ATIS-1000056

ACCESS NETWORKS ARCHITECTURE TECHNICAL REPORT

TECHNICAL REPORT

As a leading technology and solutions development organization, ATIS brings together the top global ICT companies to advance the industry's most-pressing business priorities. Through ATIS committees and forums, nearly 200 companies address cloud services, device solutions, emergency services, M2M communications, cyber security, ehealth, network evolution, quality of service, billing support, operations, and more. These priorities follow a fast-track development lifecycle — from design and innovation through solutions that include standards, specifications, requirements, business use cases, software toolkits, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). ATIS is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of oneM2M, a member and major U.S. contributor to the International Telecommunication Union (ITU) Radio and Telecommunications sectors, and a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit < www.atis.org >.

Notice of Disclaimer & Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER, NO REPRESENTATION OR WARRANTY IS MADE OFMERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

NOTE - The user's attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights. By publication of this standard, no position is taken with respect to whether use of an invention covered by patent rights will be required, and if any such use is required no position is taken regarding the validity of this claim or any patent rights in connection therewith. Please refer to [http://www.atis.org/legal/patentinfo.asp] to determine if any statement has been filed by a patent holder indicating a willingness to grant a license either without compensation or on reasonable and non-discriminatory terms and conditions to applicants desiring to obtain a license.

ATIS-1000056, *Access Networks Architecture Technical Report*

Is an ATIS Standard developed by the **Signalling, Architecture, and Control (SAC) Subcommittee** of the **ATIS Packet Technologies and Systems Committee (PTSC)**.

Published by

Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

Printed in the United States of America.

ATIS-1000056

ATIS Standard on

Access Networks Architecture Technical Report

Alliance for Telecommunications Industry Solutions

Approved October 2013

Abstract

This TR summarizes the variations of NGN access networks/technologies for wireline access networks. The wireline access technologies discussed in this document are: Digital Subscriber Line (DSL), Fiber [Broadband and Ethernet Passive Optical Networks (PONs)], Cable, and Metro Ethernet access networks. This TR serves as the reference architecture for the Emergency Telecommunications Service (ETS) wireline access requirements.

Foreword

As a leading technology and solutions development organization, the Alliance for Telecommunications Industry Solutions (ATIS) brings together the top global information and communications technology (ICT) companies to advance the industry's most-pressing business priorities. ATIS serves the public through improved understanding between carriers, customers, and manufacturers. The Packet Technologies and Systems Committee (PTSC) develops and recommends standards and technical reports related to services, architectures, and signaling, in addition to related subjects under consideration in other North American and international standards bodies. PTSC coordinates and develops standards and technical reports relevant to telecommunications networks in the U.S., reviews and prepares contributions on such matters for submission to U.S. ITU-T and U.S. ITU-R Study Groups or other standards organizations, and reviews for acceptability or per contra the positions of other countries in related standards development and takes or recommends appropriate actions.

The mandatory requirements are designated by the word *shall* and recommendations by the word *should*. Where both a mandatory requirement and a recommendation are specified for the same criterion, the recommendation represents a goal currently identifiable as having distinct compatibility or performance advantages. The word *may* denotes a optional capability that could augment the standard. The standard is fully functional without the incorporation of this optional capability.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, PTSC, 1200 G Street NW, Suite 500, Washington, DC 20005.

At the time of consensus on this document, PTSC, which was responsible for its development, had the following leadership:

M. Dolly (AT&T), PTSC Chair
V. Shaikh (Applied Communication Sciences), PTSC Vice Chair
M. Dolly (AT&T), PTSC SAC Chair
V. Shaikh (Applied Communication Sciences), Technical Editor
C. Underkoffler, ATIS Chief Editor

The Signalling, Architecture, and Control (SAC) Subcommittee was responsible for the development of this document.

Table of Contents

Table of Figures

Table of Tables

TECHNICAL REPORT **ATIS-1000056**

Technical Report on –

Access Networks Architecture Technical Report

1 Summary

This TR summarizes a set of variations of NGN access networks/technologies for wireline access networks. The wireline access technologies discussed in this document are: Digital Subscriber Line (DSL), Fiber [Broadband and Ethernet Passive Optical Networks (PONs)], Cable, and Metro Ethernet access networks. This TR serves as the reference architecture for the Emergency Telecommunications Service (ETS) wireline access requirements.

2 Purpose & Scope

The purpose of this TR is to summarize the variations of NGN access networks/technologies for wireline access networks. The wireline access technologies discussed in this document are: Digital Subscriber Line (DSL), Fiber [Broadband and Ethernet Passive Optical Networks (PONs)], Cable, and Metro Ethernet access networks. The scope of this TR is described in terms of:

- Architecture and description of functional entities.
- Call/session flows.
- Interfaces and associated protocols.
- QoS and policy mechanisms.

This TR is intended to serve as the reference architecture document for the Emergency Telecommunications Service (ETS) wireline access requirements.

3 References

The following documents contain provisions which, through reference in this text, constitute provisions of this TR. At the time of publication, the edition indicated was valid. All standards are subject to revision, and the parties to agreements based on this TR are encouraged to investigate the possibility of applying the most recent edition of the standard indicated below.

ATIS

[1] ATIS-1000049, *End-to-End NGN GETS Call Flows*.[1]

Broadband Forum[2]

[2] Broadband Forum TR-098, *Internet Gateway Device Data Model for TR-069*, v1.1.

[3] Broadband Forum TR-069, *CPE WAN Management Protocol*, v1.1.

[4] Broadband Forum TR-101, *Migration to Ethernet-Based DSL Aggregation*.

[5] Broadband Forum TR-058, *Multi-Service Architecture and Framework Requirements*,

[1] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS) at < https://www.atis.org/docstore/product.aspx?id=26039 >.

[2] These documents are available at < http://www.broadband-forum.org/ >.

[6] Broadband Forum TR-059, *DSL Evolution – Architecture Requirements for the Support of QoS Enabled IP Services*.

[7] Broadband Forum TR-156, *Using GPON Access in the Context of TR-101*.

[8] Broadband Forum TR-167, *GPON-fed TR-101 Ethernet Access Node*.

3GPP[3]

[9] 3GPP TS 23.002, *Network Architecture*.

[10] 3GPP TS 23.203, *Policy and Charging Control Architecture*.

[11] 3GPP TS 29.213, *Policy and charging control signalling flows and Quality of Service (QoS) parameter mapping*.

[12] 3GPP TS 29.211, *Rx Interface and Rx/Gx signalling flows*.

[13] 3GPP TS 29.212, *Policy and charging control over Gx reference point*.

[14] 3GPP TS 29.214, *Policy and charging control over Rx reference point*.

ITU-T[4]

[15] ITU-T Recommendation G.992.1, *Asymmetric digital subscriber line (ADSL) transceivers*.

[16] ITU-T Recommendation G.992.3, *Asymmetric digital subscriber line transceivers 2 (ADSL2)*.

[17] ITU-T Recommendation G.992.5, *Asymmetric Digital Subscriber Line (ADSL) transceivers - Extended bandwidth ADSL2 (ADSL2plus)*.

[18] ITU-T Recommendation G.993.2, *Very high speed digital subscriber line transceivers 2 (VDSL2)*.

[19] ITU-T Recommendation G.998.1, *ATM-based multi-pair bonding*.

[20] ITU-T Recommendation G.998.2, *Ethernet-based multi-pair bonding*.

[21] ITU-T Recommendation G.983, *Broadband optical access systems based on Passive Optical Networks (PON)*.

[22] ITU-T Recommendation G.984, *Gigabit-capable passive optical networks (GPON): General characteristics*.

[23] ITU-T Recommendation Q.812, *Upper layer protocol profiles for the Q and X interfaces*.

[24] ITU-T Recommendation Q.3303.3 v3, *Protocol at the interface between a Policy Decision Physical Entity (PD-PE) and a Policy Enforcement Physical Entity (PE-PE): Diameter Profile version 3*.

[25] ITU-T Recommendation Y.2111, *Resource and Admission Control Functions in Next Generation Networks*.

IEEE[5]

[26] IEEE 802.3ah, *Ethernet in the First Mile*.

[27] IEEE 802.av, *10 Gbit/s EPON*.

[3] These documents are available from the Third Generation Partnership Project (3GPP) at <http://www.3gpp.org/specs/specs.htm>.

[4] These documents are available from the International Telecommunications Union. < http://www.itu.int/ITU-T/ >

[5] These documents are available from the Institute of Electrical and Electronics Engineers (IEEE).
< http://shop.ieee.org/store/ >

CableLabs[6]

[28] CM-SP-MULPIv3.0-I08-080522, *Data-Over-Cable Service Interface Specification, DOCSIS 3.0, MAC and Upper Layer Protocols Interface Specification*.

[29] PKT-SP-MM-I04-080522, *PacketCable^{TM} Specification, Multimedia Specification*.

[30] PKT-SP-MM-WS-I02-080522, *PacketCable Multimedia Specification, PacketCable Multimedia Web Service Interface Specification*.

[31] PKT-SP-QOS-I02-080425, *PacketCable^{TM} 2.0 Quality of Service Specification*.

[32] PKT-TR-ARCH-FRM-V04-071106, *PacketCable^{TM} 2.0 Architecture Framework Technical Report*.

Metro Ethernet Forum[7]

[33] Technical Specification MEF 4, *Metro Ethernet Network Architecture Framework – Part 1: Generic Framework*.

[34] Technical Specification MEF 15, *Requirements for Management of Metro Ethernet Phase 1 Network Elements*.

4 Definitions, Acronyms, & Abbreviations

4.1 Definitions

No new definitions are defined.

4.2 Acronyms & Abbreviations

3G	3rd Generation technology
3GPP	3rd Generation Partnership Project
10GEPON	10 Gigabit Ethernet PON
AAA	AA-Answer, or Authentication, Authorization, and Accounting
AA	Authentication/Authorization
AAR	AA-Request
ACK	Acknowledgement
ACSE	Association Control Service Element
ADSL	Asymmetric DSL
AF	Assured Forwarding
AGW	Access Gateway
ANSI/SCTE	American National Standards Institute/Society of Cable Telecommunications Engineers
AN	Access Node
ANMS	Access Node Management System
APON	ATM PON
A-RACF	Access Resource Admission Control Function
AS	Application Server

[6] These documents are available from CableLabs at < http://www.cablelabs.com/specifications/>.

[7] These documents are available from the Metro Ethernet Forum at < http://metroethernetforum.org/>.

ASA	Abort Session Answer
ASR	Abort Session Request
ATIS	Alliance for Telecommunication Industry Solutions
ATM	Asynchronous Transfer Mode
AVP	Attribute Value Pair
BE	Best Effort
BK	Background
BNG	Broadband Network Gateway
BPON	Broadband PON
CCA	CC Answer
CCR	CC Request
CES	Circuit Emulation Service
CL	Controlled Load
CM	Cable Modem
CMISE	Common Management Information Service Element
CMTS	Cable Modem Termination System
COPS	Common Open Policy Service
COS	Class of Service
CPE	Customer Premises Equipment
CSCF	Call Session Control Function
DBA	Dynamic Bandwidth Allocation or Dynamic Bandwidth Assignment
DBR	Dynamic Bandwidth Report
DiffServ	Differentiated Services
DOCSIS	Data Over Cable Service Interface Specification
DSCP	DiffServ Code Point
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
DSx	Digital Service (x is a number, e.g., DS0, DS1)
DSx	Dynamic Service (x refers to type of service – addition, change, deletion)
E-DVA	Embedded Digital Voice Adaptor
EF	Expedited Forwarding
EPON	Ethernet PON
ETS	Emergency Telecommunications Service
ETSI	European Telecommunications Standards Institute
EVC	Ethernet Virtual Connection
FE	Functional Entity
FMC	Fixed-Mobile Convergence
FQDN	Fully Qualified Domain Name
FTP	File Transfer Protocol
FTTB	Fiber to the Building
FTTC	Fiber to the Curb
FTTH	Fiber to the Home
FTTN	Fiber to the Node
FTTP	Fiber to the Premises
FTTx	Fiber to the x

GEM	GPON (or GEPON) Encapsulation Method
GEPON	Gigabit Ethernet PON
GPON	Gigabit PON
GTC	GPON Transmission Convergence
GW	Gateway
HFC	Hybrid Fiber-Coaxial
HSS	Home Subscriber Server
ID	Identifier
IE	Information Element
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IP-CAN	IP-Connectivity Access Network
ITU-T	International Telecommunication Union – Telecommunication Standardization Sector
LAN	Local Area Network
LLC	Logical Link Control
LLID	Logical Link Identifier
MAC	Media Access Control
MDF	Main Distribution Frame
MPCPDU	Multi-Point Control Protocol PDU
MPLS	Multi-Protocol Label Switching
NC	Network Control
NE	Network Equipment
NID	Network Interface Device
NGN	Next Generation Network
NNI	Network-to-Network Interface
nrtPS	Non-Real-Time Polling Service
NSR	Non-Status Reporting
OAM	Operations, Administration and Maintenance
OAN	Optical Access Network
ODN	Optical Distribution Network
OLT	Optical Line Termination
OM	Operational Measurement
OMCI	ONT Management and Control Interface
ONT	Optical Network Termination
PAM	PacketCable Application Manager
PCB	Physical Control Block
PCC	Policy Control and Charging
PCEF	Policy and Charging Enforcement Function
PCRF	Policy and Charging Rules Function
P-CSCF	Proxy CSCF
PD-FE	Policy Decision Functional Entity
PE-FE	Policy Enforcement Functional Entity
PDP	Policy Decision Point

PDU	Protocol Data Unit
PEP	Policy Enforcement Point
PLOAM	Physical Layer OAM message
PON	Passive Optical Network
PPP	Point-to-Point Protocol
PSTN	Public Switched Telephone Network
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
RAA	Re-Auth-Answer
RACF	Resource and Admission Control Function
RACS	Resource and Admission Control Subsystem
RAR	Re-Auth-Request
RFC	Request For Comment
ROSE	Remote Operations Service Element
rtPS	Real-Time Polling Service
SFID	Service Flow Identifier
SGW	Serving Gateway
SID	Service Identifier
SLA	Service Level Agreement
SMASE	Systems Management Application Service Element
SNMP	Simple Network Management Protocol
STA	Session Termination Answer
STR	Session Termination Request
T-CONT	Traffic Container
TCP	Transmission Control Protocol
TDM	Time-Division Multiplexing
TDMA	Time Division Multiple Access
TISPAN	Telecommunications and Internet converged Services and Protocols for Advanced Networking
TMN	Telecommunications Management Network
TOS	Type of Service
UBR	Unspecified Bit Rate
UCD	Upstream Channel Descriptor
UDA	User-Data-Answer
UDP	User Datagram Protocol
UE	User Equipment
UGS	Unsolicited Grant Service
UGS-AD	Unsolicited Grant Service with Activity Detection
UPF	User Port Function
UNI	User-to-Network Interface
VBR-nrt	Variable Bit Rate – non real time
VBR-rt	Variable Bit Rate – real time
VC	Virtual Circuit
VDSL	Very High Speed DSL
VI	Video
VLAN	Virtual LAN

VO	Voice
VoIP	Voice over IP
VP	Virtual Path
VPN	Virtual Private Network
WDM	Wavelength Division Multiplexer
WiFi AP	Wireless Fidelity Access Point
WiMAX	Worldwide Interoperability for Microwave Access
XML	eXtensible Markup Language

5 Wireline Technologies

5.1 Digital Subscriber Line (DSL) Access Network

5.1.1 Reference Architecture

Figure 1 illustrates the DSL Access Network architecture based on the Ethernet-based DSL aggregation network architecture described in [TR-101]. The FEs are distributed among the Regional Broadband Network, the Access Node, and the Customer Premises Network. The interfaces of interest are between the Customer Premises Network and the Access Node (the U interface), and the policy control interface into the Broadband Network Gateway (BNG). Policy control in the DSL Access Network is based on the specifications found in [Y.2111], [TR-058], and [TR-059].

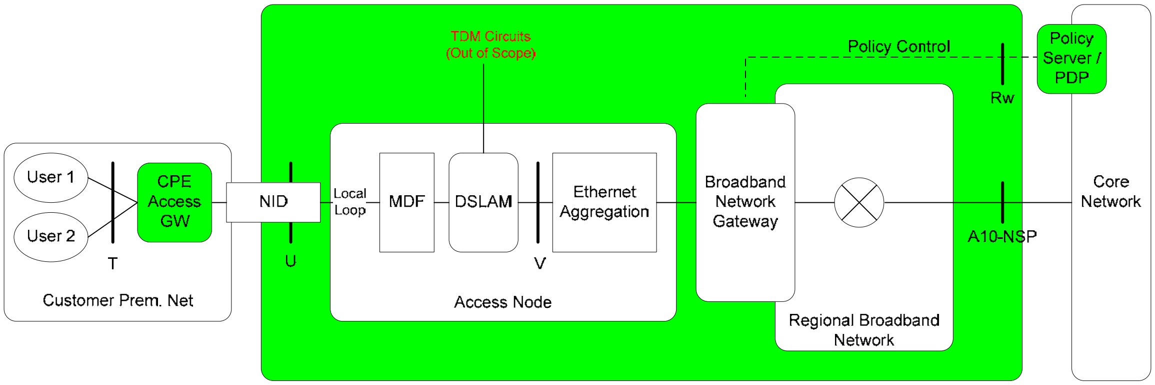


Figure 1 - DSL Access Network Architecture

The core set of specifications for Ethernet-based DSL aggregation are contained in [TR-101]. The Technical Report outlines an Ethernet-based aggregation network architecture. It provides an architectural/topological model and describes requirements for protocol translation and interworking, QoS, multicast, security, and operations, administration and maintenance (OAM) for a DSL aggregation network.

5.1.1.1 Functional Entities

5.1.1.1.1 Access Node

The Access Node encompasses the FEs of the Ethernet-based DSL network that connects the Network Interface Device (NID) at the customer premises to a BNG in an intermediate network or in the Network Service Provider network. The Access Node includes the DSL termination at the Digital Subscriber Loop Access Multiplexer (DSLAM) and may include an Ethernet Aggregation function.

5.1.1.1.2 Customer Premises Network

The Customer Premises Network consists of one or more CPE Access Gateways and the associated Users' UEs. This paragraph provides a more generic description of the CPE Access Gateway connecting a user to a Service Provider's Access Network via the User-to-Network Interface (UNI). The fundamental component of the CPE Access Gateway is the DSL modem attached to the end user's equipment associated with a single subscriber line. The (optional) telephone set that the end user uses to make voice calls also connects to the CPE Access Gateway. The data stream from the DSL modem and the voice stream from the telephone both traverse the local loop from the end user's premises to the Access Node. The two streams are differentiated on the loop by frequency; voice uses the lower frequencies on the loop and data uses the higher frequencies on the loop. In addition, the CPE Access Gateway includes the filter/splitter installed on the end user's premises to prevent interaction between the high-frequency DSL tones and the end user's telephone set.

5.1.1.1.3 Network Interface Device (NID)

The NID is a CPE device that performs interface functions, such as code conversion, protocol conversion, and buffering, required for communications to and from a network. The NID provides communication between the CPE Access Gateway and the Access Node. The NID may be a standalone device or may be integrated with the CPE Access Gateway.

5.1.1.1.4 Main Distribution Frame (MDF)

The MDF is the first point of connection inside the Access Node, providing physical connectivity between the access loop and the DSLAM.

5.1.1.1.5 Digital Subscriber Line Access Multiplexer (DSLAM)

The DSLAM terminates and multiplexes end user input using IP and performs the corresponding demultiplexing for downstream traffic. DSL termination and multiplexing functions may be integrated or may be performed in separate equipment. Each subscriber line is connected to a modem in the DSLAM, where the signaling and bearer to and from the corresponding end user undergoes protocol conversion as needed.

The DSLAM also separates the end user's voice traffic, which is delivered to the PSTN switch, from the data traffic, which is provided as part of an aggregated stream to the Ethernet Aggregation function. Similarly, for downstream traffic, the DSLAM performs the necessary protocol conversion and passes the voice traffic to the end user in the low frequency range and the data traffic in the high frequency range. DSLAM management may occur through communication with a Policy Server/Policy Decision Point (PDP) and/or Policy Enforcement Point (PEP).

5.1.1.1.6 Ethernet Aggregation

The Ethernet Aggregation function collects the Ethernet input from multiple DSLAMs for delivery to the Broadband Network Gateway (BNG).

5.1.1.1.7 Broadband Network Gateway (BNG)

The BNG is an IP edge router at the border of a Regional Broadband Network. At the BNG, the admission control and the QoS policies of the network are applied. The BNG is also the aggregation point for outbound subscriber traffic. BNG functionality includes subscriber management, advanced IP processing (including IP QoS), and enhanced traffic management capabilities. A PEP in the BNG is responsible for traffic policy enforcement of all traffic types in the BNG. Policy enforcement may be applied at an IP session, IP flow, and/or aggregate level.

5.1.1.1.8 Regional Broadband Network

The Regional Broadband Network interconnects a Core Network and an Access Node. Typically more than one Access Node is connected to a common Regional Broadband Network. Similarly, multiple Core Networks may be connected to a common Regional Broadband Network. Because of the commonality of requirements for a BNG in a Regional Broadband Network and in a Core Network, this TR does not distinguish between these two network types.

5.1.1.1.9 Policy Server/Policy Decision Point (PDP)

The Policy Server/PDP is a functional entity making decisions on subscriber policies on an IP Session, IP Flow, and an aggregate basis. For this TR, there are four possible reference models for the Policy Server/PDP:

- The International Telecommunication Union – Telecommunication Standardization Sector (ITU-T) Resource and Admission Control Function (RACF) architecture [Y.2111].
- The 3GPP Policy and Charging Control (PCC) architecture.
- The European Telecommunications Standards Institute (ETSI) Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN) Resource and Admission Control Subsystem (RACS).
- The Broadband Forum Fixed-Mobile Convergence (FMC) model.

Functionally, the ITU-T RACF and 3GPP PCC architectures are similar; the main difference is in the consolidation versus distribution of the interfaces and the protocols used. The Broadband Forum FMC interworking architecture uses the 3GPP S9 interface, and is a natural extension of PCC. Many of the existing wireline access components communicate via COPS, not Diameter, making the ITU-T RACF architecture more appropriate for a DSL Access Network. For example, the interface from the Policy Server/PDP to the Application Function for a DSL Service Provider is expected to be the 3GPP Rx interface or the ITU-T Rs interface. In addition, the ITU-T Rw interface from the Policy Server/PDP to the BNG is assumed, with the modification that an ITU-T Resource and Admission Control Function (RACF) rather than a Radius Authentication, Authorization, and Accounting (AAA) server is used.

The Policy Server/PDP is independent of the Core Network and can be used with non-IMS FEs; however, this section assumes the Policy Server/PDP is located at the border of the DSL Access Network and the Core Network. A Policy Server/PDP may manage multiple Policy Enforcement Points (PEPs) (in their separate BNGs), coordinating what policies should be enforced at the BNG. The PEP may implement static policies which it obtains from the Policy Server/PDP. These may apply to all IP flows at the BNG or may apply only to a given IP flow. For further details, refer to [TR-058] and [TR-059 .

5.1.2 Call/Session Flows

For call/session flows associated with a DSL Access Network, refer to ATIS-1000049.

5.1.3 Interfaces & Protocols

This section is informative and paraphrases information that is described in more detail in the relevant standards. It is provided as background information for readers of this TR.

This section provides the protocols, messages, and parameters for the signaling interfaces between the FEs. Section 5.1.3.1 discusses the U interface between the CPE and the DSLAM (at the NID, via the MDF). Section 5.1.3.2 discusses the V interface between the DSLAM and the Broadband Network Gateway (via the Ethernet Aggregation function). Note that for the purposes of this section, the A-10 interface uses the same protocols and procedures as the V interface. Section 5.1.3.3 discusses the interface between the Policy Server/PDP and BNG, and the interface between the Policy Server/PDP and Core Network.

5.1.3.1 CPE Access Gateway – DSLAM

The six protocol architectures with IP as the top-layer protocol identified for the U interface in [TR-101] are shown in Figure 2.

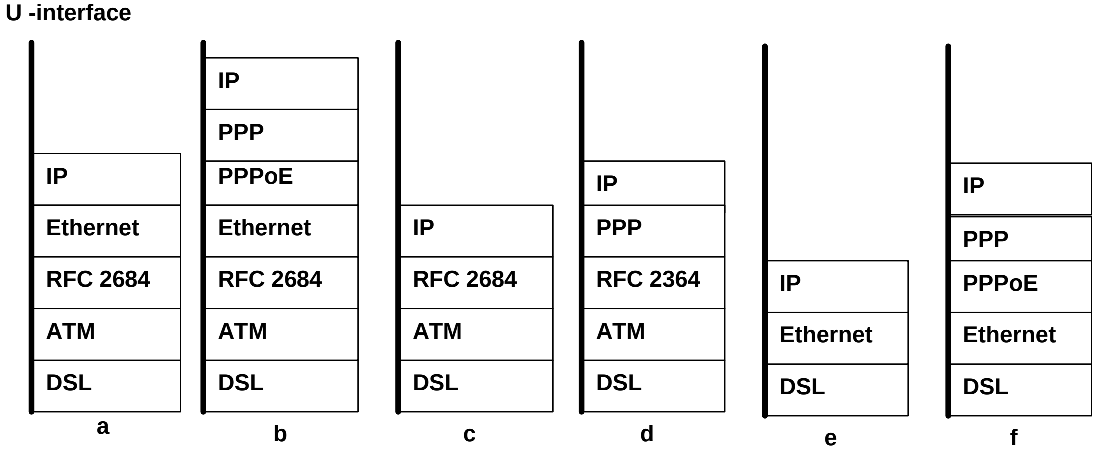


Figure 2 - Protocol Architectures at the NID – DSLAM (U) Interface

The physical layer protocols identified in [TR-101] include:

- Asymmetric DSL (ADSL) – ITU-T G.992.1
- ADSL2 - ITU-T G.992.3
- ADSL2plus - ITU-T G.992.5
- Very High Speed DSL (VDSL2) - ITU-T G.993.2
- Bonding of multiple DSL pairs – ITU-T G.998.1 (Asynchronous Transport Mode (ATM) transport) and ITU-T G.998.2 (Ethernet transport).

As can be seen in Figure 2 the DSLAM must be capable of receiving Ethernet, ATM, or Ethernet over ATM, and must be capable of handling Point-to-Point Protocol (PPP) as an intermediate layer below the IP.

5.1.3.2 DSLAM - Broadband Network Gateway

The V interface was defined to provide the capabilities of traffic aggregation, class of service distinction, and user isolation and traceability. To meet these requirements, [TR-101] specifies the V interface as a tagged Ethernet interface (also known as an 802.1ad compliant provider network port). The protocol architectures identified for the V interface in [TR-101] are shown in Figure 3.

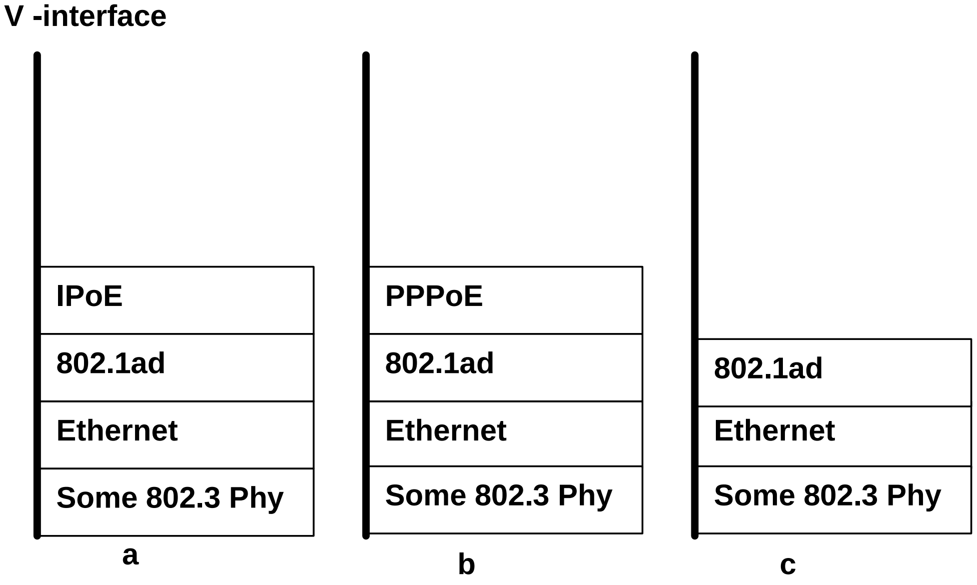


Figure 3 - Protocol Architectures at the DSLAM – BNG (via Ethernet Aggregation) (V) Interface

The functions of interest at the V interface include:

- Class of Service distinction.
- User isolation and traceability.

5.1.3.3 Policy Server/PDP-Based Interfaces

The Diameter protocol is recommended across the following interfaces, as defined in the 3GPP PCC architecture [TS 23.203] and the ITU-T RACF architecture [Y.2111]:

- The 3GPP Rx reference point can be used as reference for the definition of the interface between the Policy Server/PDP and the P-CSCF.
- The ITU-T Rw reference point [Q.3303.3] is expected to be used between the Policy Server/PDP and the BNG.

5.1.3.3.1 Core Network – Policy Server/PDP Interface

The Core Network – Policy Server/PDP interface is identical to the Rx reference point specified in [TS 29.214].

This interface enables transport of application level session information from a Core Network (i.e., P-CSCF) to a Policy Server/PDP. Such information includes, but is not limited to:

- Information to identify the service media/data flow for policy control and/or differentiated charging.
- Media/application bandwidth requirements for QoS control.

5.1.3.3.1.1 Diameter Messages

The following messages are used at this interface:

- *AA-Request (AAR)*: An AAR is sent by a P-CSCF to a PCRF to provide Session Information.
- *AA-Answer (AAA)*: An AAA is sent by a Policy Server/PDP to a P-CSCF in response to an AAR.
- *Re-Auth-Request (RAR)*: An RAR is sent by a Policy Server/PDP to a P-CSCF to indicate an Rx specific action.
- *Re-Auth-Answer (RAA)*: An RAA is sent by a P-CSCF to a Policy Server/PDP in response to an RAR.

- *Session-Termination-Request (STR)*: An STR is sent by a P-CSCF to a Policy Server/PDP to indicate that an established session is to be terminated.
- *Session-Termination-Answer (STA)*: An STA is sent by a Policy Server/PDP to a P-CSCF in response to an STR.
- *Abort-Session-Request (ASR)*: An ASR is sent by a Policy Server/PDP to a P-CSCF to indicate that bearer for the established session is no longer available.
- *Abort-Session-Answer (ASA)*: An ASA is sent by a P-CSCF to a Policy Server/PDP in response to an ASR.

5.1.3.3.1.2 Diameter AVPs

The AVPs as defined in [TS 29.214] may be used at this interface.

5.1.3.3.2 Policy Server/PDP Interface - Broadband Network Gateway Interface

The Policy Server/PDP interfaces with a PEP in a BNG using the Rw policy control interface defined in [Q.3303.3].

This interface enables a Policy Server/PDP to have dynamic control over the policy and charging functions within the DSL Access Network.

5.1.3.3.2.1 Diameter Messages

The following messages are used at this interface:

- *CC-Request (CCR)*: A CCR is sent from a BNG to a Policy Server/PDP to indicate bearer or Policy Control and Charging (PCC) rule related events or the termination of the DSL Access Network bearer and/or session.
- *CC-Answer (CCA)*: A CCA is sent by a Policy Server/PDP to a BNG in response to a CCR command. CCA is used to provision PCC rules and event triggers for the bearer/session and to provide the selected bearer control mode for the DSL Access Network session. If a Policy Server/PDP performs the bearer binding, then PCC rules are provisioned at bearer level.
- *Re-Auth-Request (RAR)*: An RAR is sent by a Policy Server/PDP to a BNG to provision PCC rules to initiate the provision of unsolicited PCC rules. An RAR is used to provision PCC rules and event triggers for the session. If the Policy Server/PDP performs the bearer binding, then PCC rules are provisioned at the bearer level.
- *Re-Auth-Answer (RAA)*: An RAA is sent from a BNG to a Policy Server/PDP in response to an RAR command.

5.1.3.3.2.2 Diameter AVPs

The AVPs as defined in [Q.3303.3] may be used at this interface.

5.1.4 QoS & Policy Mechanisms

In DSL, QoS is associated with traffic flows. A flow is defined as a bidirectional (two-way) transmission of traffic. Packets can be classified into specific flows based on:

- DSCP.
- Incoming port/interface.
- Source IP address.
- Source Fully Qualified Domain Name (FQDN).
- Destination IP address.
- IP protocol.
- Source TCP/UDP port.
- Destination TCP/UDP port.

5.1.4.1 DSL Network Policy Model

The DSL Network Policy Model contains the following elements:

- *ProtocolClassifier (Abstract)* – This element has a single attribute, named "direction", which indicates the direction of traffic that this condition applies to. Values include up (from user to network), down (from network to user), and up-down (both from user to network and from network to user).
- *IPClassifier* – This element is used to match packet flows based on their IP header 5-tuple (source IP and port, destination IP and port, protocol, priority, and DSCP/COS mask). An instance may only partially specify some of these attributes, with wildcards used for the non-specified attributes.
- *SessionClassifier* – This element is used to match packets in the context of a Session (e.g., PPP session or IP session) in the BNG.
- *ATMClassifier* – This element is used to match traffic flowing over a specific Virtual Path (VP) or Virtual Circuit (VC) in an ATM access network.
- *MAC8021Classifier* – This element is used to match traffic flowing over a specific Virtual Local Area Network (VLAN) stack in an Ethernet access network.
- *DPIClassifier* – This element is used to match traffic according to layer 4 through 7 application recognition capabilities.
- *MPLSClassifier* – This element is used to match traffic with a specific MultiProtocol Label Switching (MPLS) label stack.

The policy actions that can be associated with a classifier are:

- *Police* – Traffic matched by the policy rule is policed according to the specified attributes (normal rate, burst rate, exceed rate, conform action, exceed action).
- *StrictRate* – Traffic matched is put into a strict priority queue providing a bandwidth rate defined by the rate attribute.
- *RelativeRate* – Traffic matched is put into a queue that receives a portion of the available bandwidth defined by the percent attribute.
- *Shape* – Traffic matched is shaped according to the rate attribute.
- *Mark* – Traffic matched is marked with the specified DSCP/COS value.
- *Drop* – Traffic matched is discarded.
- *Forward* – Traffic matched is sent.
- *Redirect* – Describes a layer 3 redirect function. Traffic matched is rerouted to the specified destination address.
- *NextInterface* – Traffic matched is forwarded through the egress interface specified by the next interface attribute.

5.1.4.2 Layer 2 & Layer 3 QoS Mapping

[TR-098] provides mappings between layer 2 and layer 3 QoS parameters, as shown in Table 1.

Table 1 - Layer 2 to Layer 3 QoS Mapping

Layer 2			Layer 3	
ATM Class	**Ethernet Priority**	**Designation**	**DSCP**	**Per Hop Behavior**
UBR	001	Background (BK)		
	010	spare		
UBR	000	Best Effort (BE)	0x00	Default CS0
UBR	011	Excellent Effort (EE)	0x0e 0x0c 0x0a 0x08	AF13 AF12 AF11 CS1
VBR-nrt	100	Controlled Load (CL)	0x16 0x14 0x12 0x10	AF23 AF22 AF21 CS2
VBR-nrt	101	Video (VI)	0x1e 0x1c 0x1a 0x18	AF33 AF32 AF31 CS1
VBR-rt	110	Voice (VO)	0x26 0x24 0x22 0x20	AF43 AF42 AF41 CS4
CBR	110	Voice (VO)	0x2e 0x28	EF CS5
CBR	111	Network Control (NC)	0x30 0x38	CS6 CS7

Background traffic is non-time-critical and loss insensitive, and has lower priority than best effort. Best effort is also non-time-critical and loss insensitive, and is how traffic is normally handled. Controlled load is non-time-critical but loss sensitive. Excellent effort is also non-time-critical but loss sensitive, but of lower priority than controlled load. Video is time-critical, characterized by less than 100 ms delay. Voice is also time-critical, but is characterized by less than 10 ms delay. Network control is both time-critical and safety-critical, consisting of traffic needed to maintain and support the network infrastructure.

5.2 Fiber Access Network

Fiber to the x (FTTx) is a telecommunications network architecture that uses optical fiber to replace all or part of the copper local loop. In Fiber to the Node (FTTN) and Fiber to the Curb (FTTC), fiber-optic cables run to a cabinet serving a neighborhood and customers connect to the cabinet using coaxial cable or twisted pair wiring. FTTN and FTTC are similar to DSL and PacketCable subsystems and are not addressed further in this section.

Fiber to the Premises (FTTP) includes both Fiber to the Building (FTTB) and Fiber to the Home (FTTH). FTTP typically employs a Passive Optical Network (PON), a point-to-multipoint architecture allowing a single optical fiber to service a minimum of 32 premises. The PON consists of an Optical Line Termination (OLT) at the service provider’s central office and an Optical Network Termination (ONT) located at the customer’s premises. The OLT connects to the ONT by way of an Optical Distribution Network (ODN).

5.2.1 Reference Architecture

A reference architecture for fiber, based on the ITU-T G.983 standard, is shown in Figure 4. The reference architecture refers to an Access Node Management System (ANMS) for control of the OLT and ONT. The ANMS is assumed to be located on the border between the fiber access network and the Core Network, and provides the Policy Decision Point (PDP) functionality that is enforced by the Policy Enforcement Points (PEPs) located in the OLT and ONT.

The OLT, ODN, and ONT from the PON reference architecture can be used in place of the NID, MDF, and DSLAM in a Broadband Forum's Access Node within the DSL Access Network Architecture. Figure 5 shows this configuration, which is based on [TR-156].

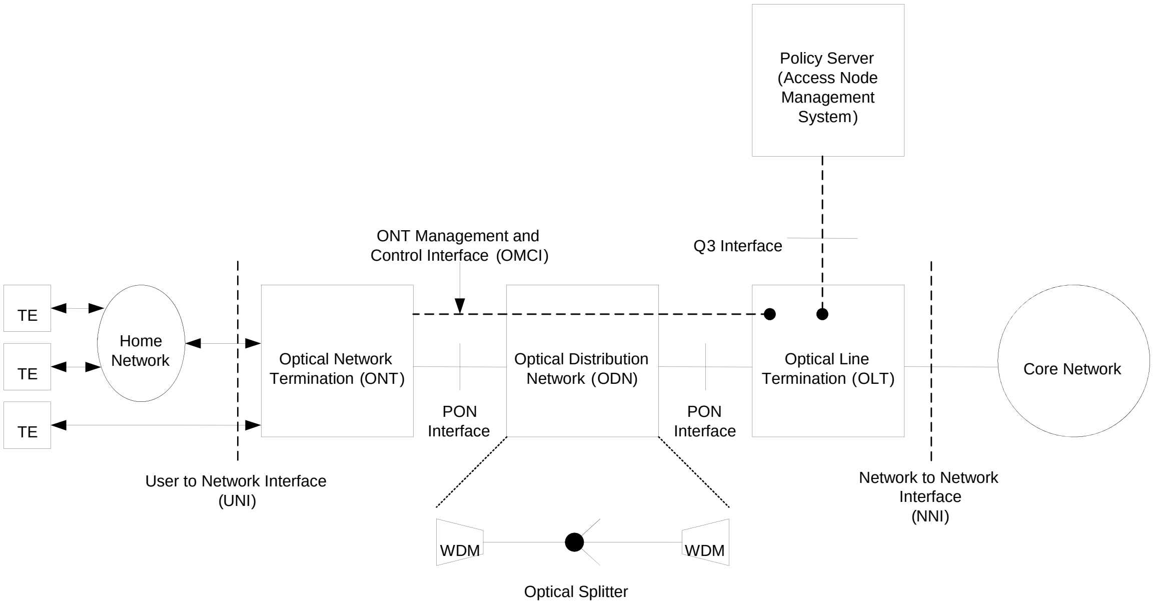

Policy Server (Access Node Management System)
Q3 Interface
ONT Management and Control Interface (OMCI)
TE
TE
TE
Home Network
Optical Network Termination (ONT)
Optical Distribution Network (ODN)
Optical Line Termination (OLT)
Core Network
PON Interface
PON Interface
User to Network Interface (UNI)
Network to Network Interface (NNI)
WDM
WDM
Optical Splitter

Figure 4 - Fiber Reference Architecture

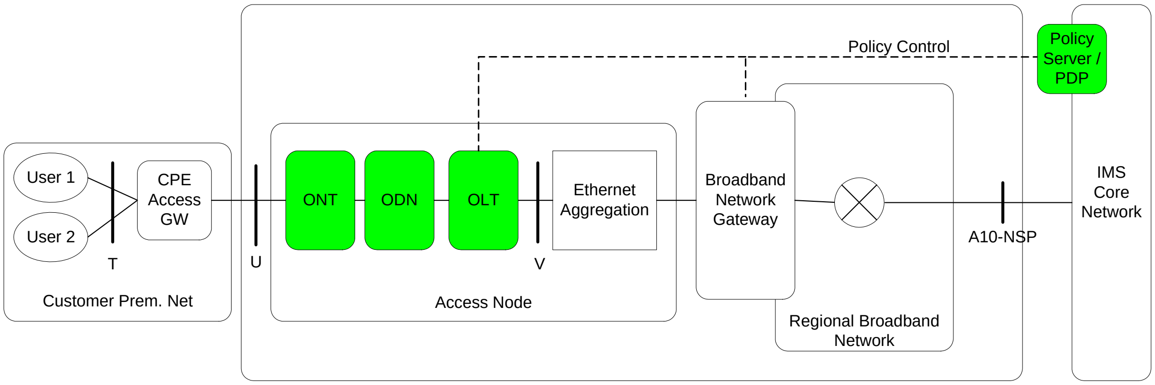


Figure 5 - Use of PON in the DSL Access Network

The two active functional entities, the OLT and the ONT, are defined in the following standards:

- IEEE 802.3ah defines the FEs for an Ethernet PON (EPON) and a Gigabit Ethernet PON (GEPON).
- IEEE 802.av defines the FEs for a 10 Gigabit Ethernet PON (10GEPON).
- ITU-T G.983 defines the FEs for an ATM Passive Optical Network (APON) and a Broadband PON (BPON).

- ITU-T G.984 defines the FEs for a Gigabit PON (GPON).

For purposes of this TR, ITU-T G.983, G.984, and IEEE 802.3ah are assumed as baseline standards.

5.2.1.1 OLT

The Optical Line Termination (OLT) provides a broadband data transport service over the PON. Downstream signals are broadcast to each premises' ONT sharing the fiber; encryption is used to prevent eavesdropping. Upstream signals are combined using either Time Division Multiple Access (TDMA) or Wavelength Division Multiplexing (WDM). The OLT "ranges" each ONT in order to provide the upstream time slot assignments, since the transmission delay from each ONT can be unique. The OLT measures delay and sets a register in each ONT to equalize delay among the ONTs.

The OLT transmits a grant, a permission to use a defined interval of time for upstream transmission, to each ONT. The OLT maintains a grant map, which is dynamically recalculated every few milliseconds.

5.2.1.2 ONT

The Optical Network Termination (ONT) is the Customer Premise Equipment (CPE) device used in conjunction with the OLT to provide broadband data transport service over the PON.

5.2.1.3 Access Node

The combination of ONT and OLT is sometimes viewed (e.g., for management purposes) as a single system, referred to as an Access Node (AN). The Access Node Management System manages that abstract entity by physically connecting to the OLT. The OLT and ONT communicate, for management purposes, via the ONT Management and Control Interface (OMCI).

5.2.1.4 ODN

The Optical Distribution Network (ODN) provides physical connectivity between the ONT and the OLT. It is made up of wavelength division multiplexers[8], fiber optic cable, and unpowered optical splitters. An OLT will generally connect many ODNs, the set of which is referred to as the Optical Access Network (OAN).

5.2.1.5 Access Node Management System

The Access Node Management System manages the Access Nodes (OLT and ONT) via aQ3 interface as defined in [Q.812].

5.2.2 Call/Session Flows

For call/session flows associated with a Fiber Access Network, refer to ATIS-1000049.

5.2.3 Interfaces & Protocols

This section is informative and paraphrases information that is described in more detail in the relevant standards. It is provided as background information for readers of this TR.

[8] The PON uses different wavelengths in the upstream and downstream direction.

5.2.3.1 Diameter - Based Interfaces

The ITU-T RACF architecture may be more appropriate for the interface from the ANMS to the Application Function. However, the 3GPP Rx interface is assumed to be consistent with IMS Core Network requirements. This Diameter-based interface is described in an earlier section.

5.2.3.2 Q3 Interface

The Q3 interface is defined in [Q.812]. The protocol stack for the Q3 interface for the interactive class of service is shown in Figure 6. In this figure, the Systems Management Application Service Element (SMASE) communicates with lower layer protocols through either the Association Control Service Element (ACSE) protocol or through the Common Management Information Service Element (CMISE)/Remote Operations Service Element (ROSE) protocols.

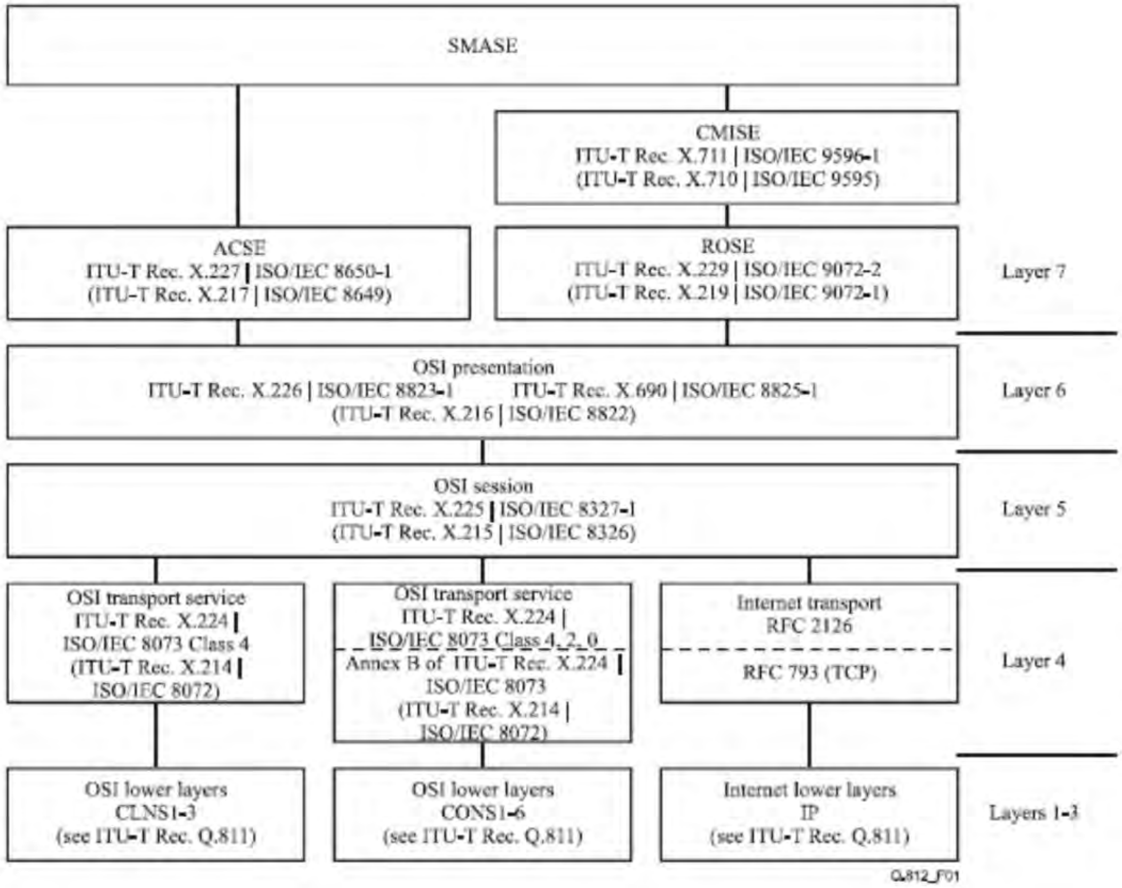


Figure 6 - Q3 and OMCI Interface Protocol Stack

5.2.3.3 ONT Management & Control Interface (OMCI)

In GPON Encapsulation Method (GEM) Mode, each ONT management and control protocol packet is encapsulated directly in a GEM packet. The packet format is:

- *GEM header* (5 bytes) – Contains the PortID of the OMCC for the addressed ONT.
- *Transaction correlation identifier* (2 bytes) – For request messages, the OLT selects any transaction identifier. A response message carries the transaction identifier of the message to which it is responding.
- *Message type* (1 byte).
- *Device identifier* (1 byte).

- *Message identifier* (4 bytes).
- *Message contents* (32 bytes).
- *OMCI trailer* (8 bytes).

In order to handle messages associated with higher priority requests, a two level priority mechanism exists within the ONT management and control protocol. Figure 7 shows the entities within the ONT to process the two priority levels of the protocol.

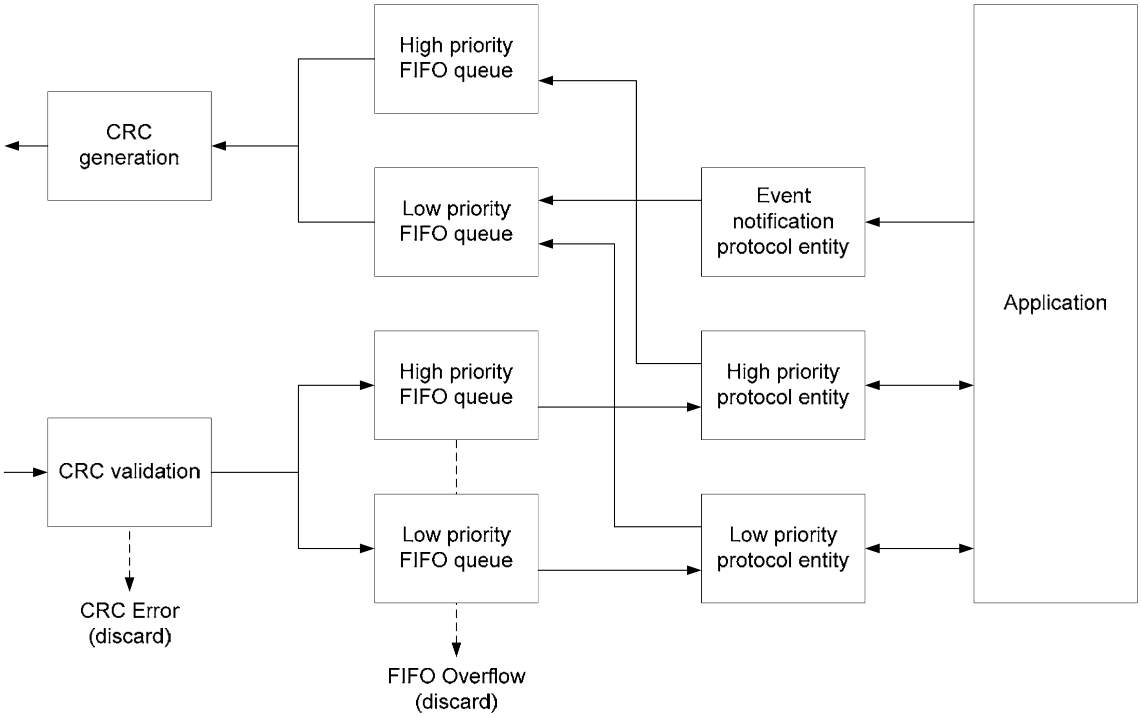


Figure 7 - Protocol Entities within the ONT

5.2.3.4 ITU-T G.984 Series GPON QoS Mechanisms

5.2.3.4.1 Physical Layer

GPON supports up to 64 ONTs on the fiber from a single OLT interface.

5.2.3.4.2 MAC Layer

Data is mapped onto the GPON physical layer through the GPON Transmission Convergence (GTC) layer.

The downstream GTC frame is 125 microseconds long, and consists of the following fields:

- *Physical Control Block (PCB)*:
  - Frame Alignment Pattern.
  - Identity.
  - Physical Layer OAM message (PLOAM).
  - Frame Error Check.
  - Downstream Payload Length Field.
  - Upstream Bandwidth Map Field.
- *Native ATM Cell Payload* (may be null).
- *GPON Encapsulation Method (GEM) Payload*.

The Upstream Bandwidth Map Field specifies the start and stop times of the Allocation IDs in the bursts within the 125 microsecond upstream frame window. The start and stop times are typically specified in units of bytes from the beginning of the frame.

The upstream GTC frame consists of the following fields:

- Preamble, Delimiter and Frame Check transmitted by an ONT at the beginning of its upstream transmission burst.
- ONT Identifier.
- Upstream Indicator for ONT status reporting.
- PLOAM message, if requested by the OLT.
- Dynamic Bandwidth Report (DBR) for a specific Allocation ID, if requested by the OLT.
- Payload for that specific Allocation ID.
- DBR and Payload for additional Allocation IDs.

Transmission Containers (T-CONTs) are defined in ITU-T G.983.4. There are five T-CONT types defined:

- *T-CONT Type I* is characterized by fixed bandwidth only. It has the highest priority in being satisfied when assignable bandwidth becomes available and is used for delay sensitive traffic.
- *T-CONT Type II* is characterized by assured bandwidth only. Assured bandwidth is defined as a fixed average bandwidth over some specified time interval. Type 2 only guarantees the average transmission rate, while Type 1 guarantees packet transfer delay and delay variation. Type 2 has the second highest priority in being satisfied.
- *T-CONT Type III* has assured bandwidth and non-assured bandwidth. T-CONT Type 3 is allocated bandwidth equivalent to its assured bandwidth only when it has a traffic queue equivalent to or greater than its assured bandwidth. Non-assured bandwidth is allocated across all T-CONTs with assured bandwidth that are requesting additional bandwidth in proportion to the assured bandwidth of the individual T-CONTs – e.g., weighted round robin method. The sum of the assured and non-assured bandwidth allocated to a T-CONT will not exceed its maximum bandwidth, which is a provisioned value. Type 3 has the third highest priority in being satisfied.
- *T-CONT Type IV* has best-effort bandwidth only. Best effort bandwidth is allocated to each T-CONT Type 4 equally – e.g., based on the round robin method, up to the maximum bandwidth. Type 4 has the lowest priority in being satisfied.
- *T-CONT Type V* is a superset of all T-CONT types, and can be downgraded to one or more of the other T-CONT types.

T-CONTs are identified by an Allocation ID. The OLT makes bandwidth assignments to an ONT on a per Allocation ID basis, where an ONT can have one or more Allocation IDs. The OLT controls the bandwidth and QoS of each Allocation ID by the number of upstream time slots assigned to the T-CONT.

Fixed and assured bandwidths are known as guaranteed bandwidth. Non-assured and best effort bandwidths are known as additional bandwidth. Surplus bandwidth is defined as the additional bandwidth minus bandwidth allocated for control, such as OAM. The surplus bandwidth is available for dynamic bandwidth assignment (DBA).

Two different DBA mechanisms are defined in G.983.4:

- *In the non-status reporting (NSR) strategy*, the OLT monitors the amount of bandwidth each ONT is using, based on the number of idle frames it receives in the upstream GTC frames. More bandwidth is assigned to an ONT if its bandwidth utilization exceeds a predefined threshold.
- *In the status reporting (SR) strategy*, a quick indication of a need for more bandwidth in a T-CONT type is communicated in the Upstream Indicator field. A more detailed report of the per T-CONT buffer status is communicated in the upstream dynamic bandwidth reports. The OLT uses the status report information to determine the appropriate bandwidth allocation for each Allocation ID.

An OLT can also use a hybrid approach for DBA.

5.2.4 Policy Control of the GPON

There is today no direct policy control of or policy enforcement within the GPON. For this TR, the following policy control process is assumed.

At subscription time (for public service), resources in the GPON are assigned to the user and associated policy is created in the Policy Server. For example, a subscriber may be given the right to have up to 5 simultaneous telephone calls. In support of these, a flow is created through the GPON, associated with the Type-II T-CONT, and mapped via the ONT User Port Function (UPF) to an interface accessible to the customer's terminal equipment (TE). Rules are also instantiated in the Policy Server to ensure that the terms of the Service Level Agreement (SLA) are upheld (e.g., that no more than five simultaneous calls are established). Finally, ”traffic conditioning” functions (packet marking and policing rules) are instantiated at the ONT and OLT.

When the subscriber attempts to establish a session, the signaling is carried via a ”data” flow (e.g., belonging to type-III T-CONT), through the GPON, and into the Core Network. The P-CSCF receives this request and invokes policy controls in the Policy Server to verify that it should be allowed.

If the request is authorized by the Policy Server, and is successful in establishing connectivity to the called party, the media path is then mapped to the Type-II T-CONT in the UPF. This ensures that the GPON queuing and scheduling mechanism provide the appropriate QoS.

To support direct policy control of or policy enforcement within the GPON, the ANMS will need to be upgraded to a real-time Policy Server, and will need to contain the following functions:

- *Final decision point*: The ANMS will make the final admission decision for media flows of a given service based on network policy rules, service information, transport subscription information, and decision on resource availability.
- *QoS mapping*: The ANMS will map the service QoS parameters and priority received over the Rx interface to network QoS parameters and priority based on the network policy rules.
- *Gate control*: The ANMS will control the OLT and ONT to install and enforce the final admission decisions via the Q3 interface. The action to pass or drop IP packetsis based on a set of IP gates and transport interface identification information (e.g., VLAN ID) as needed.
- *IP packet marking control*.
- *Rate limiting control*.

The ANMS will make the final policy decisions and will provide sufficient information to make the OLT and ONT perform the resource control operation.

The ANMS will communicate via the following interfaces:

- The 3GPP Rx reference point [TS 29.214] will be used as reference for the definition of the interface between the ANMS and the P-CSCF. Alternatively, the ANMS may communicate with the P-CSCF via an intermediary PCRF using the 3GPP S9 reference point.
- The Q3 interface is used between the ANMS and the OLT.

5.2.5 QoS & Policy Mechanisms

5.2.5.1 Priority Indication in Fiber Access Networks

Packets in the GPON utilize the GPON Encapsulation Method (GEM). GEM is very efficient in terms of encapsulation overhead, and supports frame segmentation to improve QoS for jitter-sensitive traffic such as voice. Like ATM, the QoS class with which a GEM flow is associated (referred to as a Traffic Container or T-CONT) is maintained as state information at flow endpoints (ONT and OLT). It is not indicated in the packet overhead. Within the GEM frame there may be Ethernet and IP packets, with the priority markings (P-bit, DSCP) associated with those technologies. Such markings are carried transparently through the ODN.

Individual flows are identified in the GEM packet header either by Virtual Path and Virtual Channel identifiers (for ATM payloads) or port identifier (for variable length payloads). These identifiers are then associated with one of five standard T-CONTs at the flow endpoints.

Table 2 - GPON Traffic Container (T-CONT) Types

Type	Usage
I	Fixed bandwidth applications.
II	Variable bit rate applications that require bounded jitter and delay, e.g., video and voice over IP.
III	Variable bit rate applications that require bounded delay.
IV	Best Effort.
V	Combination of 2 or more of the above (implies more sophisticated scheduling – e.g., per microflow).

The only indication of priority in the GEM frame is the Payload Type Indicator, which distinguishes OAM frames from user data frames. QoS for user data frames is provided at the ONT and OLT based on the T-CONT with which the flow is associated.

5.2.5.2 Prioritization & QoS within the GPON

A GPON system can simultaneously provide both guaranteed bandwidth (TDM) and ”bursty” (statistically multiplexed) transport. Its means of doing so combines admission control and a system of ”grants” to allocate access to upstream (ONT-to-OLT) bandwidth.

The grant allocation mechanism reflects the priorities of the T-CONTs with which individual flows are associated. Traffic containers not requiring constant bandwidth can be over-subscribed, resulting in significantly higher utilization but necessitating sophisticated queuing and scheduling mechanisms in the ONT and OLT to provide the appropriate level of QoS.

5.2.5.3 IEEE 802.3ah Ethernet-based PON (EPON) QoS Mechanisms

While the ITU-T PON protocols are based on a 125 microsecond TDM frame, the EPON protocol consists of Ethernet MAC frames in the upstream and downstream directions. Whereas the ITU-T PON protocols can carry voice traffic and circuit emulation traffic in native mode, EPON relies on VoIP and Circuit Emulation Service (CES).

In EPON, each ONT is assigned a Logical Link ID (LLID). Multi-Point Control Protocol PDUs (MPCPDUs) are control frames used by the ONTs to make their requests for bandwidth, and by the OLT to assign it. MPCPDU have a higher priority than any data packet, ensuring that bandwidth requests and grants are sent in a timely manner.

The downstream signal in EPON is a stream of Ethernet frames and Idle characters. Upstream signaling is handled as follows. An ONT makes a bandwidth request in a Report MPCPDU, which the OLT grants via a GATE message. The Report message consists of a summary of the requests for upstream bandwidth, the specific amount of bandwidth it needs, how many of the eight 802.1Q priority queues have data to transmit, and the specific number of bits to transmit from each queue. The GATE message specifies the ONT upstream start time and the transmission length. Up to four upstream transmission grants can be made to a given ONT in a single GATE message.

5.3 PacketCable

PacketCable consists of a set of CableLabs specifications supporting the convergence of voice, video, data and mobility technologies. These specifications leverage open standards from 3GPP (IMS), IETF, and other Standards Development Organizations (SDOs). PacketCable specifications are available at
< www.packetcable.com >.

5.3.1 Reference Architecture

The PacketCable reference architecture is shown in Figure 8. It is based on the IMS architecture. The dashed boxes show the scope of this TR.

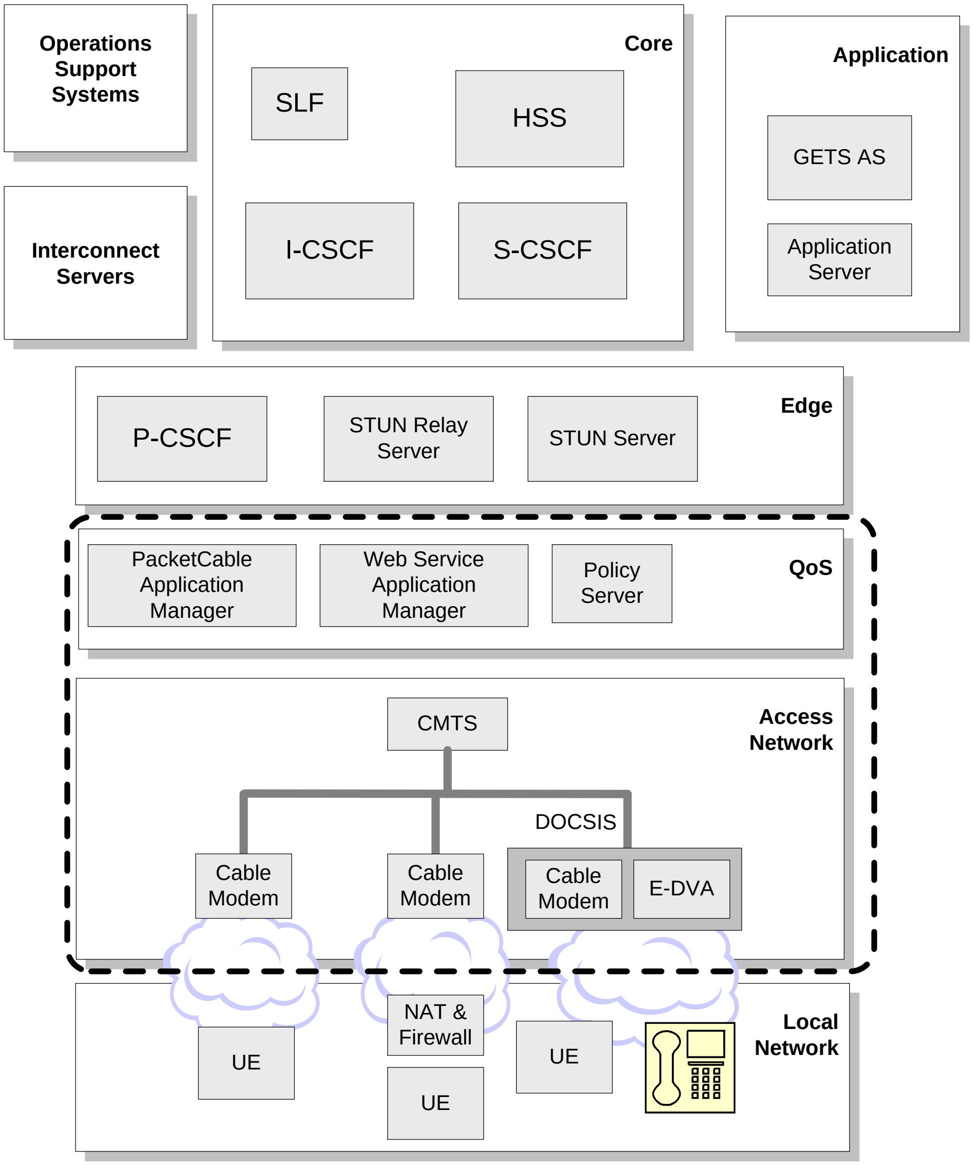


Figure 8 - PacketCable Reference Architecture

The PacketCable architecture is composed of several releases. This TR is based on the PacketCable 2.0 release, which supports SIP-based endpoints, and the PacketCable Multimedia release, which supports a service agnostic QoS and accounting framework.

5.3.2 Functional Entities

A description of all PacketCable Functional Entities can be found in the PacketCable 2.0 Architecture Framework Technical Report [PKT-TR-ARCH-FRM-V04-071106].

5.3.2.1 Cable Modem (CM)

The CM is Customer Premise Equipment (CPE) used in conjunction with the Cable Modem Termination System (CMTS) to provide broadband data transport service over the cable access network.

5.3.2.2 Embedded Digital Voice Adaptor (E-DVA)

The E-DVA is integrated into a cable modem and contains a VoIP adaptor. The E-DVA acts as a SIP UE to connect analog phones to the PacketCable 2.0 network.

5.3.2.3 Cable Modem Termination System (CMTS)

The CMTS provides broadband data transport service over the cable access network.

The CMTS is the Policy Enforcement Point (PEP) with respect to the Policy Server. Policies are enforced by Gates, a logical representation of the policy decision that has been installed on the CMTS. A Gate is unidirectional and is used to control access by a single IP flow. For a bidirectional IP session, two Gates are required, one for upstream and one for downstream.

5.3.2.4 Application Manager

PacketCable Multimedia defines Application Managers that calculate the bandwidth necessary from the session descriptor, determine the traffic scheduling type, and then determine the traffic classifiers for the signaling and media packets. Application Managers determine the number of flows necessary for the session and manage the association of the flows to the session. Application Managers are the Policy Decision Points (PDP) for the Service Control Domain. Two different Application Managers have been defined: PacketCable Application Manager and Web Service Application Manager.

5.3.2.4.1 PacketCable Application Manager

The PacketCable Application Manager interfaces with the PacketCable 2.0 P-CSCF and determines the QoS resources needed for a session based on the received session descriptors and manages the QoS resources allocated for a PacketCable 2.0 session.

5.3.2.4.2 Web Service Application Manager

The Web Service Application Manager [PKT-SP-MM-WS-I02-080522] provides a common Web Service interface, based on the Simple Object Access Protocol (SOAP)/eXtensible Markup Language (SOAP/XML), which enables an Application Server to dynamically request network resources on the cable operator's access network. The Web Service Application Manager determines the QoS resources needed for a session based on the received session descriptors and manages the QoS resources allocated for data sessions.

5.3.2.5 Policy Server

PacketCable Multimedia defines an IP-based platform for delivering QoS-enhanced services over Data Over Cable Service Interface Specification (DOCSIS) 1.1 or later. This platform provides QoS authorization and admission control, event messages for billing and other back-office functions, and security for UE communications. The Policy Server acts as an intermediary between Application Managers and CMTSes for QoS session management. It applies network policies to Application Manager requests and proxies messages between the Application Manager and CMTS. The Policy Server is the PEP with respect to the Application Manager and the PDP with respect to the CMTS.

5.3.2.6 Policy & Charging Rules Function (PCRF)

The PCRF is defined by 3GPP to encompass policy control decision and flow-based charging control functionalities. The PCRF provides network control regarding the service data flow detection, gating, QoS, and flow-based charging (except credit management) towards the Policy and Charging Enforcement Function (PCEF). PacketCable 2.0 implements this functionality in two logical entities, the PacketCable Application Manager and the PacketCable Policy Server.

5.3.3 Call/Session Flows

For call/session flows associated with a PacketCable Access Network, refer to ATIS-1000049.

5.3.4 Interfaces and Protocols

This section is informative and paraphrases information that is described in more detail in the relevant PacketCable and DOCSIS specifications. It is provided as background information for readers of this TR.

Figure 9 shows the reference point diagram for the reference points that are in-scope for this TR.

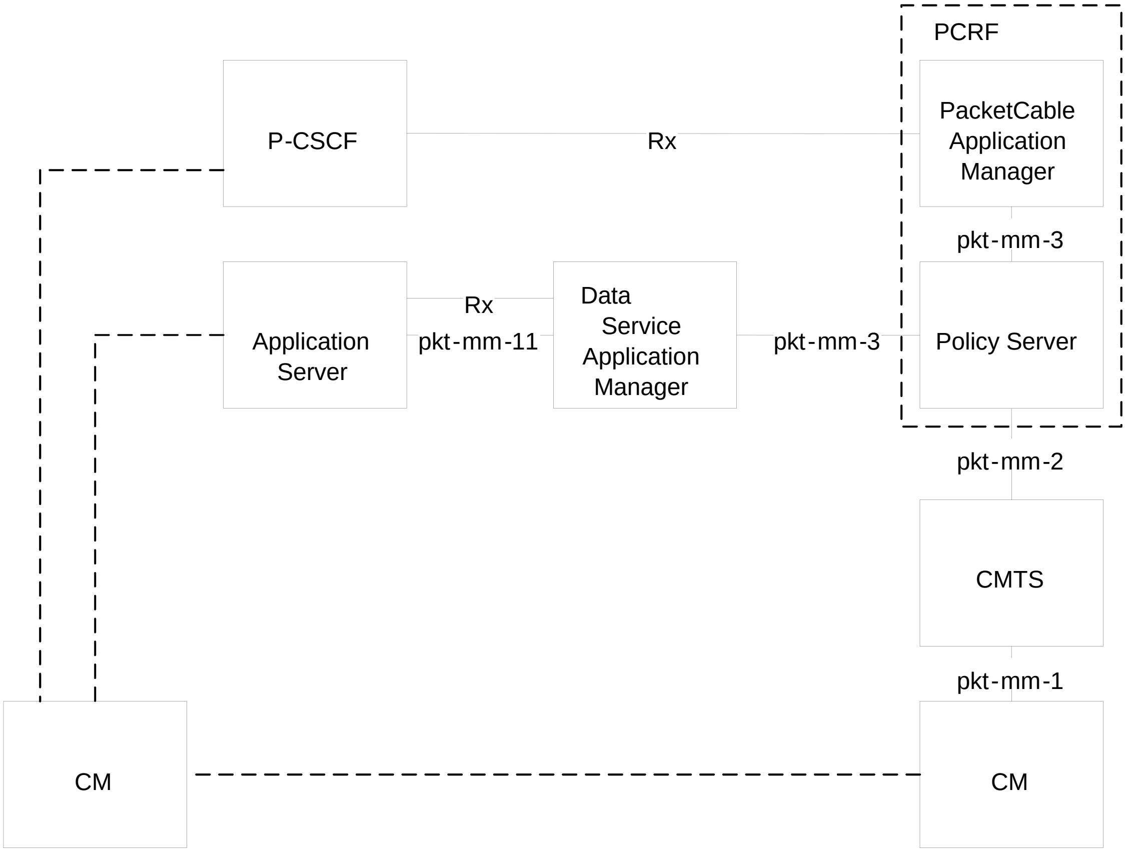


Figure 9 - Cable Access Reference Point Diagram

Table 3 lists the reference points and protocols that are considered in this TR. Certain reference points and protocols listed in this section may be consolidated in some system implementations.

Table 3 - PacketCable Reference Points and Protocols

Interface Endpoints	Reference Points	Protocols
o P-CSCF – PacketCable Application Manager o Application Server – Data Service Application Manager	Rx	This is the IMS Rx reference point that is used to request and release QoS resources for PacketCable 2.0 sessions. Diameter is used on this interface. This interface is specified in [PKT-SP-QOS-I02-080425].
o CM – CMTS	pkt-mm-1	The CMTS uses DOCSIS-defined Dynamic Service – Addition, Change, and Deletion (DSx) signaling messages to instruct the CM to setup, teardown, or change a DOCSIS service flow in order to satisfy a QoS request. This interface is specified in [PKT-SP-MM-I04-080522].
o Policy Server – CMTS	pkt-mm-2	This reference point controls policy decisions, which are pushed by the Policy Server onto the CMTS. This interface is specified in [PKT-SP-MM-I04-080522].
o PacketCable Application Manager – Policy Server o Data Service Application Manager – Policy Server	pkt-mm-3	This reference point is used by the PacketCable Application Manager to request the Policy Server to install a policy decision on the CMTS on behalf of the UE. This interface is specified in [PKT-SP-MM-I04-080522].
o Application Server – Data Service Application Manager	pkt-mm-11	This reference point is used by an Application Server to request and release QoS resources for generic service applications. SOAP/XML is used on this interface. This interface is specified in [PKT-SP-MM-WS-I02-080522].

5.3.4.1 Data over Cable Service Interface Specification (DOCSIS)

DOCSIS defines the physical and Media Access Control (MAC) layers for the Hybrid Fiber-Coaxial (HFC) cable network between the CM and CMTS.

5.3.4.1.1 Physical Layer

DOCSIS 1.1 specifies a channel width between 200 kHz and 3.2 MHz. Either 64-level Quadrature Amplitude Modulation (QAM) or 256-level QAM can be used for modulation of downstream data, and Quadrature Phase Shift Keying or 16-level QAM can be used for upstream modulation. DOCSIS 1.1 provides a downstream capability of 42.88 Mbps and an upstream capability of 10.24 Mbps.

5.3.4.1.2 MAC Layer

DOCSIS 1.1 uses Time Division Multiple Access (TDMA) for most of its transmission.

5.3.4.2 Diameter-Based Interfaces

Diameter is used on the Rx interface between the P-CSCF and the PacketCable Application Manager, and the Application Server and Data Service Application Manager. The Diameter-Based interfaces are described in an earlier section of this document.

5.3.5 QoS & Policy Mechanisms

5.3.5.1 Service Flows

The following discussion is taken from DOCSIS 3.0 MAC and Upper Layer Protocols Interface Specification [CM-SP-MULPIv3.0-I08-080522]. This information is unchanged from the DOCSIS 1.1 and DOCSIS 2.0 specifications.

The MAC layer is used to provide QoS for traffic on the access network. The principal mechanism for providing QoS is to classify packets into a (unidirectional) Service Flow and then to schedule those Service Flows according to a set of QoS parameters. Service Flows have a 32-bit Service Flow Identifier (SFID) assigned by the CMTS. All Service Flows have an SFID; active and admitted upstream (CM to CMTS) Service Flows are also assigned a 14-bit Service Identifier (SID). The CMTS assigns one or more SFIDs to each CM, corresponding to the Service Flows required by the CM.

The CM receives a configuration file which defines the Service Flows. At least two Service Flows must be defined in each Configuration file: one for upstream and one for downstream. The first upstream Service Flow describes the Primary Upstream Service Flow, and is the default Service Flow used for otherwise unclassified traffic, including both MAC Management Messages and DATA PDUs. Similarly, the first downstream Service Flow describes the Primary Downstream Service Flow, which is the default Service Flow in the downstream direction. Additional Service Flows can be defined in the Configuration file to provide additional QoS services.

Incoming packets are matched to a Classifier that determines to which QoS Service Flow the packet is to be forwarded. The Classifier can examine the logical link control (LLC) header of the packet, the IP/TCP/UDP header of the packet or some combination of the two. If the packet matches one of the Classifiers, it is forwarded to the Service Flow indicated by the SFID attribute of the Classifier. If the packet is not matched to a Classifier, it is forwarded on the Primary Service Flow.

5.3.5.2 Upstream Transmission

A single upstream channel exists in DOCSIS 1.1 and DOCSIS 2.0. In DOCSIS 3.0, multiple upstream channels may exist between the CM and the CMTS, and the CMTS can allocate bandwidth to a CM for one or more of the available upstream channels.

An upstream channel is modeled as a stream of mini-slots. The CMTS generates the time reference for identifying these slots, and controls access to these slots by the CMs. The basic mechanism for assigning bandwidth management is the Allocation MAP, which is a MAC management message which is transmitted by the CMTS on the downstream channel and which describes, for some interval, the uses of the upstream mini-slots. Each interval is an integral number of mini-slots.

A given MAP may describe some slots as grants in which particular CMs may transmit data, other slots as available for contention transmission, and other slots for DOCSIS maintenance (e.g., available for new CMs to join the network). Each mini-slot in the MAP is labeled with a usage code which defines both the type of traffic that can be transmitted during the interval and the physical layer modulation encoding. For DOCSIS 1.1 channels, a mini-slot is a power-of-two multiple of 6.25 microsecond increments, limited to 2, 4, 8, 16, 32, 64, or 128 times 6.25 microseconds.

Bandwidth allocation includes the following basic elements:

- Each CM has one or more 14-bit Service Identifiers (SIDs) as well as a 48-bit MAC address.
- Upstream bandwidth is divided into a stream of mini-slots. Each mini-slot is numbered relative to a master clock reference maintained by the CMTS. The master reference is distributed to the CMs by means of SYNC and Upstream Channel Descriptor (UCD) messages.
- CMs may issue requests to the CMTS for upstream bandwidth.

The Allocation MAP is a varying-length MAC management message with a fixed-length header followed by a variable number of Information Elements (IEs). Each IE defines the allowed usage for a range of mini-slots. Each IE consists of a 14-bit SID, a 4-bit type code, and a 14-bit starting offset. For most purposes, the duration described by the IE is inferred by the difference between the IE's starting offset and that of the following IE.

5.3.5.3 The Request Frame

The Request Frame is the basic mechanism that a CM uses to initially request bandwidth. The length of a Request Frame is six bytes, and is composed of the following fields:

- *Frame Control* – 1 byte.
- *MAC-PARM* – 1 byte representing the total number of mini-slots requested.
- *SID* – 2 bytes representing the Service ID used for requesting bandwidth.
- *Header Check Sequence* – 2 bytes.

5.3.5.4 CM Bandwidth Utilization

When a CM has data to send, it must first use any available Data Grants assigned to the Service Flow or Class of Service if it is allowed to do so. If there are no Data Grants, the CM must use an available unicast request opportunity. If there are no unicast request opportunities, then the CM can use broadcast/multicast request opportunities for which it is eligible while complying with the contention backoff requirements of the system. The intent is that the CM use Data Grants to send data when it is able to do so, and if it needs to request, then it looks for a non-contention request, if available, to make a request before resorting to request opportunities in contention.

5.3.5.5 Upstream Service Flow Scheduling Services

Scheduling services are designed to improve the efficiency of the poll/grant process.

5.3.5.6 Unsolicited Grant Service (UGS)

The UGS is designed to support real-time service flows that generate fixed-size data packets on a periodic basis. UGS offers fixed-size grants on a real-time periodic basis, which eliminate the overhead and latency of CM requests and assure that grants will be available to meet the flow's real-time needs.

5.3.5.7 Real-Time Polling Service (rtPS)

The rtPS is designed to support real-time service flows that generate variable-size data packets on a periodic basis. The service offers real-time, periodic, unicast request opportunities, which meet the flow's real-time needs and allow the CM to specify the size of the desired grant.

5.3.5.8 Unsolicited Grant Service with Activity Detection (UGS-AD)

The UGS-AD is designed to support UGS flows that may become inactive for substantial portions of time (i.e., tens of milliseconds or more), such as VoIP with silence suppression. The service provides Unsolicited Grants when the flow is active and unicast polls when the flow is inactive.

5.3.5.9 Non-Real-Time Polling Service (nrtPS)

The nrtPS is designed to support non-real-time service flows that require variable-size data grants on a regular basis. The service offers unicast polls on a regular basis which assures that the flow receives request opportunities even during network congestion. The CMTS typically polls nrtPS service flows on an interval on the order of one second or less.

5.3.5.10 Best Effort Service

In the Best Effort service, the CM uses contention request opportunities to obtain data grants.

5.3.6 Priority Indication in Cable Access Networks

The communications between the CM and CMTS (e.g., DSx messages) occur within a service flow and can be classified into a higher priority service flow to allow transmission of control messages in overload conditions.

The communications between the CMTS and the Policy Server are IP based. The CMTS can mark flows with the appropriate DSCP or VLAN markings for priority communications. The CMTS does not process packets at the Session Layer.

5.4 Metro Ethernet Networks

5.4.1 Reference Architecture

An Ethernet Access Node can be used in place of the NID, MDF, and DSLAM in a Broadband Forum's Access Reference Architecture (i.e., the DSL Access Network Architecture). Figure 10 shows the Ethernet Access Network considered for this TR.

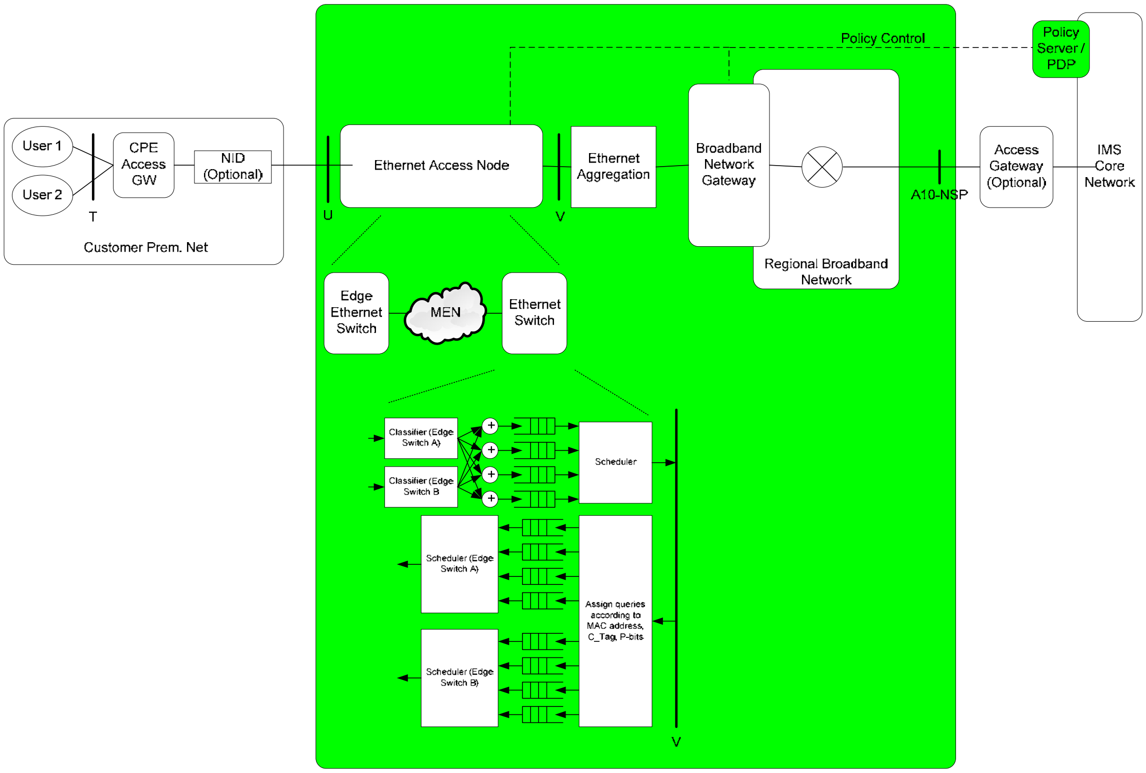

Policy Control
Policy Server / PDP
User 1
User 2
T
CPE Access GW
NID (Optional)
Customer Prem. Net
U
Ethernet Access Node
V
Ethernet Aggregation
Broadband Network Gateway
Regional Broadband Network
A10-NSP
Access Gateway (Optional)
IMS Core Network
Edge Ethernet Switch
MEN
Ethernet Switch
Classifier (Edge Switch A)
Classifier (Edge Switch B
Scheduler
Scheduler (Edge Switch A)
Assign queries according to MAC address, C_Tag, P-bits
Scheduler (Edge Switch B)
V

Figure 10 - Ethernet Access Network

5.4.2 Functional Entities

5.4.2.1 Customer Premises Network

The Customer Premises Network consists of a CPE Access Gateway and its associated users' UEs. "Simple" CPE Access Gateways transmit and receive untagged Ethernet packets to and from the Network Interface Device (NID), while "smarter" CPE Access Gateways can transmit and receive tagged 802.1 P/Q Ethernet packets.

5.4.2.2 Network Interface Device

The Network Interface Device (NID) is a CPE device that performs interface functions – such as code conversion, protocol conversion, and buffering – required for communications to and from a network. The NID transmits Ethernet packets from the CPE Access Gateway to the Edge Ethernet Switch in the network. The NID may be a standalone device or may be integrated with the CPE Access Gateway.

5.4.2.3 Edge Ethernet Switch

The Edge Ethernet Switch applies the Service Provider network's admission control and QoS policies of the network to user Ethernet frames. Edge Ethernet Switch functionality includes subscriber management, QoS, and enhanced traffic management capabilities. A Policy Enforcement Point (PEP) in the Edge Ethernet Switch is responsible for traffic policy enforcement of all traffic types in the switch.

The Edge Ethernet Switch performs the following functions:

- *For untagged Ethernet frames*:
    - At a minimum, maps the port associated with the NID (i.e., the UNI) into an Ethernet Virtual Connection (EVC).
    - If the purpose of the service is to provide "Internet" connectivity to multiple customers, then the Service Provider may use a single EVC for all UNIs connecting to an Internet Gateway. However, the MEF suggests Service Providers consider user-unique VLANs to allow for future "subscriber-unique" services.
    - A desirable function is the mapping of MAC addresses associated with a UNI into specific VLANs and EVCs, based on policy.
    - This function allows MAC addresses associated with specific devices (e.g., telephones) to be mapped into a VLAN distinct from a VLAN associated with PCs.
    - Based on policy, specifies a COS value for the frame.
    - The policy may use the UNI or MAC address, the 802.1P COS value, or the DiffServ Code Point (DSCP)/TOS value of the frame to create the COS value for this frame on the EVC. The policy may accept or ignore the COS and DSCP/TOS values received from the NID, and may preserve or reset the COS value before transmitting the frame received from the NID.
- *For tagged Ethernet frames*:
    - Supports Q-in-Q[9] (also known as stacked VLANs).
    - Maps CE-VLAN IDs to EVCs.
    - Based on policy, preserves the CE-VLAN ID across the EVC.
    - Based on policy, preserves the CE-VLAN CoS across the EVC.
    - Based on policy, specifies a CoS value for the frame.
- *Forwards packets* based on the associated 802.1P CoS values.

Frames are forwarded based on the priority of the frame and their MEF service frame "color". Typically, Edge Ethernet switches have four priority queues into which packets are placed based on their COS values. Typically, there is no weighted fair queuing algorithm associated with processing frames on the queues. "Red" (non-CIR-conformant and non-EIR-conformant) packets are discarded independent of their COS value.

5.4.2.4 Metro Ethernet Network

The MEN is used to aggregate the traffic from the Edge Ethernet switches onto an Ethernet Switch found at a Service Provider's Central Office[10].

[9] Q-in-Q refers to the fact that a subscriber's 802.1Q tag follows the service provider's 802.1Q tag. This allows the service provider to configure just one VLAN for a subscriber and for the subscriber to treat this VLAN as a trunk over which the subscriber can run her own VLAN services.

The Metro Ethernet Forum (MEF) is responsible for the core set of specifications for MENs. The generic MEN architecture specified in [MEF 4] is shown in Figure 11. This figure shows two MENs connecting four subscriber sites, as well as the key architectural interfaces. According to the MEF, Customer Premises Equipment (CPE) at the subscriber site attaches to a MEN over the User-to-Network Interface (UNI) using a standard 10 Mbps, 100 Mbps, 1 Gbps, or 10 Gbps interface.

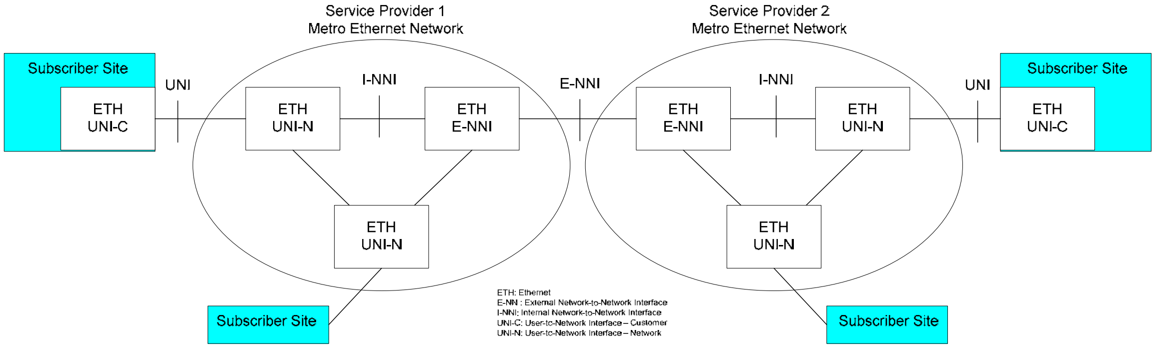


Figure 11 - Generic Metro Ethernet Network Architecture

5.4.2.5 Ethernet Switch

The Ethernet Switch provides a "UNI" to the Broadband Network Gateway for each EVC requiring a "hop off" point into the "Internet" or public access network. The Ethernet Switch's policy needs to be complementary to the policies found in the Edge Ethernet Switches to ensure that the appropriate priority is provided in the downstream (network to CPE) direction. A PEP in the Ethernet Switch is responsible for traffic policy enforcement of all traffic types in the switch.

5.4.2.6 Ethernet Aggregation

For this TR, the Ethernet Aggregation is defined as the network that connects multiple Ethernet Switches to the Broadband Network Gateway. The FE transfers Ethernet frames from the Ethernet Switches to the Broadband Network Gateway, and transfers Ethernet frames from the Broadband Network Gateway to the appropriate Ethernet Switches. [TR-167] allows a Gigabit Passive Optical Network (GPON) to be used for the Ethernet Aggregation function, and allows policy to be enforced at the GPON.

5.4.2.7 Broadband Network Gateway (BNG)

The Broadband Network Gateway (BNG) is an IP edge router at the border of a Regional Broadband Network. At the BNG, the admission control and the QoS policies of the network are applied. The BNG is also the aggregation point for outbound subscriber traffic. BNG functionality includes subscriber management, advanced IP processing, including IP QoS, and enhanced traffic management capabilities. A PEP in the BNG is responsible for traffic policy enforcement of all traffic types in the BNG. Policy enforcement may be applied at an IP session, IP flow, and/or aggregate level.

5.4.2.8 Regional Broadband Network

The Regional Broadband Network interconnects a Core Network and an Access Network Central Office. Typically multiple Central Offices are connected to a common Regional Broadband Network. Similarly, multiple Core Networks may be connected to a common Regional Broadband Network.

[10] A Central Office, as used in this document, is a Service Provider's telecommunication facility location which contains equipment supporting the access network to the customer and interconnecting equipment providing communication to and from the Core Network.

5.4.2.9 Access Gateway (AGW)

The Access Gateway (AGW) is an optional device at the border between a Regional Broadband Network and a Core Network. The Access Gateway is used to enforce security and business policies between the access network and the Core Network.

5.4.2.10 Policy Server/Policy Decision Point (PDP)

Requirement 1.1 of the MEF Technical Specification MEF 15, *Requirements for Management of Metro Ethernet Phase 1 Network Elements* [MEF 15], states:

> A Metro Ethernet Network Element (ME-NE) shall communicate with the managing systems [e.g., Element Management System (EMS) or Network Management System (NMS)] by means of a well-defined standards based management interface using an industry accepted management protocol (e.g., SNMP, TL/1, CORBA, CMIP, XML SOAP, etc.)[11].

Use of the Policy Server/PDP approach is consistent with this requirement. The Policy Server/PDP approach is described below.

Core Network requirements are based on the 3rd Generation Partnership Project (3GPP) Policy Control and Charging (PCC) architecture. Using the 3GPP S9 interface as per the Broadband Forum Fixed-Mobile Convergence (FMC) interworking architecture is a natural extension of PCC. Functionally, the International Telecommunications Union-Telecommunications Standardization Sector (ITU-T) Resource and Admission Control Function (RACF) and 3GPP PCC architectures are similar; the main difference is in the consolidation versus distribution of the interfaces and the protocols used. The interface from the Policy Server/PDP to the Application Function is assumed to be the 3GPP Rx interface. Alternatively, the Policy Server/PDP may communicate with the Application Function via an intermediary Policy and Charging Rules Function (PCRF) using the 3GPP S9 reference point.

The Policy Server/PDP is independent of the Core Network [TS 23.002] and can be used with non-IMS FEs; however, this TR assumes the Policy Server/PDP is located at the border of the Ethernet Access Network and the Core Network. A Policy Server/PDP may manage multiple PEPs, coordinating what policies should be enforced at the Network Equipments (NEs).

It is assumed that the Policy Server/PDP will use the mechanisms provided by the MEN switch vendor to push policy to the Edge Ethernet Switches and Ethernet Switches.

5.4.3 Call/Session Flows

For call/session flows associated with an Ethernet Access Network, refer to ATIS-1000049.

5.4.4 Interfaces & Protocols

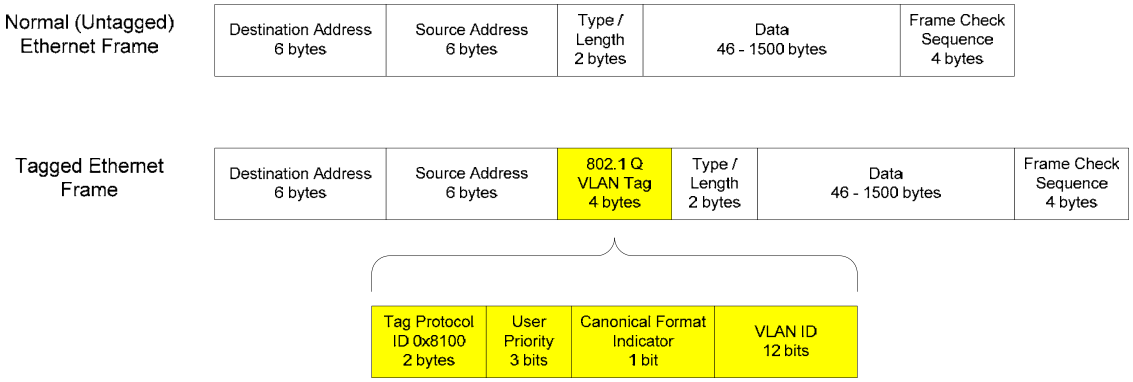
Ethernet switches are full duplex, broadcast domain devices which use a set of layer 2 (Data Link layer) protocols and interfaces. The switches keep track of which MAC address is associated with each port, and transmit a received Ethernet packet only to the intended destination(s).

An Internet Protocol (IP) subnet is a layer 3 (Network layer) construct which connects devices with IP addresses to routers. Typically each Ethernet segment supports one IP subnet.

Devices on an Ethernet segment use MAC addresses to communicate, while applications typically use IP addresses to communicate. The mapping of a 32-bit IP address to a 48-bit MAC address is handled by the Address Resolution Protocol (ARP).

[11] SNMP is Simple Network Management Protocol. TL/1 is Translation Language 1. CORBA is Common Object Request Broker Architecture. CMIP is Common Management Information Protocol. XML is Extensible Markup Language. SOAP is Simple Object Access Protocol.

An Ethernet switch may be connected to devices which can only transmit normal (untagged) Ethernet frames (Figure 12). In this case, the Ethernet switch would need to add a Virtual Local Area Network (VLAN) tag to the frame to communicate VLAN information to another Ethernet switch. VLAN tags are defined in the Institute of Electrical and Electronics Engineers (IEEE) 802.1 Q standard. This tag can also be used by devices connected to the Ethernet switch to identify the transmission priority to be given to an Ethernet frame.



Normal (Untagged) Ethernet Frame	Destination Address 6 bytes	Source Address 6 bytes	Type / Length 2 bytes	Data 46 - 1500 bytes	Frame Check Sequence 4 bytes	
Tagged Ethernet Frame	Destination Address 6 bytes	Source Address 6 bytes	802.1 Q VLAN Tag 4 bytes	Type / Length 2 bytes	Data 46 - 1500 bytes	Frame Check Sequence 4 bytes

Tag Protocol ID 0x8100 2 bytes	User Priority 3 bits	Canonical Format Indicator 1 bit	VLAN ID 12 bits

Figure 12 - Normal and Tagged Ethernet Frames

For purposes of this TR, Ethernet switches deployed by a Service Provider are assumed to provide Ethernet VLAN capabilities and to support the MEF standards. Thus, the Ethernet switches support the IEEE 802.1Q standard, and every port on the switch is associated with at least one VLAN, and may be associated with multiple VLANs. The Ethernet switch has a database which keeps track of which ports belong to which VLAN.

Each Ethernet switch is assumed to have:

- *One or more trunk ports*. A trunk port is a port with multiple VLANs that are all tagged. A trunk link connects two trunk ports. A tagged frame contains an 802.1Q tag.
- *One or more access ports*. An access port is a port associated with an untagged VLAN. An access link connects two access ports.
- *Zero or more hybrid ports*. A hybrid port is a port with both untagged and tagged VLANs. A hybrid link connects two hybrid ports.

An 802.1P/Q tag consists of four bytes which are inserted between the Source Address and Length fields of an Ethernet Packet. The 802.1P/Q tag consists of the following fields:

- *Tag Protocol Identifier (TPID)*: A 16-bit field identifying the frame as an IEEE 802.1Q-tagged frame.
- *Priority*: A 3-bit field identifying the 802.1P priority [also known as Class Of Service (COS) priority].
- *Canonical Format Indicator (CFI)*: A 1-bit field set to zero for Ethernet switches.
- *VLAN Identifier*: A 12-bit field specifying the VLAN to which the frame belongs. A value of 0 means the frame does not belong to any VLAN; in this case, the tag is referred to as an 802.1P priority tag.

Double-tagging (i.e., inserting eight bytes between the Source Address and Length fields of an Ethernet packet) allows a Service Provider to use a VLAN across its network while mixing traffic from clients that are already VLAN-tagged. The first tag encountered is called the outer tag and is associated with the Service Provider. The second tag encountered is called the inner tag and is associated with the client's VLAN.

Router functionality is required to connect the IP subnet associated with one VLAN to an IP subnet associated with another VLAN. For this IR, this functionality is assumed to be provided by a Gateway function.

5.4.5 QoS & Policy Mechanisms

The Priority field in the 802.1 P/Q tag is used to identify priority communications.