioning and/or inventory management OSS system. Some of the information varies less frequently (e.g. capacity of a DSLAM uplink), but nevertheless needs to be kept strictly in sync between the actual capacity of the uplink and the image the NAS has of it.

The following section describes ANCP messages that allow the Access Node (e.g., DSLAM) to communicate access network topology information and any corresponding updates to the NAS.

Some of the parameters that can be communicated from the DSLAM to the NAS include DSL line state, actual upstream and downstream net data rates of a synchronized DSL link, maximum attainable upstream and downstream net data rates, interleaving delay etc. Topology discovery is specifically important when the net data rate of the DSL line changes over time. The DSL net data rate may be different every time the DSL modem is turned on. Additionally, during the time the DSL modem is active, data rate changes can occur due to environmental conditions (the DSL line can get "out of sync" and can retrain to a lower value).

### 5.2.2. Message Flow

To provide expected service levels, the NAS needs to learn the initial attributes of the DSL line before the subscriber can log in and access the services provisioned for the subscription. When a DSL line initially comes up or resynchronizes to a different rate, the DSLAM generates and transmits an ANCP Port UP Event message to the NAS. The extension field in the message carries the TLVs containing DSL line specific parameters. Upon loss of signal on the DSL line, an ANCP Port DOWN message is generated by the DSLAM and sent to the NAS. Figure 7 summarizes the interaction.



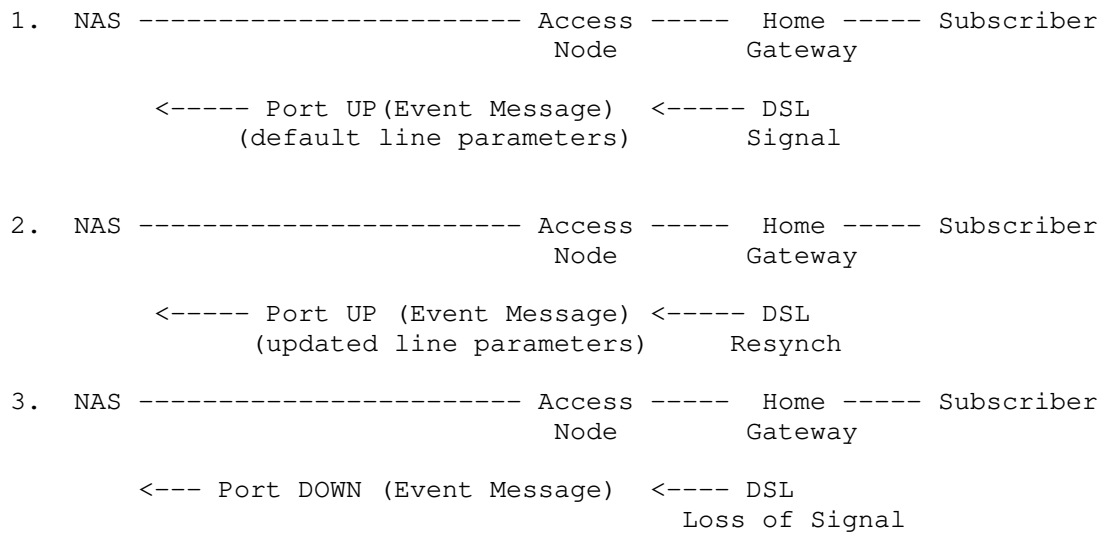


Figure 7: ANCP Message Flow For DSL Topology Discovery

The Event message with Port UP message type (80) is used for conveying DSL line attributes to the NAS. This message with relevant extensions is defined in the next section.

### 5.2.3. Specification of the ANCP DSL Topology Discovery Capability

#### 5.2.3.1. Protocol Requirements

The DSL topology discovery capability is assigned capability type 0x01. No capability data is associated with this capability. Implementations of the DSL topology discovery capability MUST support the following ANCP protocol elements:

- o ANCP Port UP and Port DOWN Event messages, which are based on the GSMPv3 [RFC3292] messages of the same name but include capability-specific modifications and extensions (Section 5.2.3.2).
- o The procedures associated with these messages and their contents (Section 5.2.3.2.1).
- o Access-Loop-Circuit-ID TLV;
- o Access-Loop-Remote-Id TLV;
- o Access-Aggregation-Circuit-ID-ASCII TLV;

- o Access-Aggregation-Circuit-ID-Binary TLV;
- o DSL-Line-Attributes TLV;
- o DSL-Type TLV;
- o Actual-Net-Data-Upstream TLV;
- o Actual-Net-Data-Rate-Downstream TLV;
- o Minimum-Net-Data-Rate-Upstream TLV;
- o Minimum-Net-Data-Rate-Downstream TLV;
- o Attainable-Net-Data-Rate-Upstream TLV;
- o Attainable-Net-Data-Rate-Downstream TLV;
- o Maximum-Net-Data-Rate-Upstream TLV;
- o Maximum-Net-Data-Rate-Downstream TLV;
- o Minimum-Net-Low-Power-Data-Rate-Upstream TLV;
- o Minimum-Net-Low-Power-Data-Rate-Downstream TLV;
- o Maximum-Interleaving-Delay-Upstream TLV;
- o Maximum-Interleaving-Delay-Downstream TLV;
- o Actual-Interleaving-Delay-Upstream TLV;
- o Actual-Interleaving-Delay-Downstream TLV;
- o DSL-line-state TLV;
- o Access Loop Encapsulation TLV.

The TLVs listed above are specified in Section 5.2.3.3.

#### 5.2.3.2. ANCP Port UP and Port DOWN Event Message Descriptions

The ANCP Port UP and Port DOWN Event messages are derived from the GSMPv3 Event message shown in Section 9 of [RFC3292]. The modified format used for DSL topology discovery is shown in Figure 8.

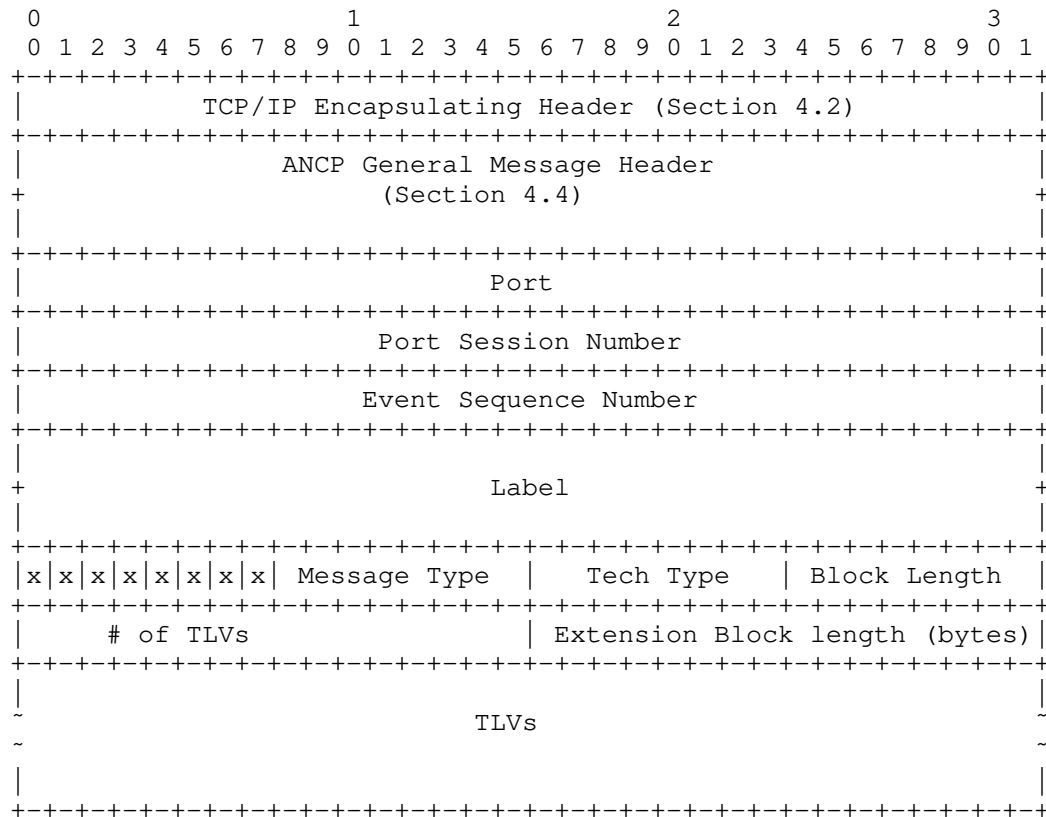


Figure 8: Format Of the ANCP Port UP and Port DOWN Event Messages For DSL Topology Discovery

See Section 4.6 for a description of the ANCP general message header. The Message Type field MUST be set to 80 for Port UP, 81 for Port DOWN. The 12 bit Code field MUST be set to 0. The 4 bit Result field MUST be set to 0 (signifying Ignore). The 24-bit Transaction Identifier field MUST be set to 0. Other fields in the general header MUST be set as described in Section 4.6.

The Port, Port Session Number, and Event Sequence Number fields are not used by the DSL Topology Discovery capability. The Label field (including the Stacked Label Indicator and the unused flags at the start of the Label field), is also unused, and **MUST** be treated as an unused fixed 8-byte field. The handling of unused/reserved fields is described in Section 4.4.

The remaining message fields are described as follows:

Extension Flags: The flag bits denoted by 'x' are currently unspecified and reserved.

Message Type: Message Type has the same value as in the general header (i.e., 80 or 81).

Tech Type: MUST be set to 0x05 (DSL).

Block Length: unused, see Section 4.4. This field was defined in early implementations, but limits what follows to 255 bytes, which is not sufficient.

# of TLVs: the number of TLVs that follow, not counting TLVs encapsulated within other TLVs.

Extension Block Length: the total length of the TLVs carried in the extension block in bytes, including any padding within individual TLVs.

TLVs: two or more TLVs to identify a DSL line and define its characteristics.

#### 5.2.3.2.1. Procedures

The GSMP Event message with Port UP message type (80) is used for conveying DSL line attributes to the NAS. The message SHOULD be generated when a line first comes UP, or any of the attributes of the line change e.g. the line re-trains to a different rate or one or more of the configured line attributes are administratively modified. Also, when the ANCP session first comes up, the DSLAM SHOULD transmit a Port UP message to the NAS for each line that is up. When a DSL line goes down (idle or silent), the DSLAM SHOULD transmit an Event message with Port DOWN message type (81) to the NAS. It is recommended that the DSLAMs use a dampening mechanism per DSL line to control the rate of state changes per DSL line, communicated to the NAS.

If a Port UP message with a Result field set to 0 is received by the NAS and the NAS is able to process the message correctly, the NAS MUST NOT generate any ANCP message in response to the Port UP. If the Port UP message received cannot be processed correctly by the NAS (e.g. the message is malformed) the NAS MAY respond with an ANCP Generic Response message (Section 6.1.3) containing the reason for the failure.

In the case of bonded copper loops to the customer premise (as per the DSL multi-pair bonding described by [G.988.1] and [G.988.2]), the DSLAM MUST report the aggregate net data rate and other attributes

for the DSL bonded circuit (represented as a single logical port) to the NAS in a Port UP message. Any change in the aggregate net data rate of the DSL bonded circuit (due to a change in net data rate or state of individual constituent DSL lines) MUST be reported by the DSLAM to the NAS in a Port UP message. The DSLAM MUST also report the aggregate state of the DSL bonded circuit to the NAS via Port UP and Port DOWN messages.

The definition of TLVs in the next section contains some additional procedural information.

#### 5.2.3.3. TLVs For DSL Topology Discovery

The following TLVs are currently defined for DSL Topology Discovery, but may be reused for other capabilities.

##### 5.2.3.3.1. Access-Loop-Circuit-ID TLV

Name: Access-Loop-Circuit-ID

Type: 0x0001

Description: a locally administered human-readable string generated by or configured on the Access Node, identifying the corresponding access loop logical port. The access loop circuit ID has local significance at the Access Node. The exact usage on the NAS is beyond the scope of this document. The format used for local loop identification in ANCP messages MUST be identical to what is used by the Access Nodes in subscriber signaling messages when the Access Nodes act as signaling relay agents as outlined in [RFC3046] and [TR\_101].

The local loop can be ATM based or Ethernet based. Section 3.9 of [TR\_101] recommends default formats for either case, with the intention that the Access Node automatically generates the identifier for a given access line using the default format unless an identifier has been configured by the operator. The recommended default format begins with a locally-configured Access Node identifier. For an ATM based local loop the remainder of the string consists of slot/port and VPI/VCI information corresponding to the subscriber's DSL connection. In ABNF notation [RFC5234], the recommended syntax is:

```
Access-Node-Identifier SP "atm" SP slot "/" port ":" vpi "."  
vci
```

where the meanings of the terms should be obvious from their names.

For a local loop which is Ethernet based (and tagged), the remainder of the string consists of slot/port and incoming VLAN tag (if any) describing the access line appearance on the Access Node. The syntax of the recommended default format in ABNF notation is:

```
Access-Node-Identifier SP "eth" SP slot "/" port [":" vlan-id]
```

This is a mandatory TLV.

Length: up to 63 bytes

Value: ASCII string

#### 5.2.3.3.2. Access-Loop-Remote-Id TLV

Name: Access-Loop-Remote-Id

Type: 0x0002

Description: This is an optional TLV. This contains an operator-configured string that uniquely identifies the user on the associated access line, as described in Section 3.9.2 of [TR\_101]. The exact usage on the NAS is out of scope of this document. It is desirable that the format used for the field be similar to what is used by the Access Nodes in subscriber signaling messages when the Access Nodes act as signaling relay agents as outlined in [RFC3046] and [TR\_101].

Length: up to 63 bytes

Value: ASCII string

#### 5.2.3.3.3. Access-Aggregation-Circuit-ID-Binary TLV

Name: Access-Aggregation-Circuit-ID-Binary

Type: 0x0006

Description: For ethernet access aggregation, where a per-subscriber (stacked) VLAN can be applied (1:1 model defined in [TR\_101]), the VLAN stack provides a convenient way to uniquely identify the DSL line. The outer VLAN is equivalent to virtual path between a DSLAM and the NAS and inner VLAN is equivalent to a virtual circuit on a per DSL line basis. In this scenario, any subscriber data received by the Access Node and transmitted out the uplink to the aggregation network will be tagged with the VLAN stack

assigned by the Access Node.

The Access-Aggregation-Circuit-ID-Binary is illustrated in Figure 9 (below). This TLV carries the VLAN tags assigned by the access node in the ANCP messages. The VLAN tags can uniquely identify the DSL line being referred to in the ANCP messages, assuming the VLAN tags are not in any way translated in the aggregation network and are unique across physical ports. Each 32 bit unsigned integer contains a 12 bit VLAN identifier (which is part of the VLAN tag defined by IEEE 802.1Q).

Also, in case of an ATM aggregation network, where the DSLAM is directly connected to the NAS (without an intermediate ATM switch), the two values can contain VPI and VCI on the DSLAM uplink (and correspond uniquely to the DSL line on the DSLAM).

This TLV is optional.

Length: 8 bytes

Value: two 32 bit unsigned integers

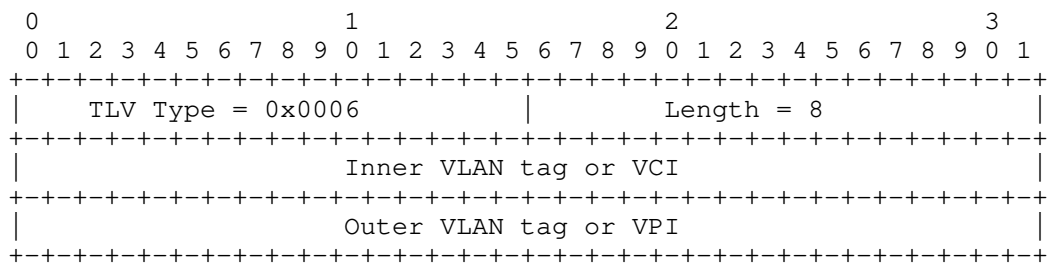


Figure 9: The Access-Aggregation-Circuit-ID-Binary TLV

#### 5.2.3.3.4. Access-Aggregation-Circuit-ID-ASCII TLV

Name: Access-Aggregation-Circuit-ID-ASCII

Type: 0x0003

Description: This field contains information pertaining to an uplink on the Access Node. For Ethernet access aggregation, assuming the Access Node assigns VLAN tags (1:1 model), typical ABNF format for the string is:

```
Access-Node-Identifier SP "eth" SP slot "/" port [":" inner-  
vlan-id] [":" outer-vlan-id]
```

The slot/port corresponds to the ethernet uplink on the Access Node towards the NAS.

For an ATM aggregation network, the typical format for the string is:

```
Access-Node-Identifier SP "atm" SP slot "/" port ":" vpi "."  
vci
```

This TLV allows the NAS to associate the information contained in the ANCP messages to the DSL line on the Access Node.

If the Access Node inserts this string in the ANCP messages, when referring to local loop characteristics (e.g. DSL line in case of a DSLAM), then it should be able to map the information contained in the string uniquely to the local loop (e.g. DSL line).

On the NAS, the information contained in this string can be used to derive an aggregation-network-facing construct (e.g. an IP interface) corresponding to the local loop (e.g. DSL line). The association could be based on local configuration on the NAS.

The Access Node can also convey to the NAS the characteristics (e.g., bandwidth) of the uplink on the Access Node. This TLV then serves the purpose of uniquely identifying the uplink whose characteristics are being defined. This version of the present document does not specify the TLVs needed to convey the uplink characteristics, in the same way that the DSL-Line-Attributes TLV and the TLVs encapsulated within it convey the characteristics of the subscriber access line.

This TLV is optional.

Length: up to 63 bytes

Value: ASCII string

#### 5.2.3.3.5. DSL-Line-Attributes TLV (Mandatory)



Name: DSL-Line-Attributes

Type: 0x0004

Description: This is a mandatory TLV providing attribute values for a DSL line serving a subscriber.

Length: variable (up to 1024 bytes)

Value: one or more encapsulated TLVs corresponding to DSL line attributes. The DSL-Line-Attributes TLV MUST contain the mandatory TLVs described below when it is present in a Port UP message. It MAY contain the optional TLVs described below when it is present in a Port UP message.

When the DSL-Line-Attributes TLV is present in a Port DOWN message it SHOULD NOT include any TLVs other than DSL-Type and DSL-Line-State.

#### 5.2.3.3.6. TLVs Delivering Line Attributes

The TLVs which follow convey DSL line attributes. They MUST be encapsulated within the DSL-Line-Attributes TLV when they are carried in a Port UP or Port DOWN message.

##### 5.2.3.3.6.1. DSL-Type TLV (Mandatory)

Name: DSL-Type

Type: 0x0091

Description: Indicates the type of transmission system in use. This is a mandatory TLV.

Length: 4 bytes

Value: 32 bit unsigned integer

ADSL1 = 1

ADSL2 = 2

ADSL2+ = 3

VDSL1 = 4

VDSL2 = 5

SDSL = 6

UNKNOWN = 7

#### 5.2.3.3.6.2. Actual-Net-Data-Rate-Upstream TLV

Name: Actual-Net-Data-Rate-Upstream

Type: 0x0081

Description: Actual upstream net data rate on a DSL line. This is a mandatory TLV.

Length: 4 bytes

Value: Rate in Kbits/s as a 32 bit unsigned integer

#### 5.2.3.3.6.3. Actual-Net-Data-Rate-Downstream TLV

Name: Actual-Net-Data-Rate-Downstream

Type: 0x0082

Description: Actual downstream net data rate on a DSL line. This is a mandatory TLV.

Length: 4 bytes

Value: Rate in Kbits/s as a 32 bit unsigned integer

#### 5.2.3.3.6.4. Minimum-Net-Data-Rate-Upstream TLV

Name: Minimum-Net-Data-Rate-Upstream

Type: 0x0083

Description: Minimum upstream net data rate desired by the operator. This is an optional TLV.

Length: 4 bytes

Value: Rate in Kbits/s as a 32 bit unsigned integer

#### 5.2.3.3.6.5. Minimum-Net-Data-Rate-Downstream TLV

Name: Minimum-Net-Data-Rate-Downstream

Type: 0x0084

Description: Minimum downstream net data rate desired by the operator. This is an optional TLV.

Length: 4 bytes

Value: Rate in Kbits/s as a 32 bit unsigned integer

#### 5.2.3.3.6.6. Attainable-Net-Data-Rate-Upstream TLV

Name: Attainable-Net-Data-Rate-Upstream

Type: 0x0085

Description: Maximum net upstream rate that can be attained on the DSL line. This is an optional TLV.

Length: 4 bytes

Value: Rate in Kbits/s as a 32 bit unsigned integer

#### 5.2.3.3.6.7. Attainable-Net-Data-Rate-Downstream TLV

Name: Attainable-Net-Data-Rate-Downstream

Type: 0x0086

Description: Maximum net downstream rate that can be attained on the DSL line. This is an optional TLV.

Length: 4 bytes

Value: Rate in Kbits/s as a 32 bit unsigned integer

#### 5.2.3.3.6.8. Maximum-Net-Data-Rate-Upstream TLV

Name: Maximum-Net-Data-Rate-Upstream

Type: 0x0087

Description: Maximum net upstream data rate desired by the operator. This is an optional TLV.

Length: 4 bytes

Value: Rate in Kbits/s as a 32 bit unsigned integer

5.2.3.3.6.9. Maximum-Net-Data-Rate-Downstream TLV

Name: Maximum-Net-Data-Rate-Downstream

Type: 0x0088

Description: Maximum net downstream data rate desired by the operator. This is an optional TLV.

Length: 4 bytes

Value: Rate in Kbits/s as a 32 bit unsigned integer

5.2.3.3.6.10. Minimum-Net-Low-Power-Data-Rate-Upstream TLV

Name: Minimum-Net-Low-Power-Data-Rate-Upstream

Type: 0x0089

Description: Minimum net upstream data rate desired by the operator in low power state. This is an optional TLV.

Length: 4 bytes

Value: Rate in Kbits/s as a 32 bit unsigned integer

5.2.3.3.6.11. Minimum-Net-Low-Power-Data-Rate-Downstream TLV

Name: Minimum-Net-Low-Power-Data-Rate-Downstream

Type: 0x008A

Description: Minimum net downstream data rate desired by the operator in low power state. This is an optional TLV.

Length: 4 bytes

Value: Rate in Kbits/s as a 32 bit unsigned integer

5.2.3.3.6.12. Maximum-Interleaving-Delay-Upstream TLV

Name: Maximum-Interleaving-Delay-Upstream

Type: 0x008B

Description: maximum one way interleaving delay. This is an optional TLV.

Length: 4 bytes

Value: Time in ms as a 32 bit unsigned integer

#### 5.2.3.3.6.13. Actual-Interleaving-Delay-Upstream TLV

Name: Actual-Interleaving-Delay-Upstream

Type: 0x008C

Description: Value corresponding to the interleaver setting. This is an optional TLV.

Length: 4 bytes

Value: Time in ms as a 32 bit unsigned integer

#### 5.2.3.3.6.14. Maximum-Interleaving-Delay-Downstream TLV

Name: Maximum-Interleaving-Delay-Downstream

Type: 0x008D

Description: maximum one way interleaving delay. This is an optional TLV.

Length: 4 bytes

Value: Time in ms as a 32 bit unsigned integer

#### 5.2.3.3.6.15. Actual-Interleaving-Delay-Downstream

Name: Actual-Interleaving-Delay-Downstream

Type: 0x008E

Description: Value corresponding to the interleaver setting. This is an optional TLV.

Length: 4 bytes

Value: Time in ms as a 32 bit unsigned integer

#### 5.2.3.3.6.16. DSL-Line-State TLV (Mandatory for Port DOWN)

Name: DSL-Line-State

Type: 0x008F

Description: The state of the DSL line. For the Port UP message, in this specification, the TLV is optional (since the message type implicitly conveys the state of the line). For Port DOWN, the TLV is mandatory, since it further communicates the state of the line as IDLE or SILENT.

Length: 4 bytes

Value: 32 bit unsigned integer

SHOWTIME = 1

IDLE = 2

SILENT = 3

#### 5.2.3.3.6.17. Access-Loop-Encapsulation TLV

Name: Access-Loop-Encapsulation

Type: 0x0090

Description: The data link protocol and, optionally, the encapsulation overhead on the access loop. This is an optional TLV. However, when this TLV is present, the data link protocol MUST minimally be indicated. The encapsulation overhead MAY be indicated. The Access Node can choose to not convey the encapsulation on the access loop by specifying a value of 0 (NA) for the two encapsulation fields

Length: 3 bytes

Value: The three bytes (most to least significant) and valid set of values for each byte are defined below.

Byte 1: Data Link

ATM AAL5 = 0

ETHERNET = 1

Byte 2: Encapsulation 1

NA = 0

Untagged Ethernet = 1

Single-tagged Ethernet = 2

Byte 3: Encapsulation 2

NA = 0

PPPoA LLC = 1

PPPoA NULL = 2

IPoA LLC = 3

IPoA NULL = 4

Ethernet over AAL5 LLC with FCS = 5

Ethernet over AAL5 LLC without FCS = 6

Ethernet over AAL5 NULL with FCS = 7

Ethernet over AAL5 NULL without FCS = 8

The Access-Loop-Encapsulation TLV is illustrated in Figure 10.

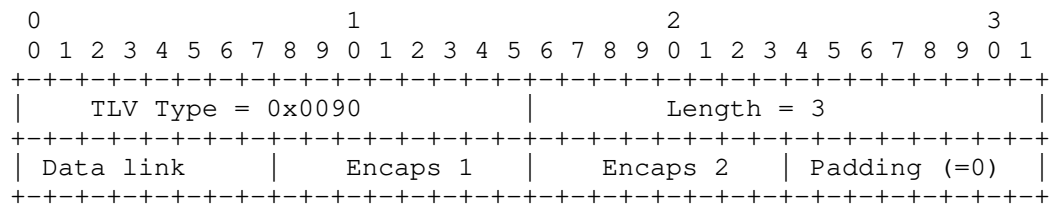


Figure 10: The Access-Loop-Encapsulation TLV

### 5.3. ANCP based DSL Line Configuration

#### 5.3.1. Goals

Following dynamic discovery of access topology (identification of DSL line and its attributes) as assisted by the mechanism described in the previous section (topology discovery), the NAS may query a subscriber management OSS system (e.g., RADIUS server) to retrieve subscriber authorization data (service profiles). Most of such service mechanisms are typically enforced by the NAS itself, but there are a few cases where it may be useful to push such service parameters to the DSLAM for local enforcement of a mechanism (e.g. DSL-related) on the corresponding subscriber line.

One such example of a service parameter that can be pushed to the DSLAM for local enforcement is DSL "interleaving delay". Longer interleaving delay (and hence stringent error correction) is required for a video service to ensure better video "quality of experience", whereas for a VoIP service or for "shoot first" gaming service, a very short interleaving delay is more appropriate. Another relevant application is downloading per subscriber multicast channel entitlement information in IPTV applications where the DSLAM is performing IGMP snooping or IGMP proxy function. Using ANCP, the NAS can achieve the goal of pushing line configuration to the DSLAM by an interoperable and standardized protocol.

If a subscriber wants to choose a different service, it can require an operational-expense-intensive reconfiguration of the line via a network operator, possibly implying a business-to-business transaction between an ISP and an access provider. Using ANCP for line configuration from the NAS dramatically simplifies the OSS infrastructure for service management, allowing fully centralized subscriber-related service data (e.g., RADIUS server back-end) and avoiding complex cross-organization business-to-business interactions.

The best way to change line parameters is by using profiles. These profiles (DSL profiles for different services) are pre-configured on the DSLAMs. The NAS can then send a reference to the right DSL profile via ANCP. Alternatively, discrete DSL parameters can also be conveyed by the NAS in ANCP.

#### 5.3.2. Message Flow

Triggered by topology information reporting a new DSL line or triggered by a subsequent user session establishment (PPP or DHCP), the NAS may send line configuration information (e.g. reference to a DSL profile) to the DSLAM using ANCP Port Management messages. The



NAS may get such line configuration data from a policy server (e.g., RADIUS). Figure 11 summarizes the interaction.

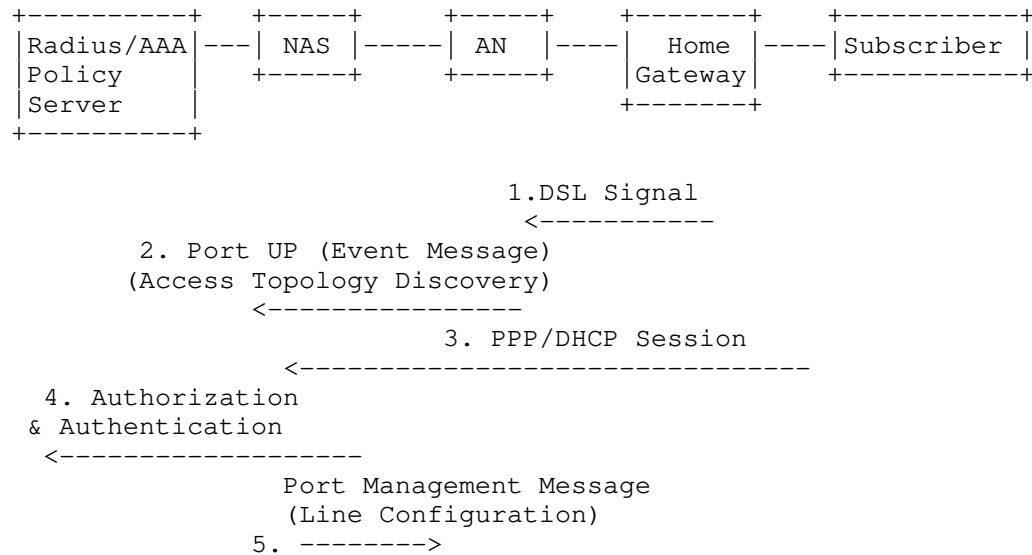


Figure 11: Message Flow - ANCP Mapping For Initial Line Configuration

The NAS may update the line configuration due to a subscriber service change (e.g. triggered by the policy server). Figure 12 summarizes the interaction.

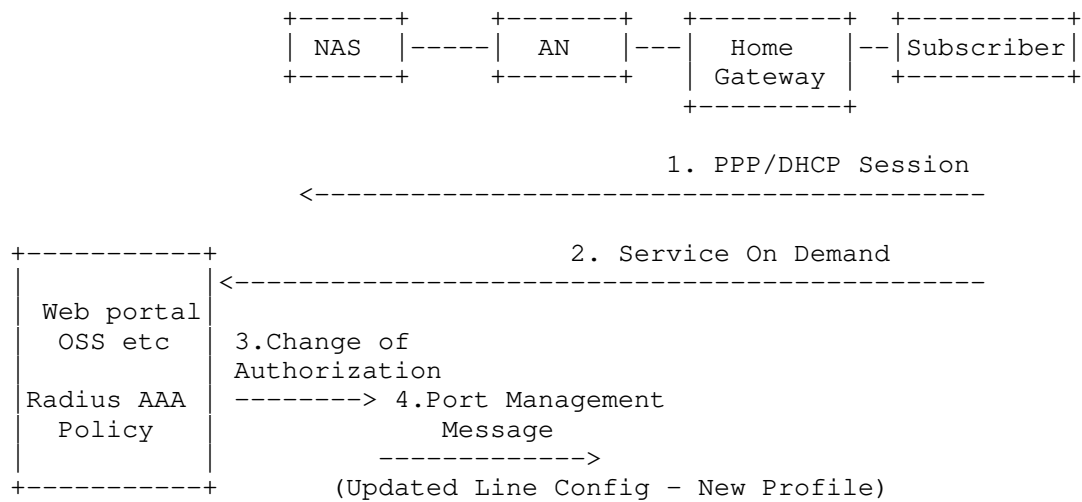


Figure 12: Message flow - ANCP Mapping For Updated Line Configuration

The format of relevant extensions to port management message is defined in section Section 5.3.3. The line configuration models could be viewed as a form of delegation of authorization from the NAS to the DSLAM.

### 5.3.3. Specification of the ANCP DSL Line Configuration Capability

#### 5.3.3.1. Protocol Requirements

The DSL line configuration capability is assigned capability type 0x02. No capability data is associated with this capability. Implementations of the DSL line configuration capability MUST support the following ANCP protocol elements:

- o ANCP Port Management message, which is based on the GSMPv3 [RFC3292] message of the same name but includes capability-specific modifications and extensions (Section 5.3.3.2).
- o The procedures associated with this message and its contents (Section 5.3.3.3).
- o Access-Loop-Circuit-ID TLV (as defined in Section 5.2.3.3);
- o Access-Aggregation-Circuit-ID-Binary TLV (as defined in Section 5.2.3.3);

- o Access-Aggregation-Circuit-ID-ASCII TLV (as defined in Section 5.2.3.3);
- o Service-Profile-Name TLV (as defined in Section 5.3.3.4).

#### 5.3.3.2. ANCP Port Management Message Format For DSL Line Configuration

The ANCP Port Management message for DSL line configuration has the format shown in Figure 13.

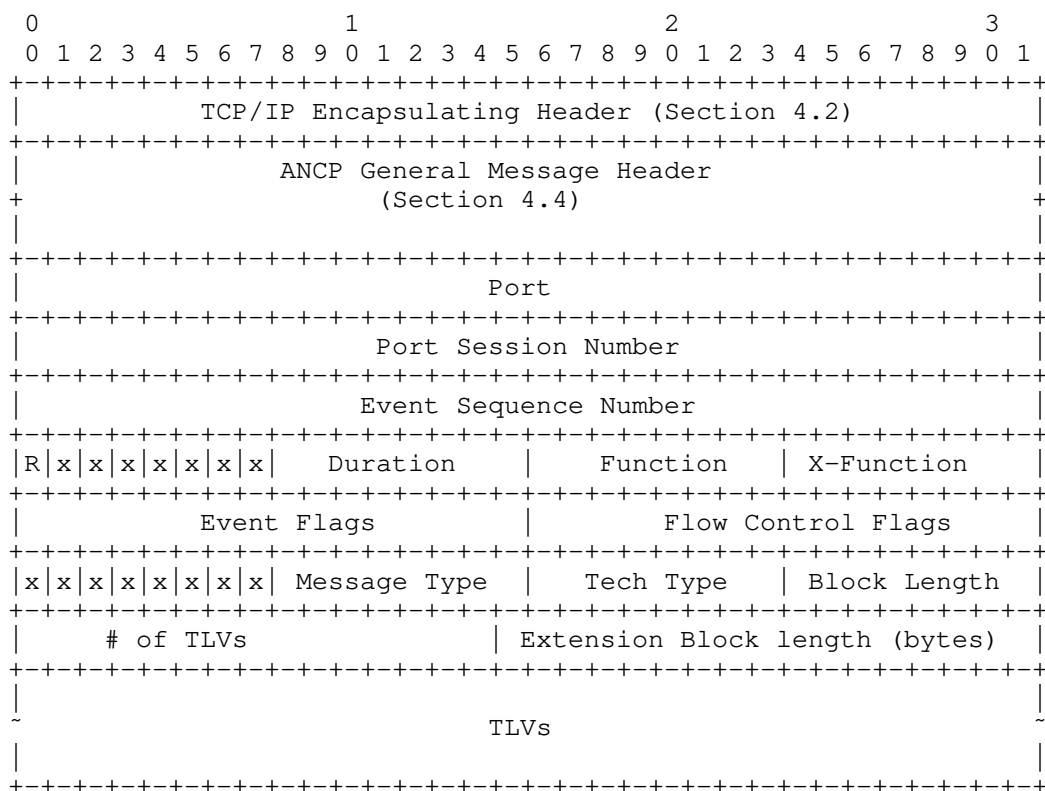


Figure 13

See Section 4.6 for a description of the ANCP general message header. The Message Type field **MUST** be set to 32. The 12 bit Code field **MUST** be set to 0. The 4 bit Result field **MUST** be set to either 1 (Nack) or 2 (AckAll), as determined by policy on the NAS. The 24-bit Transaction Identifier field **MUST** be set to a positive value. Other fields in the general header **MUST** be set as described in Section 4.6.

The Port Management message format defined in [RFC3292] has been

modified to contain additional data at the end of the message. Also, the original two byte Function field has been modified to contain one byte for the Function field indicating a specific action to be taken by the recipient of the message, and one byte for X-Function field, which further qualifies the action specified in the Function field. Any Function specific data MUST be carried in TLVs in the extension block.

The Port, Port Session Number, and Event Sequence Number fields are not used by the DSL Line Configuration capability and MUST be considered reserved. The handling of unused/reserved fields is described in Section 4.4.

The remaining message fields are described as follows:

R Flag: not used by ANCP.

Additional Port Management flags: the flag bits marked 'x' following the R flag are not used by ANCP.

Duration: not used for DSL line configuration.

Function: action to be performed. For DSL line configuration, Function MUST be set to 8 (Configure Connection Service Data). This action type requests the Access Node (i.e., DSLAM) to apply service configuration data contained in the extension value (TLVs) to the DSL line (identified by one of the TLVs in the extension value).

X-Function: qualifies the action set by Function. For DSL line configuration, this field MUST be set to 0.

Event Flags: not used by ANCP.

Flow Control Flags: not used by ANCP.

Extension Flags: the flag bits denoted by 'x' before the Message Type field are reserved for future use.

Message Type: Message Type has the same value as in the general header (i.e., 32).

Tech Type: MUST be set to 0x05 (DSL).

Block Length: unused.

# of TLVs: the number of TLVs that follow, not counting TLVs encapsulated within other TLVs.

Extension Block Length: the total length of the TLVs carried in the extension block in bytes, including any padding within individual TLVs.

TLVs: two or more TLVs to identify a DSL line and configure its service data.

#### 5.3.3.3. Procedures

Section 5.3.2 Describes the circumstances under which the NAS sends a Port Management message to the AN to configure DSL service parameters for a specific subscriber line. To identify the line, the NAS MUST include one of Access-Loop-Circuit-ID TLV, Access-Aggregation-Circuit-ID-Binary TLV, or Access-Aggregation-Circuit-ID-ASCII TLV in the Port Management message, depending upon the deployment scenario. The NAS MUST include one or more TLVs to configure line service parameters for that line. Section 5.3.3.4 currently identifies only one such TLV, Service-Profile-Name, but other TLVs may be added by extensions to ANCP.

If the NAS sets Result to AckAll (0x1) and the AN processes the Port Management message successfully, the AN MUST return a Port Management message in reply, containing a Result field set to Success (0x3). All other fields of the returned message MUST be identical to those received in the request.

If an error occurs during the processing of the Port Management message, then the AN MUST always return a Port Management message with the Result field set to Failure (0x4). The Code field MUST be set to indicate the reason for failure. The remainder of the message MUST be copied from the request. The AN MAY add a Status-Info TLV (Section 6.2.3) to provide further information on the error, in which case the various length fields and the # of TLVs field within the message MUST be adjusted accordingly.

#### 5.3.3.4. TLVs For DSL Line Configuration

Currently only the following TLV is specified for DSL line configuration. More TLVs may be defined in a future version of this specification or in ANCP extensions for individual service attributes of a DSL line (e.g. rates, interleaving delay, multicast channel entitlement access-list).

Name: Service-Profile-Name

Type: 0x0005

Description: Reference to a pre-configured profile on the DSLAM that contains service specific data for the subscriber.

Length: up to 64 bytes

Value: ASCII string containing the profile name (which the NAS learns from a policy server after a subscriber is authorized).

#### 5.4. ANCP Based DSL Line Testing Capability

In a mixed Ethernet and ATM access network (including the local loop), it is desirable to provide similar mechanisms for connectivity checks and fault isolation, as those used in an ATM based architecture. This can be achieved using an ANCP based mechanism until end-to-end Ethernet OAM mechanisms are more widely implemented in various network elements.

A simple solution based on ANCP can provide the NAS with an access line test capability and to some extent fault isolation. Controlled by a local management interface the NAS can use an ANCP operation to trigger the Access Node to perform a loopback test on the local loop (between the Access Node and the CPE). The Access Node can respond via another ANCP operation with the result of the triggered loopback test. In the case of ATM based local loop the ANCP operation can trigger the Access Node to generate ATM (F4/F5) loopback cells on the local loop. In the case of Ethernet, the Access Node can trigger an Ethernet loopback message(per EFM OAM) on the local loop.

##### 5.4.1. Message Flow

The Port Management message can be used by the NAS to request Access Node to trigger a remote loopback test on the local loop. The result of the loopback test can be asynchronously conveyed by the Access Node to the NAS in a Port Management response message. The formats of the relevant extensions to the Port Management message are defined in Section 5.4.2.2. Figure 14 summarizes the interaction.

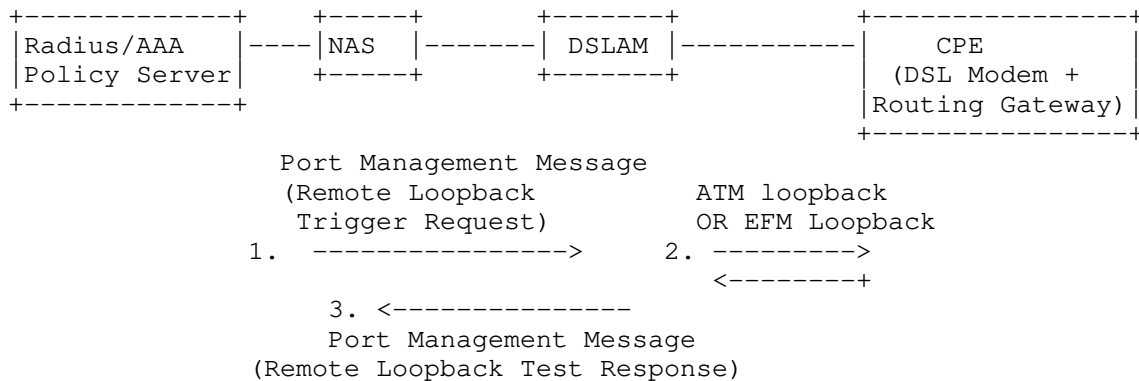


Figure 14: Message Flow For ANCP based OAM

#### 5.4.2. Specification of the ANCP DSL Line Testing Capability

##### 5.4.2.1. Protocol Requirements

The DSL line testing capability is assigned capability type 0x04. No capability data is associated with this capability. Implementations of the DSL line testing capability MUST support the following ANCP protocol elements:

- o ANCP Port Management message, which is based on the GSMPv3 [RFC3292] message of the same name but includes capability-specific modifications and extensions (Section 5.4.2.2).
- o The procedures associated with this message and its contents (Section 5.4.2.3).
- o Access-Loop-Circuit-ID TLV (as defined in Section 5.2.3.3);
- o Access-Aggregation-Circuit-ID-Binary TLV (as defined in Section 5.2.3.3);
- o Access-Aggregation-Circuit-ID-ASCII TLV (as defined in Section 5.2.3.3);
- o OAM-Loopback-Test-Parameters TLV;
- o Opaque-Data TLV;
- o OAM-Loopback-Test-Response-String TLV.

If not otherwise indicated, the TLVs listed above are defined in

## Section 5.4.2.4.

## 5.4.2.2. Message Format

The Port Management message for DSL line testing has the same format as for DSL line configuration (see Section 5.3.3.2), with the following differences:

- o The Result field in the request SHOULD be set to AckAll (0x1), to allow the NAS to receive the information contained in a successful test response.
- o The Function field MUST be set to 9 (Remote Loopback). (The X-Function field continues to be 0.)
- o The appended TLVs in the extension value field include testing-related TLVs rather than subscriber service information.

## 5.4.2.3. Procedures

The ANCP Port Management message as described in Section 5.4.2.2 MAY be used by the NAS to trigger the Access Node to run a loopback test on the local loop. To identify the line to be tested, the NAS MUST include one of Access-Loop-Circuit-ID TLV, Access-Aggregation-Circuit-ID-Binary TLV, or Access-Aggregation-Circuit-ID-ASCII TLV in the Port Management message, depending upon the deployment scenario. The NAS MAY include the OAM-Loopback-Test-Parameters and/or Opaque-Data TLVs (defined in Section 5.4.2.4) to configure the loopback test for that line.

The Access Node SHOULD generate a Port Management response when it deems the loopback test to be complete. (The exception is described with reference to the Timeout field in the OAM-Loopback-Test-Parameters TLV in Section 5.4.2.4.) The Result field MUST be set to Success (0x3) or Failure (0x4) as applicable. The Code field SHOULD be set to one of the following values if applicable.

1280 (0x500): Specified access line does not exist

1281 (0x501): Loopback test timed out

1282 (0x502): Reserved

1283 (0x503): DSL line status showtime



- 1284 (0x504): DSL line status idle
- 1285 (0x505): DSL line status silent
- 1286 (0x506): DSL line status training
- 1287 (0x507): DSL line integrity error
- 1288 (0x508): DSLAM resource not available
- 1289 (0x509): Invalid test parameter

All other fields including the appended TLVs MUST be copied from the request, except that the OAM-Loopback-Test-Parameters TLV MUST NOT appear in the response and the OAM-Loopback-Test-Response-String TLV SHOULD appear in the response.

Section 5.4.2.4 contains additional procedures relating to specific TLVs.

#### 5.4.2.4. TLVs For the DSL Line Test Capability

The following TLVs have been defined for use with the DSL line testing capability.

##### 5.4.2.4.1. OAM-Loopback-Test-Parameters TLV

Name: OAM-Loopback-Test-Parameters

Type: 0x0007

Description: Parameters related to a loopback test. This is an optional TLV. If this TLV is not present in the request message, the DSLAM SHOULD use locally determined default values for the test parameters.

Length: 2 bytes

Value: two 1 byte fields described below (listed in order of most to least significant).

Byte 1: Count. Number of loopback cells/messages that should be generated on the local loop as part of the loopback test. The NAS SHOULD restrict the "count" to be greater than 0 and less than or equal to 32. The DSLAM SHOULD discard a request for a loopback test, if the received test parameters contain an out of range value for the "count" field. The AN MAY include a Code value of 0x509 "Invalid test parameter" in the resulting

failure response to the NAS.

Byte 2: Timeout. Upper bound on the time in seconds that the NAS will wait for a response from the DSLAM. If the total time taken by the DSLAM to complete a test with requested parameters, exceeds the specified "timeout" value, it MAY choose to omit the generation of a response to the NAS. The DSLAM SHOULD use a locally determined value for Timeout, if the received value of the Timeout parameter is 0.

The OAM-Loopback-Test-Parameters TLV is illustrated in Figure 15

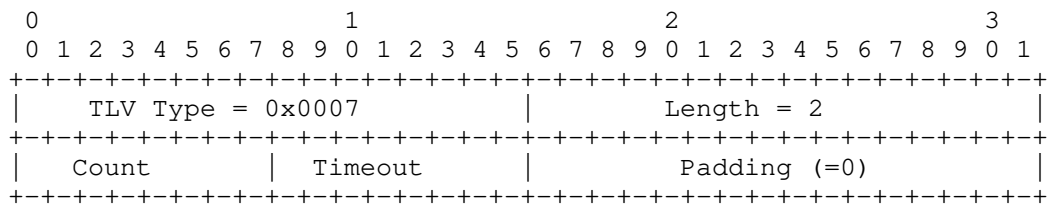


Figure 15: The OAM-Loopback-Test-Parameters TLV

#### 5.4.2.4.2. Opaque-Data TLV

Name: Opaque-Data

Type: 0x0008

Description: This is an optional TLV. If it is present in the request message, the DSLAM SHOULD reflect it back in the response unmodified.

Length: 8 bytes

Value: Two 32 bit unsigned integers inserted by the NAS (not to be interpreted by the DSLAM, but just reflected back in the response).

#### 5.4.2.4.3. OAM-Loopback-Test-Response-String TLV

Name: OAM-Loopback-Test-Response-String

Type: 0x0009

Description: Suitably formatted string containing useful details about the test that the NAS will display for the operator, exactly as received from the DSLAM (no manipulation/interpretation by the NAS). This is an optional TLV, but it is strongly RECOMMENDED

that in case of ATM based local loop, the DSLAM at the very least indicates, via this TLV, the total loopback cells generated and the total loopback cells successfully received as part of executing the requested loopback test.

Length: up to 128 bytes

Value: UTF-8 encoded string of text.

## 6. Additional ANCP Messages and TLVs

This section defines two messages and a number of TLVs that may be useful in multiple capabilities. Typically the content is unspecified, with the intention that particular capabilities spell out the remaining details.

### 6.1. Additional Messages and General Messaging Principles

#### 6.1.1. General Principles for the Design of ANCP Messages

The GSMPv3 protocol [RFC3292] allows for two messaging constructs to support request/response interaction:

- a. The same message type is used for both the request message and the response message. The Result and Code field settings are used to differentiate between request and response messages.
- b. The request and response messages use two different message types.

The first approach is illustrated by the protocol specifications in Section 5. The purpose of this section is to provide more details about the second approach in order to allow the use of this messaging construct for the development of additional ANCP extensions.

As Section 4.6 indicated, all ANCP messages other than adjacency messages share a common header format. When the response message type is different from that of the request, the specification of the request message will typically indicate that the Result field is set to Ignore (0x0) and provide procedures indicating explicitly when the receiver should generate a response and what message type it should use.

The Transaction ID field is used to distinguish between request messages and to associate a response message to a request. Specifications of ANCP messages for applications not requiring response correlation should indicate that the Transaction ID must be

set to zero in requests. Applications that require response correlation should refer to the Transaction ID behaviour described in Section 4.6.1.

The specification for a response message should indicate in all cases that value of the Transaction Identifier must be set to that of the corresponding request message. This allows the requester to establish whether or not correlation is needed (by setting a non-zero or zero value for the Transaction ID).

### 6.1.2. Provisioning Message

The Provisioning message is sent by the NAS to the AN to provision information of global scope on the AN. The Provisioning message has the format shown in Figure 16.

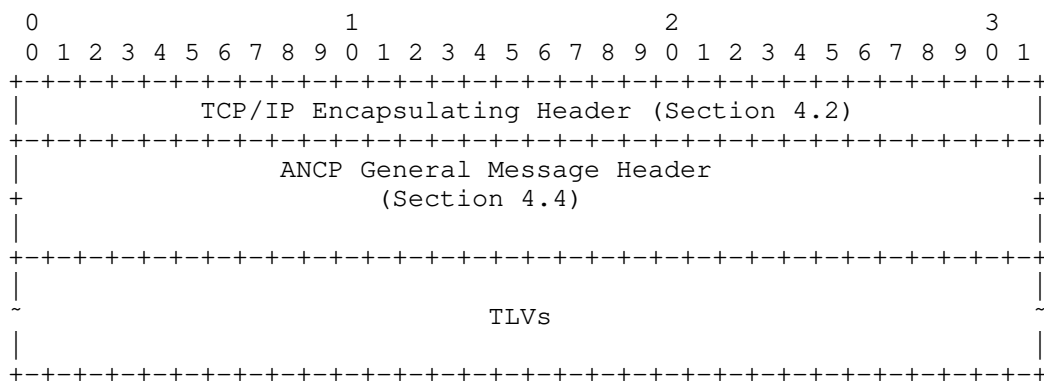


Figure 16: Format of the Provisioning Message

This document specifies the following fields. The remaining fields in the ANCP general message header **MUST** be set as specified in Section 4.6.1. The TLVs are specified elsewhere on a per-capability basis. The Provisioning message **MAY** be used to carry data relating to more than one capability at once, assuming that the capabilities concerned can co-exist and have all been negotiated during adjacency establishment.

Message Type: MUST be set to 93.

Result: MUST be set to 0x0 (Ignore).

Code: MUST be set to zero.

Transaction ID: MUST be populated with a non-zero value chosen in the manner described in Section 4.6.1.

If the AN can process the message successfully and accept all the provisioning directives contained in it, the AN MUST NOT send any response.

If not otherwise specified, if the AN fails to process the message successfully it MUST send a Generic Response message (Section 6.1.3) indicating failure and providing appropriate diagnostic information.

#### 6.1.3. Generic Response Message

This section defines the Generic Response message. The Generic Response message may be specified as the appropriate response to a message defined in an extension to ANCP, instead of a more specific response message. As a general guideline, specification of the Generic Response message as a response is appropriate where no data needs to be returned to the peer other than a result (success or failure), plus, in the case of a failure, a code indicating the reason for failure and a limited amount of diagnostic data. Depending on the particular use case, the Generic Response message MAY be sent by either the NAS or the AN.

The AN or NAS MAY send a Generic Response message indicating a failure condition independently of a specific request before closing the adjacency as a consequence of that failure condition. In this case, the sender MUST set the Transaction ID field in the header and the Message Type field within the Status-Info TLV to zeroes. The receiver MAY record the information contained in the Status-info TLV for management use.

The format of the Generic Response message is shown in Figure 17

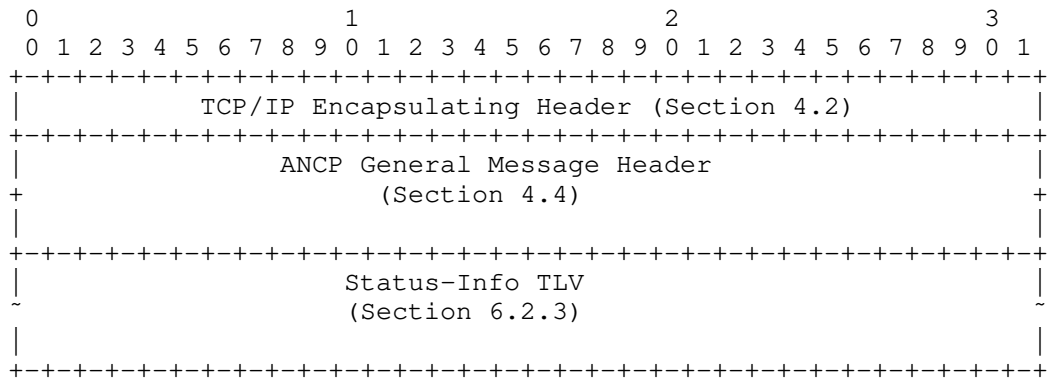


Figure 17: Structure of the Generic Response Message

This document specifies the following fields. The remaining fields in the ANCP general message header **MUST** be set as specified in Section 4.6.1.

Message Type: **MUST** be set to 91.

Result: **MUST** be set to 0x3 (Success) or 0x4 (Failure).

Code: **MUST** be set to zero for success or an appropriate non-zero value for failure.

Transaction ID: **MUST** be copied from the message to which this message is a response.

Status-Info TLV: **MAY** be present in a success response, to provide a warning as defined for a specific request message type. **MUST** be present in a failure response. See Section 6.2.3 for a detailed description of the Status- Info TLV. The actual contents will depend on the request message type this message is responding to.

## 6.2. TLVs For General Use

This section contains the definitions of some TLVs that are intended to be re-usable across different message types and capabilities.

### 6.2.1. Target TLV

Name: Target

Type: 0x1000 to 0x1020 depending on the specific content. Only 0x1000 has been assigned in this specification (see below).

Description: The Target TLV (0x1000 - 0x1020) is intended to be a general means to represent different types of objects.

Length: Variable, depending on the specific object type.

Value: Target information as defined for each object type. The field can consist of sub-TLVs.

TLV Type 0x1000 is assigned to a variant of the Target TLV representing a single access line and encapsulating one or more sub-TLVs identifying the target. Figure 18 illustrates the message format for a single port identified by an Access-Loop-Circuit-ID TLV (0x0001) that could be derived from a Port-UP message:

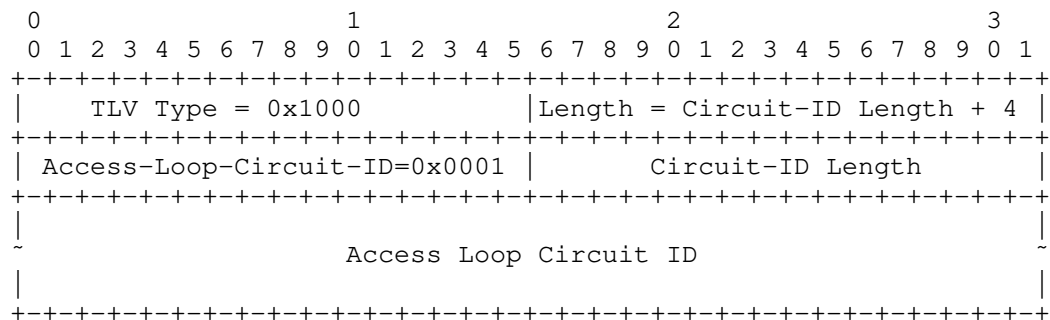


Figure 18: Example of Target TLV For Single Access Line

#### 6.2.2. Command TLV

Name: Command

Type: 0x0011

Description: The Command TLV (0x0011) is intended to be a general means of encapsulating one or more command directives in a TLV oriented message. The semantics of the command can be specified for each message type using it. I.e., the specification of each message type that can carry the Command TLV is expected to define the meaning of the content of the payload, although re-use of specifications is, of course, permissible when appropriate.

Length: Variable, depending on the specific contents.

Value: Command information as defined for each message type. The field can include sub-TLVs. The contents of this TLV MUST be specified as one "command" or alternatively a sequence of one or more "commands", each beginning with a one-byte Command Code and possibly including other data following the Command Code. An IANA registry has been established for Command Code values. This document reserves the Command Code value 0 as an initial entry in the registry.

### 6.2.3. Status-Info TLV

Name: Status-Info

Type: 0x0106

Description: The Status-Info-TLV is intended to be a general container for warning or error diagnostics relating to commands and/or requests. It is a supplement to the Code field in the ANCP general header. The specifications for individual message types may indicate the use of this TLV as part of responses, particularly for failures. As mentioned above, the Generic Response message will usually include an instance of the Status-Info TLV.

Length: Variable, depending on the specific contents.

Value: The following fixed fields. In addition, sub-TLVs may be appended to provide further diagnostic information.

Reserved: see Section 4.4 for handling of reserved fields.

Msg Type: Message Type of the request for which this TLV is providing diagnostics.

Error Message Length: Number of bytes in the error message, excluding padding. This MAY be zero if no error message is provided.

Error Message: Human-readable string providing information about the warning or error condition. Padded with zeroes as necessary to extend to a four-byte word boundary.

The following TLVs are RECOMMENDED to be appended if the indicated Code values are given in the header of the message containing the Status-info TLV:



- \* Code value 4 or 5: the Target or other TLV identifying the unknown or unavailable port.
- \* Code value 84: the TLV that is unsupported or contains the unsupported value.

Figure 19 illustrates the Status-Info TLV.

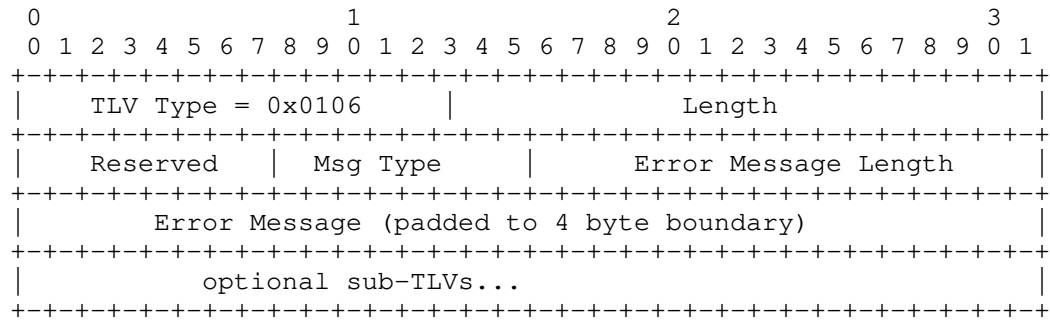


Figure 19: The Status-Info TLV

## 7. IANA Considerations

RFC EDITOR'S NOTE: please replace "RFCXXXX" with the number of this specification.

### 7.1. Summary

This section requests the following IANA actions:

- o addition of message types to the GSMPv3 Message Type Name Space registry;
- o addition of a result type to the GSMPv3 Result Type Name Space registry; [Editor's Note: may need an ANCP registry instead. Coordination between the two protocols is unnecessary because of ANCP's reorganization of the Result field.]
- o extension of limits [Editor's Note: assuming we are allowed to do this!] and addition of failure codes to the GSMPv3 Failure Response Message Name Space registry;
- o establishment of the following new ANCP registries:

ANCP Function Codes;

ANCP Technology Types;

ANCP Command Codes;

ANCP TLV Types;

ANCP Capabilities.

## 7.2. IANA Actions

IANA is requested to add a new message category to the GSMPv3 Message Type Name Space registry: "Access Network Control Protocol (ANCP) Messages". IANA is requested to add the following entries under that category:

Message Name	Message Number	Status	Reference
Generic Response	91		RFCXXXX
Provisioning	93		RFCXXXX

IANA is requested to implement the following modification to the General Switch Management Protocol version 3 (GSMPv3) Result Type Name Space registry:

Result Value	Result Type Name	Reference
0	Ignore (was Reserved)	RFCXXXX

IANA is requested to implement the following modifications to the GSMPv3 Failure Response Message Name Space:

- o Add the following note to the registry:

This registry is shared with the Access Node Control Protocol (ANCP) [RFCXXXX]. GSMPv3 [RFC3292] allows values up to a maximum of 255. ANCP extends this maximum to 4095. Hence values above 255 are applicable to ANCP only.

- o Extend the table of registration procedures as indicated.
- o Add entries to the failure response message name table as indicated.

- o Replace the ranges of unassigned codes at the end of the failure response message name table as indicated.

Range	Registration Procedure	Notes
256-4095	IETF Consensus	ANCP use only

Value	Failure Response Message Name	Reference
81	Request message type not implemented (0x51)	RFCXXXX
82	Transaction identifier out of sequence (0x52)	RFCXXXX
83	Malformed message (0x53)	RFCXXXX
84	TLV or value not supported by negotiated capability set (0x54)	RFCXXXX
85	Invalid value in TLV (0x55)	RFCXXXX
1280	Specified access line does not exist (0x500)	RFCXXXX
1281	Loopback test timed out (0x501)	RFCXXXX
1282	Reserved (0x502)	RFCXXXX
1283	DSL line status showtime (0x503)	RFCXXXX
1284	DSL line status idle (0x504)	RFCXXXX
1285	DSL line status silent (0x505)	RFCXXXX
1286	DSL line status training (0x506)	RFCXXXX
1287	DSL line integrity error (0x507)	RFCXXXX
1288	DSLAM resource not available (0x508)	RFCXXXX
1289	Invalid test parameter (0x509)	RFCXXXX

Value	Failure Response Message Name	Reference
8-9	Unassigned	
47-59	Unassigned	
86-127	Unassigned	
160-255	Unassigned	
256-1279	Unassigned (ANCP use only)	
1290-4095	Unassigned (ANCP use only)	

IANA is requested to create a new ANCP Port Management Function Name registry, with the following initial entries. Additions to this registry will be by IETF Consensus. Values may range from 0 to 255.

NOTE: future extensions of ANCP may need to establish sub-registries of permitted X-Function values for specific values of Function.

Function Value	Function Name	Reference
0	Reserved	RFCXXXX
1-7	Unassigned	
8	Configure Connection Service Data	RFCXXXX
9	Remote Loopback	RFCXXXX
10-255	Unassigned	

IANA is requested to create a new ANCP Version registry, with additions by IETF consensus. The initial entries are as follows:

Version	Sub-Version	Name	Reference
3	1	Pre-standard	
3	2	ANCPv1	RFCXXXX

IANA is requested to create a new ANCP Technology Type registry, with additions by IETF Consensus. Values may range from 0 to 255. The initial entries are as follows:

Tech Type Value	Tech Type Name	Reference
0	Any technology	RFCXXXX
1	PON	RFCXXXX
2-4	Unassigned	
5	DSL	RFCXXXX
6-254	Unassigned	
255	Reserved	RFCXXXX

IANA is requested to create a new ANCP Command Code registry, with additions by IETF Consensus. The initial entry is as follows:

Command Code Value	Command Code Directive Name	Reference
0	Reserved	RFCXXXX

IANA is requested to create a new ANCP TLV Type registry, with additions by IETF Consensus. Values may range from 0x0000 to 0xFFFF. New assignments should be in the range of values from 0x0100 upwards. The initial entries are as follows:

Type Code	TLV Name	Reference
0x0000	Reserved	RFCXXXX
0x0001	Access-Loop-Circuit-ID	RFCXXXX
0x0002	Access-Loop-Remote-Id	RFCXXXX
0x0003	Access-Aggregation-Circuit-ID-ASCII	RFCXXXX
0x0004	DSL Line Attributes	RFCXXXX
0x0005	Service-Profile-Name	RFCXXXX
0x0006	Access-Aggregation-Circuit-ID-Binary	RFCXXXX
0x0007	OAM-Loopback-Test-Parameters	RFCXXXX
0x0008	Opaque-Data	RFCXXXX
0x0009	OAM-Loopback-Test-Response-String	RFCXXXX
0x000a-0x0010	Unassigned	
0x0011	Command	RFCXXXX
0x0012-0x0080	Unassigned	
0x0081	Actual-Net-Data-Upstream	RFCXXXX
0x0082	Actual-Net-Data-Rate-Downstream	RFCXXXX
0x0083	Minimum-Net-Data-Rate-Upstream	RFCXXXX
0x0084	Minimum-Net-Data-Rate-Downstream	RFCXXXX
0x0085	Attainable-Net-Data-Rate-Upstream	RFCXXXX
0x0086	Attainable-Net-Data-Rate-Downstream	RFCXXXX
0x0087	Maximum-Net-Data-Rate-Upstream	RFCXXXX
0x0088	Maximum-Net-Data-Rate-Downstream	RFCXXXX
0x0089	Minimum-Net-Low-Power-Data-Rate-Upstream	RFCXXXX
0x008A	Minimum-Net-Low-Power-Data-Rate-Downstream	RFCXXXX
0x008B	Maximum-Interleaving-Delay-Upstream	RFCXXXX
0x008C	Actual-Interleaving-Delay-Upstream	RFCXXXX
0x008D	Maximum-Interleaving-Delay-Downstream	RFCXXXX
0x008E	Actual-Interleaving-Delay-Downstream	RFCXXXX
0x008F	DSL line state	RFCXXXX
0x0090	Access Loop Encapsulation	RFCXXXX
0x0091	DSL-Type	RFCXXXX
0x0092-0x0105	Unassigned	
0x0106	Status-info	RFCXXXX
0x0107-0x0FF	Unassigned	
0x1000	Target (single access line variant)	RFCXXXX
0x1001 - 0x1020	Reserved for Target variants	RFCXXXX
0x1021-0xFFF	Unassigned	

IANA is requested to create a new ANCP Capability registry, with additions by IETF Consensus. Values may range from 0 to 255. The specification for a given capability MUST indicate whether it applies to a specific access technology or applies to all access technologies. The specification MUST further indicate whether the capability is associated with any capability data. The initial entries in the ANCP capability registry are as follows:

Value	Capability Type Name	Technology	Capability Data	Reference
0	Reserved			RFCXXXX
1	DSL Topology Discovery	DSL	None	RFCXXXX
2	DSL Line Configuration	DSL	None	RFCXXXX
3	Reserved			RFCXXXX
4	DSL Line Testing	DSL	None	RFCXXXX
5-255	Unassigned			

## 8. Security Considerations

Security of the ANCP protocol is discussed in [RFC5713]

## 9. Acknowledgements

The authors would like to thank everyone who provided comments or inputs to this document. Swami Subramanian was an early member of the authors' team. The ANCP Working Group is grateful to Roberta Maglione, who served as design team member and primary editor of this document for two years before stepping down. The authors acknowledge the inputs provided by Wojciech Dec, Peter Arberg, Josef Froehler, Derek Harkness, Kim Hyldgaard, Sandy Ng, Robert Peschi, and Michel Platnic.

## 10. References

### 10.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
- [RFC3046] Patrick, M., "DHCP Relay Agent Information Option",

RFC 3046, January 2001.

- [RFC3292] Doria, A., Hellstrand, F., Sundell, K., and T. Worster, "General Switch Management Protocol (GSMP) V3", RFC 3292, June 2002.
- [RFC3293] Worster, T., Doria, A., and J. Buerkle, "General Switch Management Protocol (GSMP) Packet Encapsulations for Asynchronous Transfer Mode (ATM), Ethernet and Transmission Control Protocol (TCP)", RFC 3293, June 2002.
- [RFC3629] Yergeau, F., "UTF-8, a transformation format of ISO 10646", STD 63, RFC 3629, November 2003.
- [RFC5234] Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, January 2008.

#### 10.2. Informative References

- [G.988.1] "ITU-T recommendation G.998.1, ATM-based multi-pair bonding", 2005.
- [G.988.2] "ITU-T recommendation G.998.2, Ethernet-based multi-pair bonding", 2005.
- [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.
- [TR\_058] Elias, M. and S. Ooghe, "DSL Forum TR-058, Multi-Service Architecture & Framework Requirements", September 2003.
- [TR\_059] Anschutz, T., "DSL Forum TR-059, DSL Evolution - Architecture Requirements for the Support of QoS-Enabled IP Services", September 2003.
- [TR\_092] "DSL Forum TR-092, Broadband Remote access server requirements document", 2005.
- [TR\_101] Cohen et al, "Architecture & Transport: "Migration to Ethernet Based DSL Aggregation", DSL Forum TR-101", 2005.
- [US\_ASCII]

American National Standards Institute, "Coded Character Set - 7-bit American Standard Code for Information Interchange", ANSI X.34, 1986.

#### Authors' Addresses

Sanjay Wadhwa  
Juniper Networks  
10 Technology Park Drive  
Westford, MA 01886  
USA

Phone:  
Fax:  
Email: [swadhwa@juniper.net](mailto:swadhwa@juniper.net)

Jerome Moisand  
Juniper Networks  
10 Technology Park Drive  
Westford, MA 01886  
USA

Phone:  
Fax:  
Email: [jmoisand@juniper.net](mailto:jmoisand@juniper.net)

Thomas Haag  
Deutsche Telekom  
Heinrich-Hertz-Strasse 3-7  
Darmstadt, 64295  
Germany

Phone: +49 6151 628 2088  
Fax:  
Email: [haagt@telekom.de](mailto:haagt@telekom.de)

Norbert Voigt  
Nokia Siemens Networks  
Siemensallee 1  
Greifswald 17489  
Germany

Email: [norbert.voigt@nsn.com](mailto:norbert.voigt@nsn.com)



Tom Taylor (editor)  
Huawei Technologies  
Ottawa  
Canada

Email: tom111.taylor@bell.net

