Network Working Group	S. Wadhwa
Internet-Draft	J. Moisand
Intended status: Standards Track	S. Subramanian
Expires: August 30, 2010	Juniper Networks
	T. Haag
	Deutsche Telekom
	N. Voigt
	Siemens
	R. Maglione
	Telecom Italia
	February 26, 2010

TOC

Protocol for Access Node Control Mechanism in Broadband Networks
draft-ietf-ancp-protocol-09

Abstract

This document describes proposed extensions to the GSMPv3 protocol to allow its use in a broadband environment, as a control plane between Access Nodes (e.g. DSLAM) and Broadband Network Gateways (e.g. NAS). These proposed extensions are required to realize a protocol for "Access Node Control" mechanism as described in [ANCP-FRAMEWORK] (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,” February 2010.). The resulting protocol with the proposed extensions to GSMPv3 [RFC3292] (Doria, A., Hellstrand, F., Sundell, K., and T. Worster, “General Switch Management Protocol (GSMP) V3,” June 2002.) is referred to as "Access Node Control Protocol" (ANCP). This document currently focuses on specific use cases of access node control mechanism for topology discovery, line configuration, and OAM as described in ANCP framework document [ANCP-FRAMEWORK] (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,” February 2010.). It is intended to be augmented by additional protocol specification for future use cases considered in scope by the ANCP charter.
ANCP framework document [ANCP-FRAMEWORK] (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,” February 2010.) describes the ANCP use-cases in detail. Illustrative text for the use-cases is included here to help the protocol

implementer understand the greater context of ANCP protocol interactions.

Status of this Memo

Copyright Notice

Table of Contents

---

1. Specification Requirements

TOC

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] (Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” March 1997.).

2. Introduction

TOC

DSL is a widely deployed access technology for Broadband Access for Next Generation Networks. Several specifications like [TR-059] (Anschutz, T., “DSL Forum TR-059, DSL Evolution - Architecture Requirements for the Support of QoS-Enabled IP Services,” September 2003.), [TR-058] (Elias, M. and S. Ooghe, “DSL Forum TR-058, Multi-Service Architecture & Framework Requirements,” September 2003.), [TR-092] (, “DSL Forum TR-092, Broadband Remote access server requirements document,” 2005.) describe possible architectures for these access networks. In the scope of these specifications are the delivery of voice, video and data services.

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

This draft defines extensions and modifications to GSMPv3 (specified in [RFC3292] (Doria, A., Hellstrand, F., Sundell, K., and T. Worster, “General Switch Management Protocol (GSMP) V3,” June 2002.)) and certain new mechanisms to realize a control plane between a service-oriented layer 3 edge device (the NAS) and a layer2 Access Node (e.g. DSLAM) in order to perform QoS-related, service- related and subscriber-related operations. The control protocol as a result of these extensions and mechanisms is referred to as "Access Node Control Protocol" (ANCP). Although ANCP is based on GSMPv3, it is not interoperable with GSMPv3 defined in [RFC3292] (Doria, A., Hellstrand, F., Sundell, K., and T. Worster, “General Switch Management Protocol (GSMP) V3,” June 2002.).

ANCP uses the option of transporting GSMPv3 over TCP/IP. TCP encapsulation for GSMPv3 is defined in [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),” June 2002.). GSMPv3 encapsulation directly over Ethernet and ATM as defined in [RFC3293] is not considered for ANCP.

ANCP uses a subset of GSMPv3 messages to implement currently defined use-cases. These relevant GSMPv3 messages are identified in section Section 5 (Access Node Control Protocol (ANCP)). GSMPv3 procedures with suitable extensions, as used by ANCP, are described in sections Section 5.1 (ANCP/TCP connection establishment), Section 5.2 (ANCP Connection keepalive) and Section 5.3 (Capability negotiation). GSMPv3 general extensions and GSMPv3 message specific extensions required by ANCP are described in sub-sections of Section 5.4 (GSMP Message Extensions for Access Node Control). In addition to specifying extensions and modifications to relevant GSMP messages applicable to

ANCP, this draft also defines the usage of these messages by ANCP. Not all the fields in relevant GSMP messages are used by ANCP. This draft indicates the value that ANCP should set for the fields in these GSMP messages.
At the time of writing of this specification some implementations of the ANCP protocol, based on pre-standards drafts are already available. All these early-draft implementations use protocol version/sub-version 3.1; standard ANCP protocol will use version/sub-version 3.2 [Editor's note: sub-version needs to be changed from 1 to 2 upon publication.] Adopting a new sub-version value provides a way to disambiguate the two protocols and allows for supporting 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 details in Section 5.2 (ANCP Connection keepalive). It is important to note that this mechanism does not guarantee backwards compatibility of the ANCP RFC specification to those early-draft implementations.

2.1. Terminology

TOC

*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 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 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 case of DSL, the Home Gateway is a DSL network termination that could either operate 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.

---

3. Broadband Access Aggregation

TOC

3.1. ATM-based broadband aggregation

TOC

End to end DSL network consists of network and application service provider networks (NSP and ASP networks), regional/access network, and customer premises network. Figure 1 (ATM Broadband Aggregation Topology) shows ATM broadband access network components.
The Regional/Access Network consists of the Regional Network, Network Access Server, and the Access Network as show in Figure 1 (ATM Broadband Aggregation Topology). 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 could consist of DSLAM in the central office, or remote DSLAM, or a Remote Access Multiplexer (RAM). 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 the 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, NAS is also the injection point for policy management and IP QoS in the Regional/Access Networks. In order 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] (Anschutz, T., “DSL Forum TR-059, DSL Evolution - Architecture

Requirements for the Support of QoS-Enabled IP Services," September 2003.), preserves IP QoS over the ATM network between the NAS and the RGs 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.
[ANCP-FRAMEWORK] (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," February 2010.) provides detailed definition and functions of each network element in the broadband reference architecture.

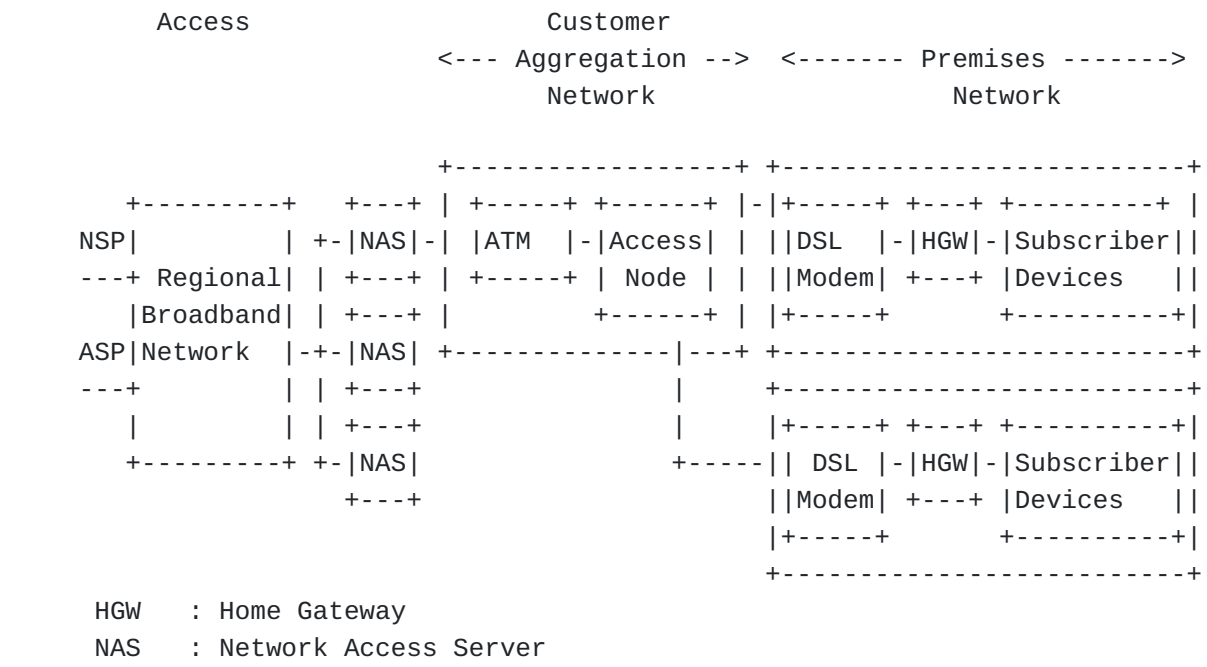


Figure 1: ATM Broadband Aggregation Topology

3.2. Ethernet-based broadband aggregation

TOC

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 could be used to create a form of "virtual path" between a given DSLAM and a given NAS. And "inner" VLAN tags to create a form of "virtual circuit" on a per DSL line basis. This is 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 N:1 VLAN allocation model. Architectural and topological models of an Ethernet aggregation network in context of DSL aggregation are defined in [TR-101] (Cohen et al, “Architecture & Transport: "Migration to Ethernet Based DSL Aggregation", DSL Forum TR-101,” 2005.)

---

4. Access Node Control Protocol

TOC

4.1. Overview

TOC

A dedicated control protocol between NAS and access nodes can facilitate "NAS managed" tight QOS control in the access network, simplified OSS infrastructure for service management, optimized multicast replication to enable video services over DSL, subscriber statistics retrieval on the NAS for accounting purposes, and fault isolation capability on the NAS for the underlying access technology. This dedicated control plane is referred to as "Access Node Control Protocol" (ANCP). This document specifies relevant extensions to GSMPv3 as defined [RFC3292] (Doria, A., Hellstrand, F., Sundell, K., and T. Worster, “General Switch Management Protocol (GSMP) V3,” June 2002.) to realize ANCP.
Following sections discuss the use of ANCP for implementing:

*Dynamic discovery of access topology by the NAS to provide tight QOS control in the access network.

*Pushing to the access-nodes, subscriber and service data retrieved by the NAS from an OSS system (e.g. radius server), to simplify OSS infrastructure for service management.

*Optimized, "NAS controlled and managed" multicast replication by access-nodes at L2 layer.

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

In addition to DSL, alternate broadband access technologies (e.g. Metro-Ethernet, Passive Optical Networking, WiMax) will have similar challenges to address, and could benefit from the same approach of a control plane between a NAS and an Access Node (e.g. OLT), providing a unified control and management architecture for multiple access technologies, hence facilitating migration from one to the other and/or parallel deployments.
GSMPv3 is an ideal fit for implementing ANCP. It is extensible and can be run over TCP/IP, which makes it possible to run over different access technologies.

4.2. ANCP based Access Topology Discovery

TOC

4.2.1. Goals

TOC

[TR-059] (Anschutz, T., “DSL Forum TR-059, DSL Evolution - Architecture Requirements for the Support of QoS-Enabled IP Services,” September 2003.) 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.
Following section describes ANCP messages that allow the Access Node (e.g. DSLAM) to communicate to the NAS, access network topology information and any corresponding updates.
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 in case 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).

4.2.2. Message Flow

TOC

When a DSL line initially comes up or resynchronizes to a different rate, the DSLAM generates and transmits a GSMP PORT UP EVENT message to the NAS. The extension field in the message carries the TLVs containing DSL line specific parameters. On a loss of signal on the DSL line, a GSMP PORT DOWN message is generated by the DSLAM to the NAS. In order to provide expected service level, NAS needs to learn the initial attributes of the DSL line before the subscriber can log in and access the provisioned services for the subscriber. Figure 2 (Message flow (ANCP mapping) for topology discovery) summarizes the interaction.

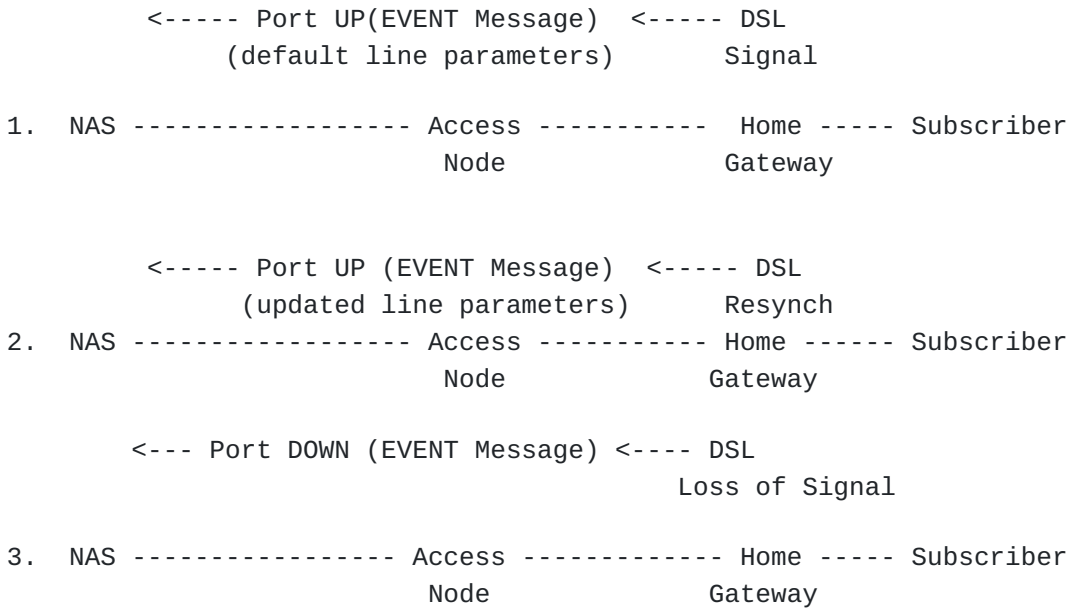


Figure 2: Message flow (ANCP mapping) for topology discovery

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 section Section 5.4.2 (Topology Discovery Extensions).

4.3. ANCP based Line Configuration

TOC

4.3.1. Goals

TOC

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 could then query a subscriber management OSS system (e.g. RADIUS server) to retrieve subscriber authorization data (service profiles, aka user entitlement). Most of such service mechanisms are typically enforced by the NAS itself, but there are a few cases where it might be useful to push such service parameter 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 could 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 OPEX 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 B2B interactions.
The best way to change line parameters would be by using profiles. These profiles (DSL profiles for different services) are pre-configured on the DSLAMs. The NAS can then indicate a reference to the right DSL profile via ANCP. Alternatively, discrete DSL parameters can also be conveyed by the NAS in ANCP.

4.3.2. Message Flow

TOC

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 GSMP Port Management messages. The NAS may get such line configuration data from a policy server (e.g. RADIUS). Figure 3 (Message flow - ANCP mapping for Initial Line Configuration) summarizes the interaction.

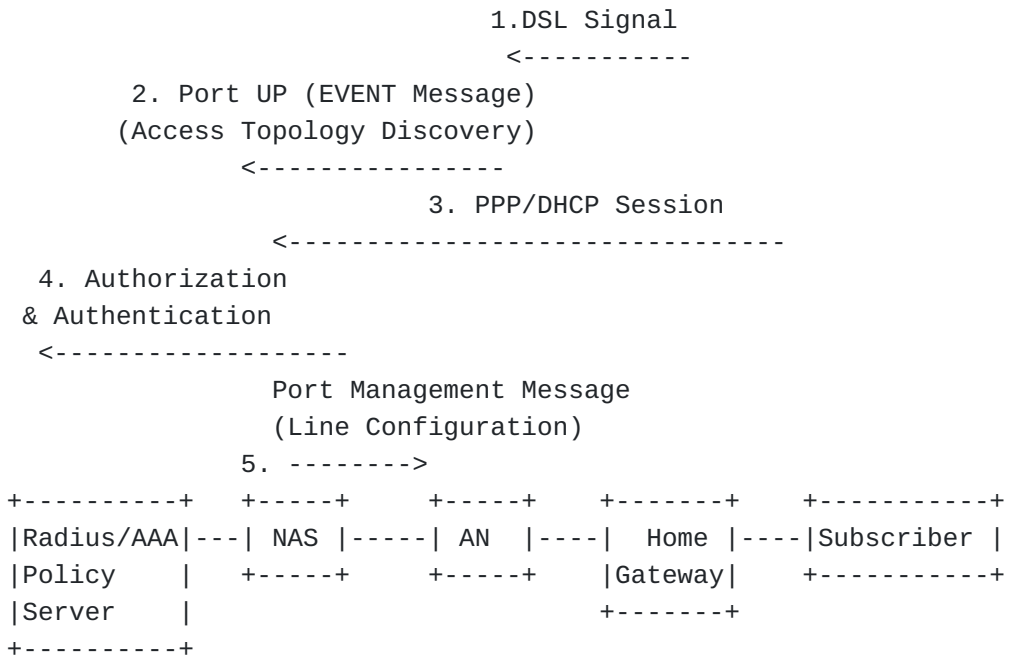


Figure 3: Message flow - ANCP mapping for Initial Line Configuration

The NAS may update the line configuration due to a subscriber service change (e.g. triggered by the policy server). Figure 4 (Message flow - ANCP mapping for Updated Line Configuration) summarizes the interaction.

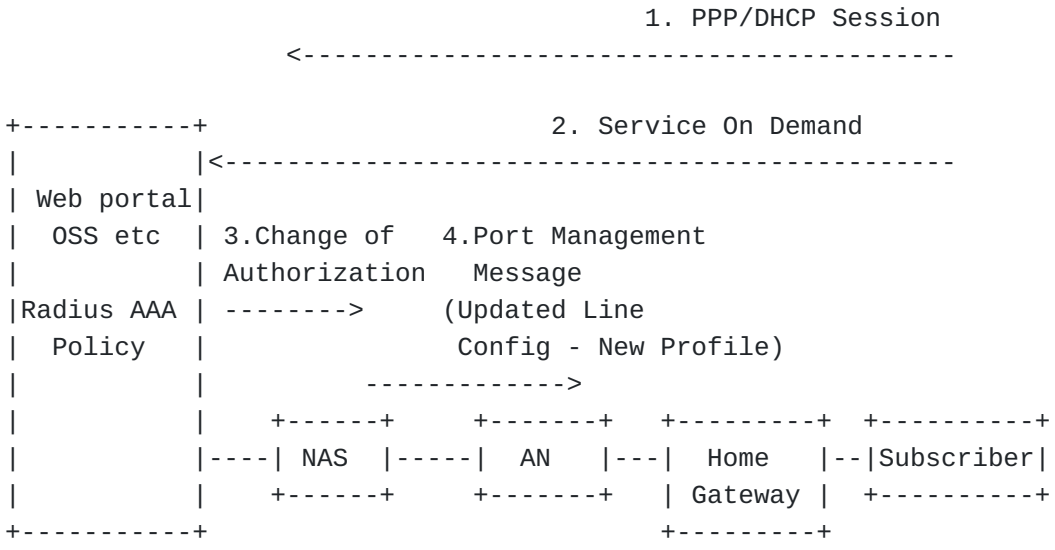


Figure 4: Message flow - ANCP mapping for Updated Line Configuration

---

The format of relevant extensions to port management message is defined in section Section 5.4.3 (Line Configuration Extensions). The line configuration models could be viewed as a form of delegation of authorization from the NAS to the DSLAM.

4.4. ANCP based OAM

TOC

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 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 the result of the triggered loopback test. In 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 case of Ethernet, the access-node can trigger an Ethernet loopback message(per EFM OAM) on the local-loop.

TOC

4.4.1. Message Flow

"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 format of relevant extensions to port management message is defined in section The format of relevant extensions to port management message is defined in section Section 5.4.4 (OAM Extensions). Figure 5 (Message Flow: ANCP based OAM) summarizes the interaction.

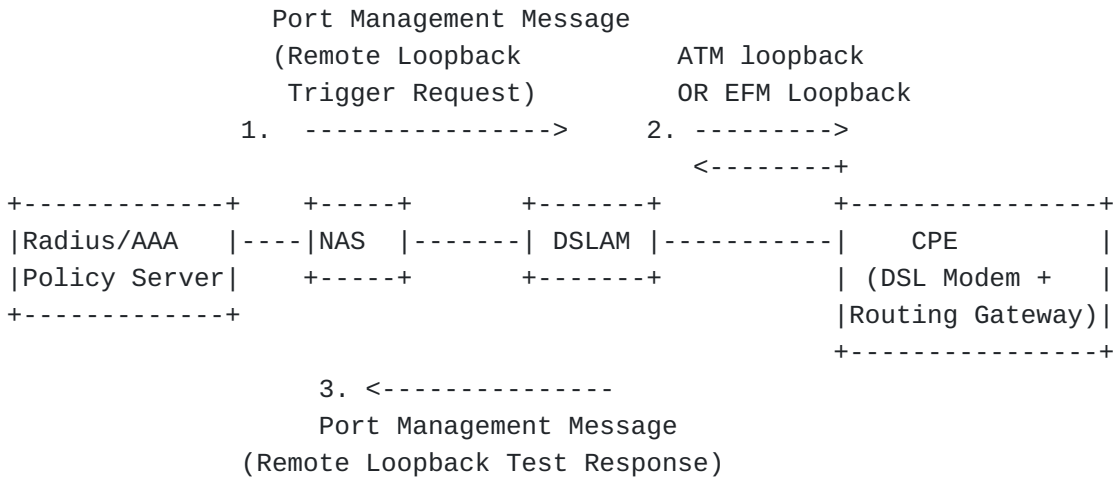


Figure 5: Message Flow: ANCP based OAM

5. Access Node Control Protocol (ANCP)

TOC

ANCP uses a subset of GSMPv3 messages described in [RFC3292] to implement currently defined use-cases. GSMPv3 general message format, used by all GSMP messages other than adjacency protocol messages, is defined in section 3.1.1 of GSMPv3 [RFC3292] (Doria, A., Hellstrand, F., Sundell, K., and T. Worster, “General Switch Management Protocol (GSMP) V3,” June 2002.). ANCP modifies this base GSMPv3 message format. The modified GSMPv3 message format is defined as follows:

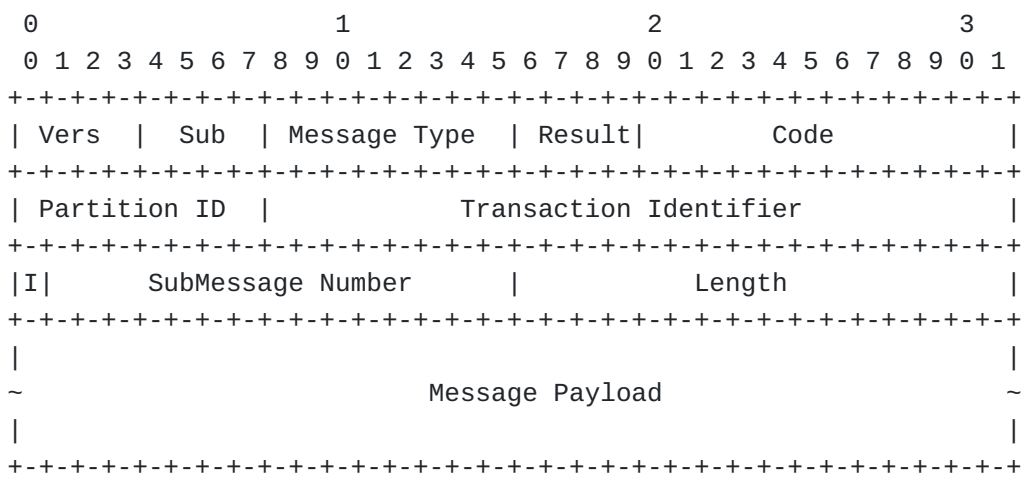


Figure 6: Modified GSMPv3 message format

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 GSMP protocol. ANCP uses version 3 and sub-version 1 of the GSMP protocol. An ANCP implementation SHOULD always set the version field to 3, and the sub-version field to 1. The Result field in the message header has been modified to be 4 bits long, and the Code field to be 12 bits long. Version:

> The version number of the GSMP protocol being used in this session. ANCP uses version 3.

Sub-Version:

> The sub-version number of the GSMP protocol being used in this session. ANCP uses sub-version 1 of the GSMP protocol. [RFC Editor's note: sub-version needs to be changed from 1 to 2 upon publication]

Result:

> The Result field derived from GSMP [RFC3292] (Doria, A., Hellstrand, F., Sundell, K., and T. Worster, “General Switch Management Protocol (GSMP) V3,” June 2002.) has the following codes:
>
> > Ignore:
> >
> > > Res = 0x00 – Ignore this field on receipt and follow the procedures specified for the received message type.

Nack:

> Res = 0x01 – 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 that of the contained directive(s).

AckAll:

> Res = 0x02 – Result code indicating that a response to the message is requested in all cases. It is specifically intended to be used in some cases for Request messages only, and is not to be used in Event messages.

Success:

> Res = 0x03 – Set by receiver to indicate successful execution of all directives in the corresponding Request message.

Failure:

> Res = 0x4 – Set by receiver in the Response message if one or more directives in the corresponding Request message fails.

Message-Type:

> The GSMP and ANCP message type.

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 is set to zero. In an adjacency protocol message, the Code field is used to determine the function of the message.
>
> 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, including the case where "Port" is interpreted to mean Target as defined in section Section 5.4.5.1.1 (Target TLV)
Instead of the value:

3 The specified request is not implemented on this switch

specified by [RFC3292] (Doria, A., Hellstrand, F., Sundell, K., and T. Worster, "General Switch Management Protocol (GSMP) V3," June 2002.), 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 0x0100 through 0x01ff 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.
>
> AN and NAS MAY agree on the partition ID using one of the following possible options:
>
> 1 - The partition ID could be configured on the AN and learnt by NAS in the adjacency message;
>
> 2 - The partition ID could 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. The receiver of a Request message reflects the transaction ID from the Request message in the corresponding Response message. For event messages, the transaction identifier SHOULD be set to zero. The Transaction Identifier is not used, and the field is not present, in the adjacency protocol.

I flag:

> An ANCP implementation SHOULD set "I" and subMessage fields to 1 to signify no fragmentation.

Length:

> Length of the GSMP message including its header fields and defined GSMP message body.

Additional General Message Information:

- *Any field in a GSMP message that is unused or defined as "reserved" MUST be set to zero by the sender and ignored by the receiver;

- *Flags that are undefined will be designated as: x: reserved.

Following are the relevant GSMPv3 messages defined in [RFC3292], that are currently used by ANCP. Other than the message types explicitly listed below, no other GSMPv3 messages are used by ANCP currently.

- *Event Messages

  - -Port UP Message

-Port DOWN Message

These messages are used by ANCP topology discovery use-case.

*Port Management Messages

-These messages are used by ANCP "line configuration" use-case and ANCP OAM use-case.

*Adjacency Protocol Messages

-These messages are used to bring up a protocol adjacency between a NAS and an AN.

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

*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 5.3 (Capability negotiation)

*TCP connection establishment procedure in ANCP deviates slightly from the connection establishment in GSMPv3 as specified in [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)," June 2002.). This is described in section Section 5.1 (ANCP/TCP connection establishment)

*ANCP makes GSMPv3 messages extensible and flexible by adding a general "extension block" to the end of the relevant GSMPv3 messages. The "extension block" contains a TLV structure to carry information relevant to each ANCP use-case. The format of the "extension block" is defined in section Section 5.4.1.1 (Extension TLV).

*

5.1. ANCP/TCP connection establishment

TOC

ANCP will use TCP for exchanging protocol messages [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)," June 2002.). defines the GSMP message encapsulation for TCP. The TCP session is initiated from the DSLAM (access node) to the NAS (controller). This is necessary

to avoid static provisioning on the NAS for all the DSLAMs that are being served by the NAS. It is easier to configure a given DSLAM with the single IP address of the NAS that serves the DSLAM. This is a deviation from [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)," June 2002.) which indicates that the controller initiates the TCP connection to the switch.
When GSMP messages are sent over a TCP connection a four-byte TLV header field is prepended to the GSMP message to provide delineation of GSMP messages within the TCP stream.

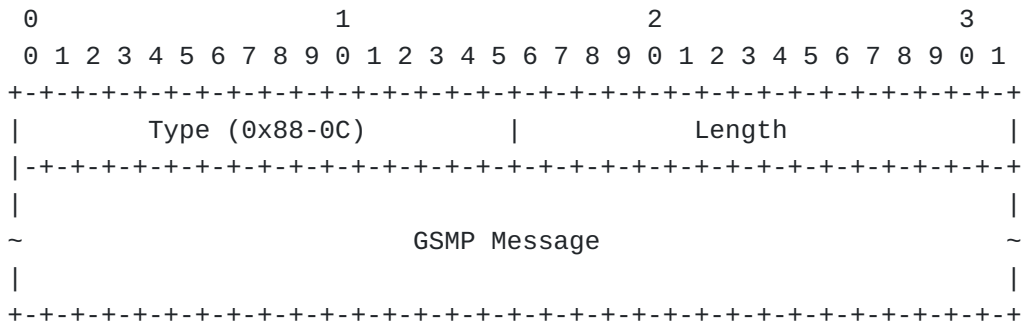


Figure 7: GSMPv3 with TCP/IP Encapsulation message format

Type

> This 2-byte field indicates the type code of the following message. The type code for GSMP messages is 0x88-0C (i.e., the same as GSMP's Ethertype).

Length

> This 2-byte unsigned integer indicates the total length of the GSMP message only. It does not include the 4-byte TLV header.

NAS listens for incoming connections from the access nodes. Port 6068 is used for TCP connection. Adjacency protocol messages, which are used to synchronize the NAS and access-nodes and maintain handshakes, are sent after the TCP connection is established. ANCP messages other than adjacency protocol messages may be sent only after the adjacency protocol has achieved synchronization.
In the case of ATM access, a separate PVC (control channel) capable of transporting IP would be configured between NAS and the DSLAM for ANCP messages.

In 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).

5.2. ANCP Connection keepalive

TOC

GSMPv3 defines an adjacency protocol. The adjacency protocol is used to synchronize states across the link, to negotiate which version of the GSMP protocol to use, to discover the identity of the entity at the other end of a link, and to detect when it changes. GSMP is a hard state protocol. It is therefore important to detect loss of contact between switch and controller, and to detect any change of identity of switch or controller. No protocol messages other than those of the adjacency protocol may be sent across the link until the adjacency protocol has achieved synchronization. There are no changes to the base GSMP adjacency protocol for implementing ANCP.
The NAS will set the M-flag in the SYN message (signifying it is the master). Once the adjacency is established, periodic adjacency messages (type ACK) are exchanged. The default ACK interval as advertised in the adjacency messages is 10 sec for ANCP. It SHOULD be configurable and is an implementation choice. It is recommended that both ends specify the same timer value, in order to achieve this behavior both ends look at the timer values in the received (initial) adjacency message and agree to use the higher of the two values. That is, the node that receives a higher timer value than its own, will reply in its subsequent adjacency messages (such as SYNACK, ACK) with the higher timer value.
The GSMP adjacency message defined in [RFC3292] (Doria, A., Hellstrand, F., Sundell, K., and T. Worster, “General Switch Management Protocol (GSMP) V3,” June 2002.) is extended for ANCP and is shown in section 5.3 immediately following this section. The 8-bit "version" field in the adjacency protocol messages is modified to carry the version and sub-version of the GSMP protocol for version negotiation. ANCP uses version 3 and sub-version 1 of GSMP protocol. [RFC Editor's note: sub-version needs to be changed from 1 to 2 upon publication.] In the adjacency protocol the version and the 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 understood will ignore that message. A receiver receiving a SYN message with a version/sub-vresion lower than its own highest version/sub-version, but a version/sub-version that it understands, will 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 protocol remains

synchronised. All other messages will use the agreed version in the version/sub-version fields.
The semantics and suggested values for Code, "Sender Name", "Receiver Name", "Sender Instance", and "Receiver Instance" fields are as defined in [RFC3292] (Doria, A., Hellstrand, F., Sundell, K., and T. Worster, "General Switch Management Protocol (GSMP) V3," June 2002.). The "Sender Port", and "Receiver Port" should be set to 0 by both ends. The pType field should be set to 0. The pFlag should be set to 1.
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 would continue to listen for new connection requests. The DSLAM will try to re-establish the TCP connection and both sides will 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 draft.

5.3. Capability negotiation

TOC

The adjacency message as defined in [RFC3292] (Doria, A., Hellstrand, F., Sundell, K., and T. Worster, "General Switch Management Protocol (GSMP) V3," June 2002.) is extended to carry "Capability TLVs". Both the NAS and the access node will advertise supported capabilities in the originated adjacency messages. If a received adjacency message indicates absence of support for a capability that is supported by the receiving device, it will turn off the capability locally and will send an updated adjacency message with the capability turned off to match the received capability set. This process will eventually result in both sides agreeing on the minimal set of supported capabilities. The adjacency will not come up unless the capabilities advertised by the controller and the controlled device match.
After initial synchronization, if at anytime a capability mismatch is detected, the adjacency will be brought down (RSTACK will be generated by the device detecting the mismatch), and synchronization will be re-attempted.

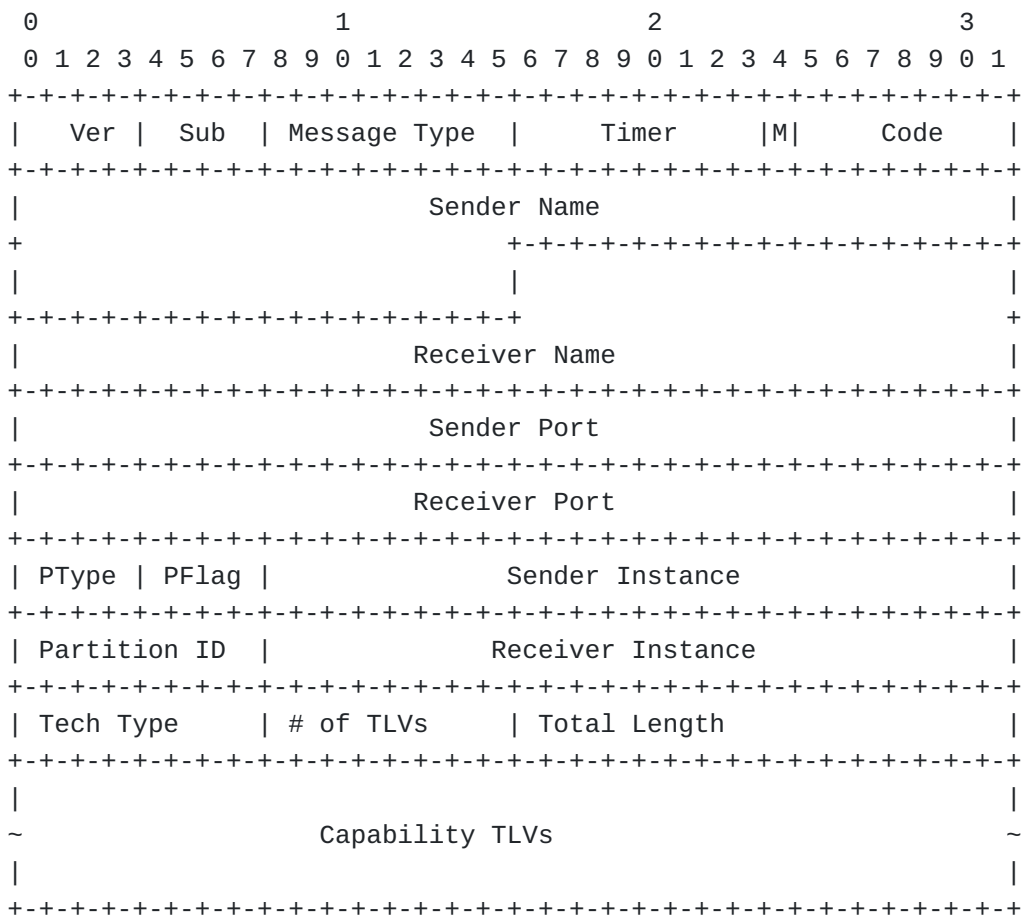


Figure 8

The format of capability TLV is:

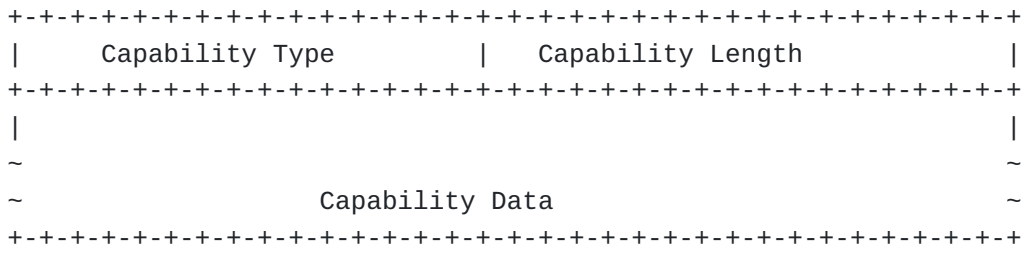


Figure 9: Capability TLV

The Tech Type field type indicates the technology to which the capability extension applies. For access node control in case of DSL networks, new type "DSL" is proposed. The value for this field is 0x05. This is the first available value in the range that is not currently allocated. It will need to be reserved with IANA.
Capability length is the number of actual bytes contained in the value portion of the TLV. The TLV is padded to a 4-octet alignment. Therefore, a TLV with no data will contain a zero in the length field (if capability data is three octets, the length field will contain a three, but the size of the actual TLV is eight octets). Capability data field can be empty if the capability is just a boolean. In case the capability is a boolean, it is inferred from the presence of the TLV (with no data).
Capability data provides the flexibility to advertise more than mere presence or absence of a capability. Capability types can be registered with IANA. Following capabilities are defined for ANCP as applied to DSL access:

1. Capability Type : Dynamic-Topology-Discovery = 0x01

   > Length (in bytes) : 0
   >
   > Capability Data : NULL

2. Capability Type : Line-Configuration = 0x02

   > Length (in bytes) : 0
   >
   > Capability Data : NULL

3. Capability Type : Transactional-Multicast = 0x03 (controller i.e. NAS terminates IGMP messages from subscribers, and via l2 control protocol, signals state to the access-nodes (e.g. DSLAMs) to enable layer2 replication of multicast streams. In ATM access network this implies that NAS instructs the access-node to setup a P2MP cross-connect. The details of this will be covered in a separate ID.

   > Length (in bytes) : 0
   >
   > Capability Data : NULL

4. Capability Type : OAM = 0x04

   > Length (in bytes) : 0
   >
   > Capability Data : NULL

5.4. GSMP Message Extensions for Access Node Control

TOC

5.4.1. General Extensions

TOC

Extensions to GSMP messages for various use-cases of "Access Node Control" mechanism are defined in sections Section 5.4.2 (Topology Discovery Extensions) to Section 5.4.4 (OAM Extensions). However, sub-sectionSection 5.4.1.1 (Extension TLV) below defines extensions to GSMP that have general applicability and section Section 5.4.5 (Additional GSMP Extensions for future use cases) introduces anothor messaging principle and additional general purpose TLVs that could be used to develop new use cases in future.

5.4.1.1. Extension TLV

TOC

In order to provide flexibility and extensibility certain GSMP messages such as "PORT MANAGEMENT" and "EVENT" messages defined in [RFC3292] (Doria, A., Hellstrand, F., Sundell, K., and T. Worster, “General Switch Management Protocol (GSMP) V3,” June 2002.) have been modified to include an extension block that follows a TLV structure. Individual messages in the following sections describe the usage and format of the extension block.
All Extension TLVs will be designated as follow:

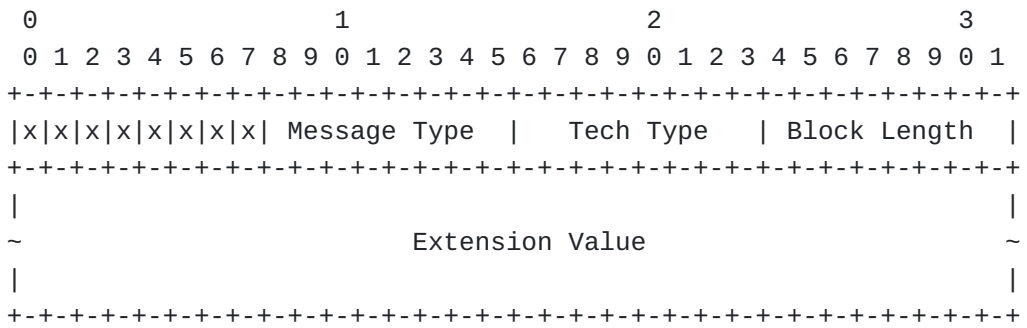


Figure 10: Extension TLV

x: Reserved Flags

These are generally used by specific messages and will be defined in those messages.

Message Type

An 8-bit field corresponding to the message type where the extension block is used.

Tech Type

An 8-bit field indicating the applicable technology type value. The Message Type plus the Tech Value uniquely define a single Extension Type and can be treated as a single 16 bit extension type. "Tech Type" value of 0x05 SHOULD be used by ANCP for DSL technology and 0x01 for PON technology.

0x00 Extension block not in use

0x01 PON

0x05 DSL

0x06 - 0xFE Reserved

0xFF Base Specification Use

Block Length

A 8-bit field indicating the length of the Extension Value field in bytes. When the Tech Type = 0x00, the length value MUST be set to 0.

Extension Value

A variable length field that is an integer number of 32 bit words long. The Extension Value field is interpreted according to the specific definitions provided by the messages in the following sections..

5.4.2. Topology Discovery Extensions

TOC

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.

Not all the fields in GSMP Event message are applicable to ANCP. The fields that are not applicable MUST be set to zero by the ANCP sender and ignored by the ANCP receiver. The fields in the PORT UP and PORT DOWN messages to be set by the ANCP sender, and corresponding handling by the ANCP receiver is described below.

The version field MUST be set to 3, and the sub field MUST be set to 1. As defined in [RFC3292] (Doria, A., Hellstrand, F., Sundell, K., and T. Worster, “General Switch Management Protocol (GSMP) V3,” June 2002.), the one byte Message Type field MUST be set to 80 for PORT UP Event message, and to 81 for PORT DOWN Event Message. The 12 bit Code field MUST be set to 0. The 4 bit Result field MUST be set to 0 (signifying Ignore.) 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 Error Message (TBD) containing the reason of the failure. The 24-bit Transaction Identifier field MUST be set to 0. The "I" bit and the SubMessage field MUST be set to 1 to signify no fragmentation. The Length field is two bytes and MUST contain the length of the message (including header and the payload) in bytes.

The "Port" field, "Port Session Number" field and "Event Sequence Number" field are 4 bytes each, and MUST be set to 0 by the ANCP sender. LABEL field in event messages is defined as a TLV in [RFC3292] (Doria, A., Hellstrand, F., Sundell, K., and T. Worster, “General Switch Management Protocol (GSMP) V3,” June 2002.). ANCP does NOT use the Label TLV. In both PORT UP and PORT DOWN event messages an ANCP sender MUST treat the Label field, immediately following the "Event Sequence Number" field, as a fixed 8 byte field, and MUST set these 8 bytes to 0. The receiver MUST NOT interpret the LABEL field as a TLV and MUST ignore the 8 bytes immediately following the "Event Sequence Number" field. In future versions of ANCP, if necessary, the un-used fields in GSMP Event message, which do not have ANCP specific semantics, can be used partially or completely, by re-naming appropriately, and associating valid semantics with these fields.

The Tech Type field is extended with new type "DSL". The value for this field is 0x05.

In case of bonded copper loops to the customer premise (as per DSL multi-pair bonding described by [G.988.1] (, “ITU-T recommendation G. 998.1, ATM-based multi-pair bonding,” 2005.) and [G.988.2] (, “ITU-T recommendation G.998.2, Ethernet-based multi-pair bonding,,” 2005.)), 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 of individual constituent DSL lines or due to change in state of the 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.

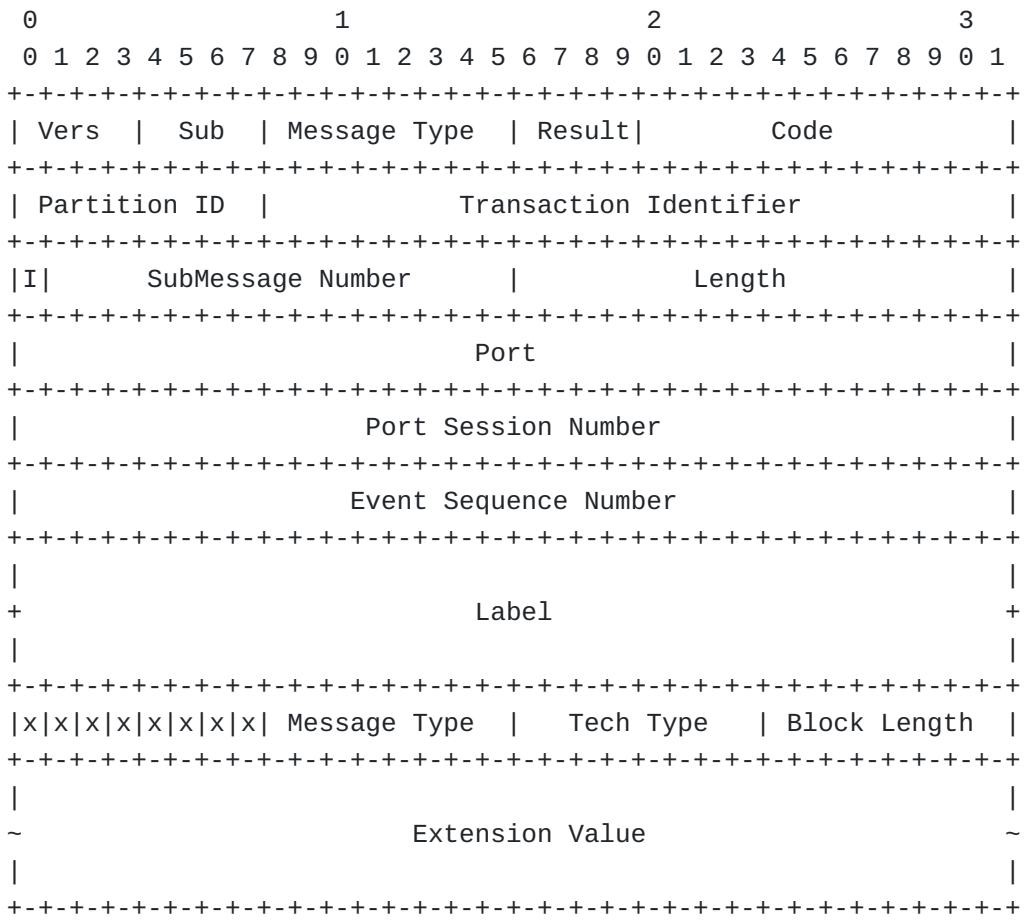


Figure 11

The format of the "Extension Value" field for Tech Type "DSL" is as follows :

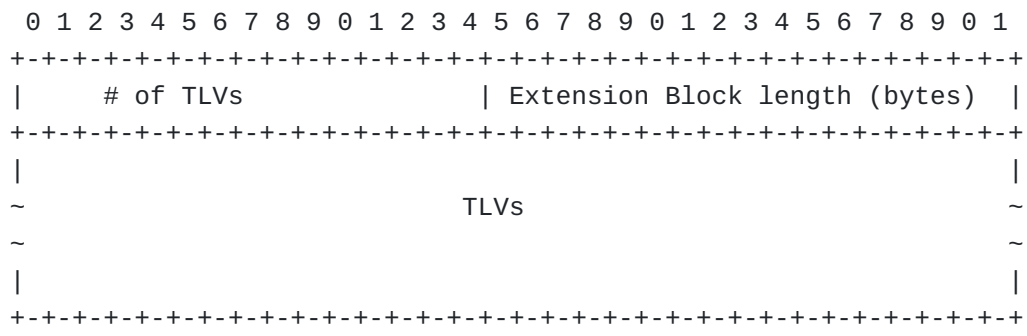


Figure 12: Extension Value

The "Extension Value" contains one or more TLVs to identify a DSL line and define its characteristics. A TLV can consist of multiple sub-TLVs. First 2 byte of the "Extension Value" contains the number of TLVs that follow. The next 2 bytes contain the total length of the TLVs carried in the extension block in bytes (existing "Block Length" field in the GSMP message is limited to 255 bytes and is not sufficient).
General format of a TLV is :

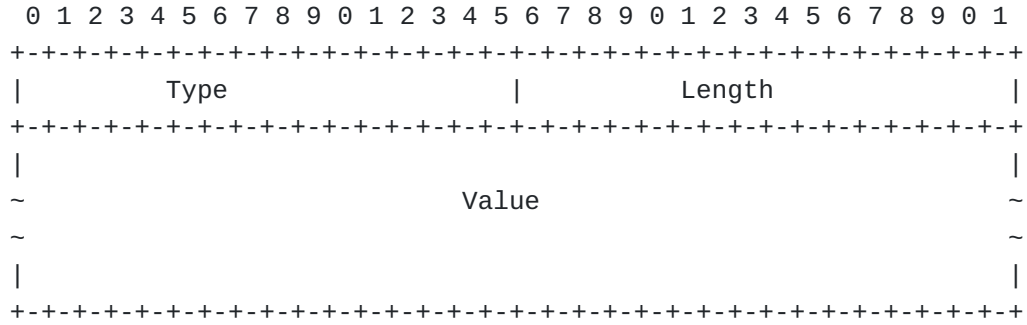


Figure 13: General TLV

The value field in each TLV is padded to a 4-octet alignment. The Length field in each TLV contains the actual number of bytes in the TLV (not including the padding if present). If a TLV is not understood by the NAS, it is silently ignored. Currently defined types start from 0x01.
Following TLVs are currently defined:

1. Type (Access-Loop-Circuit-ID = 0x01): This is a mandatory TLV and contains an identifier of the subscriber's connection to the access node (i.e. "local loop"). The "local loop" can be

ATM based or Ethernet based. 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] (Patrick, M., “DHCP Relay Agent Information Option,” January 2001.) and [TR-101] (Cohen et al, “Architecture & Transport: "Migration to Ethernet Based DSL Aggregation", DSL Forum TR-101,” 2005.).

> Length : (up to 63 bytes)
>
> Value : ASCII string
>
> For an ATM based local loop the string consists of slot/port and VPI/VCI information corresponding to the subscriber's DSL connection. Default syntax for the string inserted by the access node as per [TR-101] (Cohen et al, “Architecture & Transport: "Migration to Ethernet Based DSL Aggregation", DSL Forum TR-101,” 2005.) is:
>
> > "Access-Node-Identifier atm slot/port:vpi.vci"
>
> The Access-Node-Identifier uniquely identifies the access node in the access network. The slot/port and VPI/VCI uniquely identifies the DSL line on the access node. Also, there is one to one correspondence between DSL line and the VC between the access node and the NAS.
>
> For local loop which is Ethernet based (and tagged), the string consists of slot/port and VLAN tag corresponding to the subscriber. Default syntax for the string inserted by the access node as per [TR-101] (Cohen et al, “Architecture & Transport: "Migration to Ethernet Based DSL Aggregation", DSL Forum TR-101,” 2005.) is:
>
> > "Access-Node-Identifier eth slot/port[:vlan-id]"

2. Type (Access-Loop-Remote-Id = 0x02): This is an optional TLV and contains an identifier to uniquely identify a user on a local loop on the access node. The exact usage on the NAS is out of scope of this document. It is desirable that the format used for the field is 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] (Patrick, M., “DHCP Relay Agent Information Option,” January 2001.) and [TR-101] (Cohen et al, “Architecture & Transport: "Migration to Ethernet Based DSL Aggregation", DSL Forum TR-101,” 2005.).

Length : (up to 63 bytes)

Value : ASCII string

3. Type (Access-Aggregation-Circuit-ID-Binary = 0x06)

Length : (8 bytes)

Value : two 32 bit integers

For ethernet access aggregation, where a per-subscriber (stacked) VLAN can be applied (1:1 model defined in [TR-101] (Cohen et al, “Architecture & Transport: "Migration to Ethernet Based DSL Aggregation", DSL Forum TR-101,” 2005.)), 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

This TLV can carry 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 integer (least significant bits) 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 can uniquely identify the DSL line on the DSLAM).

This is optional.

4. Type (Access-Aggregation-Circuit-ID-ASCII = 0x03)

Length : (up to 63 bytes)

Value : ASCII string

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 format for the string is:

> "Access-Node-Identifier eth 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, typical format for the string is:

> "Access-Node-Identifier atm 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. A separate set of sub-TLVs will be defined for the uplink characteristics (TBD).

This TLV is optional.

5. Type (DSL Line Attributes = 0x04):

Length : variable (up to 1024 bytes)

Value : This is a mandatory TLV and consists of one or more Sub-TLVs corresponding to DSL line attributes. No sub-TLVs other than the "DSL type" and "DSL line state" SHOULD be included in a PORT DOWN message.

The general format of the sub-TLVs is identical to the general TLV format. The value field in each sub-TLV is padded to a 4-octet alignment. The Length field in each sub-TLV contains the actual number of bytes in the TLV

(not including the padding if present). Current defined sub-TLV types are start from 0x81.

Following sub-TLVs are currently defined :

*Type (DSL-Type = 0x91) : Defines the type of transmission system in use. This is a mandatory TLV.

> Length : (4 bytes)
>
> Value : (Transmission system : ADSL1 = 0x01, ADSL2 = 0x02, ADSL2+ = 0x03, VDSL1 = 0x04, VDSL2 = 0x05, SDSL = 0x06, UNKNOWN = 0x07).

*Type (Actual-Net-Data-Upstream = 0x81): Actual upstream net data rate on a DSL line. This is a mandatory TLV.

> Length : (4 bytes)
>
> Value : (Rate in Kb/sec)

*Type (Actual-Net-Data-Rate-Downstream = 0x82) : Actual downstream net data rate on a DSL line. This is a mandatory TLV.

> Length : (4 bytes)
>
> Value : (Rate in Kb/sec)

*Type (Minimum-Net-Data-Rate-Upstream = 0x83) : Minimum net data rate desired by the operator. This is optional.

> Length : (4 bytes)
>
> Value : (Rate in Kb/sec)

*Type (Minimum-Net-Data-Rate-Downstream = 0x84) : Minimum net data rate desired by the operator. This is optional.

> Length : (4 bytes)
>
> Value : (Rate in Kb/sec)

*Type (Attainable-Net-Data-Rate-Upstream = 0x85) : Maximum net upstream rate that can be attained on the DSL line. This is an optional TLV.

Length : (4 bytes)

Value : (Rate in Kb/sec)

*Type (Attainable-Net-Data-Rate-Downstream = 0x86) : Maximum net downstream rate that can be attained on the DSL line. This is an optional TLV.

Length : (4 bytes)

Value : (Rate in Kb/sec)

*Type (Maximum-Net-Data-Rate-Upstream = 0x87) : Maximum net data rate desired by the operator. This is optional.

Length : (4 bytes)

Value : (Rate in Kb/sec)

*Type (Maximum-Net-Data-Rate-Downstream = 0x88) : Maximum net data rate desired by the operator. This is optional.

Length : (4 bytes)

Value : (Rate in Kb/sec)

*Type (Minimum-Net-Low-Power-Data-Rate-Upstream = 0x89) : Minimum net data rate desired by the operator in low power state. This is optional.

Length : (4 bytes)

Value : (Rate in Kb/sec)

*Type (Minimum-Net-Low-Power-Data-Rate-Downstream = 0x8A) : Minimum net data rate desired by the operator in low power state. This is optional.

Length : (4 bytes)

Value : (Rate in Kb/sec)

*Type (Maximum-Interleaving-Delay-Upstream = 0x8B) : maximum one way interleaving delay. This is optional.

Length : (4 bytes)

Value : (Time in msec)

*Type (Actual-Interleaving-Delay-Upstream = 0x8C) :
Value corresponding to the interleaver setting. This
is optional.

> Length : (4 bytes)
>
> Value : (Time in msec)

*Type (Maximum-Interleaving-Delay-Downstream = 0x8D) :
maximum one way interleaving delay. This is optional.

> Length : (4 bytes)
>
> Value : (Time in msec)

*Type (Actual-Interleaving-Delay-Downstream = 0x8E) :
Value corresponding to the interleaver setting. This
is optional.

> Length : (4 bytes)
>
> Value : (Time in msec)

*Type (DSL line state = 0x8F) : The state of the DSL
line. For PORT UP message, at this time, 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 : { SHOWTIME = 0x01, IDLE = 0x02, SILENT =
> 0x03 }

*Type (Access Loop Encapsulation = 0x90) : 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 can be optionally indicated.

> Length : (3 bytes)
>
> Value : The three bytes (most to least
> significant) and valid set of values for each
> byte are defined below.

```
Data Link (1 byte): {ATM AAL5 = 0,
ETHERNET = 1}

Encaps 1 (1 byte): {

    NA = 0,

    Untagged Ethernet = 1,

    Single-tagged Ethernet = 2}

Encaps 2 (1 byte):{

    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}
```

If this TLV is present, the Data Link protocol MUST be indicated as defined above. However, 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

---

5.4.3. Line Configuration Extensions

TOC

The Port Management message format defined in [RFC3292] (Doria, A., Hellstrand, F., Sundell, K., and T. Worster, "General Switch Management Protocol (GSMP) V3," June 2002.) has been modified to contain an

extension block (described above in section Section 5.4.1.1 (Extension TLV)) 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 could further qualify the action specified in the Function field. Any Function specific data MUST be carried in the extension block.
Not all the fields in GSMP Port Management message are applicable to ANCP. The fields that are not applicable MUST be set to zero by the ANCP sender and ignored by the ANCP receiver.
The NAS uses the extension block in the Port Management messages to convey service attributes of the DSL lines to the DSLAM. TLVs are defined for DSL line identification and service data for the DSL lines. Port number is set to 0 in the message. A new action type "Configure Connection Service Data" (value 0x8) is defined. The "Function" field is set to the action type. This action type indicates to the device being controlled (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). For the action type "Configure Connection Service Data", X-Function field MUST be set to 0. The Tech Type field is extended with new type "DSL". The value for this field is 0x05.

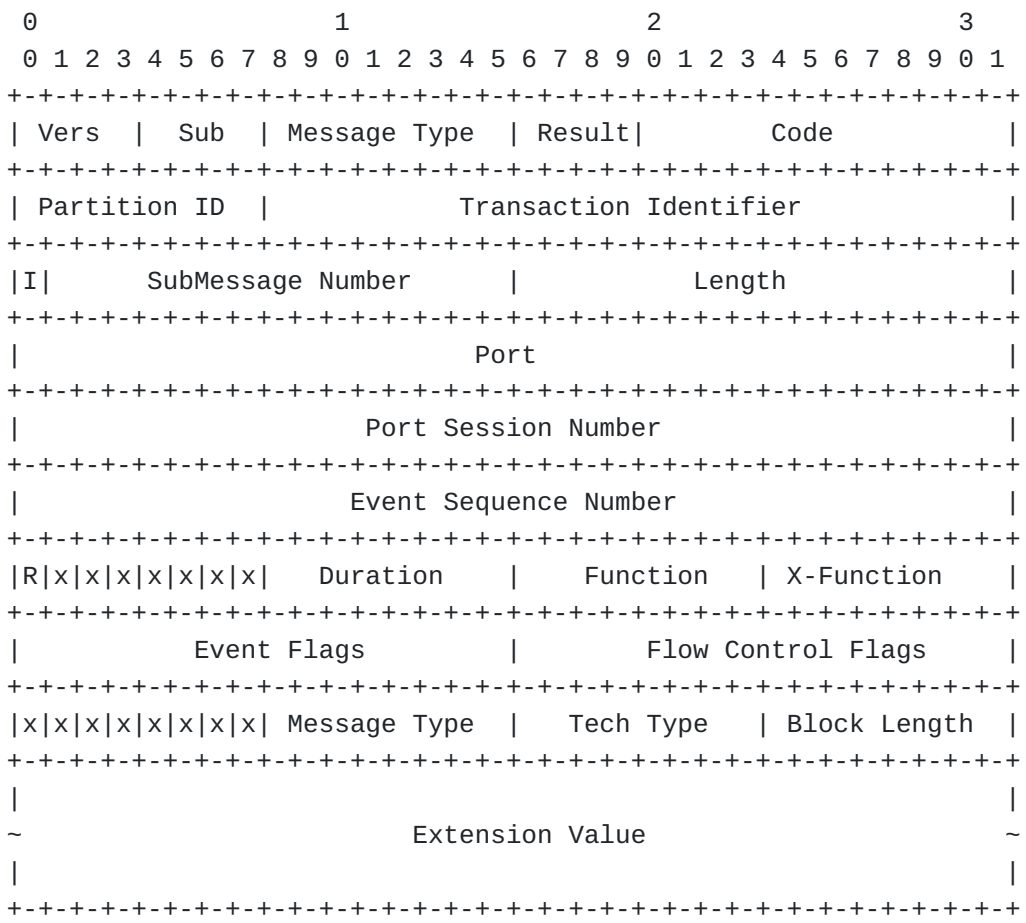


Figure 14

The format of the "Extension Value" field is as follows:

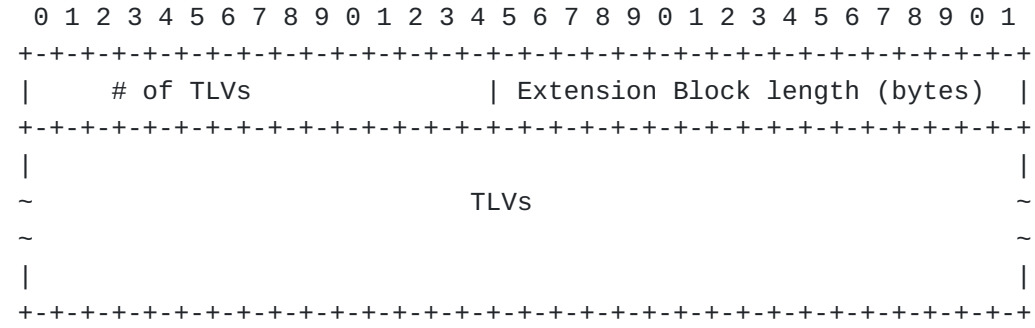


Figure 15: Extension Value

The "Extension Value" field contains one or more TLVs containing DSL line identifier and desired service attributes of the the DSL line. First 2 byte of the "Extension Value" contains the number of TLVs that follow. The next 2 bytes contain the total length of the extension block in bytes (existing "Block Length" field in the GSMP message is limited to 255 bytes and is not sufficient).
General format of a TLV is:

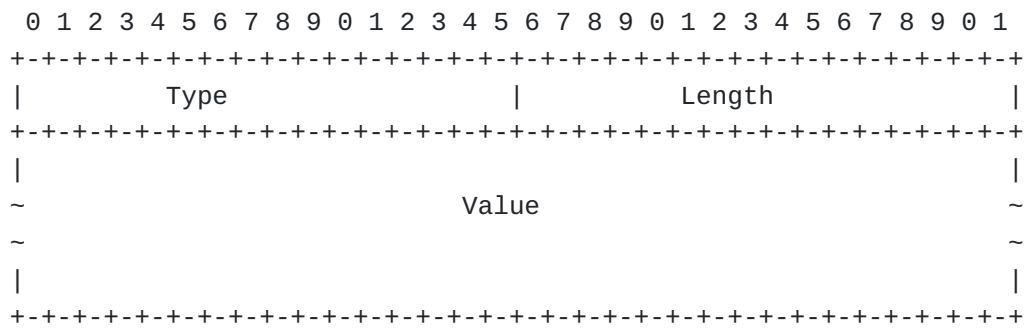


Figure 16: General TLV

The value field is padded to a 4-octet alignment. The Length field in each TLV contains the actual number of bytes in the TLV (not including the padding if present). If a TLV is not understood by the access-node, it is silently ignored. Depending upon the deployment scenario, the NAS may specify "Access Loop Circuit-ID" or the "Access Aggregation Circuit-ID") as defined in section Section 5.4.1 (General Extensions). Following TLVs can appear in this message:

*Type (Access-Loop-Circuit-ID = 0x01) : defined in section Section 5.4.1 (General Extensions)

*Type (Access-Aggregation-Circuit-ID-Binary = 0x06): defined in section Section 5.4.1 (General Extensions)

*Type (Access-Aggregation-Circuit-ID-ASCII = 0x03): defined in section Section 5.4.1 (General Extensions)

*Type (Service-Profile-Name = 0x05): 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 (NAS learns from a policy server after a subscriber is authorized).

In future, more TLVs MAY be defined for individual service attributes of a DSL line (e.g. rates, interleaving delay, multicast channel entitlement access-list etc)

5.4.3.1. Provisioning Message

TOC

The Provisioning message is sent by the NAS to the AN to provision information in the AN. This message can be used to provision global scope information on the Access Node.
The Message Type for the Provisioning message is 93.
The NAS sending the Provisioning message MUST set the Result field to 0x00.
The NAS MUST populate the ANCP Transaction Identifier field with a distinct non-zero, linearly incrementing value for each request per adjacency, as described in Section 5.4.5 (Additional GSMP Extensions for future use cases) .
The ANCP Provisioning message payload MAY contain different TLVs, like for example Service-Profile-Name TLV. The Service-Profile-Name TLV MAY appear zero, one or multiple times.
On receipt of the Provisioning message, the AN MUST:

- ignore the Result field

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

5.4.4. OAM Extensions

TOC

GSMP "Port Management" message (type 32) SHOULD be used by the NAS to trigger access node to run a loopback test on the local loop. The message format is defined in section Section 5.4.2 (Topology Discovery Extensions). The version field SHOULD be set to 3 and sub-version field SHOULD be set to 1. The remaining fields in the GSMP header have standard semantics. The function type used in the request message SHOULD be set to "remote loopback" (type = 0x09). The port, "port session number", "event sequence number", duration, "event flags", "flow control flags" and code fields SHOULD all be set to 0. The result field SHOULD be set to "AckAll" to indicate requirement for the access node to send a success or failure response. The transaction ID SHOULD contain a sequence number inserted by the NAS in each request that it generates.

Not all the fields in GSMP Port Management message are applicable to ANCP. The fields that are not applicable MUST be set to zero by the ANCP sender and ignored by the ANCP receiver.
The extension field format is also defined above in section Section 5.4.2 (Topology Discovery Extensions). The extension value field can contain one or more TLVs including the access-line identifier on the DSLAM and OAM test characteristics desired by the NAS.
The TLV format is defined above in section Section 5.4.2 (Topology Discovery Extensions). The value field is padded to a 4-octet alignment. The Length field in each TLV contains the actual number of bytes in the TLV (not including the padding if present). If a TLV is not understood by the NAS, it is silently ignored. Depending upon the deployment scenario, the NAS may specify "Access Loop Circuit-ID" or the "Access Aggregation Circuit-ID") as defined in section Section 5.4.1 (General Extensions). Following TLVs can appear in this message:

*Type (Access-Loop-Circuit-ID = 0x01) : defined in section Section 5.4.1 (General Extensions)

*Type (Access-Aggregation-Circuit-ID-Binary = 0x06): defined in section Section 5.4.1 (General Extensions)

*Type (Access-Aggregation-Circuit-ID-ASCII = 0x03): defined in section Section 5.4.1 (General Extensions)

*Type (OAM-Loopback-Test-Parameters = 0x07): Parameters related to 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 : (4 bytes)
>
> Value : two 1 byte numbers described below (listed in order of most to least significant). Thus, the 4 bytes consist of 1 byte of Count, followed by 1 byte of Timeout, followed by two pad bytes of zero.
>
> -Count (1 byte) : 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 the request for a loopback test, if the received test parameters contain an out of range value for the "count" field. The DSLAM MAY optionally send a failure response to the NAS with the code "invalid test parameter".
>
> -Timeout (1 byte) : Upper bound on the time in seconds that the NAS would 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 can choose to omit the generation of a response to the NAS. DSLAM SHOULD use a locally determined value for the "timeout", if the received value of the "timeout" parameter is 0.

*Type (Opaque-Data = 0x08) : This is an optional TLV. If present in the request message, the DSLAM SHOULD reflect it back in the response unmodified

> Length : (8 bytes)
>
> Value : Two 32 bit integers inserted by the NAS (not to be interpreted by the DSLAM, but just reflected back in the response).

The access node generates a success or failure response when it deems the loopback test to be complete. "Port Management" message (type 32) is used. The result field SHOULD be set to success or failure. The function type SHOULD be set to 0x09. The transaction ID SHOULD be copied from the sequence number contained in the corresponding request. The other parameters not explicitly defined here SHOULD be set as specified in the request message above. The code field SHOULD be set to a value in the range 0x500 to 0x5ff (to be reserved with IANA) to indicate the status of the executed test. The valid values defined are (can be extended in future):

> 0x500 : Specified access line does not exist
>
> 0x501 : Loopback test timed out
>
> 0x502 : Reserved
>
> 0x503 : DSL line status showtime
>
> 0x504 : DSL line status idle
>
> 0x505 : DSL line status silent
>
> 0x506 : DSL line status training
>
> 0x507 : DSL line integrity error
>
> 0x508 : DSLAM resource not available
>
> 0x509 : Invalid test parameter

The Extension value can contain one or more TLVs including the TLV to identify the access line on which the test was performed, and details

from executing the test. The access line identifier SHOULD be identical to what was contained in the request. The relevant TLVs are:

*Type (Access-Loop-Circuit-ID = 0x01) : defined in section Section 5.4.1 (General Extensions)

*Type (Access-Aggregation-Circuit-ID-Binary = 0x06): defined in section Section 5.4.1 (General Extensions)

*Type (Access-Aggregation-Circuit-ID-ASCII = 0x03): defined in section Section 5.4.1 (General Extensions)

*Type (Opaque-Data = 0x08) : Data inserted by the NAS in the request reflected back by the DSLAM.

> Length : (up to 8 bytes)
>
> Value : Two 32 bit integers as received in the request (opaque to the DSLAM).

*Type (OAM-Loopback-Test-Response-String = 0x09)

> Length : (up to 128 bytes)
>
> Value : Suitably formatted ASCII 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.

5.4.5. Additional GSMP Extensions for future use cases

TOC

GSMP protocol defined in [RFC3292] (Doria, A., Hellstrand, F., Sundell, K., and T. Worster, "General Switch Management Protocol (GSMP) V3," June 2002.) allows for two messaging principles in case of Request/ Response interaction:

*The same message type used for both request message and response message where result field and code field settings are used to differentiate between request and response messages;

*Two different message types for request message and response messages.

First message principle has been adopted for use cases defined in sections Section 5.4.2 (Topology Discovery Extensions) to Section 5.4.4 (OAM Extensions), the purpose of this section is to specify the second type of approach in order to allow the use of this message principle for the development of future use cases.
In the new message paradigm different message types are used as ANCP Request Message and ANCP Response Message: the format of a generic ANCP message starts with the common GSMP header as in the case of the existing ANCP implementation, but the Result field is set to Ignore in order to instruct the receipt to ignore this field and follow the procedures specified for the received message type. The Transaction Identifier field is used to distinguish between request messages and to associate a response message to a request. Applications that require such response correlation MUST set the Transaction Identifier to a value in the range (1, 2^24 – 1). When used in this manner, the Transaction Identifier 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. Message types not requiring response message correlation SHOULD set the Transaction Id field to 0x0. In the event of an ANCP transport protocol failure, all pending ANCP messages destined to the disconnected recipient can be discarded until the transport is re- established following which the Transaction Identifier is re- initialized.
The value of the Transaction Identifier in a Response message MUST be set to that of the respective Request message. This allows the Requester to correlate the Response to the original Request. The Transaction Identifier is not used in ANCP adjacency messages. Also, other ANCP applications not requiring it SHOULD set the Transaction Identifier to 0x0 in their messages.
All TLVs within the ANCP message have to be 32 bit aligned, and when necessary padded with 0s to the 32 bit boundary. The padding is not reflected in the message length field.

5.4.5.1. General well known TLVs

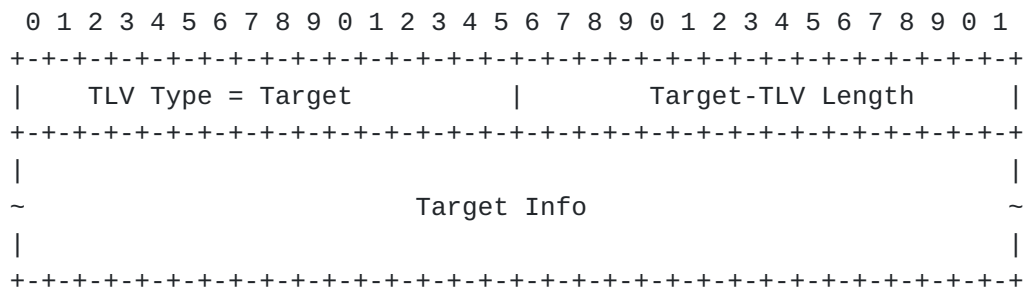
TOC

This section contains the definitions of three general well known TLVs. These TLVs are intended to be re-usable across different messages.

TOC

5.4.5.1.1. Target TLV

The Target TLV (0x1000 - 0x01020) is intended to be a general well known TLV allowing the representation of different types of objects. Its use is not restricted to any specific Message Type.



Target TLV:

> TLV (0x1000 - 0x1020) indicating the type of target being addressed. Target TVL 0x1000 indicates a single Access-Port.

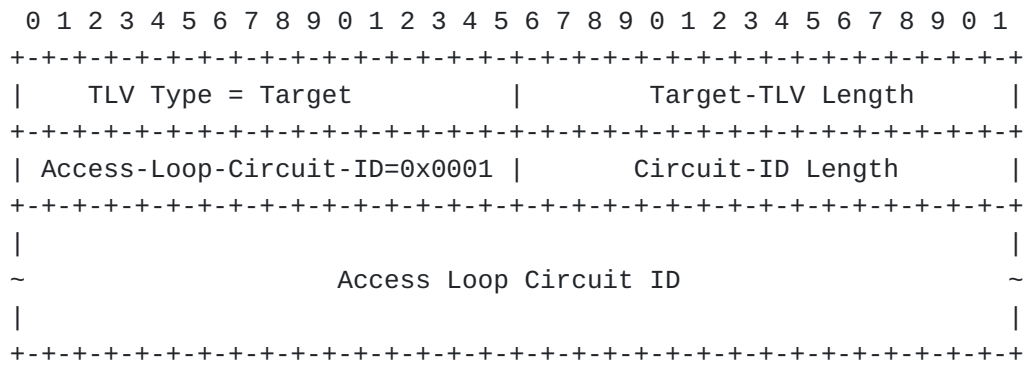
Target TLV Length:

> Length in bytes of Target Info. Excludes TLV header

Target Info:

> Target information as defined for each the given target. The field can consist of sub-TLVs.

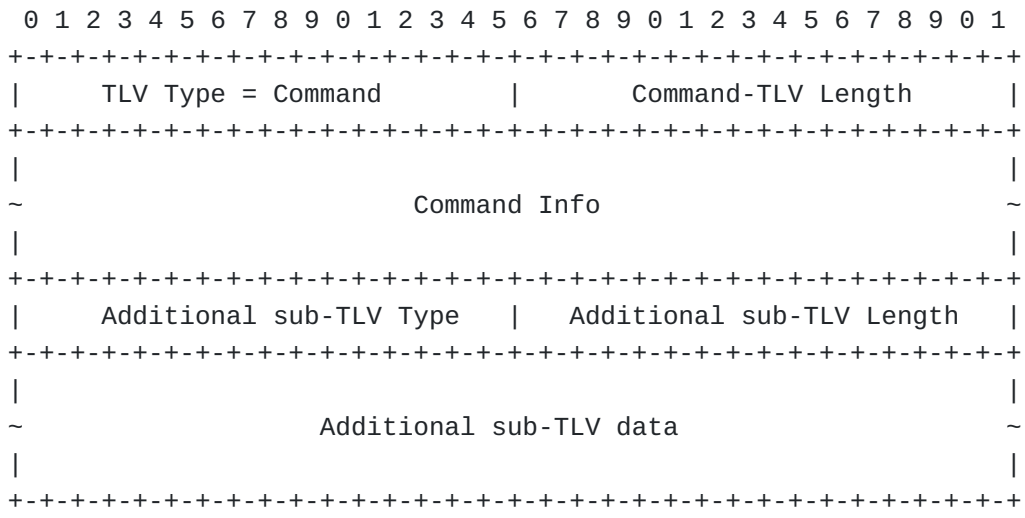
In its simplest form, when targeting a single access line the Target-TLV will be set to a value of (0x1000), and carry in its payload one or more sub-TLVs identifying the target. The following example illustrates the message format for a single port identified by an Access-Loop-Circuit-ID TLV (0x0001) that could be derived from a Port-UP message:



TOC

5.4.5.1.2. Command TLV

The Command TLV (0x11) is intended to be a general well known TLV allowing the encapsulation of one or more command directives in a TLV oriented message. The semantics of the command are allowed to be specified for each message type, ie different message types that choose to carry the Command TLV are expected to define the meaning of the content of the payload, which could be re-used from those already defined elsewhere if appropriate.



Command TLV:

> TLV (0x11) indicating the contents to be one or more command directives.

Command TLV Length:

> Combined length in bytes of the data in Command Info and sub-TLV. Excludes the Command TLV header

Commad-Info:

> Command information as defined for each message type. The field can consist of sub-TLVs.

Additional sub-TLV:

> Additional sub-TLVs can be present in a command TLV. Any such sub-TLVs must directly follow each command.

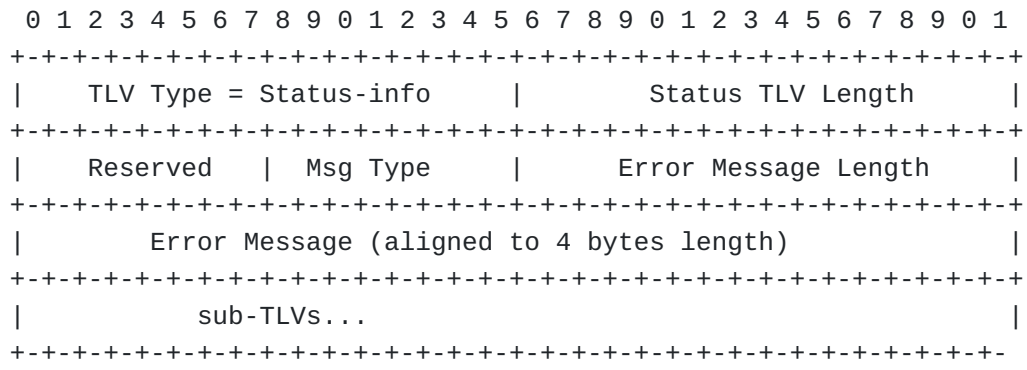
Additional sub-TLV Length:

> Number of actual bytes contained in the value portion of each additional sub-TLV

5.4.5.1.3. Status-info TLV

TOC

The Status-info-TLV is intended to be a general well known TLV used to convey the status code regarding commands and/or requests. The format of the Status-info-TLV (0x0106) is shown below.



Status-info TLV:

> TLV (0x106) conveying the status or error response of a command

Status TLV Length:

> Specifies the length in bytes of the Status Info TLV payload. Excludes the TLV header

Reserved:

> This field MUST be set to all zeroes by the sender and ignored by the receiver.

Msg Type:

> The message type value of the message the Status-info TLV is reporting on

Error Message Length:

> It contains the length of an optional error message or 0 if none.

Error message:

> It contains a human-readable description of the error being reported by the Status-info field.

TLVs:

> This field is of indeterminate length, and contains zero or more of the TLVs associated with the Status-info TLV. The following TLVs are RECOMMENDED to be provided 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.

5.4.5.2. Generic Response Message

TOC

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 Identifier 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 (Structure of the Generic Response Message)

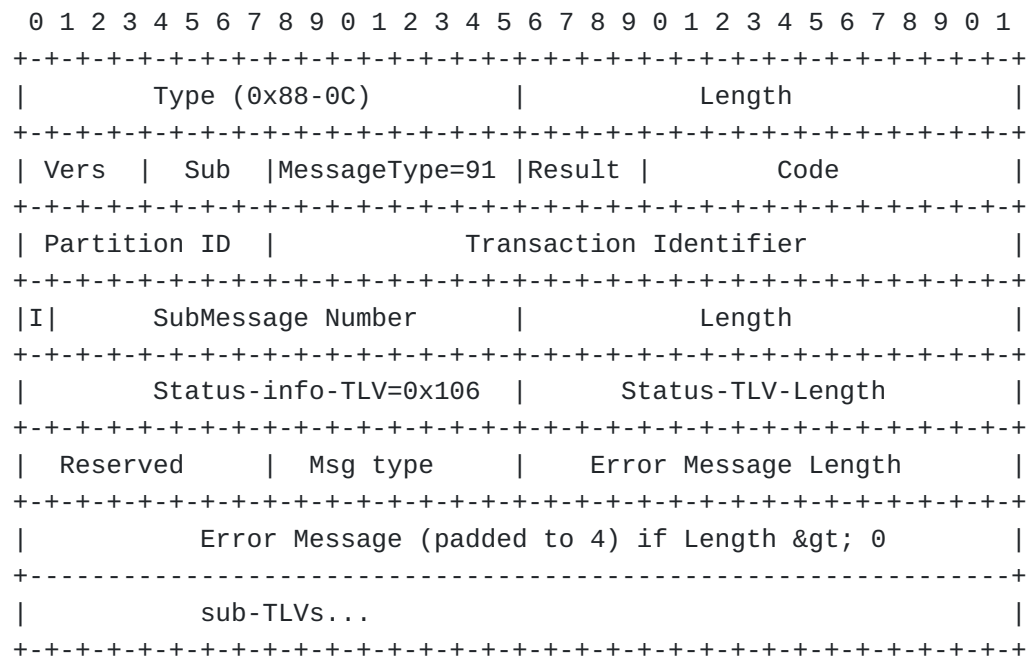


Figure 17: Structure of the Generic Response Message

Message Type:

> The message type value for the Generic Response message is 0x91.

Result:

> The value of the Result field for the Generic Response message MUST be either Success (0x03) or Failure (0x04).

Code:

> The Code field MUST have value zero if Result is set to Success (0x03). It MUST have an appropriate non-zero value if Result is set to Failure (0x04). As discussed in section 5, extensions to ANCP MAY define new Code values for use in failure responses for specific request message types.

Partition ID:

> As specified in section Section 5 (Access Node Control Protocol (ANCP)).

Transaction Identifier:

> The Transaction Identifier MUST be copied from the request to which the Generic Response message is responding.

I, Sub-message Number, Length:

> As specified in Section 5 (Access Node Control Protocol (ANCP)).

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. The Message Type field value is copied from the header of the request message. The Error Message field contains human-readable diagnostic text. The description of the response for a particular request message type MAY specify further sub-TLVs to be included in Status-info, either generally or for specific failure Code values.

5.5. ATM-specific considerations

TOC

The 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" which has only local significance on the DSLAMs.
The access loop circuit identifier can be carried as an ASCII 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 such identifier can be correlated to the context of an "aggregation network" facing IP interface (corresponding to the subscriber) on the NAS. This would typically require local configuration of such IP interfaces, or of the underlying ATM interfaces.

5.6. Ethernet-specific considerations

TOC

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 could 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 to uniquely identify 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 hve 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 such 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 Section 5.4.1 (General Extensions) defines "Access Loop Circuit ID".

---

6. IANA Considerations

TOC

This document defines the following additions to the GSMPv3 Message Type Name Space registry:

Message	Number	Source
Provisioning	93	This document

This document defines 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 (from Reserved)	This document

This document defines the following addition to the GSMPv3 Message Function Name Space registry [editor's note GMSPv3 did not define a Name Space for Function even if RFC3292 defines values for function field]:

Function Value	Function Name	Reference
0x09	Remote loopback	This document

The GSMPv3 Failure Response Message Name Space is extended from the GSMPv3 limit of 255 to a new upper limit of 4095 and this document adds the following values to the GSMPv3 Failure Response Message Name Space registry:

Failure Response Message Value	**Failure Response Message Name**	**Reference**
81d	Request message type not implemented (0x51)	This document
82d	Transaction identifier out of sequence (0x52)	This document
83d	Malformed message (0x53)	This document
84d	TLV or value not supported by negotiated capability set (0x54)	This document
85d	Invalid value in TLV (0x55)	This document
From 256d to 499d	Reserved for IETF use (0x0100 - 0x1F3)	This document
1280d	Specified access line does not exist (0x500)	This document
1281d	Loopback test timed out (0x501)	This document
1282d	Reserved (0x502)	This document
1283	DSL line status showtime (0x503)	This document
1284	DSL line status idle (0x504)	This document
1285	DSL line status silent (0x505)	This document
1286	DSL line status training (0x506)	This document
1287	DSL line integrity error (0x507)	This document
1288	DSLAM resource not available (0x508)	This document
1289	Invalid test parameter (0x509)	This document
From 509d to 4095d	Reserved for IETF use (0x1FD - 0XFFF)	This document

This document reserves the values 256 to 499 and 509 to 4095 within the GSMPv3 Failure Response Message Name Space registry for use by extensions to the Access Node Control Protocol (ANCP).
This document defines a new ANCP Version Space registry. The initial entry is as follows:

ANCP Version Value	ANCP Version Name	Reference
3	ANCP Version	This document

This document defines a new ANCP Sub-Version Space registry. The initial entry is as follows:

ANCP Sub-Version Value	ANCP Sub-Version Name	Reference
1 [*]	ANCP Sub-Version	This document

[*] Editor's note: sub-version needs to be changed from 1 to 2 upon publication
This document defines a new ANCP Tech Type Name Space registry. The initial entries are as follows:

Tech Type Value	Tech Type Name	Reference
0x00	Extension block not in use	This document
0x01	PON	This document
0x05	DSL	This document
0x06 - 0xFE	Reserved	This document
0xFF	Base Specification Use	This document

This document defines a new ANCP Command Code registry. The initial entries are as follows:

Command Code Directive Name	Command Code Value	Reference
Reserved	0x00	This document

This document defines a new ANCP TLV Type registry. The initial entries are as follows:

TLV Name	Type Code	Reference
Access-Loop-Circuit-ID	0x01	This document
Access-Loop-Remote-Id	0x02	This document
Access-Aggregation-Circuit-ID-ASCII	0x03	This document
DSL Line Attributes	0x04	This document
Service-Profile-Name	0x05	This document
Access-Aggregation-Circuit-ID-Binary	0x06	This document
OAM-Loopback-Test-Parameters	0x07	This document

Opaque-Data	0x08	This document
OAM-Loopback-Test-Response-String	0x09	This document
Reserved	0x0a-0x0f	This document
Target	0x1000 - 0X1020	This document
Command	0x11	This document
Status-info	0x0106	This document

This document defines a new ANCP Capability registry. The initial entries are as follows:

Capability Type Name	**Capability Type Code**	**Reference**
Dynamic-Topology-Discovery	0x01	This document
Line-Configuration	0x02	This document
Transactional-Multicast	0x03	This document
OAM	0x04	This document

This document defines a new ANCP sub-TLV Type registry. The initial entries are as follows:

sub-TLV Name	**Type Code**	**Reference**
Actual-Net-Data-Upstream	0x81	This document
Actual-Net-Data-Rate-Downstream	0x82	This document
Minimum-Net-Data-Rate-Upstream	0x83	This document
Minimum-Net-Data-Rate-Downstream	0x84	This document
Attainable-Net-Data-Rate-Upstream	0x85	This document
Attainable-Net-Data-Rate-Downstream	0x86	This document
Maximum-Net-Data-Rate-Upstream	0x87	This document
Maximum-Net-Data-Rate-Downstream	0x88	This document
Minimum-Net-Low-Power-Data-Rate-Upstream	0x89	This document
Minimum-Net-Low-Power-Data-Rate-Downstream	0x8A	This document
Maximum-Interleaving-Delay-Upstream	0x8B	This document
Actual-Interleaving-Delay-Upstream	0x8C	This document
Maximum-Interleaving-Delay-Downstream	0x8D	This document
Actual-Interleaving-Delay-Downstream	0x8E	This document
DSL line state	0x8F	This document
Access Loop Encapsulation	0x90	This document
DSL-Type	0x91	This document

7. Security Considerations

TOC

Security of the ANCP protocol is discussed in [RFC5713] (Moustafa , H., Tschofenig, H., and S. De Cnodder, “Security Threats and Security Requirements for the Access Node Control Protocol (ANCP),” January 2010.)

---

8. Acknowledgements

TOC

The authors would like to thank everyone that has provided comments or inputs to this document. In particular, the authors acknowledge the inputs provided by Wojciech Dec, Peter Arberg, Josef Froehler, Derek Harkness, Kim Hyldgaard, Sandy Ng, Robert Peschi, Michel Platnic and Tom Taylor.

---

9. References

TOC

9.1. Normative References

TOC

[RFC2119]	Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” BCP 14, RFC 2119, March 1997 (TXT, HTML, XML).
[RFC3046]	Patrick, M., “DHCP Relay Agent Information Option,” RFC 3046, January 2001 (TXT).
[RFC3292]	Doria, A., Hellstrand, F., Sundell, K., and T. Worster, “General Switch Management Protocol (GSMP) V3,” RFC 3292, June 2002 (TXT).
[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 (TXT).

9.2. Informative References

TOC

[ANCP-FRAMEWORK]	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,” draft-ietf-ancp-framework-13.txt, work in progress, February 2010.
[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),” January 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.

Authors' Addresses

TOC

	Sanjay Wadhwa
	Juniper Networks
	10 Technology Park Drive
	Westford, MA 01886
	USA
Phone:	
Fax:	
Email:	swadhwa@juniper.net
	Jerome Moisand
	Juniper Networks
	10 Technology Park Drive
	Westford, MA 01886
	USA
Phone:	
Fax:	
Email:	jmoisand@juniper.net

	Swami Subramanian
	Juniper Networks
	10 Technology Park Drive
	Westford, MA 01886
	USA
Phone:	
Fax:	
Email:	ssubramanian@juniper.net
	Thomas Haag
	Deutsche Telekom
	Heinrich-Hertz-Strasse 3-7
	Darmstadt, 64295
	Germany
Phone:	+49 6151 628 2088
Fax:	
Email:	haagt@telekom.de
	Norber Voigt
	Siemens
Phone:	
Fax:	
Email:	norbert.voigt@siemens.com
	Roberta Maglione
	Telecom Italia
	via Reiss Romoli 274
	Torino
	Italy
Phone:	
Email:	roberta.maglione@telecomitalia.it