User Network Interface (UNI) 2.0 Signaling Specification

OIF-UNI-02.0-Common -
User Network Interface (UNI) 2.0 Signaling Specification: Common Part

February 25, 2008

Implementation Agreement created and approved
by the Optical Internetworking Forum
www.oiforum.com

Working Group: **Architecture and Signaling**

TITLE: **User Network Interface (UNI) 2.0 Signaling Specification: Common Part**

SOURCE:

TECHNICAL EDITOR

Stephen Shew
Nortel Networks
3500 Carling Ave.
Ottawa, ON K2H 8E9
Canada
Phone: +1.613.763.2462
Email: sdshew@nortel.com

WORKING GROUP CHAIR

Jonathan Sadler
Tellabs
1415 West Diehl Road
Naperville, IL 60563
USA
Phone: +1.630.798.6182
Email: jonathan.sadler@tellabs.com

ABSTRACT: This Implementation Agreement (IA) specifies the content and operation of the OIF UNI 2.0 signaling protocol in a protocol neutral manner. It allows a client device to dynamically request the establishment of a service across an operator's network. UNI signaling functions, along with the OIF E-NNI 2.0 and I-NNI signaling protocols (the latter not specified by OIF), are used to establish end-to-end connection services. This IA is based on the common part of the UNI 1.0 R2 spec [OIF-UNI-01.0-R2-Common].

The OIF is an international non profit organization with over 85 member companies, including the world's leading carriers and vendors. Being an industry group uniting representatives of the data and optical worlds, OIF's purpose is to accelerate the deployment of interoperable, cost-effective and robust optical internetworks and their associated technologies. Optical internetworks are data networks composed of routers and data switches interconnected by optical networking elements.

With the goal of promoting worldwide compatibility of optical internetworking products, the OIF actively supports and extends the work of national and international standards bodies. Formal liaisons have been established with The ATM Forum, IEEE 802.3, IETF, ITU-T Study Group 13, ITU-T Study Group 15, MEF, NPF, ATIS-TMOC, ATIS-OPTXS, TMF, UXPi and the XFP MSA Group.

For additional information contact:
The Optical Internetworking Forum, 48377 Fremont Blvd.,
Suite 117, Fremont, CA 94538

510-492-4040 *mf* info@oiforum.com

www.oiforum.com

List of Contributors

The UNI 2.0 was based on the UNI 1.0r2 and we acknowledge the work of the contributors to the UNI 1.0r2:

Osama Aboul-Magd	William Goodson	Zhi-Wei Lin	Arnold Sodder
Stefan Ansorge	Gert Grammel	Ling-Zhong Liu	John Strand
K. Arvind	Richard Graveman	Ben Mack-Crane	George Swallow
Krishna Bala	Eric Gray	Larry McAdams	Ewart Tempest
Sandra Ballarte	Riad Hartini	Wilson Nheu	Eve Varma
Ayan Banerjee	Eric Mannie	Lyndon Ong	Cary Wright
Rick Barry	Raj Jain	Dimitiri Papadimitriou	Yangguang Xu
Debashis Basak	LiangYu Jia	Dimitrios Pendarakis	Yong Xue
Greg Bernstein	Jim Jones	Kavi Prabhu	Tao Yang
Richard Bradford	Suresh Katukam	Bala Rajagopalan	Jennifer Yates
Curtis Brownmiller	Nooshin Komaee	Anil Rao	John Z. Yu
Yang Cao	Jonathan P. Lang	Robert Rennison	Alex Zinin
John Drake	Monica Lazer	Jonathan Sadler	Zhensheng Zhang
Hans-Martin Foisel	Fong Liaw	Stephen Shew	

We acknowledge the work of the contributors to the UNI 2.0 extensions:

Evelyne Roch (Co-editor)	Lyndon Ong
Alessandro D'Alessandro	Vijay Pandian
Hans-Martin Foisel	Rajender Razdan
Richard Graveman	Jonathan Sadler
Fred Gruman	Stephen Shew (Co-editor)
Jim Jones	Eve Varma
Monica Lazer	Lucy Yong
Thierry Marcot	

1 Table of Contents

LIST OF CONTRIBUTORS **4**

1 TABLE OF CONTENTS 5
2 LIST OF FIGURES 7
3 LIST OF TABLES 7
4 INTRODUCTION 9
4.1 Problem Statement *10*
4.2 Scope *10*
4.3 Relationship to other Standards Bodies *11*
4.4 Merits to OIF *11*
4.5 Working Group(s) *11*
4.6 Document Organization *11*
4.7 Keywords *11*
5 TERMINOLOGY AND ABBREVIATIONS 12
5.1 Terminology *12*
5.2 Abbreviations *14*
6 SERVICES OFFERED OVER THE UNI (VERSION 2.0) 17
6.1 Call Control *17*
6.2 SONET/SDH Services Including Low-Order Signal Support *19*
6.3 Transport of Ethernet Services *21*
6.4 Transport of OTN Connections *25*
6.5 Enhanced Security *27*
6.6 Non-Disruptive Service Parameters Modification *34*
6.7 Supporting Procedures *37*
6.8 Compatibility between UNI 1.0 and UNI 2.0 ..... *38*
6.9 Compatibility between UNI 2.0 and ENNI 1.0 Signaling *39*
7 UNI SERVICE INVOCATION REFERENCE CONFIGURATIONS 40
7.1 The Direct Invocation Model *40*
7.2 The Indirect Invocation Model *40*
7.3 Service Invocation Configurations *41*
8 SIGNALING TRANSPORT CONFIGURATIONS 43
8.1 In-fiber Signaling over SONET/SDH Line or Section DCC Bytes *43*
8.2 In-fiber Signaling over OTN GCC0 ..... *44*
8.3 In-fiber Signaling over Ethernet OAM Frames *45*
8.4 Out-of-Fiber Signaling *45*
9 ADDRESSING 47
9.1 UNI Identifiers Spaces *47*
9.2 Structure of TNA Names *50*
9.3 Role of TNA Names in UNI Signaling *50*
10 UNI ABSTRACT MESSAGES 52
10.1 Connection Setup Request *54*
10.2 Connection Setup Indication *55*
10.3 Connection Setup Confirm *55*
10.4 Connection Release Request *56*
10.5 Connection Release Indication *57*
10.6 Connection Query Request *57*
10.7 Connection Query Indication *58*
10.8 Connection Notify *58*
10.9 Connection Modify Request *59*
10.10 Connection Modify Indication *59*
10.11 Connection Modify Confirm *60*

10.12 Signaling Adjacency Maintenance *60*
10.13 Description of Attributes *60*
10.14 SC and SPC Interworking *65*
11 REFERENCES 66
12 APPENDIX A: LIST OF COMPANIES BELONGING TO OIF WHEN DOCUMENT IS APPROVED 68

2 List of Figures

FIGURE 5-1: CALL (SERVICE) ASPECT OF OPTICAL CONTROL PLANE 9
FIGURE 5-2: EXAMPLE OF CONTROL PLANE SUBDIVIDED INTO MULTIPLE CONTROL DOMAINS 10
FIGURE 5-3 – CALL SEGMENTATION AND CALL/CONNECTION SEPARATION 18
FIGURE 5-4 UNI 2.0 ETHERNET TRANSPORT MODEL 21
FIGURE 5-5 – SERVER LAYER CALLS AND CONNECTIONS VS. ETHERNET CONNECTIONS AND ETHERNET CALLS 22
FIGURE 5-6 ETHERNET PRIVATE LINE – SCENARIO 1 23
FIGURE 5-7 ETHERNET VIRTUAL PRIVATE LINE – SCENARIO 2 23
FIGURE 5-8 – BANDWIDTH PROFILE PER MEF UNI (MEF10.1 FIGURE 14) 25
FIGURE 5-9 – BANDWIDTH PROFILE PER EVC (MEF10.1 FIGURE 15) 25
FIGURE 5-10 - BANDWIDTH PROFILE PER COS WITHIN AN EVC (MEF10.1 FIGURE 16) 25
FIGURE 5-11 **– OTN SERVICE MODEL** 26
FIGURE 5-12 – OPTICAL TRANSPORT NETWORK LAYER RELATIONSHIPS 26
FIGURE 5-13 – OPTICAL CHANNEL LAYER RELATIONSHIPS 27
FIGURE 5-15 IPSEC/UNI/NNI SCENARIO 1. 32
FIGURE 5-16 IPSEC/UNI/NNI SCENARIO 2. 32
FIGURE 5-17 BANDWIDTH MODIFICATION FOR [G805] LAYER NETWORK 35
FIGURE 5-18 - BANDWIDTH MODIFICATION FOR ETHERNET INTERFACE 36
FIGURE 5-19 - VLAN SET MODIFICATION 37
FIGURE 5-20 - DIRECT SERVICE INVOCATION MODEL 1 41
FIGURE 5-21 - DIRECT SERVICE INVOCATION MODEL 2 41
FIGURE 5-22 - INDIRECT SERVICE INVOCATION MODEL 1 42
FIGURE 5-23 - INDIRECT SERVICE INVOCATION MODEL 2 42
FIGURE 5-24 – SONET/SDH IN-FIBER EMBEDDED COMMUNICATION LINKS 43
FIGURE 5-25 - DCC ENCAPSULATION 44
FIGURE 5-26 – OTN IN-FIBER EMBEDDED COMMUNICATION LINKS 44
FIGURE 5-27 - GCC ENCAPSULATION 45
FIGURE 5-27 SEPARATION OF NODE ID, SC PC ID, SC PC SCN ADDRESS AND TNE OR CLIENT DEVICE 48
FIGURE 5-28 DATA LINKS, LOGICAL LINKS AND TNAS 49
FIGURE 5-29 CLIENT AND TNE LOGICAL PORT IDENTIFIER MAPPING 50

3 List of Tables

TABLE 5-1 – SDH CONNECTION TYPES SUPPORTED 20
TABLE 5-2 – SONET CONNECTION TYPES SUPPORTED 21
TABLE 5-3 – ETHERNET INTERFACE TYPES SUPPORTED 24
TABLE 5-4 – OTN CONNECTION TYPES SUPPORTED 27
TABLE 5-5 – MANDATORY AND OPTIONAL PROCEDURES UNDER UNI 2.0 38
TABLE 5-6 COMPATIBILITY BETWEEN UNI 2.0 AND E-NNI 1.0 39
TABLE 5-7 EFM OAM FOR IN-FIBER COMMUNICATION 45
TABLE 5-8 UNI CALL MESSAGES 53
TABLE 5-9 UNI CONNECTION MESSAGES 53
TABLE 5-10 UNI SIGNALING ADJACENCY MAINTENANCE MESSAGE 53
TABLE 5-11 CONNECTION SETUP REQUEST 54
TABLE 5-12 CONNECTION SETUP INDICATION 55
TABLE 5-13 CONNECTION SETUP CONFIRM 56
TABLE 5-14 CONNECTION RELEASE REQUEST 57
TABLE 5-15 CONNECTION RELEASE INDICATION 57
TABLE 5-16 CONNECTION QUERY REQUEST 57
TABLE 5-17 CONNECTION QUERY INDICATION 58

TABLE 5-18 CONNECTION NOTIFY 59
TABLE 5-19 CONNECTION MODIFY REQUEST 59
TABLE 5-20 CONNECTION MODIFY INDICATION 60
TABLE 5-21 CONNECTION MODIFY CONFIRM 60

4 Introduction

This document specifies the content and operation of the OIF UNI 2.0 signaling protocol. It allows a client device to dynamically request the establishment of a service across an operator's network. UNI signaling functions, along with the OIF E-NNI 2.0 and I-NNI signaling protocols (the latter not specified by OIF), are used to establish end-to-end connection services.

The deployment of Automatically Switched Optical Networks (ASONs) into new and existing networks occurs within the context of commercial operator business practices and heterogeneous transport networks (e.g., with respect to transport technologies, vendors, approach to management/control). This is true even within a single carrier's network. These business and operational considerations lead to the need for optical control plane architecture and supporting protocols to inherently enable protection of such commercial business operating practices that, for example, generally segment transport networks into domains according to managerial and/or policy considerations. Per G.8080, the term domain is used to express differing administrative and/or managerial responsibilities, trust relationships, addressing schemes, infrastructure capabilities, survivability techniques, distributions of control functionality, etc. The control plane supports establishment of services through the automatic provisioning of end-to-end transport connections across one or more domains. This involves both call and connection aspects:

- The call (service) aspect involves the provisioning of end-to-end services, while respecting commercial business operating practices, as shown in Figure 5-1. (It should be noted that for management initiated calls, Call Control would reside in the Management Plane.)
- The connection aspect involves the automatic provisioning of connections in support of end-to-end services that may span one or more domains.

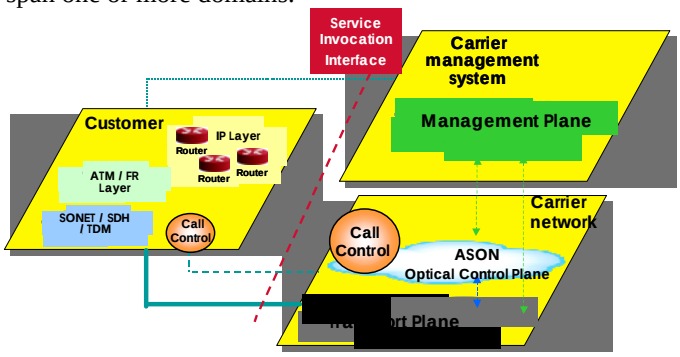

Figure 5-1: Call (Service) Aspect of Optical Control Plane

As mentioned above, domains are established by operator policies and have a range of membership criteria; i.e., a domain represents a collection of entities that are grouped for a particular purpose. Therefore, a control domain is comprised of a collection of control plane architectural components (such as signaling controllers or routing controllers). A control domain is an architectural construct that provides for encapsulation and information hiding, and the characteristics of the control domain are the same as those of its constituent set of distributed architectural components. The interconnection between and within domains is described in terms of reference points. As domains are established via operator policies, inter-domain reference points are service demarcation points (i.e., points where call control is provided).

- The reference point between a user and a provider domain is the UNI, which represents a user-provider service demarcation point.
- The reference point between domains is the E-NNI, which represents a service demarcation point supporting multi-domain connection establishment. The nature of the information exchanged between control domains across the E-NNI reference point captures the common semantics of the information exchanged amongst its constituent components, while allowing for different representations inside each control domain.

- The reference point within a domain is an I-NNI, which represents a connection point supporting intra-domain connection establishment.

Figure 5-2 illustrates a simple example of control plane configuration for a multi-domain network. This subdivision enables business boundaries and signaling protocol heterogeneity to be handled. It should be noted that from a UNI Client perspective, it does not matter how many carriers or domains exist in the network as the UNI client does not have any visibility of the carrier's network.

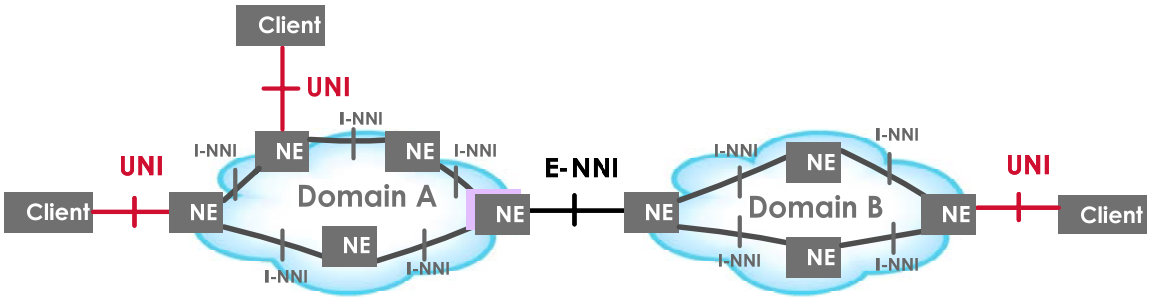

Figure 5-2: Example of Control Plane Subdivided into Multiple Control Domains

This document deals with the following topics:

- Definition of UNI signaling reference configurations: Two sets of configurations covering direct and indirect service invocation are defined.
- Definition of services offered over the UNI.
- Definition of different signaling channel configurations for in-fiber and out-of-fiber signaling.
- Definition of the addressing scheme used under UNI 2.0.
- Definition of UNI signaling messages and attributes.
- Description of security issues in UNI 2.0.

4.1 Problem Statement

The advent of the automatic switched optical network has necessitated the development of interoperable procedures for requesting and establishing dynamic connection services across heterogeneous networks. The development of such procedures requires the definition of

- Control domains and associated reference points (UNI, I-NNI, E-NNI)
- Services offered by the optical transport network across control domains
- Signaling protocols used to invoke the services across UNI interfaces
- Mechanisms used to transport signaling messages

The first phases of specifying the UNI signaling interface and External Network Node Interface (E-NNI) signaling protocols has been completed in [OIF-UNI-01.0-R2] and [OIF-ENNI-SIG-01]. This revised UNI Signaling specification includes UNI1.0 principal ballot comments resolutions and updates from interoperability demonstration findings and support of new UNI 2.0 features described in Section 6. UNI 2.0 is an enhancement of UNI 1.0 and is backwards compatible with UNI 1.0 as described in section 6.8.

4.2 Scope

The scope of this agreement is to define the set of services, the signaling protocols used to invoke the services and the mechanisms used to transport signaling messages all of which are to be implemented by client and transport network equipment vendors to support UNI 2.0. This document is scoped to allow an early implementation based on reusing existing signaling protocols along with current and newly available technologies and capabilities in vendor equipment. It should be noted that only signaling for service invocation is within the scope of UNI 2.0. Discovery, routing, reachability and address resolution protocols

are outside the scope. The specification focuses on SONET/SDH, OTN (i.e., G.709), and Ethernet connection services. This implementation agreement is not intended to restrict additions of further capabilities in future versions of the UNI.

4.3 Relationship to other Standards Bodies

This document, to the maximum extent possible, utilizes standards and specifications already available from other organizations (within the scope of its updates). The SONET/SDH structure and format definitions are based on [G707], OTN on [G709], and Ethernet Service on [G8011]. The signaling protocols are based on IETF Generalized MPLS specifications. The signaling specifications in UNI 1.0 Release 1 and 2 have been used, unchanged, by [G7713.2] and [G7713.3]. The UNI concept is an inherent part of the ASON architecture in [G8080]. The auto-discovery mechanism in UNI 1.0 Release 1 was based on IETF Link Management Protocol (LMP) specifications; however as a separate discovery IA is underway, auto-discovery has been removed from UNI 2.0. The Ethernet service supports services developed in the Metro Ethernet Forum and ITU-T SG15. Attributes of the Ethernet service are taken from [MEF.6], [MEF.10.1], [MEF.11], [G8011], [G8011.1] and [G8011.2].

The UNI 2.0 signaling protocols are described in separate companion documents. At the time or writing, RSVP protocol details for UNI 2.0 are described in [OIF-UNI-02.0-RSVP]. Future UNI 2.0 protocol documents could be created at a later time.

4.4 Merits to OIF

The UNI 2.0 specification is a key step towards the implementation of an open transport network that allows dynamic interconnection of client layers like IP, Ethernet, SONET and others. This activity supports the overall mission of the OIF.

4.5 Working Group(s)

Architecture and Signaling Working Group
OAM&P Working Group

4.6 Document Organization

This document is organized as follows:

- Section 5describes the terminology and abbreviations used in the rest of the document
- Section 6 defines the services offered under UNI 2.0
- Section 7 describes the UNI signaling reference configurations
- Section 8 describes the signaling transport mechanisms
- Section 9 describes the addressing scheme under UNI 2.0
- Section 10 defines the UNI abstract messages and attributes
- Section 11 contains the references.

4.7 Keywords

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].

5 Terminology and Abbreviations

The key terminology and abbreviations used in the rest of the document are summarized below.

5.1 Terminology

CE-VLAN ID	Customer Edge Virtual Local Area Network Identifier: The identifier derivable from the content of a service frame that allows the service frame to be associated with an EVC at the UNI.
Connection	A series of contiguous link connections and/or subnetwork connections between termination connection points (G.805).
In-Fiber Signaling	In-fiber signaling refers to the transport of signaling traffic over a communication channel embedded in the data-bearing physical link.
Logical Port ID	A control plane identifier for a port. For SONET/SDH and OTN links, there is a one-to-one correspondence between a logical port ID and a port. For Ethernet, it is possible to have a single logical port ID representing multiple ports in the case where link aggregation is used as this is modeled by a single logical port by the control plane.
Node ID	Control plane identifier for the network element on the client or network sides of the UNI reference point.
Out-of-Fiber Signaling	Out-of-fiber signaling refers to the transport of signaling traffic over a communication link, separate from the data-bearing link, between the signaling entities.
Port	The hardware interface in an optical or user network element that terminates a bi-directional link between network elements. Examples include OC-48 or OC-192 ports in a TNE.
SC PC ID	Signaling Controller Protocol Controller Identifier. The SC PC provides the protocol specific processing of signaling messages, including mapping to and from abstract interfaces of the control plane components.
Signal Type	A SDH/SONET or OTN signal type, such as STS-1 or ODU1.
Signaling Communications Network (SCN)	A network that transports signaling messages between the signaling controllers.
Transport Network	The functional resources of the network that convey user information from one to another location bi-directionally or uni-directionally. A transport network can also transfer various kinds of network control information (e.g., operations and maintenance information).
Transport Network Assigned (TNA) Name	A name assigned to data bearing links connecting a UNI-N and a UNI-C. The TNA name is assigned by the transport service provider, either via a protocol or by configuration.
Transport Network Element (TNE)	A network element (within the transport network) having optical interfaces, such as an optical cross-connect (OXC) or an optical add/drop multiplexer.
UNI	The user-network interface is the service control interface between a client device and the transport network.

UNI-C	The logical entity that performs UNI signaling on the user device side.
UNI-N	The logical entity that performs UNI signaling on the network device side.
User or Client	Network equipment that is connected to the transport network for utilizing optical transport services. Examples of clients include IP routers, ATM switches, Ethernet Switches, SDH/SONET Cross-connects, etc.

5.2 Abbreviations

ADM	Add-Drop Multiplexer
AH	Authentication Header
ANSI	American National Standard Institute
ASON	Automatically Switched Optical Network
ATM	Asynchronous Transfer Mode
CBS	Committed Burst Size
CC	Connection Controller
CCC	Calling/Called Party Call Controller
CE-VLAN	Customer Equipment VLAN
CF	Color Flag
CIR	Committed Information Rate
CM	Color Mode
COPS	Common Open Policy Service
CORBA	Common Object Request Broker Architecture
CoS	Class of Service
CR-LDP	Constraint based Label Distribution Protocol
DCC	Data Communication Channel
DCM	Distributed Call and Connection Management
EBS	Excess Burst Size
EFM	Ethernet in the First Mile
EIR	Excess Information Rate
EMS	Element Management System
EPL	Ethernet Private Line
ESP	Encapsulating Security Payload
EVC	Ethernet Virtual Connection
EVPL	Ethernet Virtual Private Line
E-NNI	External NNI
FEC	Forward Error Correction
FR	Frame Relay
GbE	Gigabit Ethernet
GCC	General Communication Channel
G-PID	Generalized Payload Identifier
GFP	Generic Framing Procedure
GMPLS	Generalized Multi-Protocol Label Switching
GSMP	Generic Switch Management Protocol
HDLC	High-level Data-Link Control
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
I-NNI	Internal Network-Network Interface
IPsec	Internet Protocol Security
I-NNI	Internal NNI
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISI	Internal Signaling Interface
ITU-T	International Telecommunications Union – Telecommunications Standardization Sector
LC	Link Connection
LCAS	Link Capacity Adjustment Scheme
LDAP	Lightweight Directory Access Protocol

LDP	Label Distribution Protocol
LMP	Link Management Protocol
LSP	Label Switched Path
MAC	Medium Access Control
MEF	Metro Ethernet Forum
MPLS	Multi-Protocol Label Switching
MT	Multiplier
NAT	Network Address Translation
NCC	Network Call Controller
NE	Network Element
NMC	Number of Multiplexed Components
NMI	Network Management Interface
NNI	Network Node Interface
NSAP	Network Service Access Protocol
NVC	Number of Virtual Components
OAM	Operations, Administration, and Management
OC	Optical Carrier
OCC	Optical Channel Carrier
OC-N	Optical Carrier level N
OCh	Optical Channel
ODUk	Optical Data Unit of order k
OH	Overhead
OIF	Optical Internetworking Forum
OMS	Optical Multiplex Section
ONE	Optical Network Element
OPU	Optical Payload Unit
OSC	Optical Supervisory Channel
OTH	Optical Transport Hierarchy
OTM	Optical Transport Module
OTN	Optical Transport Network as defined in [G709]
OTS	Optical Transmission Section
OTUk	Optical Transport Unit of order k
OUI	Organizationally Unique Identifier
OXC	Optical Cross-Connect
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PPP	Point to Point Protocol
RCC	Requested Contiguous Concatenation Type
RSVP	Resource reSerVation Protocol
RSVP-TE	RSVP with Traffic Engineering extensions
SA	Security Association
SC	Switched Connection
SC PC SCN	Signaling Controller Protocol Controller Signaling Control Network
SC PC ID	Signaling Controller Protocol Controller Identifier
SCN	Signaling Communications Network
SDH	Synchronous Digital Hierarchy
SLA	Service Level Agreement
SNC	Subnetwork Connection
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical NETwork
SPC	Soft permanent connection
SRLG	Shared Risk Link Group

ST	Signal Type
STM-M	Synchronous Transport Module level M
STS-N	Synchronous Transport Signal level N
TDM	Time Division Multiplexing
TLV	Type-Length-Value encoding
TNA	Transport-Network Assigned
TNE	Transport network Element
UDP	User Datagram Protocol
UNI	User Network Interface
UNI-N	UNI Signaling Agent – Network
UNI-C	UNI Signaling Agent – Client
VC	Virtual Component
VCAT	Virtual Concatenation
VCG	Virtual Concatenation Group
VLAN	Virtual Local Area Network

6 Services Offered over the UNI (Version 2.0)

The primary service offered by the transport network over the UNI is the ability to create and delete connections on-demand. The connection can be either unidirectional or bi-directional. Under UNI 2.0, this definition includes SONET/SDH, OTN, and Ethernet connections. The properties of the connection are defined by the attributes specified during connection establishment.
Features added in UNI 2.0 are:

1. Call Control – covered in section 6.1.
2. SONET/SDH Low-order Signals – an extension to existing SONET/SDH services – covered in section 6.2.
3. Transport of Ethernet Services – covered in section 6.3
4. Transport of OTN Interfaces – covered in section 6.4
5. Enhanced Security – covered in section 6.5
6. Non-Disruptive Service Parameters Modification – covered in section 6.6

Of these, the only mandatory UNI 2.0 feature is support for Call Control.

6.1 Call Control

6.1.1 Calls and Connections

UNI 2.0 follows the call and connection architecture from ASON. The call controller and connection controller concepts are described in [G8080] and [G7713]. The call is defined as follows [G8080]:

> Call: An association between two or more users and one or more domains that supports an instance of a service through one or more domains. Within domains, the association is supported by network entities that contain call state. Between a user and a network call control entity and between network call control entities, there are call segments. The call consists of a set of concatenated call segments.
> Call segment: An association between two call control entities (as per [Q2982], which is equivalent to [G8080] call controllers). Each call segment has zero or more associated connections. Call segments between network call control entities have zero or more supporting server layer calls.

Calls are controlled by call controllers. There are two types of call controllers (refer to Figure 5-3) :

1. Calling/Called party Call Controller (CCC)
2. Network Call Controller (NCC)

A calling party call controller interacts with a called party call controller by means of one or more intermediate network call controllers.

The NCC function is provided at the network edge (i.e., UNI-N), and the functions performed by NCCs at the network edge are defined by the policies associated by interactions between users and the network. As such, an end-to-end call is considered to consist of multiple call segments, when the call traverses multiple network call controllers. Each call segment could have one or more connections, i.e., associated link connections (LC) or subnetwork connections (SNC).

The number of connections associated with call segments MAY not be the same even in one end-to-end call. In Figure 5-3, the UNI call segment has one LC associated with it, and the subnetwork call segment has two SNCs associated with it.

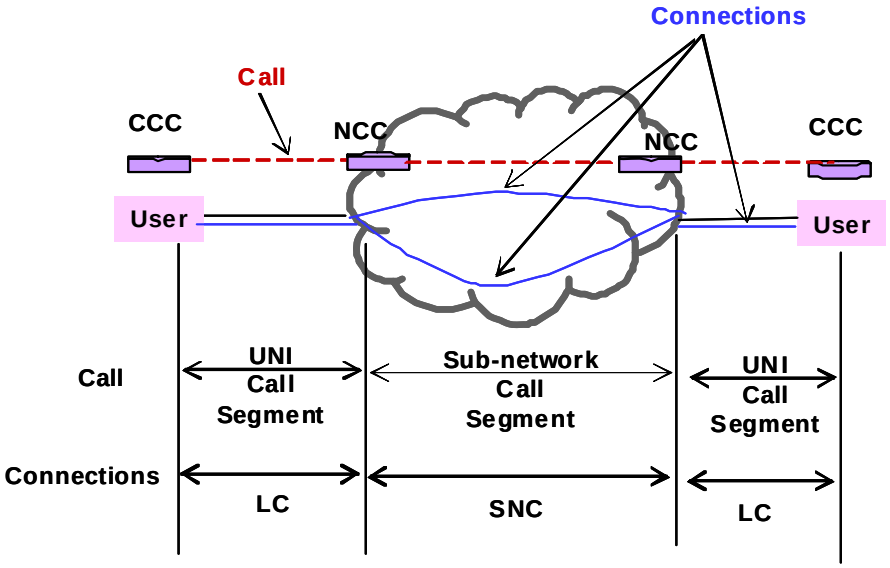

Figure 5-3 – Call Segmentation and Call/Connection Separation

Each connection MAY exist independently of other connections within the call, i.e., each connection is setup and released with separate connection messages. The concept of the call allows for flexibility in how end-points set up connections and how network offers services to users. Key features of call control are:

- A call with multiple associated connections enables some enhanced services, such as virtual concatenation or 1+1 path protection, where each connection can travel on different diverse paths inside the network. It can also reroute connections without changing the call state by separating the call state from connection state.
- Connections are always associated with a call. The connections can be added and/or deleted without call state changes. This is used by the non-disruptive call modification feature.
- A call with zero associated connections enables the identification of the call initiator (with both network call controller as well as destination user) prior to connections, which MAY result in decreasing contention during resource reservation. This call control feature is not supported in UNI 2.0. The deletion of the last link connection at the UNI deletes the call. Note that in the case of network failures resulting in the deletion of the last sub-network connection associated with the call, the call remains in place at the UNI while the sub-network connection is restored.

6.1.2 Connection Types

ITU ASON standards [G8080] define three basic connection types according to the distribution of connection management functionality between the control and the management planes. The following connection types have been identified:

- **PC**: Permanent connection: A PC is a connection type that is provisioned by the management system.
- **SC**: Switched Connection: A SC is any connection that is established, as a result of a request from the end user, between connection end points using a signaling/control plane and involves the dynamic exchange of signaling information between signaling elements within the control plane(s).
- **SPC**: Soft Permanent Connection: An SPC is a user-to-user connection where the user-to-network portion of the end-to-end connection is established by the network management system as a PC. The network portion of the end-to-end connection is established as a switched connection using

the control plane. In the network portion of the connection, requests for establishment of the connection are initiated by the management plane and setup by the control plane.

UNI Signaling is involved in Switched Connections and a UNI-N may also originate/terminate a Soft Permanent Connection. It is possible to have hybrid SC-SPC connections where the end user is involved in signaling at one UNI but not the other. It is an SC at one UNI and an SPC at the other UNI.

6.1.3 UNI 2.0 Signaling Actions

UNI signaling refers to the message exchange between a UNI-C and a UNI-N entity to invoke transport network services. Under UNI 2.0 signaling, the following actions may be invoked:

1. *Connection creation*: This action allows a connection with the specified attributes to be created between a pair of access points. Connection creation may be subject to network-defined policies (e.g., user group connectivity restrictions) and security procedures. The creation of the first connection of a call instantiates the call.
2. *Connection deletion*: This action allows an existing connection to be deleted. The deletion of the last link connection of a call deletes the call.
3. *Call and Connection status enquiry*: This action allows the status of certain parameters of the call and its connections to be queried.
4. *Call Modification:* Non-disruptive service parameters modification is supported via call modification by adding or removing a connection from an existing call or by modifying an existing connection as described below. This is not supported under UNI 1.0. It is compatible however, with UNI 2.0 features.
5. *Connection modification,* which allows service parameters of an already established connection to be modified. It is a valid mechanism for achieving call modification and may only be requested as a call modification procedure. This is not supported under UNI 1.0. It is compatible however, with UNI 2.0 features.

6.2 SONET/SDH Services Including Low-Order Signal Support

The scope of this service is to enable transport of SONET/SDH low-order and high-order signals.

Connection type is defined by a combination of framing (e.g., SONET or SDH), concatenation (contiguous or virtual concatenation), and transparency of the signal type carried. UNI 2.0 specification supports the following combinations. Even though UNI 2.0 signaling supports all these connection types, a given transport network may support only a subset of them.

Framing: SONET/SDH and OTN framed signals are supported. In addition, Ethernet client signals are supported.
Transparency: With SONET framing, the client may request the network to be “transparent” to different overhead bytes, i.e., the network must not modify these overhead bytes. The following transparency types are supported:

Section transparency: The section, line, and path overhead bytes should not be modified.

Line transparency: The line and path overhead bytes should not be modified.

Path transparency: The path overhead bytes should not be modified (default).

The corresponding terminology under SDH framing are Regenerator Section (RS), Multiplex Section (MS) and Virtual Container (VC) transparency, respectively.

Signal Types: SONET "elementary" signal types VT1.5, VT2, STS-1 SPE, STS-3c SPE, STS-1, STS-3, STS-12, STS-48, STS-192 and STS-768 are supported. SDH "elementary" signal types VC-11, VC-12, VC-3, VC-4, STM-0, STM-1, STM-4, STM-16, STM-64 and STM-256 are supported.

Concatenation: In addition to the "non-concatenated" signal types (defined above) concatenation of permitted "elementary" signal types is also supported. Two methods for concatenation are defined, contiguous and virtual concatenation. Both methods provide concatenated bandwidth of X times Container-N at the path termination. Virtual concatenation is not supported in UNI 2.0 and is currently for further study. [1]

Contiguous concatenation maintains the contiguous bandwidth throughout the whole transport. This requires concatenation functionality at each network element. Mapping of contiguous concatenated signals must be consistent with applicable standards [G.707][GR253].

Contiguous concatenation of X VC-4 signals (VC-4-Xc, X = 4, 16, 64, 256): A VC-4-Xc provides a payload area of X Container-4. The VC-4-Xc is transported in X contiguous AU-4 in the STM-N signal.

SONET equivalent is defined as the contiguous concatenation of X STS-3c SPE signals (STS-3c-Xc, X = 4, 16, 64, 256).

Connection Type Summary

Table 5-1 summarizes the valid combinations of the signal type, the transparency levels and the concatenation types supported by SDH UNI 2.0 client interfaces:

SDH Signal Type	Transparency	Concatenation	Remark
VC-11	Path	No Concatenation	VC-11 (only VC Transparency)
VC-12	Path	No Concatenation	VC-12 (only VC Transparency)
VC-3	Path	No Concatenation	VC-3 (only VC Transparency)
VC-4	Path	No Concatenation	VC-4 (only VC Transparency)
	Path	Contiguous Concatenation	VC-4-Xc (only VC Transparency)
STM-0	RS/MS	Not applicable	
STM-1	RS/MS	Not applicable	
	RS/MS	Contiguous Concatenation	Correspond to VC-4 with Transport OH
STM-4	RS/MS	Not applicable	
	RS/MS	Contiguous Concatenation	STM-4c: VC-4-4c (with Transport OH)
STM-16	RS/MS	Not applicable	
	RS/MS	Contiguous Concatenation	STM-16c: VC-4-16c (with Transport OH)
STM-64	RS/MS	Not applicable	
	RS/MS	Contiguous Concatenation	STM-64c: VC-4-64c (with Transport OH)
STM-256	RS/MS	Not applicable	
	RS/MS	Contiguous Concatenation	STM-64c: VC-4-256c (with Transport OH)

Table 5-1 – SDH Connection Types Supported

[1] Support of virtual concatenation in the UNI context implies signaling via the UNI 2.0 from the originating UNI-C to the terminating UNI-C that the indicated VCs are to be virtually concatenated. The transport network domains themselves are not involved in the virtual concatenation function. The network may choose to transport a client signal using virtual concatenation, without using the UNI to control virtual concatenation.

Table 5-2 summarizes the valid combinations of the signal type, the transparency levels and the concatenation types supported by SONET UNI 2.0 client interfaces:

SONET Signal Type	Transparency	Concatenation	Remark
VT1.5 SPE	Path	No Concatenation	VT1.5 SPE (only Path Transparency)
VT2 SPE	Path	No Concatenation	VT2 SPE (only Path Transparency)
STS-1 SPE	Path	No Concatenation	STS-1 SPE (only SPE Transparency)
STS-3c SPE	Path	No Concatenation	STS-3c SPE (only SPE Transparency)
	Path	Contiguous Concatenation	STS-3c-Xc SPE (only SPE Transparency)
STS-1	Section/Line	Not applicable	
STS-3	Section/Line	Not applicable	
	Section/Line	Contiguous Concatenation	STS-3c (with Transport OH)
STS-12	Section/Line	Not applicable	
	Section/Line	Contiguous Concatenation	STS-12c (with Transport OH)
STS-48	Section/Line	Not applicable	
	Section/Line	Contiguous Concatenation	STS-48c (with Transport OH)
STS-192	Section/Line	Not applicable	
	Section/Line	Contiguous Concatenation	STS-192c (with Transport OH)
STS-768	Section/Line	Not applicable	
	Section/Line	Contiguous Concatenation	STS-768c (with Transport OH)

Table 5-2 – SONET Connection Types Supported

Note: STS-Nc SPE with N = 3 * X (i.e. STS-3c-Xc SPE) signals are supported only when both STS-3c SPE elementary signal type and Contiguous Concatenation type are supported.

6.3 Transport of Ethernet Services

6.3.1 Service Definition

The scope of this service allows for Ethernet service transport across SONET/SDH and other G.805 server layer networks. The service model is shown in Figure 5-4. The UNI-C is connected to the UNI-N with an Ethernet interface with a physical rate that can be 10 Mbps, 100Mbps, 1Gbps, or 10 Gbps. The scope of network connectivity is point-to-point Ethernet Private Line service and Ethernet Virtual Private Line service [MEF.6] [G8011].

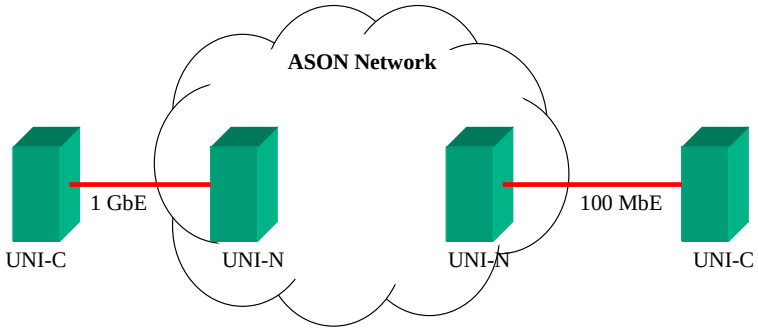

Figure 5-4 UNI 2.0 Ethernet Transport Model

For each Ethernet service required between two Ethernet UNI clients, an Ethernet call is created. This results in the creation of one or more Ethernet connections. The Ethernet connection may not be established until the underlying server layer connections are created.

An Ethernet call is therefore adapted into one or more server layer calls. In turn, each server layer call consists of one or more server layer connections. This is an instance of a multi-layer call and the architecture of multi-layer calls is taken from [G8080] which defines a relationship between UNI-N functions at different layers.

Non-disruptive bandwidth modification and CE-VLAN ID modification are available with this service. Several mechanisms can be used to provide the non-disruptive modification. All mechanisms involve call modification (Section 6.6).

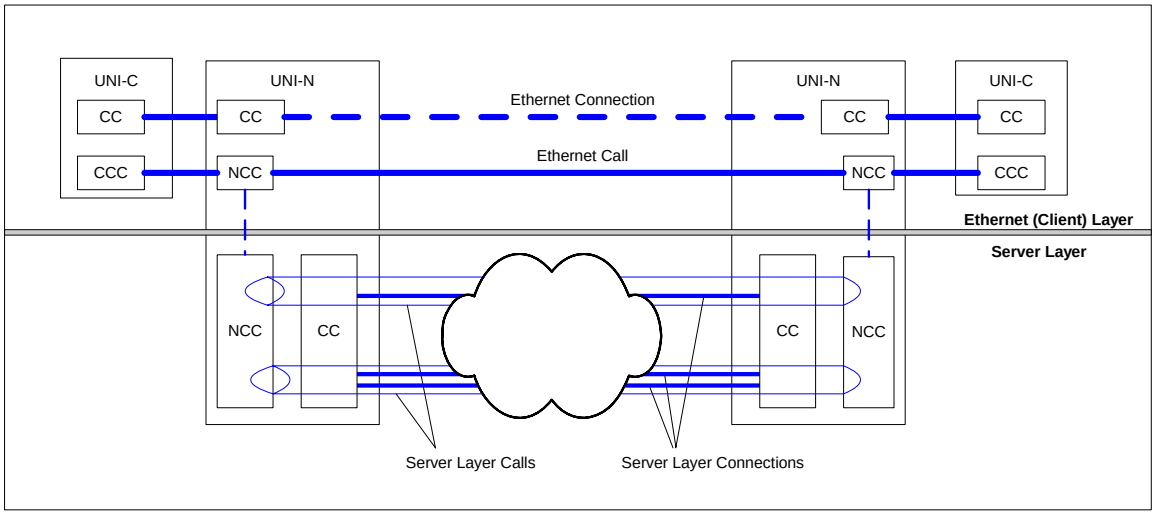

Figure 5-5 – Server Layer Calls and Connections vs. Ethernet Connections and Ethernet calls

In Figure 5-5, the UNI-N function is shown as ASON Network Call Controllers (NCCs). When a server layer (e.g., SONET/SDH) is supporting a client layer (e.g., Ethernet), the UNI-Ns are aware of the interlayer relationship. The server layer calls created upon request by an Ethernet NCC could in turn make an interlayer request to their server layer in a recursive manner.

6.3.2 Service Architecture

Two service scenarios are described here:

Scenario 1 – Ethernet Private Line (EPL)

As shown in Figure 5-6, two Ethernet clients share a single point-to-point connection provided by the network, an Ethernet Virtual Connection (EVC). A single Ethernet call is created. This corresponds to the Ethernet Private Line service defined in [G8011.1] and E-LINE with all-to-one bundling in [MEF10.1].

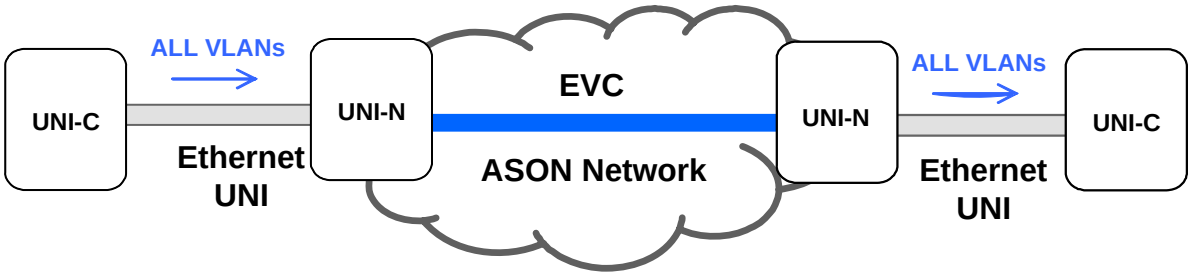

Figure 5-6 Ethernet Private Line – Scenario 1

The Ethernet services provided by UNI SHOULD allow Ethernet clients to:

- Use any standard Ethernet interface of 10G, 1G, 100M and 10M to access the network
- Request dynamic connection services from the Network Management Interface (NMI), or User to Network Interface (UNI). Note in the case of the NMI, the calling call controller is not involved
- Request one point-to-point connection between the two Ethernet interfaces with any bandwidth profile up to its UNI PHY data rate.
- Increase or decrease the Committed Information Rate for existing connections up to its UNI PHY rate. [MEF.13] recommends specific granularities for the Committed Information Rate.
- Request end-to-end Ethernet service even in the case where the source and destination Ethernet interfaces operate at different rates.
- Setup, modify and tear down UNI connections via out-of-band, out-of-fiber or in-fiber signaling methods.

Scenario 2 – Ethernet Virtual Private Line

Shown in Figure 5-7 are four Ethernet Virtual Connections (EVCs). Each EVC is dedicated to a set of Ethernet CE-VLAN identifiers on an Ethernet interface. Each Ethernet Virtual Connection requires an Ethernet call; therefore we have four Ethernet calls. This is an example of the Ethernet Virtual Private Line service defined in [G8011.2] and E-LINE in [MEF10.1]. EVPL services also provide support for untagged and priority-tagged frames. In this case, the CE-VLAN ID associated with untagged and priority-tagged frames is configured on the UNI-C and UNI-N. On the UNI interface, the frames are not tagged but they are mapped on the EVC based on the configured mapping at the UNI-N.

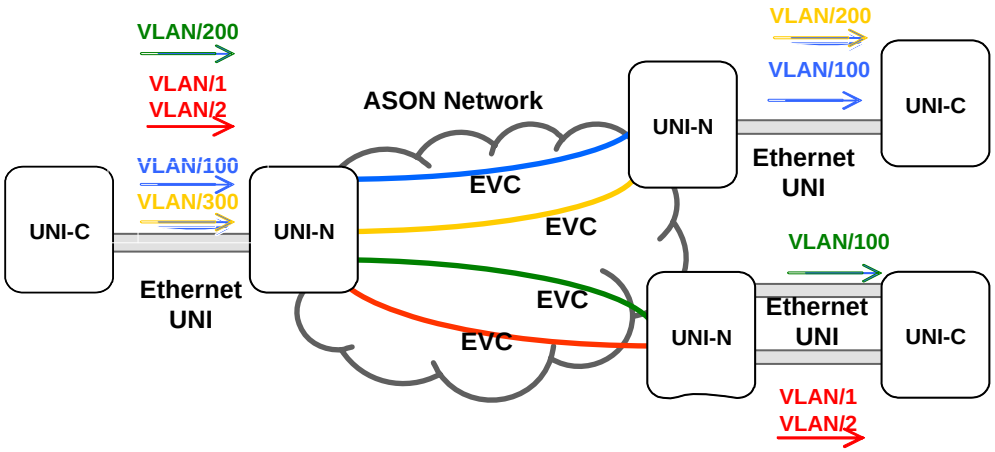

Figure 5-7 Ethernet Virtual Private Line – Scenario 2

In addition to the capabilities described for Scenario 1, Ethernet Virtual Private Line services allow the Ethernet client to:

- Request multiple Ethernet connections between the same pair of Ethernet interfaces, and each Ethernet connection can be with any bandwidth profile up to its UNI PHY rate. The aggregate of all requested Committed Information Rates must not exceed the UNI PHY rate.
- Request any one connection to be dedicated to a certain set of CE-VLAN identifiers in order to guarantee service level for a subset of the traffic on an Ethernet interface.
- Request multiple connections from the same Ethernet interface, each to an Ethernet interface at a different UNI. Each connection can be with any bandwidth profile up to its UNI PHY rate. The aggregate of all ingress Committed Information Rates must not exceed the UNI PHY rate and at any egress, the aggregate of all terminating Committed Information Rates must not exceed the UNI PHY rate.
- The traffic is directed to the appropriate connection based on a set of CE-VLAN identifiers.
- Allow for optional end-to-end CE-VLAN preservation. CE-VLAN preservation is illustrated with CE-VLAN ids 1 and 2 in Figure 5-7. CE-VLAN preservation is mandatory if there are multiple CE-VLAN identifiers mapped onto the same EVC. If a single CE-VLAN identifier is mapped onto an EVC, CE-VLAN preservation is optional and the CE-VLAN identifier used at both ends could differ. This is illustrated in Figure 5-7 with CE-VLAN identifier 200 on the left UNI being swapped to 100 at the right UNI.

6.3.3 Ethernet Interfaces

Table 5-3 summarizes the supported Ethernet client interfaces.

Ethernet Interface Type
10 Mbit/s (10Base)
100 Mbit/s (100Base)
1 Gbit/s (1000Base)
10 Gbit/s (10Gbase)

Table 5-3 – Ethernet Interface Types Supported

6.3.4 Bandwidth Profiles

There are three types of bandwidth profiles that can be applied to Ethernet services: per MEF UNI, e.g. OIF UNI logical port, per EVC and per CoS within an EVC. The services offered over UNI 2.0 have the same bandwidth profile at the source UNI and destination UNI.

6.3.4.1 Bandwidth Profile for EPL

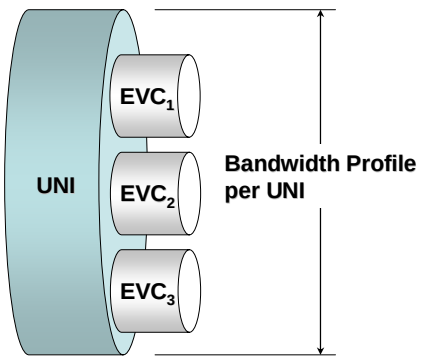

Figure 5-8 – Bandwidth Profile per MEF UNI (MEF10.1 Figure 14)

For UNI 2.0 EPL services, the bandwidth profile can be applied to a MEF UNI as described in Figure 5-8 but applies in the case where there is a single EVC per MEF UNI.

6.3.4.2 Bandwidth Profile for EVPL

For EVPL services, the bandwidth profile can be applied to either an EVC, as illustrated in Figure 5-9 or a class of service within an EVC, as illustrated in Figure 5-10.

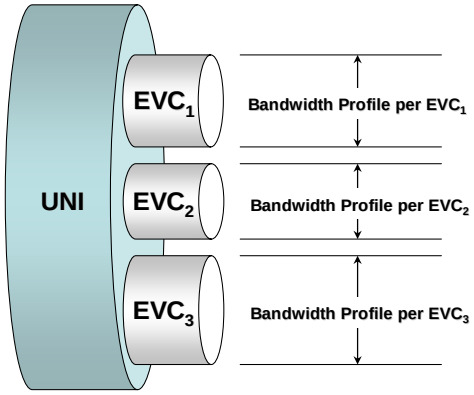

Figure 5-9 – Bandwidth Profile per EVC (MEF10.1 Figure 15)

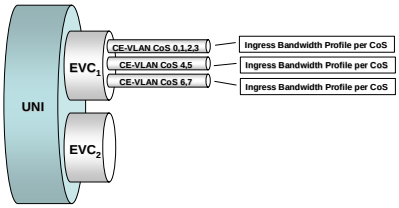

Figure 5-10 - Bandwidth Profile Per CoS within an EVC (MEF10.1 Figure 16)

6.4 Transport of OTN Connections

6.4.1 Service Definition

The scope of this service is to enable requests for Optical Data Unit of order k (ODUk) or an Optical Channel (OCh) connection service across G.805 server layer networks. This service assumes that OCh links are provisioned at the UNI and E-NNI level.

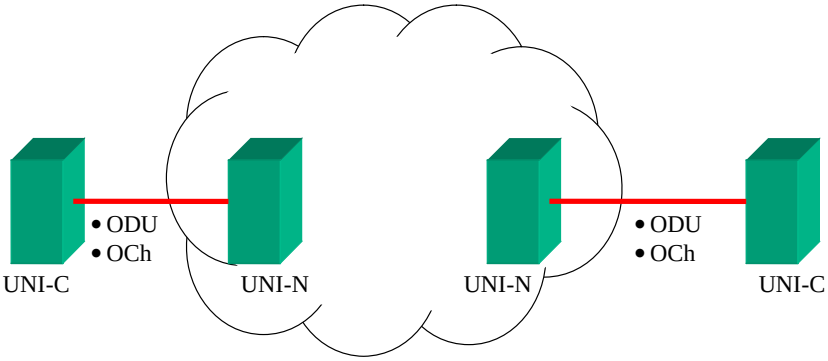

Figure 5-11 – OTN Service Model

6.4.2 Service Architecture

[G872] defines a layered structure for the OTN. It defines the hierarchy and relationships between an individual wavelength signal and multi-wavelength signals. Figure 5-12 shows the following relationships between different layers of the OTN:

- Optical Channel (OCh) Layer. This layer provides end-to-end networking of optical channels for transparently conveying client information of various formats. Each OCh can be mapped into an Optical Channel Carrier (OCC), which is an individual wavelength.
- Optical Multiplex Section (OMS) layer. This layer provides functionality for networking of a multi-wavelength optical signal. A "multi-wavelength" signal includes the case of just one optical channel.
- Optical Transmission Section (OTS) layer. This layer provides functionality for transmission of optical signals on optical media of various types.

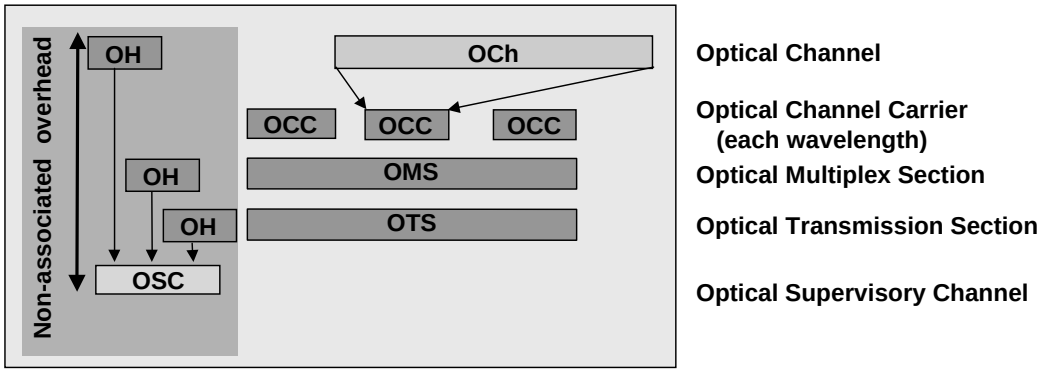

Figure 5-12 – Optical Transport Network Layer Relationships

The OCh layer is further partitioned as shown in Figure 5-13. [G709] defines additional layering and overhead using a digital wrapper containing both additional overhead bytes and FEC bytes. Also shown in Figure 5-13 are three OCh sub-layers:

- The Optical Payload Unit (OPU). Client signals are mapped into an OPU frame.
- The Optical Data Unit (ODU). An OPU is mapped into an ODU, which is a digital switching layer to support client connection protection and monitoring.
- The Optical Transport Unit (OTU). An ODU is mapped into an OTU, which is a networking layer providing FEC and protection and monitoring of the optical section. The value of the suffix k in OTUk

indicates the order, or bit rate. (A k value of 1, 2 or 3 indicates an OTU capacity of 2.5G, 10G and 40G, respectively.)

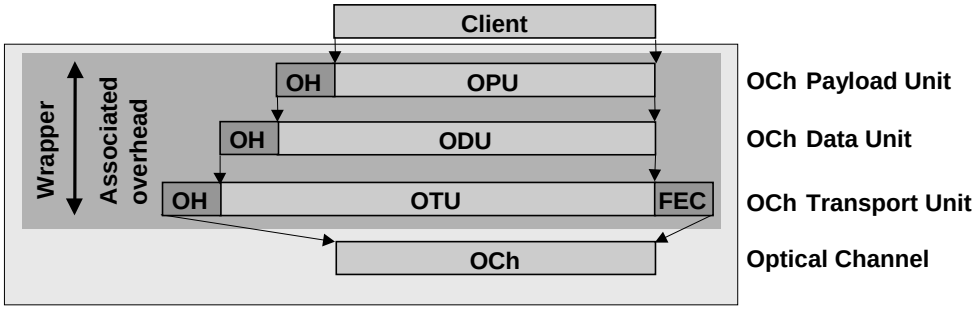

Figure 5-13 – Optical Channel Layer Relationships

Although [G709] defines several networking layers only the OCh and the ODUk layers are defined as switching layers. Therefore UNI connections will be supported at the ODUk and OCh layers.

Table 5-4 summarizes the valid combinations of the signal type and the concatenation types supported by OTN client interfaces.

OTN Signal Type	Concatenation
ODU1	No Concatenation
ODU2	No Concatenation
ODU3	No Concatenation
OCh	Not Applicable

Table 5-4 – OTN Connection Types Supported

The signaling transport configuration for an OTN UNI could use out-of-fiber signaling or in-fiber signaling using the GCC0 byte (as in section 8.2).

6.5 Enhanced Security

Policy Control does not include any enhancements since UNI 1.0 but is included for completeness in sections 6.5.1, 6.5.2 and 6.5.3. Security enhancements are described in section 6.5.4.

6.5.1 UNI Policy Control

The transport network MUST provide appropriate mechanisms to ensure accurate and authorized usage of network resources and client accountability. Collectively, these mechanisms are often referred to as *policy control*. Policy-based criteria are applied in addition to resource availability considerations when deciding whether a connection request can be accommodated within the transport network. Policy control rules MAY define conditions on parameters such as source and destination addresses, priorities, bilateral agreements among service providers, time-of-day constraints, cost constraints, etc. Policy control is also commonly associated with the mechanisms required to perform accounting. Upon initial deployment, policy control might employ simple rules, like for example, *"approve all requests on behalf of a given user*

group received from a given UNI-C agent, if the identity of the requestor can be verified". As more experience is gathered from initial deployments, it is envisioned that policy rules will become increasingly more sophisticated.

In order to support policy control, two main architectural entities are needed: the Policy Decision Point (PDP), where policy decisions are made and the Policy Enforcement Point (PEP), where policy decisions are actually enforced. The PEP resides within a transport network node, such as an OXC. The location of the PDP, however, depends on multiple factors, such as:

- The complexity of policy rules, including the computational load, type of software support and data access required. For example a policy might require complex cryptographic operations not supported within an OXC or access to a credit database which is physically located on a remote server. In this case, the PDP SHOULD be located in a remote server.

- The frequency of events requiring policy decisions. For example, connection set-up requests might be received infrequently thus reducing the computational complexity on the PDP.

- The intelligence and flexibility of the transport networking device. A sophisticated and easily upgrade-able transport network node is a better candidate to host the PDP.

The combination of the above factors determines whether the PDP SHOULD be co-located with the UNI-N agent or implemented on a remote policy server. If an external policy server is employed, a standardized protocol SHOULD be used for the communication between the PEP and PDP. This allows management of multiple PEPs from a single PDP and facilitates the integration of (standard) policy servers with multiple transport network elements. The COPS protocol [RFC2748] has been standardized by the IETF for PEP-PDP communication.

Specification of the UNI protocol does not depend on the placement of PEP and PDP modules within the transport network. Whether an external PDP is needed depends on the above factors, namely the frequency and complexity of policy decisions and the processing capabilities of the transport network element. If an external PDP is required, it is RECOMMENDED that the COPS protocol be employed.

As shown in Figure 5-14, the PDP MAY further access an external server or database, for example to retrieve policy rules, centrally stored accounting information, etc. These additional mechanisms are not being specified by the OIF.

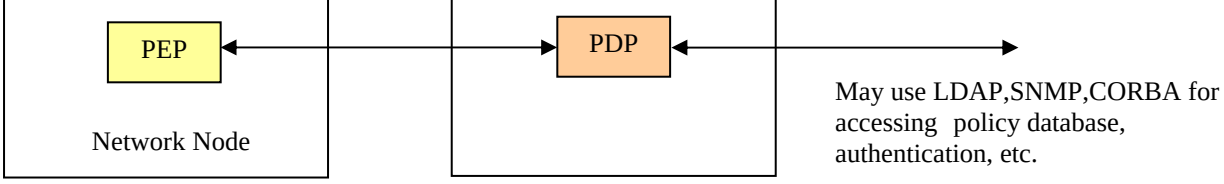

Figure 5-14 - PEP and PDP

6.5.2 Sample Policies Applicable to Connection Provisioning

This section discusses sample policies that could be employed for controlling connection provisioning across the UNI. It is included for informational purposes only and is not intended to suggest

standardization of any policies. In each of the cases presented, the information required to make the policy decision is also identified.

6.5.2.1 Time-Of-Day-Based Provisioning

A user's contract with a carrier allows placement of connection requests during a specific time of the day and/or day of the week. As an example, the connection could be used for data backup over a storage area network during night hours. In this scenario the UNI-N agent needs to verify whether connection requests are received during the contracted hours. All information required to make the policy decision (time of request receipt) is implicitly contained in the UNI signaling message.

6.5.2.2 Identity And Credit Verification For Connection Requestor

A carrier's carrier operates a *bandwidth exchange* which allows carriers to dynamically "trade" optical connections. The bandwidth exchange receives requests from a very large number of carriers. Multiple UNI-C agents, representing different carriers, might be contacting the same UNI-N agent in the carrier's carrier network. It is imperative for the carrier's carrier to be able to verify the identity of the originator of the request. Additionally, the ability of the requestor to pay for the service MAY also need to be verified. This might require information such as an account number or credit authorization. Policy based admission control at the UNI-N involves positive verification of the identity and creditworthiness of the requestor. In this scenario, the information required to make the policy decision might extend beyond that contained in mandatory attributes. Reference [RFC2752] describes identity representation when RSVP is used as the UNI 2.0 signaling protocol.

6.5.2.3 Usage-Based Accounting

Usage-based accounting can be supported using the contract identifier, which refers to the service contract of the connection owner. The contract identifier MAY be carrier specific, and it can be used for accounting, billing and SLA verification. Due to the sensitivity of the information contained, the contract identifier might be encrypted to protect the privacy of the originator.

6.5.3 Policy Control Mechanisms Associated with UNI Signaling Protocols

The protocol specific implementation agreements define a policy data object that can be used to map optional objects that MAY be used for policy control across the UNI. Use of the policy data object to carry the contract ID is defined in the protocol specific implementation agreements. This object MAY be used to carry other policy-related data in the future.

6.5.4 UNI 2.0 Security

The security functionality for UNI 2.0 has been enhanced from the security functionality provided in UNI 1.0 and therefore supersedes the security guidance provided for UNI 1.0. The security functionality in UNI 1.0 is, for the most part, based on what is specified in the underlying protocols. The UNI 1.0 Implementation Agreement states that this was an expedient choice and was likely to change in subsequent versions of the UNI. Overall, the goal of the Security Extension for the UNI 2.0 control protocol is to support confidentiality, data origin authentication, data integrity, and replay detection on a per-message basis. The security mechanisms are optional to implement. The Security Extension can be found in [OIF-SEP-01.1] and [OIF-SEP-02.0]. Below is an overview and rationale for the Security Extension.

6.5.4.1 UNI 2.0 Security Requirements

Security mechanisms are required to protect the signaling and routing of optical connections, because these connections carry high volumes of data and consume significant network resources. Security mechanisms safeguard transport networks against attacks that compromise their control plane, seek unauthorized use of their resources, or attempt to gain unauthorized information about their configuration and usage.

Communication protocols usually require two main security mechanisms: *integrity* and *confidentiality*. Integrity mechanisms ensure *data origin authentication* and *message integrity* of UNI messages so that unauthorized UNI operations can be detected and discarded. For example, the UNI message integrity service can prevent a malicious UNI-C agent from causing denial of service at a service provider by sending an excessive number of forged connection creation requests. Integrity mechanisms detect and reject attempts to forge messages and to reorder, duplicate, truncate, or otherwise tamper with the proper sequence of messages. These mechanisms can provide *replay protection* and *non-repudiation.* Replay protection is used to detect any reinsertion of previously used messages into the communications channel, which can be used to gain unauthorized access. Replay protection is normally achieved by adding sequence numbers to the messages or by relying on another protocol (e.g., TCP) to guarantee the proper sequencing of the message stream above the integrity service. Non-repudiation provides evidence that prohibits a sender from denying sending a message, thus holding the sender accountable. This may be desirable for accounting and billing purposes.

Message integrity and confidentiality are normally achieved using symmetric cryptographic algorithms. These algorithms require pairwise shared secret keys and do not provide non-repudiation. To facilitate the use integrity and confidentiality services, public-key or *asymmetric* cryptographic algorithms are typically used, initially, to provide *two-way peer entity authentication* and *key agreement.* Asymmetric algorithms also provide *digital signatures,* which can be used to implement a non-repudiation service. The use of asymmetric algorithms MAY be supported by a public-key infrastructure (PKI) or some other, community-defined, key assignment scheme. Asymmetric algorithms are typically more computationally intensive than symmetric algorithms. *It is expected that from the point of view of UNI 2.0 requirements, the most important security feature could be message integrity.* Confidentiality of UNI messages is also likely to be desirable, especially in cases where UNI message attributes include information private to the communicating parties (client and transport network operator). Examples of such attributes include details about the users, such as account numbers, contract identification numbers, etc.

The potential use of non-co-located equipment increases security requirements. In this scenario, it is assumed that the UNI-C and UNI-N nodes are connected via networking devices such as layer 2 switches and IP routers. Because these devices can belong to different network operators and may be outside the control of the service provider, control communication between the UNI-C and UNI-N is subject to increased security threats, such as IP address spoofing, eavesdropping, denial of service attacks, and unauthorized intrusion attempts. To counter these threats, appropriate security services need to be deployed to protect the UNI signaling and SCN.

Just as any other functionality, security consumes resources, and it must be designed from a point of view that keeps the costs and benefits properly aligned. Therefore, security SHOULD be:

- *Optional to implement and to use.* Some users MAY decide that they can implement adequate protection by other means (e.g., perimeter access controls and firewalls), so that protocol security is unnecessary. Vendors who choose to serve these users MAY offer a product without the security services.
- *Interoperable.* The purpose of having a standard set of security services in UNI 2.0 and NNI is to ensure that protocol security interoperates between vendors' products within carriers' networks. Thus, the security services defined SHOULD have as few methods, formats, optional features, and algorithms as possible. The same methods SHOULD work with different Layer 2 protocols and with IPv4 or IPv6.
- *Synergistic with other functionality.* Security for control protocols (including signaling, routing, and discovery) is less costly and less error prone to implement and deploy if it is the same solution used for bearer traffic, management, or user services like VPNs.
- *High assurance.* Solutions SHOULD be preferred if they are already well standardized, extensively analyzed, and widely used.

- *Readily available in reference implementations.* This encourages the development of complete, interoperable implementations.
- *High quality.* The algorithms and protocols SHOULD be chosen based on the level of security they provide. There SHOULD be no known defects or serious weaknesses, and the security SHOULD be designed to provide secure operation within a broad model of both active and passive attacks.
- *Efficient.* Standard state-of-the-art microprocessors SHOULD be able to perform many instances of the authentication and key negotiation protocol and tens of megabits of traffic protection per second of processing time. Dedicated hardware modules SHOULD be able to increase these numbers by two orders of magnitude.

In summary, to satisfy the above requirements, security for UNI 2.0 control protocols MUST support confidentiality, data origin authentication, data integrity, and replay detection on a per-message basis. Two-way authentication of the parties MUST be integrated with an automated key management system.

6.5.4.2 Service Architecture

The UNI and NNI define an allowable set of Service Invocation Configurations and a set of Signaling Transport Configurations between UNI-C, UNI-N, and NNI devices. Note that all of these devices are called ONEs (Optical Network Elements) in [SEC EXT]. The relationship between IPsec and these invocation and transport configurations must be understood in order to describe fully the security environment and solution proposed by this security extension.

Figure 5-15 demonstrates a possible deployment scenario using the minimum acceptable implementation for UNI compliance. In this case, the SCN Realization is provided through Out-of-Fiber Signaling with direct service invocation. Note that this diagram demonstrates the simplest case of Service Invocation Configuration options, where the UNI-C and UNI-N agents are providing direct services for the Clients and TNEs. A single IPsec SA pair is required to secure the UNI communication link. Due to the nature of IP networks, it is likely that the communication link may need to traverse an intervening Firewall or NAT device. This results in a requirement to use IPsec encapsulated in UDP or IPsec in Tunnel mode with the intervening device providing the IPsec Tunnel endpoint.

Figure 5-16 demonstrates a more complicated scenario. Security Extensions are deployed in a UNI/NNI network where proxy agents and optional services are used. A proxy agent is used for both the UNI-C and UNI-N. In addition, the UNI option for multiple SCNs is demonstrated. The UNI specification considers the Internal Signaling Interface (ISI) as out-of-scope and therefore could be another IP Network vulnerable to threat agents. IPsec SHOULD be used to secure these connections as well. The result is a scenario in which the IPsec policy may be required to be granular to the UNI/NNI protocol level to map to the IPsec services properly.

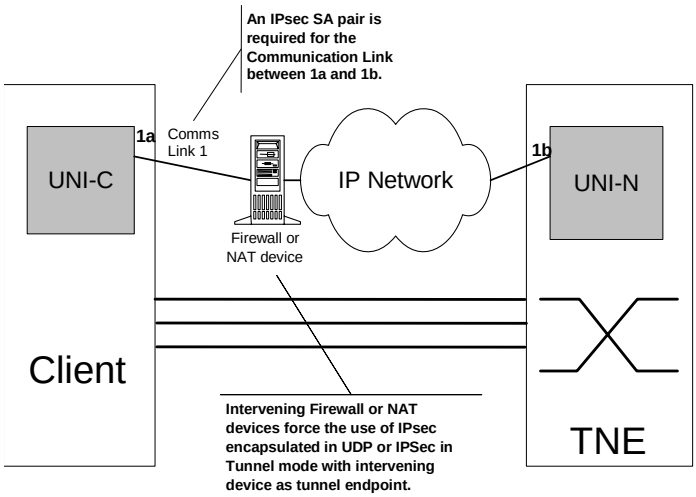

Figure 5-15 IPsec/UNI/NNI Scenario 1.

Under the UNI/NNI architecture, Client and TNE systems may be deployed using a variety of proxy or direct UNI-C and UNI-N agents. Furthermore, each proxy UNI-C or UNI-N device can serve as the Agent for multiple UNI Clients or TNE systems. This would result in multiple IPsec SA pairs being used for each combination of Client and TNE devices. The implementation selection of direct or proxy agents should be considered when developing systems that support these security extensions. Even though the scenarios described here have been limited to services provided between UNI elements, the same principles apply between NNI elements.

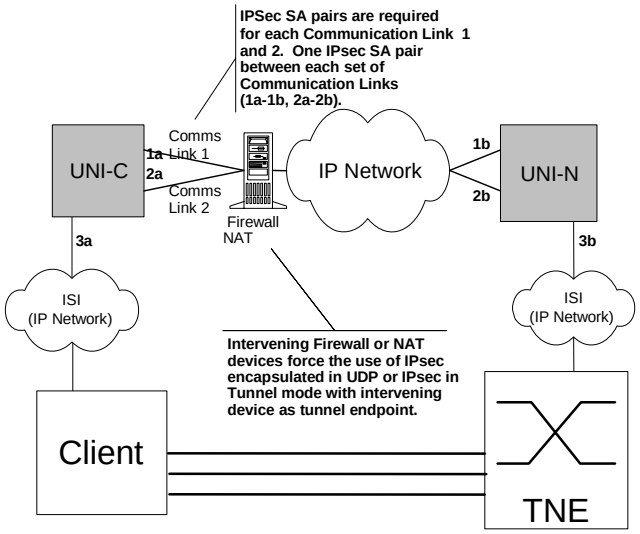

Figure 5-16 IPsec/UNI/NNI Scenario 2.

6.5.4.3 Security Services and Mechanisms for UNI 2.0

The UNI 1.0 IA specifies a single security service per signaling protocol. It does not satisfy many of the requirements above. It also stated:

The standardization of more flexible and inclusive security options, such as IPsec, as well as the profiling of such mechanisms to make their implementation simpler, more efficient and more straightforward, may be considered in future versions of the optical UNI.

UNI 2.0 moves forward to consider such security options.

During the design of UNI 2.0, analysis of UNI 1.0 security services revealed:

1. *Incompleteness.* Certain needs like confidentiality and key management were not met.
2. *Inflexibility.* Algorithms, key sizes, and other parameters cannot be adjusted, as needs change.
3. *Incompatibility.* Protocol-by-protocol solutions specified in subtly different ways were provided for no technical reason.
4. *Lack of requirements driven design.* Security should follow from requirements, not from what's "on the shelf."
5. *Error proneness.* It takes a lot of effort to get security right once, so it is far better to reduce the number of distinct security solutions. This becomes more important as the number of protocols included in the UNI increases.
6. *Unenforceability.* No method exists to enforce what security must be used where.

The UNI 2.0 Enhanced Security feature provides:

- A single, optional, security system with a complete set of security services to work across the UNI 2.0 signaling, discovery, and any other control protocols.
- An *optional* Security Extension to *implement* and to *use*. The goal is to make security *interoperate* when it is implemented and used.

Therefore, use of the UNI 1.0 security services are deprecated in UNI 2.0, and optional use of a common network layer security system based on IPsec, as stipulated in the UNI 2.0 Security Extension [OIF-SEP-01.1] and [OIF-SEP-02.0], is specified as the method for protecting all of the IP-based protocols in UNI 2.0.

The benefits of the Security Extension [OIF-SEP-01.1] and [OIF-SEP-02.0] are:

1. To move the decision as to what security services and mechanisms to use from the protocol designer to the network operator.
2. To reduce the number of distinct security solutions and therefore the total cost of implementation and deployment.
3. Similarly, to increase the assurance that security is working correctly.
4. To add confidentiality, which may be needed to protect customers' billing and call records and other data including details about users, traffic loads, and network configurations.
5. To add automated key management, which increases interoperability and reduces the likelihood that manual intervention is required to make security work.
6. To provide a policy-driven solution that allows users to ensure security is working where needed.

The Security Extension [OIF-SEP-01.1] contains a profile for using IPsec [RFC4301], which defines a suite of protocols for providing various security services at the IP layer, for both IPv4 and IPv6. These include traffic protection, using the *Encapsulating Security Payload (ESP)* [RFC2406], and key management, using the *Internet Key Exchange (IKE)* [RFC2409, RFC2407]. The services offered by IPsec include entity authentication, connectionless integrity, data origin authentication, replay protection and confidentiality (encryption). An important characteristic is that these services are provided at the IP layer, *offering protection for IP and upper layer protocols.* As such, IPsec can be applied to all IP based protocols used to realize the UNI signaling, as well as to protect other control plane protocols, e.g., for discovery.

Since the approval of [OIF-SEP-01.1], the IETF has revised the above components of IPsec to improve their functionality, performance, and security. Therefore, the OIF has incorporated these revisions into [OIF-SEP-02.0]. See [RFC4306], [RFC4303], and [RFC4301] for additional details. Also, [OIF-SEP-02.0]

specifies newer, more secure cryptographic methods, in particular the Advances Encryption Standard (AES) and the replacement of the now broken hash function MD5.

ESP provides integrity, data origin authentication, replay protection, and confidentiality. The mechanisms are designed to be algorithm independent and, IPsec accommodates an extensible range of cryptographic algorithms. IKE is an elaborate two-way peer entity authentication, key management and security services negotiation protocol, which include multiple algorithms and modes of authentication.

It is recognized that IPsec is a relatively complex and heavyweight suite of protocols. Therefore, the profile in the Security Extension [OIF-SEP-01.1] aims at reducing the number of options needed. The most complex part of IPsec is the key management, IKE, and IKE has been redesigned by the IETF to simplify it, remove unneeded options, improve the documentation, and make minor improvements. The resulting protocol, IKEv2, is specified and profiled in [OIF-SEP-02.0].

It is also recognized in this specification that using the IPsec suite of protocols to protect UNI control messages offers a number of advantages. In particular, IPsec provides confidentiality, which is offered by neither of the signaling transport mechanisms, includes a key management protocol, and allows for a single security solution for all protocols used to realize the UNI signaling, as well as link state routing protocols (OSPF and IS-IS).

6.6 Non-Disruptive Service Parameters Modification

Several mechanisms can be used to provide non-disruptive service parameters modification. All mechanisms involve Call Modification. It is possible to perform call modification by adding or removing a connection from an existing call or by modifying the service parameters of an existing connection within an existing call.

6.6.1 Bandwidth modification

There are two main service architectures to be considered, one for bandwidth modification of calls over Ethernet UNIs, and one for bandwidth modification of calls over TDM. These two architectures arise due to the fact that changing the bandwidth of an existing connection in the Ethernet case does not result in a change in adaptation, whereas for the SONET/SDH or OTN case an adaptation change MAY be required. Therefore, an Ethernet connection bandwidth can be modified but in the SONET/SDH case, we only allow changes that do not modify the adaptation.

Knowledge of the use of UNI connections in a Virtual Concatenation Group (VCG), the use of LCAS, or the use of GFP adaptation, is not necessarily shared by the UNI-C and UNI-N. If a client device combines several of its connections into a VCG and uses a virtual concatenation payload, this is independent of UNI control since this constitutes client use of the connections and is effectively a client application. Similarly, if the network side accepts a UNI-C request and chooses to use GFP, VCAT, and/or LCAS, this is not visible to the client device.

6.6.1.1 Bandwidth modification principle

Bandwidth modifications can be requested by the UNI-C as long as the request does not require a change in the adaptation. The UNI-C may request bandwidth modification by one of the following:

- Changing the bandwidth of a connection by modifying the rate directly. This applies to Ethernet only.
- Changing the bandwidth of a connection by modifying the multiplier field of an existing connection.
- Adding connections to an existing call.
- Removing connections from an existing call.

6.6.1.2 SONET/SDH service

When the UNI resources are SONET/SDH (as in UNI 1.0), there are a number of bandwidth modification cases to consider. These are:

1. VCn changes. Do not allow n to change as this is an adaptation change and is considered a major service change, i.e., cannot change VC11 to VC12. A new call is needed.
2. VCn-xc changes. Do not allow x to change because it is considered an adaptation change, i.e., cannot change VC4-4c to VC4-16c. A new call is needed. Changes to n are prohibited because it is considered an adaptation change as per #1.
3. m*VCn changes. Allow changes to m, i.e., 1*VC4 to 5*VC4. This adds/removes connections from a single call and does not change the adaptation in use for the call. Changes to n are prohibited because it is considered an adaptation change as per #1.
4. m*VCn-xc. Allow changes to m, i.e., 1*VC4-4c to 3*VC4-4c. Changes to n or x are prohibited as they are considered adaptation changes as per #1 and #2.

Figure 5-17 shows an example where bandwidth is added to a TDM call by changing the multiplier field, i.e., m. For example, there could be one STM-16 link for a UNI bearer. A call has one VC3 in one of the STM-16 links. When the call is modified to add bandwidth, a 2nd VC3 is added to the call. It can come from any of the 3 STM-16s.

The client is free to put the two connections into a common Virtual Concatenation Group. This is not visible to the UNI.

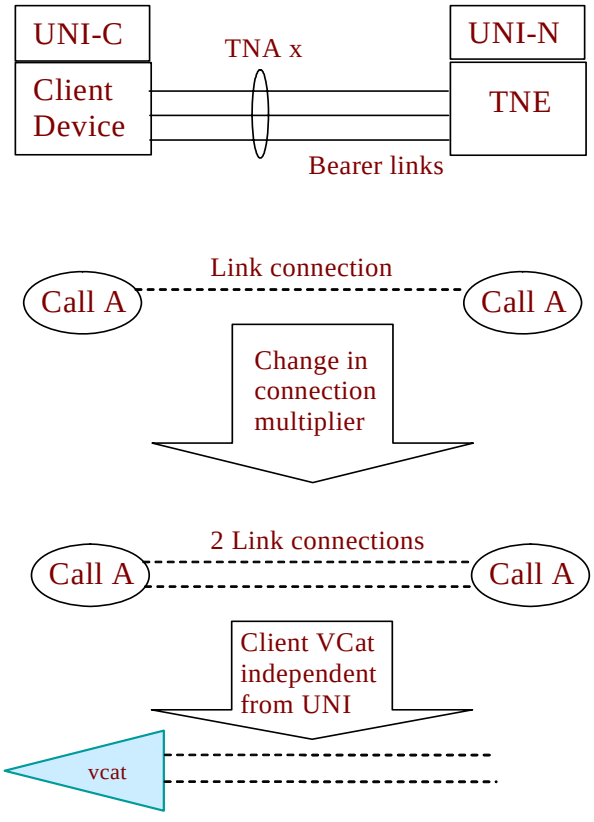

Figure 5-17 Bandwidth Modification for [G805] Layer Network

6.6.1.3 OTN Interfaces

For OTN clients, the number of connections MAY be modified in the OTN Traffic parameters attribute using the Multiplier (MT) field. As with HO SONET/SDH service, the principle of adding/removing integral number of connections is applied.

6.6.1.4 Ethernet service

Bandwidth modification can be applied to Ethernet services. Ethernet service support is described in Section 6.3. The signaling request includes a value with 1Mb/s increment for the Bandwidth Encoding based on the data service bandwidth that has been requested. To modify the bandwidth of an Ethernet call, there are two cases to consider - modifying the bandwidth value or modifying the number of connections associated with the call. These are illustrated in Figure 5-18 in which the bearer consists of 3 GE links.

The call could be modified to increase or decrease the bandwidth of an existing connection, or a connection could be added or deleted from the call.

6.6.2 Non-Disruptive CE-VLAN ID modification

For EVPL services, it is also possible to non-disruptively modify the CE-VLAN ID to EVC mapping. The modification is non-disruptive to the traffic associated with the CE-VLANs for which the CE-VLAN ID to EVC mapping is not modified but traffic associated with CE-VLANs for which the mapping is modified is impacted. This is illustrated in Figure 5-19. The original mapping of CE-VLAN IDs 1, 2 and 3 to an EVC is modified by removing CE-VLAN ID 3 from the mapping. This results in a final mapping of CE-VLAN IDs 1 and 2 to the EVC without any disruption to their respective traffic. Traffic associated with CE-VLAN ID 3 is impacted by this mapping modification.

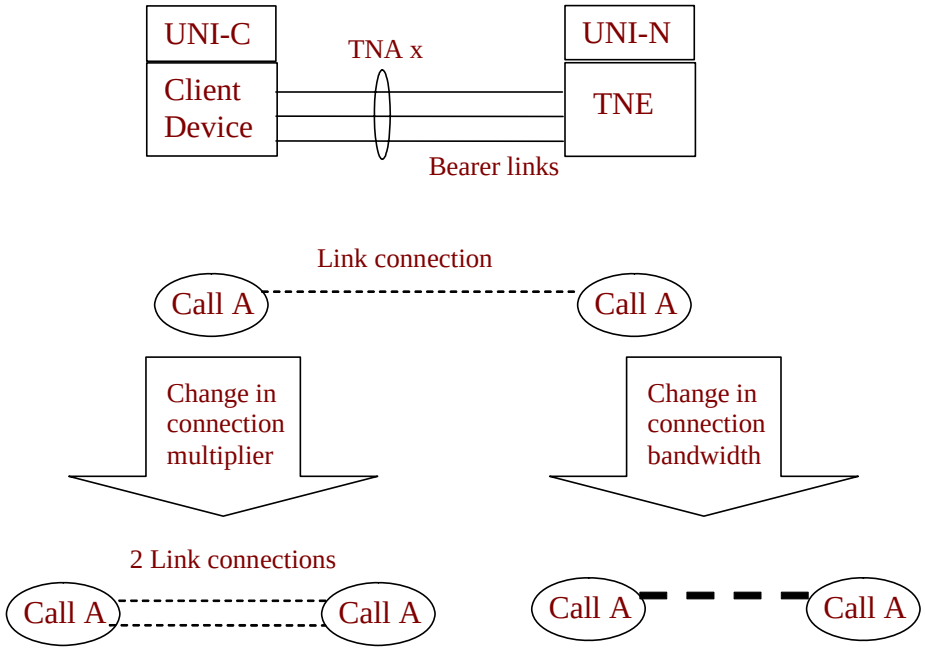

Figure 5-18 - Bandwidth Modification for Ethernet Interface

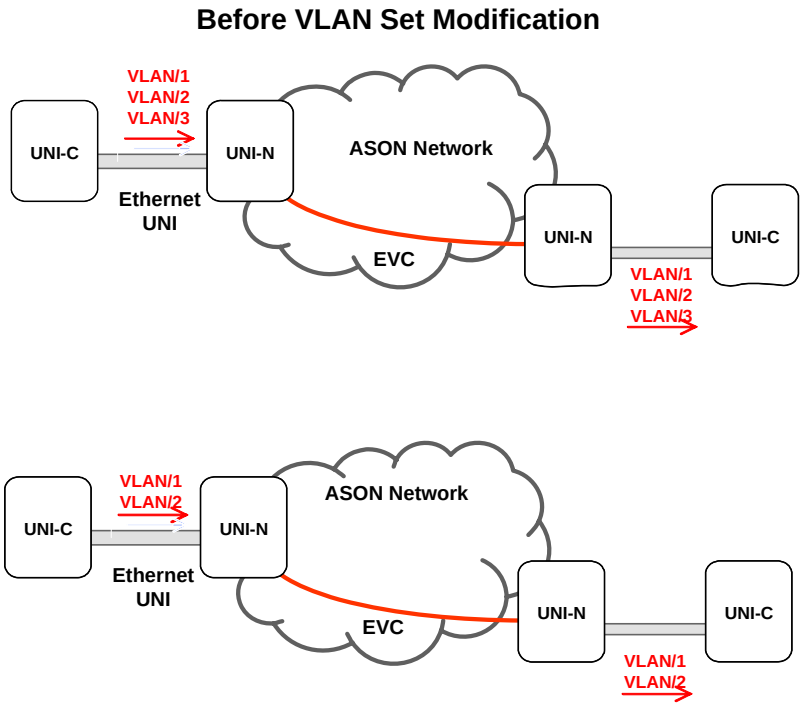

Figure 5-19 - VLAN set modification

6.7 Supporting Procedures

The following procedures that support UNI signaling are specified in this document.

6.7.1 Signaling Adjacency Maintenance

UNI signaling requires a signaling adjacency between the client-side and the network-side signaling entities. Different SCN configurations are possible, as defined in Section 8. UNI 2.0 supports procedures for maintenance of the signaling adjacency under all these configurations, as described in the protocol specific IAs.

6.7.2 Mandatory and Optional Procedures

As mentioned here above, several procedures are described within the UNI 2.0 specification. Some of them are mandatory (e.g., signaling protocol and signaling adjacency maintenance procedures) while others are optional. In order to be UNI 2.0 compliant, a device (UNI-C or UNI-N) MUST implement all the mandatory procedures and their corresponding protocol implementations. Among mandatory procedures, there are sometimes choices. For UNI signaling to work, the UNI-N and the UNI-C MUST use compatible choices for mandatory procedures. This can only be ensured by prior administrative communication.

Table 5-5 summarizes the UNI 2.0 procedures, the mandatory and optional status of these, the choices available for implementing the procedure, and the minimum acceptable implementation for UNI 2.0 compliance:

UNI 2.0 Procedures	Status	Choices	Minimum Acceptable Implementation for UNI 2.0 Compliance
Signaling	Mandatory	Refer to the protocol specific implementation agreements.	Compliance to at least one of the protocol specific implementation agreements.
SCN Realization	Mandatory	In-fiber, Section DCC; In-fiber, Line DCC; In-fiber, GCC0; Out-of-fiber, IP network; In-fiber, Ethernet OAM frames; Out-of-fiber, Dedicated SONET/SDH, OTN or Ethernet Connection	At least one of the choices listed.
Call Control	Mandatory		
Low-order SONET/SDH Signals	Optional		
Transport of Ethernet Services	Optional		
Transport of OTN Interfaces	Optional		
Enhanced Security	Optional		
Non-Disruptive Service Parameters Modification	Optional	Call Modification by Adding/Removing Connections or by Modifying the service parameters of an Existing Connection	

Table 5-5 – Mandatory and Optional Procedures under UNI 2.0

6.8 Compatibility between UNI 1.0 and UNI 2.0

It is expected that network operators would upgrade all UNI-N devices within a subnetwork to UNI 2.0 before offering UNI 2.0 services to attached clients. It is also expected that UNI-C devices would not enable UNI 2.0 functionality until it was supported within the carrier network. However, neither of the above expectations is a requirement to utilize UNI 2.0. Thus, the possibility exists that the devices used in establishing UNI connections will contain a mix of UNI 1.0 and UNI 2.0-compliant devices. The following compatibility requirement applies to UNI 2.0:

1. A UNI 2.0-compliant system SHOULD support all the functionality of a UNI 1.0-compliant system that is comparably-equipped (in terms of supported interface types and optional features).
2. The encoding of UNI 2.0 messages and objects SHOULD NOT cause erroneous behavior in a UNI 1.0 device that receives them.

The UNI 2.0 introduces separation of the following identifiers: Node Id, SC PC ID and SC PC SCN Address in Section 9.1. In UNI 1.0, all these identifiers were combined together to form the Node Id. If a UNI 2.0 implementation has to support UNI 1.0 interfaces, it has to use the same value for Node Id, SC PC ID and SC PC SCN Address as those identifiers were combined in a single Node Id value in UNI 1.0. The address separation did not result in new protocol-specific objects beyond those already defined in UNI 1.0.

For backwards compatibility, it is sufficient for a UNI 2.0 implementation to use the same value for Node Id, SC PC ID and SC PC SCN address.

The LMP procedures introduced in UNI 1.0 are not replicated in the UNI 2.0 document. Discovery procedures will be covered in a separate implementation agreement, including backwards compatibility procedures with UNI 1.0 discovery procedures. Until the new discovery implementation agreement is published, it is possible for a UNI 2.0 implementation to support UNI 1.0 discovery procedures with the following limitations:

- SONET/SDH high-order signal support only; no OTN, Ethernet or low-order SONET/SDH signals.
- No Node ID/SC PC ID separation possible.

For UNI 2.0 implementations that support in-band signaling over DCC, they MUST be prepared to receive IP frames before it completes negotiation of LCP and NCP in order to be backwards compatible with UNI 1.0 implementations.

In order to be UNI 2.0 compliant, an implementation that supports in-fiber packet data communication over DCC MUST support IP/PPP/HDLC/DCC. UNI 2.0 implementations that support in-band signaling over DCC MAY also optionally support IP/PPP/ISO 9577/LAP-D/DCC as described in the UNI 1.0 specification for the purpose of interworking with a UNI 1.0 implementation. Since this feature is not included in ITU-T G.7712 as a standardized method for carrying IP over the SONET/SDH DCC, it is anticipated to be deprecated in a future UNI release.

UNI 2.0 requires that a signaling adjacency be established between a UNI-C and UNI-N before accepting any other signaling message. Under UNI 1.0, signaling messages can be accepted before a signaling adjacency is established. Interworking with a UNI 1.0 implementation requires one of the following:

- The UNI 1.0 implementation supports establishment of the signaling adjacency before other signaling messages exchange or;
- The UNI 2.0 implementation allows for configuration of the adjacency behavior to support UNI 1.0 implementations.

6.9 Compatibility between UNI 2.0 and ENNI 1.0 Signaling

Features in UNI 2.0 that are added beyond UNI 1.0r2 have the following compatibility with ENNI 1.0 Signaling. Compatibility means that two UNI 2.0 clients in two separate domains can setup/release calls/connections that cross an ENNI 1.0 between those two domains.

UNI 2.0 specific feature	**Compatibility with ENNI 1.0 Signaling**
Call Control	Yes
Transport of Low-Order SONET/SDH Signals	Yes
Transport of Ethernet Services	No
Transport of OTN Connections	No
Enhanced Security	Yes
Non-Disruptive Bandwidth Modification	No

Table 5-6 Compatibility between UNI 2.0 and E-NNI 1.0

7 UNI Service Invocation Reference Configurations

The reference configurations described in this section indicate different ways in which transport network services may be invoked. There are two service invocation models, one called *direct* invocation and another called *indirect* invocation. Under both models, the client-side and network-side UNI signaling agents are referred to as UNI-C and UNI-N, respectively. In the direct invocation model, the client invokes transport network services directly. The UNI-C functionality is therefore present in the client itself. In the indirect invocation model, an entity called the *Proxy* UNI-C performs UNI functions on behalf of one or more clients. The clients are not required to be co-located with the Proxy UNI-C. Four basic configurations are described in this section, two each for the direct and the indirect invocation models. In each of these configurations, UNI signaling messages between the UNI-C and the UNI-N are transported over an IP SCN, as described in Section 8.

The two endpoints of an optical connection MAY be handled by any of the following combinations:

- Two separate embedded UNI-Cs, one for each endpoint
- Proxy UNI-C and embedded UNI-C
- Two separate Proxy UNI-Cs, one for each endpoint
- The same Proxy UNI-C for both endpoints.

7.1 The Direct Invocation Model

Under this model, the UNI-C functionality is implemented in the client itself. There are two basic configurations under this model, as shown in Figure 5-20 and Figure 5-21. The difference between these two configurations is that under the first configuration (Figure 5-20), the UNI-N functionality is implemented in the transport network element (TNE), whereas in the second (Figure 5-21) the UNI-N is a proxy. When the UNI-N is implemented in a proxy entity, there is no restriction on where the proxy is located. An internal signaling interface (ISI) within the transport network is used to carry out signaling between the UNI-N and the TNE, as shown in Figure 5-21. The details of this internal interface are not relevant to the specification of the UNI.

The SCN realization between the UNI-C and the UNI-N can be in-fiber or out-of-fiber, as described in Section 8. The trigger for the client to invoke transport network services may come from a management system in the client network or via traffic engineering decisions made by the client itself. Within the transport network, the services requested over the UNI may be provided through a centralized provisioning system or by the use of distributed protocols. These aspects are not considered in the definition of the UNI.

7.2 The Indirect Invocation Model

Under this model (Figure 5-22 and Figure 5-23), clients invoke transport network services using proxy signaling. An entity called the Proxy UNI-C performs UNI signaling functions on behalf of one or more clients. The clients are not required to be co-located with the Proxy UNI-C. Under this model,

1. The Proxy UNI-C performs signaling on behalf of the clients it represents.
2. The Proxy UNI-C and a client it represents may communicate using a proprietary or standard internal signaling interface (ISI). Such interfaces (e.g., GSMP) are beyond the scope of this specification.

The Proxy UNI-C and the UNI-N MUST run the UNI signaling protocols defined in a protocol-specific IA for UNI 2.0. The SCN between the Proxy UNI-C and the UNI-N MAY be in-fiber or out-of-fiber, as described in Section 8. The UNI-N entity MUST be aware of each Proxy UNI-C that is authorized to signal on behalf of clients.

The parameters that MUST be configured in the Proxy UNI-C for each client it represents include:

- The identifiers that the UNI proxy uses to communicate with the client equipment.
- The TNA names assigned to data bearing links connecting a UNI-N and a UNI-C.
- The node ID and logical port ID of the client endpoints connected to the transport network (if automatic neighbor discovery is not implemented).
- The SC PC SCN address to which signaling messages should be sent.
- The SC PC ID to use for exchanging signaling protocol messages. The value of this identifier MAY be the same as the SC PC SCN address.
- The characteristic and capabilities of the client (e.g. SONET/SDH signal type).

A Proxy UNI-C MAY support multiple clients.

There are two basic configurations under this model as shown in Figure 5-22 and Figure 5-23. Figure 5-22 shows the case where the UNI-N functionality is resident in the TNE. Figure 5-23 shows the case where the UNI-N functionality is outside of the TNE, with an internal signaling interface.

7.3 Service Invocation Configurations

Under this specification, it is permissible to use more than one UNI service invocation method in the same network. For example, some clients MAY use direct invocation while others use indirect invocation. Similarly, on the network side, it is permissible to have some TNEs with UNI signaling capability while others utilize proxy agents. Finally, clients at each end of a connection are allowed to use different service invocation methods.

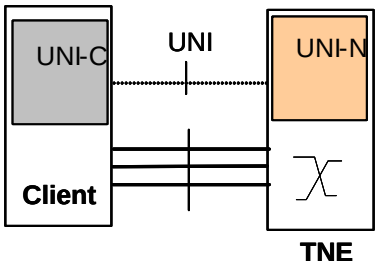

Figure 5-20 - Direct Service Invocation Model 1

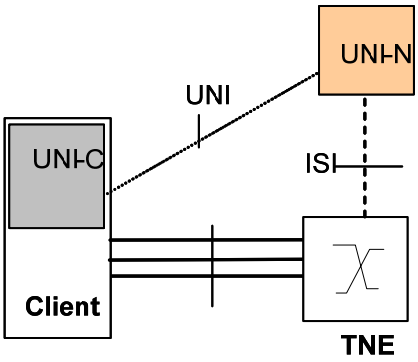

Figure 5-21 - Direct Service Invocation Model 2

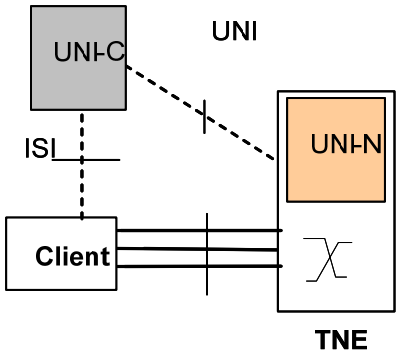

Figure 5-22 - Indirect Service Invocation Model 1

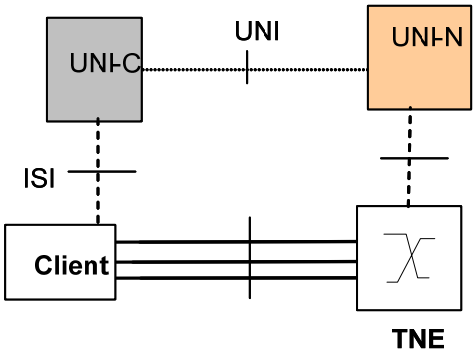

Figure 5-23 - Indirect Service Invocation Model 2

8 Signaling Transport Configurations

As per the UNI service invocation reference configurations described in Section 7, a communication link is required between the UNI-C and the UNI-N to transport signaling messages. The UNI 2.0 specification supports the following types of SCN configurations:

In-fiber: The signaling messages are carried over a communication link embedded in the data-carrying link between the client and the TNE.

Out-of-fiber: The signaling messages are carried over a communication link between the UNI-C and the UNI-N, separate from the data-bearing links.

Both in-fiber and out-of-fiber SCN configurations can support all the service invocation models described in Section 7.

Under UNI 2.0, an SCN may be realized using one or more communications links as described in the following sections. Although four distinct signaling transport options are recognized, this specification does not preclude the implementation of more than one type of signaling transport link between a client and a TNE. For instance, a client and a TNE could have both in-fiber and out-of-fiber communication links. Similarly, a TNE could have different types of communication links with different clients. Thus, configuration is required in clients and TNEs to indicate which type of communication links is implemented for which sets of data links.

8.1 In-fiber Signaling over SONET/SDH Line or Section DCC Bytes

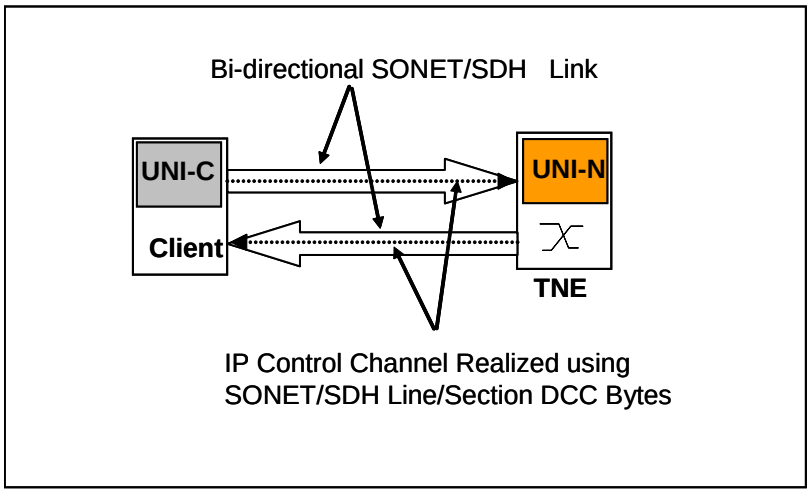

Figure 5-24 – SONET/SDH In-Fiber Embedded Communication Links

This configuration is shown in Figure 5-24. Here, the client and the TNE are connected by one or more bi-directional SONET/SDH links. Each bi-directional link consists of a pair of unidirectional links, one from the client to the TNE, and another from the TNE to the client. Certain SONET/SDH overhead bytes in *one or more* such bi-directional links are then used to realize bi-directional communication links.

If there are multiple communication links available between a client and a TNE, an IP packet MAY be transmitted on any one of them as per a local decision procedure.

Under this specification, an in-fiber communication link MUST be realized using SONET line/SDH Multiplex Section (MS) or SONET section/SDH Regenerator Section (RS) DCC (Data Communication Channel) bytes:

- **Section (RS) DCC:** This consists of D1, D2, and D3 section overhead bytes. Used as a transparent sequence of bytes, these three bytes provide a 192 Kbps message channel.
- **Line (MS) DCC:** This consists of D4–D12 line overhead bytes. Overall available bandwidth is 576Kbps.

Encapsulating IP packets over DCC bytes follows [G7712]. IP packets are encapsulated using PPP in HDLC like framing as per [RFC1662], with bit stuffed framing.

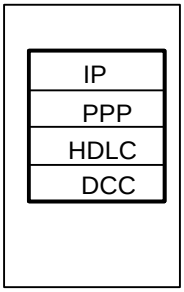

Figure 5-25 - DCC Encapsulation

8.2 In-fiber Signaling over OTN GCC0

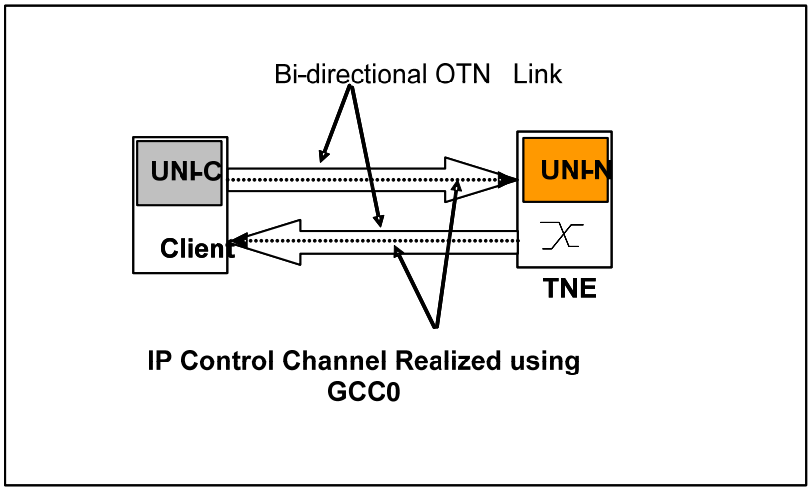

Figure 5-26 – OTN In-Fiber Embedded Communication Links

This configuration is shown in Figure 5-26. Here, the client and the TNE are connected by one or more bi-directional OTN links. Each bi-directional link consists of a pair of unidirectional links, one from the client to the TNE, and another from the TNE to the client. The GCC0 overhead byte in *one or more* such bi-directional links are then used to realize bi-directional communication links.

If there are multiple communication links available between a client and a TNE, an IP packet MAY be transmitted on any one of them as per a local decision procedure.

Under this specification, an OTN in-fiber communication link MUST be realized using GCC0 byte.

Encapsulating IP packets over GCC bytes follows [G7712]. IP packets are encapsulated using PPP in HDLC like framing as per [RFC1662], with bit stuffed framing.

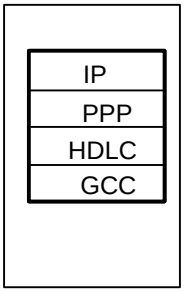

Figure 5-27 - GCC Encapsulation

8.3 In-fiber Signaling over Ethernet OAM Frames

When the UNI client interface is Ethernet, signaling messages may be transported in-fiber utilizing OAM frames. The scope of these OAM message is confined to the link and is generally described in IEEE 802.3ah clause 57 (EFM OAM) [IEEE 802.3].

An Organization Specific OAMPDU (message) is used and the OIF's OUI (Organizationally Unique Identifier) value of 0x00-0F-40 has been assigned by the IEEE. The data portion of the OAM frame can be used to carry the signaling messages defined for OIF UNI control communications. The data field in Table 5-7 is filled with an IP message whose detailed format is described in the protocol specific IA.

When there are multiple Ethernet logical ports (G.805 links) at the UNI, it MUST be possible to specify which one will be used to transmit and receive the signaling messages.

The OAM message format is shown in Table below.

Field Size in Octets	**Fields in MAC Frame**	**Value(s)**
6	Destination Address	0x01-80-C2-00-00-02 (Slow_Protocols_Multicast address)
6	Source Address	
2	Type/Length	0x88-09 (Slow_Protocols_Type field value)
1	Subtype	0x03 (OAM)
2	Flags	
1	Code	0xFE (vendor unique)
3	Data/Pad	0x00-0F-40 (OIF OUI)
39-1493		Data – IP packet as described in the protocol-specific IA
4	FCS	

Table 5-7 EFM OAM for In-Fiber communication

8.4 Out-of-Fiber Signaling

Out-of-fiber signaling applies to all four reference configurations described in Section 7. Two options are available for this under UNI 2.0, as described next. Under both these options, an out-of-fiber communication link is realized by establishing IP connectivity between the UNI-C and the UNI-N independent of the number of data links between the corresponding client and the TNE.

8.4.1 Out-of-Fiber Signaling over an External IP Transport Network

In this case, UNI signaling messages are carried over an external IP transport network. The nature of the external IP transport network is not specified in this document. Control messages MAY be sent over either

network without coordination. But each entity, UNI-C and UNI-N, MUST be configured with the IP address of the other to be able to send control messages. Since section 6.5 provides mechanisms to secure communication links, no additional protocol-specific procedures are specified to ensure secure signaling message transfer over external control networks.

There could be more than one bi-directional communication links established in this manner.

8.4.2 Out-of-Fiber Signaling over a Dedicated Signaling Channel

In this case, a dedicated, bi-directional connection MAY be established between the UNI-C and the UNI-N. This connection is then used as the communication link and the signaling messages are sent in the payload. Under this specification, the establishment of the connection and its usage are controlled by suitable manual configuration at the peer entities. There could be more than one bi-directional communication link established in this manner. Any one of them MAY be used for sending a particular signaling message. For SONET/SDH connections, this specification requires that IP packets sent over a communication link realized using a dedicated connection SHOULD use PPP over SONET/SDH, as defined in [RFC 2615]. In this option, signaling is carried in the SONET/SDH payload. It differs from Section 8.1 where the signaling channel is realized using the Line or Section DCC.

9 Addressing

UNI addressing enables the identification and reachability of various entities associated with the transport network and the connection control plane. In order to describe the multiple identifier spaces involved in the operation of the UNI protocol, it is necessary to introduce the entities that need to be identified, as well as the relevant terminology.

The terminology and addressing used in this specification differ from GMPLS. A comparison of both addressing models is outside the scope of this specification.

9.1 UNI Identifiers Spaces

The following identifier spaces are relevant to UNI signaling:

1. **Node ID**: These are identifiers for the network elements on the client and network sides of the UNI reference point.

2. **UNI-N and UNI-C Signaling Controller Protocol Controller Identifier (SC PC ID)**: This is an identifier for the signaling controller protocol controller termination in a UNI-C or a UNI-N. The SC PC ID is invariant to changes in the SCN addresses or status of the underlying communication links. Under UNI 2.0, the SC PC ID is a 32-bit identifier, which MUST be unique within the domain of operation of the communicating UNI-C and UNI-N nodes. The SC PC ID need not be globally unique, but it MUST be unique only in the domain within which each node can uniquely identify the respective peer it is communicating with. Note that this requirement is trivially satisfied if the SC PC ID is globally unique. SC PC ID is identified in Figure 5-28 within the nodes shown. The SC PC ID is assigned by the network operator managing the node.

3. **SC PC SCN Address**: This is an IPv4 address on both the client and network sides of the UNI reference point that is reachable on the SCN.

4. **Transport Network Assigned (TNA) Name**: UNI connection endpoints are identified by Transport Network Assigned (TNA) names, shown in Figure 5-28. Each TNA is a globally unique name assigned by the transport network to one or more data bearing links connecting a client and TNE and scoped by a UNI-C and UNI-N pair. The basis on which the transport network operator assigns TNA names to data links is a matter of transport network operator policy. The structure of TNA names is discussed in Section 9.2. The TNA is an instantiation of the [G8080] UNI Transport Resource Identifier.

5. **Logical Port Identifier:** A control plane identifier for a port. For SONET/SDH and OTN links, there is a one-to-one correspondence between a logical port ID and a port. For Ethernet, it is possible to have a single logical port ID representing multiple ports in the case where link aggregation is used as this is modeled by a single logical port by the control plane.

Note that while these identifier spaces are separate, network operators may choose to assign the same value to multiple identifiers for ease of administration or UNI 1.0 compatibility.

There are additional identifier spaces that are not relevant to UNI signaling such as the identifiers of the clients or TNEs that are used for internal routing, provisioning and network management purposes.

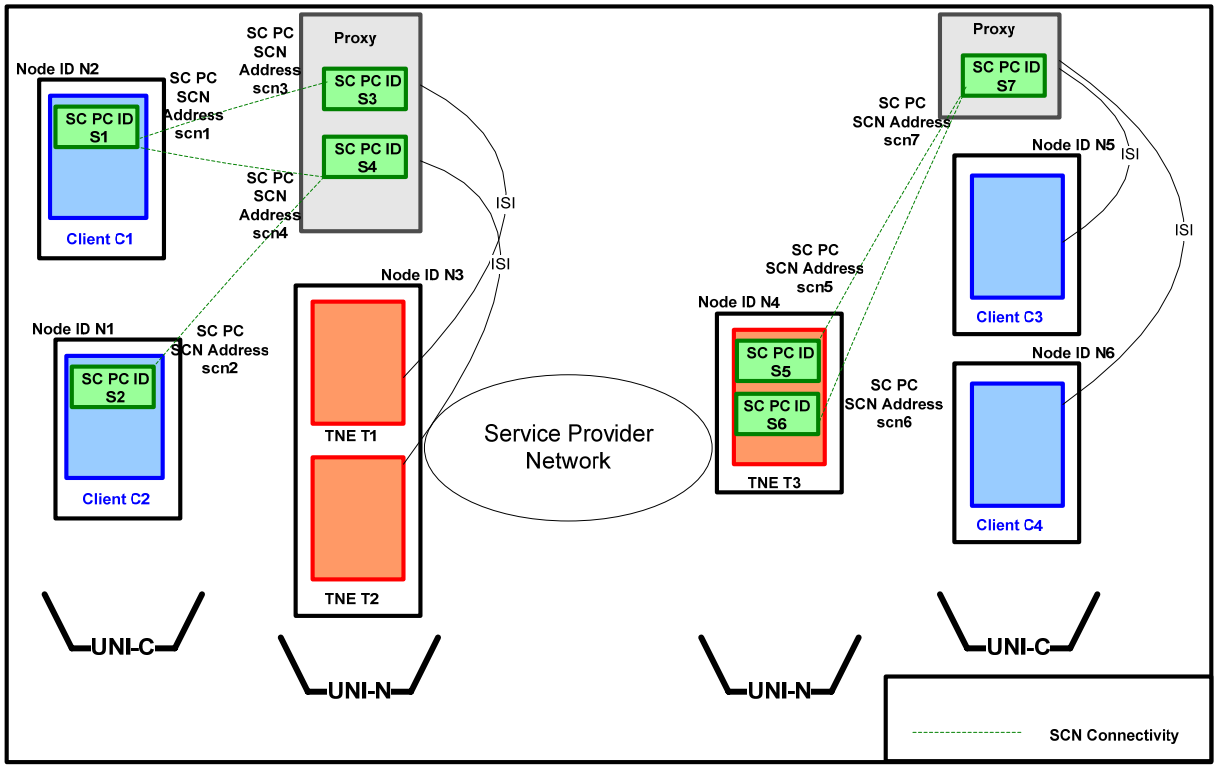

Figure 5-28 Separation of Node ID, SC PC ID, SC PC SCN address and TNE or Client device

Figure 5-28 illustrates that a Node can have one or more TNEs. The same principle could be applied to the UNI-C where a node could contain multiple Clients. It also illustrates that an SC PC can provide the signaling for one or many nodes. Note that in UNI 2.0, each SC PC MUST be reachable through a single SC PC SCN address and each SC PC SCN address MUST provide SCN connectivity to a single SC PC. Removal of this limitation is for future study.

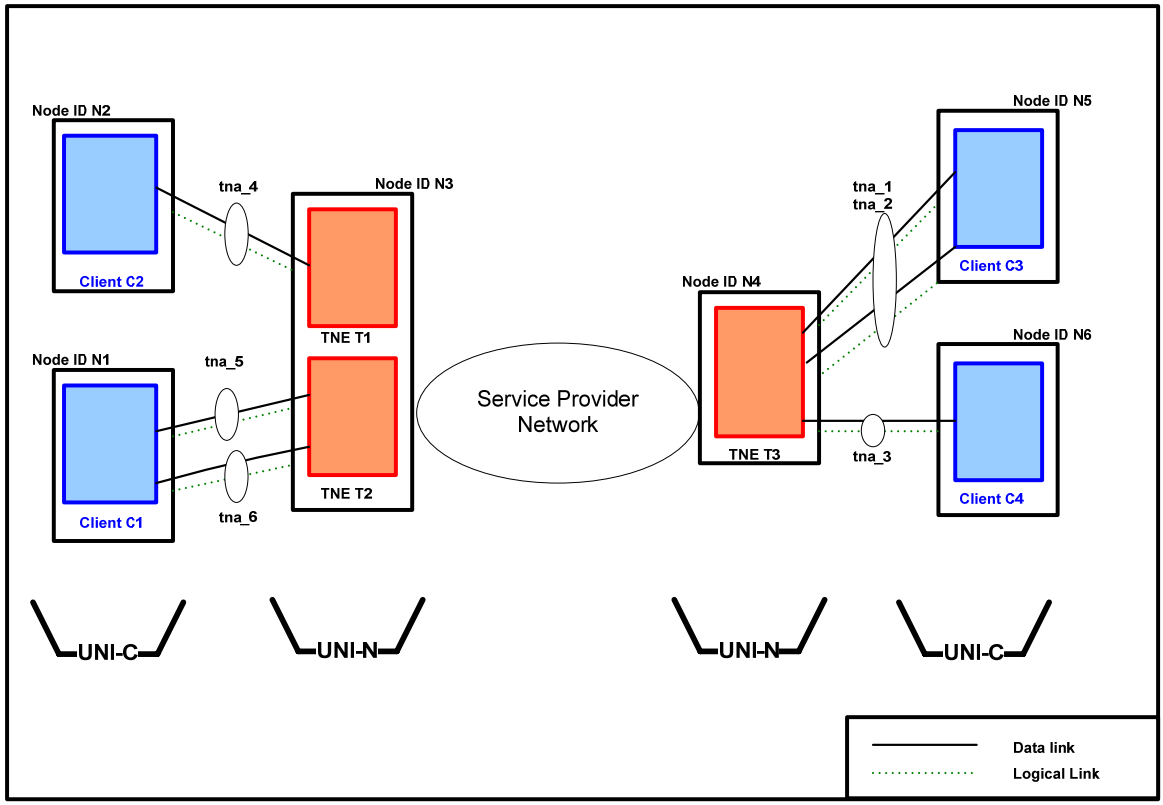

Figure 5-29 Data links, logical links and TNAs

Figure 5-29 shows that TNAs represent one or more data bearing links connecting a UNI-N and UNI-C. It also shows that many TNA names can be assigned to the same set of data bearing links.

As described above, a single TNA name may denote one or more data links. An individual data link within a group of links sharing the same TNA name is identified by a *logical port identifier* at each end. Assignment of logical port identifiers is a *local decision of the node at each end*. Thus, each data link connecting a client and a TNE will be associated with two logical port identifiers, one on the client side and one on the TNE side. For UNI 2.0, a logical port identifier is encoded as a 32-bit integer and MUST be unique within a node.

Each logical port identifier corresponds on a one-to-one basis to a physical port. The numbering schemes used for logical port identifiers and physical ports may, however, be different. This allows a network operator to avoid exposing its internal port numbering scheme to clients. Additionally, an operator may maintain the same logical port identifier for a data link to a given client device, regardless of the identity of the physical port within the TNE on which the link is terminated. This allows a data link to a client to change from one physical port to another within the same TNE.

Figure 5-30 shows a client and a TNE with multiple data links between them. The corresponding logical port identifiers on each side are denoted as, CP_i and NP_i, respectively. Correct operation of UNI signaling relies on *unambiguous mapping between the client and TNE logical port identifiers*, as these are carried in connection establishment and tear-down messages. This mapping MUST be established either

- Automatically, using neighbor discovery and link verification procedures. The definition of the discovery procedures are beyond the scope of this implementation agreement or;
- Manually, by configuring the mapping in the corresponding UNI-C and UNI-N entities.

Figure 5-30 Client and TNE Logical Port Identifier Mapping

9.2 Structure of TNA Names

TNA names are used to identify the endpoints of a UNI connection. The TNA name space should be large enough to accommodate global networks and it should be capable of supporting hierarchies and summarization.

UNI 2.0 TNA names are capable of accommodating either of the IP or NSAP formats. The following three types of TNA names are supported by the UNI 2.0 signaling protocols:

1. IPv4 formats (32 bits)
2. IPv6 formats (128 bits)
3. NSAP formats (160 bits) (The NSAP format is structured according [ISO_IEC8348] (identical to [X213])).

9.3 Role of TNA Names in UNI Signaling

TNA names are carried in UNI signaling messages to uniquely identify the data endpoints of a connection. In addition to its TNA name, each data link is qualified using a *logical port identifier*. In this case, the combination of TNA name and logical port identifier is required to uniquely identify a data link. Furthermore, depending on the nature of the selected interface and the requested service, de-multiplexing information such as channel must be selected. This information is carried in signaling messages as a "label". A "label" indicates the detailed multiplexing information required to identify logical channels within the scope of a given data link. These details are described in OIF protocol specific signaling IAs.

Under UNI 2.0, connections between heterogeneous types of TNA names are allowed. For example, the source endpoint could be identified by an IPv4 formatted TNA name, while the destination endpoint is identified by an NSAP formatted TNA name. Any interworking that may be required in this case is beyond the scope of the UNI specification. Details of how these TNA names are carried in signaling messages are given in OIF protocol specific signaling IAs

The means by which the transport network maintains the mapping between TNAs and internal transport network addresses is beyond the scope of the UNI 2.0 specification.

10 UNI Abstract Messages

The UNI signaling messages are described in this section. These messages are denoted "abstract" since the actual realization depends on the signaling protocol used. OIF protocol specific signaling IAs describe messages corresponding to the abstract messages defined here. In the following description, the terms "initiating UNI-C" and "terminating UNI-C" are used to identify the entities at the two ends of a call. The "initiating UNI-C" refers to the UNI-C that originally requested the call. The "terminating UNI-C" refers to the UNI-C that originally responded to the call request. Note that for proxy signaling, the same proxy UNI-C could be used for both end points of the call (see Section 7).

In UNI 2.0, the UNI abstract call messages are implicitly included in the connection messages. UNI 2.0 does not support calls without connections and the abstract call attributes are included in the abstract connection messages. For each connection message type, each attribute is classified as an attribute of the call, the connection or both.

The following abstract call messages (Table 5-8) are currently defined:

Abstract Message	**Message Direction**	**Implicit Signaling**
Call Setup Request	UNI-C→UNI-N & UNI-N→UNI-C	Implicitly signaled in the Connection Setup Request for the first connection of the call.
Call Setup Indication	UNI-N→UNI-C & UNI-C→UNI-N	Implicitly signaled in the Connection Setup Indication for the first connection of the call.
Call Setup Confirm	UNI-C→UNI-N & UNI-N→UNI-C	Implicitly signaled in the Connection Setup Confirm for the first connection of the call.
Call Release Request	UNI-C→UNI-N & UNI-N→UNI-C	Implicitly signaled in the Connection Release Request of the last connection of the call.
Call Release Indication	UNI-N→UNI-C & UNI-C→UNI-N	Implicitly signaled in the Connection Release Indication of the last connection of the call.
Call Query Request	UNI-C→UNI-N & UNI-N→UNI-C	Implicitly signaled in the Connection Query Request for each connection within the call.
Call Query Indication	UNI-N→UNI-C & UNI-C→UNI-N	The call information is piggybacked onto the Connection Query Indication for each connection within the call.
Call Modify Request	UNI-C→UNI-N & UNI-N→UNI-C	- If the call is modified by changing the bandwidth of an existing connection, the Call Modify Request is implied in the Connection Modify Request. - If the call is modified by adding a connection, the Call Modify Request is implied in the Connection Setup Request. - If the call is modified by removing a connection, the Call Modify Request is implied in the Connection Release Request.
Call Modify Indication	UNI-N→UNI-C & UNI-C→UNI-N	- If the call is modified by changing the bandwidth of an existing connection, the Call Modify Indication is implied in the

Abstract Message	Message Direction	Implicit Signaling
		Connection Modify Indication. - If the call is modified by adding a connection, the Call Modify Indication is implied in the Connection Setup Indication. - If the call is modified by removing a connection, the Call Modify Request is implied in the Connection Release Indication.
Call Modify Confirm	UNI-C→UNI-N & UNI-N→UNI-C	- If the call is modified by changing the bandwidth of an existing connection, the Call Modify Confirm is implied in the Connection Modify Confirm. - If the call is modified by adding a connection, the Call Modify Request is implied in the Connection Setup Confirm. - If the call is modified by removing a connection, there is no Call Modify Confirm.

Table 5-8 UNI Call Messages

The following abstract connection messages (Table 5-9) are currently defined:

Message No.	Abstract Message	Message Direction
1	Connection Setup Request	UNI-C→UNI-N & UNI-N→UNI-C
2	Connection Setup Indication	UNI-N→UNI-C & UNI-C→UNI-N
3	Connection Setup Confirm	UNI-C→UNI-N & UNI-N→UNI-C
4	Connection Release Request	UNI-C→UNI-N & UNI-N→UNI-C
5	Connection Release Indication	UNI-N→UNI-C & UNI-C→UNI-N
6	Connection Query Request	UNI-C→UNI-N & UNI-N→UNI-C
7	Connection Query Indication	UNI-N→UNI-C & UNI-C→UNI-N
8	Connection Notify	UNI-N→UNI-C
9	Connection Modify Request	UNI-C→UNI-N & UNI-N→UNI-C
10	Connection Modify Indication	UNI-N→UNI-C & UNI-C→UNI-N
11	Connection Modify Confirm	UNI-C→UNI-N & UNI-N→UNI-C

Table 5-9 UNI Connection Messages

The following abstract signaling adjacency maintenance message (**Table 5-10**) is currently defined:

Message No.	Abstract Message	Message Direction
1	Signaling Adjacency Maintenance	UNI-C→UNI-N & UNI-N→UNI-C

Table 5-10 UNI Signaling Adjacency Maintenance Message

A list of UNI attributes is associated with each UNI message. Some of these attributes are required (mandatory) for a given signaling message, while others are optional. These are described in the following sections. In addition, a network may not support all of the requested attributes. In such cases, the network SHALL send appropriate indications to the client in indication messages. The encoding of these attributes

is not defined in this section since this too depends on the particular signaling protocol used. Refer to OIF UNI signaling protocol IAs.

The manner in which the UNI abstract messages are mapped to actions *within* the transport network, and the signaling protocol used within the transport network to realize the actions are outside the scope of this specification.

The UNI abstract messages are described in detail below. Each attribute is followed by (M) if mandatory or (O) if optional. When the attribute is mandatory for one case and optional for the other, the attribute is followed by (M-1, O-2) to indicate the attribute is mandatory for case 1 and optional for case 2 followed or (O-1, M-2) to indicate that the attribute is optional for case 1 and mandatory for case 2.

10.1 Connection Setup Request

The connection setup request message is used by a client to request a connection between specified source and destination clients. It defines the set of attributes that describe the service requirements for the connection. It also implicitly contains the Call Setup Request if this is the first connection of the call or the Call Modify Request if this connection is added to an existing call .

The connection setup request message is sent from
1. the initiating UNI-C to UNI-N to request the creation of a connection;
2. the UNI-N to the terminating UNI-C to indicate an incoming connection setup request.

Not all of the attributes are applicable in each of the cases 1 (UNI-C->UNI-N) and 2 (UNI-N->UNI-C) above. The "Applicability" column indicates the case in which the corresponding parameter is applicable. The section in which each attribute is described is also indicated.

Attributes	Applicability	Call/Conn	Reference
Source TNA Name (M)	Cases 1 and 2	Call	Section 10.13.1.1
Source Logical Port Identifier (M)	Case 1	Connection	Section 10.13.1.2
Source Generalized Label (O)	Case 1	Connection	Section 10.13.1.3
Destination TNA Name (M)	Cases 1 and 2	Call	Section 10.13.1.1
Destination Logical Port Identifier (O-1, M-2)	Cases 1 and 2	Connection	Section 10.13.1.2
Destination Generalized Label (O-1, M-2)	Cases 1 and 2	Connection	Section 10.13.1.2
Local connection ID (M)	Cases 1 and 2	Connection	Section 10.13.1.4
Contract ID (O)	Case 1	Call	Section 10.13.4.1
Encoding Type (M)	Cases 1 and 2	Call/Connection	Section 10.13.2.1
Switching Type (M)	Cases 1 and 2	Call/Connection	Section 10.13.2.2
SONET/SDH, OTN or Ethernet traffic parameters (M)	Cases 1 and 2	Call/Connection	Section 10.13.2.3
Directionality (O)	Cases 1 and 2	Connection	Section 10.13.2.4
Generalized Payload Identifier (O)	Cases 1 and 2	Call	Section 10.13.2.5
Service Level (M-1, O-2)	Cases 1 and 2	Call	Section 10.13.2.6
Diversity (M)	Cases 1	Call/Connection	Section 10.13.3.1
Call Name (O-1,M-2) [1]	Cases 1 and 2	Call	Section 10.13.1.5
Bandwidth Modification Support(M)	Cases 1 and 2	Connection	Section 10.13.2.7

Table 5-11 Connection Setup Request

Note[1]: The UNI-N is responsible for assigning the call name if it was not present in the Call and Connection Setup Request received from the initiating UNI-C. The call name is only inserted by the source UNI-C if the connection setup request is used to add a connection to an existing call.

A UNI 2.0 UNI-C can initiate a request to an SPC endpoint by specifying a source TNA, a destination TNA and inserting a destination Generalized Label if required by the termination point or available at the source UNI-C.

An EMS can create a call from an SPC endpoint to a UNI enabled destination. The request minimally includes a source and destination TNA. A destination Generalized Label and destination logical port identifier MAY optionally be specified.

An SPC endpoint can be distinguished by its TNA or the contents of the destination generalized label. In the case SPC endpoint to SC endpoint and SC endpoint to SPC endpoint connections, all parameters in Table 5-11 would apply as follows:
- SPC endpoint to SC endpoint: Signaling at destination UNI only, i.e., Case 2.
- SC endpoint to SPC endpoint: Signaling at source UNI only, i.e., Case 1.

10.2 Connection Setup Indication

The connection setup indication message is used to acknowledge the establishment of the connection to the UNI-C that initiated the connection request. The corresponding client MAY then start transmission of data on the established connection.

The connection setup indication mesage is sent from
1. the terminating UNI-C to UNI-N to accept or reject an incoming setup indication;
2. the UNI-N to the initiating UNI-C to indicate the successful creation of (or failure to create) a connection requested previously.

When the first connection within a call is established, the Connection Setup Indication message is combined with the Call Setup Indication message.

The attributes carried in this message are listed below, together with the applicability in each of the cases above:

Attributes	Applicability	Call/Conn	Reference
Source Logical Port Identifier (M)	Case 2	Connection	Section
Source Generalized Label (M)	Case 2	Connection	Section
Destination Logical Port Identifier (M-1, O-2)	Cases 1 and 2	Connection	Section
Destination Generalized Label (M-1,O-2)	Cases 1 and 2	Connection	Section
Local Connection ID (M)	Cases 1 and 2	Connection	Section
Connection Status (M)	Cases 1 and 2	Connection	Section
Error Code (O)	Cases 1 and 2	Call/Connection	Section
Call Name (M)	Cases 1 and 2	Call	Section
Bandwidth Modification Support (M)	Cases 1 and 2	Connection	Section

Table 5-12 Connection Setup Indication

10.3 Connection Setup Confirm

The connection setup confirm message is used to acknowledge the establishment of the connection to the UNI-C that terminated the connection setup indication. The corresponding client MAY then start

transmission of data on the established connection. The connection setup confirm message for the first connection implicitly signals the Call Setup Confirm.

The connection setup confirm is sent from
1. the initiating UNI-C to UNI-N to acknowledge completion of the connection establishment or to indicate an error in the connection establishment;
2. the UNI-N to the terminating UNI-C to indicate that the connection has been successfully created (or has failed to be created) and that the corresponding client MAY start transmitting data over the connection.

The attributes carried in this message are listed below, together with the applicability in each of the cases above:

Attributes	Applicability	Call/Conn	Reference
Source Logical Port Identifier (O)	Case 1	Connection	Section 10.13.1.2
Source Generalized Label (O)	Case 1	Connection	Section 10.13.1.3
Destination Logical Port Identifier (O)	Cases 1 and 2	Connection	Section 10.13.1.2
Destination Generalized Label (O)	Cases 1 and 2	Connection	Section 10.13.1.3
Local Connection ID (M)	Cases 1 and 2	Connection	Section 10.13.1.4
Connection Status (M)	Cases 1 and 2	Connection	Section 10.13.5.1
Error Code (O)	Cases 1 and 2	Call/Connection	Section 10.13.5.2
Call Name (M)	Cases 1 and 2	Call	Section 10.13.1.5

Table 5-13 Connection Setup Confirm

10.4 Connection Release Request

The connection release request message is used to initiate the deletion of a connection. If the connection deletion is being initiated by a UNI-C, then this UNI-C SHOULD maintain the connection control state and the corresponding client SHOULD maintain the data plane until the connection deletion has been acknowledged. This avoids alarms being generated by the client at the other end of the connection. The UNI-C terminating the connection deletion request MAY delete the connection state upon receipt of the connection release request (the corresponding client MAY delete the data plane state).

The network may also wish to delete a connection (a forced deletion) due to scenarios such as:
- Internal network failures, which force the network to terminate connections
- A deletion indication is not received by the UNI-N within a pre-defined timeout

When the network initiates a connection release request for the scenarios described above, a connection release indication is not required and the UNI-N MAY terminate all connection control state and the data path as the connection release request is initiated.

The connection release request message is sent from
1. the initiating or terminating UNI-C to UNI-N to delete a connection;
2. the UNI-N to the initiating or terminating UNI-C to indicate deletion by far end;

The deletion of the last connection within a call deletes the call state.

The attribute carried in this message and its applicability are listed below:

Attributes	Applicability	Call/Conn	Reference
Local Connection ID (M)	All cases	Connection	Section 10.13.1.4
Call Name (M)	All cases	Call	Section 10.13.1.5

Table 5-14 Connection Release Request

Note that connection deletion can be initiated by either ends of a connection, not just the end that originally initiated the connection request.

10.5 Connection Release Indication

The connection release indication message signals the completion of the connection deletion procedure. The UNI-C that initiated the connection deletion MAY delete connection control state upon receipt of the connection release indication (the corresponding client MAY delete the data plane state of the connection).

The connection release indication message is sent from
1. the originating or terminating UNI-C to UNI-N to acknowledge an incoming connection release request;
2. the UNI-N to the initiating or terminating UNI-C to indicate the successful deletion of the connection as requested.

The deletion of the last connection within a call deletes the call state.

The attributes carried in this message and their applicability are listed below:

Attributes	Applicability	Call/Conn	Reference
Local Connection ID (M)	Cases 1 and 2	Connection	Section 10.13.1.4
Connection Status (M)	Cases 1 and 2	Connection	Section 10.13.5.1
Error Code (O)	Cases 1 and 2	Connection	Section 10.13.5.2
Call Name (M)	Cases 1 and 2	Call	Section 10.13.1.5

Table 5-15 Connection Release Indication

10.6 Connection Query Request

The connection query request message is used to query the state and attributes of a given connection.

The connection query request message is sent from
1. the UNI-C to UNI-N to enquire about the status and/or the attributes of one or more connections;
2. the UNI-N to either UNI-C to enquire about the status and/or the attributes of one or more connections.

The attributes carried in this message and their applicability are listed below:

Attribute	Applicability	Call/Conn	Reference
TNA Name (O)	Cases 1 and 2	Call	Section 10.13.1.1
List of Local Connection IDs (O)	Cases 1 and 2	Connection	Section 10.13.1.4
Call Name (O)	Cases 1 and 2	Call	Section 10.13.1.5

Table 5-16 Connection Query Request

All attributes are optional. If no attributes are specified, all connections managed by the UNI-C or UNI-N SC PC MUST be returned. Multiple local connection IDs MAY be included in a single connection status enquiry. If a TNA Name but no local connection ID is specified then the attributes of all connections owned by the TNA is returned. Otherwise, the status of the indicated connection(s) is returned.

Note that a connection query request can be initiated by the UNI-C at either end of a connection, not just by the UNI-C that initiated the original connection request.

10.7 Connection Query Indication

The connection query indication message returns the status of the specified connection and the associated attributes.

The connection query indication message is sent from
1. the UNI-N to the UNI-C to indicate the status of connection attributes as requested previously;
2. the UNI-C to UNI-N to indicate the status of connection attributes as requested previously.

The attributes carried in this message and their applicability are listed below. If the status of multiple connections is being returned, the contents shown MUST be repeated for each connection. The "Local Logical Port Identifier" and the "Local Generalized Label" indicate the port and channel information at the side (source or destination) where the Connection Query Indication message is received. In other words, this message does not include the remote port and channel information.

Attributes	Applicability	Call/Conn	Reference
Local Connection ID (M)	Cases 1 and 2	Connection	Section 10.13.1.4
Connection Status (M)	Cases 1 and 2	Connection	Section 10.13.5.1
Source TNA Name (O)	Cases 1 and 2	Call	Section 10.13.1.1
Destination TNA Name (O)	Cases 1 and 2	Call	Section 10.13.1.5
Local Logical Port Identifier (O)	Cases 1 and 2	Connection	Section 10.13.1.2
Local Generalized Label (O)	Cases 1 and 2	Connection	Section 10.13.1.3
Contract ID (O)	Case 1	Call	Section 10.13.4.1
Encoding Type (O)	Cases 1 and 2	Call/Connectio	Section 10.13.2.1
Switching Type (O)	Cases 1 and 2	Call/Connectio	Section 10.13.2.2
SONET/SDH, OTN or Ethernet traffic parameters (O)	Cases 1 and 2	Call/Connectio n	Section 10.13.2.3
Directionality (O)	Cases 1 and 2	Connection	Section 10.13.2.4
Generalized Payload Identifier (O)	Cases 1 and 2	Call	Section 10.13.2.5
Service Level (O)	Cases 1 and 2	Call	Section 10.13.2.6
Diversity (O)	Cases 1 and 2	Call/Connectio	Section 10.13.3.1
Error Code (O)	Cases 1 and 2	Call/Connectio	Section 10.13.5.2
Call Name (M)	Cases 1 and 2	Call	Section 10.13.1.5

Table 5-17 Connection Query Indication

10.8 Connection Notify

The connection notify message is sent autonomously by a UNI-N to either UNI-C to indicate a change in the status of the connection (e.g., unrestorable connection failure) or to request that the UNI-C triggers the deletion. The attributes carried in this message are listed below:

Attributes	Applicability	Call/Conn	Reference
Local Connection ID (M)	All cases	Connection	Section 10.13.1.4
Connection Status (M)	All cases	Connection	Section 10.13.5.1
Error Code (M)	All cases	Call/Connectio	Section 10.13.5.2
Call Name (M)	All cases	Call	Section 10.13.1.5

Table 5-18 Connection Notify

10.9 Connection Modify Request

The connection modify request message is used by a client to request a modification to an existing connection. In UNI 2.0, the bandwidth and label related attributes can be modified. For Ethernet EVPL services case, the generalized label representing the CE-VLAN identifiers can be modified. See section 6.6 for more details.

The connection modify request message is sent from

1. the initiating UNI-C to UNI-N to request the modification of a connection;
2. the UNI-N to the terminating UNI-C to indicate an incoming modify request.

The attributes listed in the table below are used to identify the connection or they are user modifiable attributes of the connection.

Attributes	Applicability	Call/Conn	Reference	Modifiable
Source TNA Name (M)	Cases 1 and 2	Call	Section 10.13.1.1	No
Source Logical Port Identifier (M)	Case 1	Connection	Section 10.13.1.2	No
Source Generalized Label (O)	Case 1	Connection	Section 10.13.1.3	Yes
Destination TNA Name (M)	Cases 1 and 2	Call	Section 10.13.1.5	No
Destination Logical Port Identifier (O)	Cases 1 and 2	Connection	Section 10.13.1.5	No
Destination Generalized Label (O)	Cases 1 and 2	Connection	Section 10.13.1.3	Yes
Local connection ID (M)	Cases 1 and 2	Connection	Section 10.13.1.4	No
SONET/SDH, OTN or Ethernet traffic parameters (M)	Cases 1 and 2	Call/Connection	Section 10.13.2.3	Yes
Call Name (M)	Cases 1 and 2	Call	Section 10.13.1.5	No

Table 5-19 Connection Modify Request

10.10 Connection Modify Indication

The connection modify indication message is used to acknowledge the modification of the connection to the UNI-C that initiated the connection request. The corresponding client MAY then start transmission of data using the new connection parameter.

The connection modify indication message is sent from

1. the terminating UNI-C to UNI-N to accept or reject an incoming modification request;
2. the UNI-N to the initiating UNI-C to indicate the successful modification of (or failure to modify) a connection modification.

The attributes carried in this message are listed below, together with the applicability in each of the cases above:

Attributes	Applicability	Call/Conn	Reference
Source Logical Port Identifier (M)	Case 2	Connection	Section 10.13.1.2
Source Generalized Label (M)	Case 2	Connection	Section 10.13.1.3
Destination Logical Port Identifier (M-1, O-2)	Cases 1 and 2	Connection	Section 10.13.1.2
Destination Generalized Label (M-1,O-2)	Cases 1 and 2	Connection	Section 10.13.1.3
Local Connection ID (M)	Cases 1 and 2	Connection	Section 10.13.1.4

Connection Status (M)	Cases 1 and 2	Connection	Section 10.13.5.1
Error Code (O)	Cases 1 and 2	Call/Connection	Section 10.13.5.2
Call Name (M)	Cases 1 and 2	Call	Section 10.13.1.5

Table 5-20 Connection Modify Indication

10.11 Connection Modify Confirm

The connection modify confirm message is used to acknowledge the modification of the connection to the UNI-C that terminated the connection modify indication. The corresponding client MAY then start transmission of data on the established connection.

The connection modify confirm message is sent from
1. the initiating UNI-C to UNI-N to acknowledge completion of the connection modification or to indicate an error in the connection establishment;
2. the UNI-N to the terminating UNI-C to indicate that the connection modification has been successfully completed and that the corresponding client MAY start transmitting data over the connection using the new connection parameters.

The attributes carried in this message are listed below, together with the applicability in each of the cases above:

Attributes	Applicability	Call/Conn	Reference
Source Logical Port Identifier (O)	Case 1	Connection	Section 10.13.1.2
Source Generalized Label (O)	Case 1	Connection	Section 10.13.1.3
Destination Logical Port Identifier (O)	Cases 1 and 2	Connection	Section 10.13.1.2
Destination Generalized Label (O)	Cases 1 and 2	Connection	Section 10.13.1.3
Local Connection ID (M)	Cases 1 and 2	Connection	Section 10.13.1.4
Connection Status (M)	Cases 1 and 2	Connection	Section 10.13.5.1
Error Code (O)	Cases 1 and 2	Call/Connection	Section 10.13.5.2
Call Name (M)	Cases 1 and 2	Call	Section 10.13.1.5

Table 5-21 Connection Modify Confirm

10.12 Signaling Adjacency Maintenance

The signaling adjacency maintenance message is used to monitor the status of a signaling adjacency between two neighbors. The signaling adjacency MUST be established prior to exchanging call and connection messages.

Both the UNI-C and UNI-N in an adjacency send this message as a keep alive mechanism to maintain the signaling adjacency.

10.13 Description of Attributes

The attributes are classified into identification-related, service-related, routing-related, policy-related and miscellaneous. The encoding of these attributes would depend on the signaling protocol used and are described in OIF protocol specific signaling IAs. In this section, the attributes are described in a general manner.

10.13.1 Identification-Related Attributes

10.13.1.1 Transport Network Assigned (TNA) Name

Transport Network Assigned (TNA) Names are assigned by the service provider to one or more data links (see Section 9). For UNI 2.0, the supported TNA formats are IPv4, IPv6 and NSAP.

10.13.1.2 Logical Port Identifier

The Logical Port Identifier is an index that indicates a client or TNE port (Section 9).

10.13.1.3 Generalized Label

10.13.1.3.1 SONET/SDH Generalized Label

The SONET/SDH Generalized Label is a structure that indicates a multiplexed channel within the signal carried over the specified data link. For instance, this identifier could indicate an STS-48 channel within an STS-192 link. In general, this structure can indicate several levels of multiplexing. The encoding of this structure is left up to the signaling protocol specification.

10.13.1.3.2 OTN Generalized Label

ODUk Label Space

As described in [G709], in addition to the support of ODUk mapping into OTUk (k = 1, 2, 3), ODUk multiplexing is supported. It refers to the multiplexing of ODUj (j = 1, 2) into an ODUk (k > j) signal, in particular:

- ODU1 into ODU2 multiplexing
- ODU1 into ODU3 multiplexing
- ODU2 into ODU3 multiplexing
- ODU1 and ODU2 into ODU3 multiplexing

ODUj into ODUk multiplexing (k > j) is defined when an ODUj is multiplexed into an ODUk Tributary Unit Group. Therefore, the label space structure is a tree whose root is an OTUk signal and the leaves are the ODUj signals (k >= j) that can be transported via the tributary slots and switched between these slots. A G.709 Digital Path layer label identifies the exact position of a particular ODUj signal in an ODUk multiplexing structure.

OCh Label Space

At the Optical Channel layer, the label space is a flat space whose values reflect the local assignment of OCh identifiers corresponding to the OTM-n.m sub-interface signals (m = 1, 2 or 3). Note that these identifiers do not cover the OCh with reduced functionality (OChr) from [G709].

The OCh label space values are defined by either absolute values (channel identifiers or wavelength identifiers) or relative values (channel spacing or inter-wavelength spacing). The latter is strictly confined to a per-port label space while the former could be defined as a local or a global (per node) label space. Such an OCh label space is applicable to both OTN Optical Channel layer and pre-OTN Optical Channel layer.

10.13.1.3.3 Ethernet Generalized Label

The label for EVPL is a set of CE-VLAN identifiers. The label for EPL is the logical port identifier.

10.13.1.4 Local Connection ID

The Local Connection ID identifies a connection locally at a UNI. The local connection ID MUST be unique over a given UNI, but is not required to be unique across the entire network. The local connection ID is assigned by the UNI-C that initiates a connection setup request at the initiating end, and by the UNI-N at the terminating end. Thus, a local connection ID is carried in each connection create request message sent from the initiating UNI-C to the UNI-N, and in each connection create message sent from the UNI-N

to the terminating UNI-C. The local connection ID values generated for the same connection at the initiating and terminating end need not be the same. The UNI-N MUST verify the uniqueness of any UNI-C-assigned local ID (at the initiating end).

10.13.1.5 Call Name

This attribute represents a globally unique name assigned to a call at the UNI-N call boundary. The call name is end-to-end significant and remains constant across call modification operations, i.e., across the "life" of the call. For each connection that is part of a call, there is a Local Connection ID associated with the Call Name of that call.

10.13.2 Service-Related Attributes

10.13.2.1 Encoding Type

The Encoding Type specifies the encoding format of the signal to be transported across the UNI. The encoding options specified are :

- SDH ITU-T [G707]
- SONET ANSI [T1.105]
- ODUk layer [G709]
- OCh layer [G709]
- Ethernet IEEE PHY 802.3 [IEEE802.3]

10.13.2.2 Switching Type

Indicates the type of switching that SHOULD be performed on a particular link: The switching type options specified are Layer 2 (Ethernet), TDM (SONET, SDH, OTN ODUk), Lambda (OTN OCh) or Data Channel Switching Capable (DCSC).

10.13.2.3 Traffic Parameters

10.13.2.3.1 SONET/SDH traffic parameters

Note: Implementation specific values are defined in [RFC3471] and [RFC4606]. The following parameters are defined in [RFC4606]:

Signal type

The signal type defines the elementary signal on which multiple transforms can be applied successively to build the final signal being requested for the connection. The elementary signal types are defined in Section 6 of this document.

Requested Contiguous Concatenation Type (RCC)

The contiguous concatenation type indicates the type of SONET/SDH contiguous concatenation to apply on the elementary signal.

Number of Contiguous Components (NCC)

The number of contiguous components indicates the number of identical SONET/SDH SPEs/VCs that are requested to be contiguously concatenated, as specified in the RCC field.

Number of Virtual Components (NVC)

The Number of Virtual Components field indicates the number of identical signals that are to be virtually concatenated. These signals can be either identical elementary signal SPEs/VCs, or identical contiguously concatenated signals. In the latter case, this attribute allows the virtual concatenation of contiguously

concatenated signals to be requested, for instance, the virtual concatenation of several STS-3c SPEs, or any STS-Xc SPEs (to obtain an STS-Xc-Yv SPE). This field is not used in UNI 2.0.

Multiplier

The Multiplier field indicates the number of identical signals that form the final signal constituting the connection. These signals can be identical elementary signals, identical contiguously concatenated signals, or identical virtually concatenated signals. Note that all of these signals belong to the same connection.

Transparency

The transparency field is a vector of flags that indicates the type of transparency requested. Several flags can be combined to provide different types of transparency. Not all combinations are necessarily valid. See Section 6 for more details.

Profile

This field is intended to indicate particular capabilities that MUST be supported for the connection, for example monitoring capabilities. No standard profile is currently defined and the usage of this field is as per [RFC4606].

10.13.2.3.2 OTN Traffic Parameters

Note: Implementation specific values are defined in [RFC3471] and [RFC4328]. The following parameters are defined in [RFC4328].

Signal Type (ST)

The signal type defines the elementary signal on which multiple transforms can be applied successively to build the final signal being requested for the connection. The elementary signal types are defined in Section 6 of this document.

Number of Multiplexed Components (NMC)

The NMC attribute indicates the number of ODU tributary slots used by an ODUj when multiplexed into an ODUk (k > j). This field is not applicable when an ODUk is mapped into an OTUk and irrelevant at the Optical Channel layer.

Number of Virtual Components (NVC)

The NVC attribute is dedicated to ODUk virtual concatenation purposes. It indicates the number of ODU1, ODU2 or ODU3 Elementary Signals that are requested to be virtually concatenated to form an ODUk-Xv signal. By definition, these signals MUST be of the same type. This field is not used in UNI 2.0.

Multiplier (MT)

The Multiplier attribute indicates the number of identical Elementary Signals or Composed Signals requested for the connection. A Composed Signal is the resulting signal from the application of the NMC and NVC fields to an elementary Signal Type.

10.13.2.3.3 Ethernet Traffic Parameters

The following Ethernet Traffic Parameters are defined in [G8011.1], [G8011.2] and [MEF.10.1].

- Committed Information Rate (CIR)
- Committed Burst Size (CBS)
- Excess Information Rate (EIR)
- Excess Burst Size (EBS)

- Color Mode (CM)
- Color Flag (CF)

For EPL services and EVPL services with a per EVC bandwidth profile, the Ethernet Traffic Parameters apply to the entire service.

For EVPL services with a per Class of Service bandwidth profile, the Ethernet Traffic Parameters apply to one or many Classes of Service. There may be multiple Ethernet Traffic Parameters required to describe the EVPL service.

10.13.2.4 Directionality

The Directionality attribute indicates whether the connection is uni-directional or bi-directional. Default is bi-directional.

10.13.2.5 Generalized Payload Identifier

The Generalized Payload Identifier (G-PID) indicates the payload carried within the established connection (i.e., identifies the client layer of the connection). G-PID values are defined in [RFC3471].

10.13.2.6 Service Level

The Service Level attribute indicates a class of service. A carrier MAY specify a range of different classes of service (e.g. gold, silver, bronze) with predefined characteristics (e.g. restoration plans). The pre-defined service types MAY correspond to different types of network restoration (e.g. no restoration, 1+1 protection), connection set-up and hold priorities, reversion strategies for the connection after failures have been repaired, and retention strategies. The definition of the different service classes and their default values are set by the service provider by policy.

10.13.2.7 Bandwidth Modification Support

The Bandwidth Modification Support attribute indicates whether connection bandwidth modification can be performed on the connection.

10.13.3 Routing-Related Attributes

10.13.3.1 Diversity

For a new connection being created, this attribute indicates a list of *n* existing connections sourced from the same UNI-C with which diversity within the transport network is required. This attribute contains *n* items of the form <*diversity type, local connection ID*>, where the diversity type is selected from the following set:

- Node diverse. The new connection SHALL NOT use any network nodes that are in the path of the connection denoted by *local connection ID*.
- Link Diverse. The new connection SHALL NOT use any network links that are in the path of the connection denoted by *local connection ID*.
- SRLG diverse. The new connection SHALL NOT use any link that has the same SRLG as those in the path of the connection denoted by *local connection ID*.
- Shared Path. The new connection SHALL use the same links as those used by the connection denoted by *local connection ID*.

Note that a client MAY request connections that MUST be SRLG diverse, but not node diverse. To request node *and* SRLG diversity (for example), the client SHOULD have two separate entries in the list of diversity requirements - one for node diversity and one for SRLG diversity.

Note that the diversity feature has not been enhanced to support combinations with other UNI 2.0 features, including call control and non-disruptive service parameters modification as it is supported for backwards compatibility only. This leads to several limitations. For example, if a connection is established diverse to a another connection and the original connection is later modified, then it is no longer guaranteed that the connections are diverse as there is no forward linkage and the original connection is not aware of the diversity constraint.

10.13.4 Policy-Related Attributes

10.13.4.1 Contract ID

This identifier is assigned by the service provider and configured in clients. This is not interpreted by the clients.

10.13.5 Miscellaneous Attributes

10.13.5.1 Connection Status

This indicates the status of a connection. The following values are defined:

- Connection active
- Connection does not exist
- Connection unavailable
- Connection pending

10.13.5.2 Error Code

The error code is used to describe the errors resulting from connection actions. Protocol-specific errors that may generally arise during connection establishment are defined as part of the specification of these protocol specific implementation agreements. In addition, the following error codes are defined specific to the UNI:

- Unauthorized sender (policy error)
- Unauthorized receiver (policy error)
- Service level not available
- Diversity not available
- Invalid / unknown connection ID
- Unknown Call Name

10.14 SC and SPC Interworking

To enable a UNI-C to signal to a destination that only supports SPC and vice versa, TNA names must be assignable to data bearing links to a client, whether the UNI is signaling enabled, i.e. SC, or not, i.e. SPC.

11 References

[G707] ITU-T Rec. G.707, Network Node Interface for the Synchronous Digital Hierarchy (SDH)
[G709] ITU-T Recommendation G.709/Y.1331 (2003), "Interfaces for the optical transport network (OTN)"
[G7712] ITU-T Recommendation G.7712/Y.1703 (2003), "Architecture and specification of data communication network"
[G7713] ITU-T Recommendation G.7713/Y.1704 (2006), "Distributed Call and Connection Management (DCM)"
[G7713.2] ITU-T Rec. G.7713.2/Y.1704.2, DCM Signalling Mechanism Using GMPLS RSVP-TE
[G7713.3] ITU-T Rec. G.7713.3/Y.1704.3, DCM Signalling Mechanism Using GMPLS CR-LDP
[G8011] ITU-T Rec. G.8011/Y.1307 (2004), "Ethernet Services Framework"
[G8011.1] ITU-T Rec. G.8011.1/Y.1307.1 (2004), "Ethernet Private Line Service"
[G8011.2] ITU-T Rec. G.8011.2/Y.1307.2 (2005), "Ethernet Virtual Private Line Service"
[G805] ITU-T Rec. G.805 (2000),"Generic functional architecture of transport networks"
[G8080] ITU-T Rec. G.8080/Y.1304 (2006), Architecture of the Automatically Switched Optical Network (ASON)
[G872] ITU-T Rec. G.872 (2001), Architecture of optical transport networks
[GR253] Telcordia Technologies Generic Requirements GR-253-CORE Issue 4 (December 2005), "Synchronous Optical Network (SONET) Transport Systems: Common Generic Criteria"
[IEEE802.3] IEEE 802.3-2005: IEEE Standard for Information technology - Telecommunications and information exchange between systems - IEEE standard for local and metropolitan area networks - Specific requirements – Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications.
[ISO_IEC8348] ISO/IEC 8348:2002: Information technology -- Open Systems Interconnection -- Network service definition
[MEF.6] Metro Ethernet Forum, MEF.6 - Ethernet Services Definition, Phase 1, Jun3 2004
[MEF.10.1] Metro Ethernet Forum, MEF.10.1 - Ethernet Services Attributes Phase 2, Nov. 2006
[MEF.11] Metro Ethernet Forum, MEF.11 - User Network Interface (UNI) Requirements and Framework, Nov. 2004
[MEF.13] Metro Ethernet Forum, MEF.13 - User Network Interface (UNI) Type 1 Implementation Agreement
[OIF-ENNI-SIG-01] OIF Implementation Agreement OIF-E-NNI-Sig-01.0, "Intra-Carrier E-NNI Signaling Specification", February 2004
[OIF-UNI-01.0-R2] OIF Implementation Agreement OIF-UNI-01.0-R2, "User Network Interface (UNI) 1.0 Signaling Specification, Release 2: Common Part", February 2004
[OIF-UNI-02.0-RSVP] OIF Implementation Agreement OIF-UNI-02.0-RSVP, "RSVP Extensions for User Network Interface (UNI) 2.0 Signaling", February 2008
[OIF-SEP-01.1] OIF Implementation Agreement, *Security Extension to UNI and NNI*, May 2003.
[OIF-SEP-02.0] OIF Implementation Agreement, "Addendum to the Security Extension for UNI and NNI, October 2005.
[Q2982] ITU-T Rec. Q.2982, Broadband integrated services digital network (B-ISDN) - Digital Subscriber Signalling System No. 2 (DSS2) - Q.2931-based separated call control protocol, December 1999
[RFC1662] W. Simpson, Ed., "PPP in HDLC-Like Framing", IETF RFC 1662.
[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", IETF RFC 2119.
[RFC2406] S. Kent and R. Atkinson, "IP Encapsulating Security Payload (ESP)," IETF RFC 2406.
[RFC2407] D. Piper, "The Internet IP Security Domain of Interpretation for ISAKMP," IETF RFC 2407.
[RFC2409] D. Harkins and D. Carrel, "The Internet Key Exchange (IKE)", IETF RFC 2409.
[RFC2434] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs," IETF RFC 2434.
[RFC2615] A. Malis and W. Simpson, "PPP over SONET/SDH," IETF RFC 2615.

[RFC2748] D. Durham, et al., "The COPS (Common Open Policy Service) Protocol," IETF RFC2748.
[RFC2752] S. Yadav, "Identity Representation for RSVP," IETF RFC 2752, January 2000.
[RFC3471] L. Berger, et. al, "Generalized MPLS - Signaling Functional Description, IETF RFC 3471
[RFC4301] Kent, S., and K. Seo, "Security Architecture for the Internet Protocol," IETF RFC 4301
[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)," IETF RFC 4303
[RFC4306] Kaufman, C., ed., "Internet Key Exchange (IKEv2) Protocol," IETF RFC 4306
[RFC4328] GMPLS Signaling Extensions for G.709 Optical Transport Networks Control January 2006
[RFC4606] E. Mannie, et. al, "Generalized Multi-Protocol Label Switching (GMPLS) Extensions for Synchronous Optical Network (SONET) and Synchronous Digital Hierarchy (SDH) Control" IETF RFC 4606.
[X213] ITU-T Rec. X.213 (2001), "Information technology – Open Systems Interconnection – Network service definition"

12 Appendix A: List of companies belonging to OIF when document is approved

ADVA Optical Networking
Agilent Technologies
Alcatel-Lucent
Altera
AMCC
Analog Devices
Anritsu
AT&T
Avago Technologies Inc.
Avanex Corporation
Bookham
Booz-Allen & Hamilton
Broadcom
BT
China Telecom
Ciena Corporation
Cisco Systems
ClariPhy Communications
CoreOptics
Cortina Systems
Data Connection
Department of Defense
Deutsche Telekom
Ericsson
Finisar Corporation
Flextronics
Force 10 Networks
Foxconn
France Telecom
Freescale Semiconductor
Fujitsu
Furukawa Electric Japan
Huawei Technologies
IBM Corporation
IDT
Infinera
Intel
IP Infusion
JDSU
KDDI R&D Laboratories
Level 3 Communications
LSI Logic
Marben Products
MergeOptics GmbH
Mintera
MITRE Corporation
Mitsubishi Electric Corporation

Molex
NEC
NeoPhotonics
Nokia Siemens
Nortel Networks
NTT Corporation
Opnext
PMC Sierra
PMC Sierra
Sandia National Laboratories
Santur
Sierra Monolithics
Silicon Logic Engineering
Soapstone Networks
Sycamore Networks
Syntune
Tektronix
Telcordia Technologies
Telecom Italia Lab
Tellabs
Texas Instruments
Time Warner Cable
Transwitch
Tyco Electronics
Verizon
Vitesse Semiconductor
Yokogawa Electric Corporation
ZTE Corporation