



D A2.1 – From Reference Applications to Layer 2 and Layer 3 Services

EDITOR:

Rainer Stademann
Siemens AG, D-81359 München
Rainer.stademann@siemens.com

ADDITIONAL CONTRIBUTORS:

Alcatel:	Peter Vandaele
BT:	Chris Pitt
France Telecom:	Frederic Jounay
Infineon:	Andreas Foglar
Portugal Telecom Inovação:	Vitor Simoes Ribeiro
Telefónica Investigación y Desarrollo:	Georgina Gallizo

Identifier:	Deliverable D A2.1
Class:	Report
Version:	1.01
Version Date:	24/06/2004
Distribution:	Public
Responsible Partner:	SIE
Filename:	MUSE_DA2.1_v1.0.doc

DOCUMENT INFORMATION

Project ref. No.	IST-6thFP-507295
Project acronym	MUSE
Project full title	Multi-Service Access Everywhere
Security (distribution level)	PU
Contractual delivery date	M5
Actual delivery date	11.06.2004
Deliverable number	DA2.1
Deliverable name	From Reference Applications to Layer 2 and Layer 3 Services
Type	Report
Status & version	V1.01
Number of pages	47
WP / TF contributing	WP A2
WP / TF responsible	Jeanne De Jaegher
Main contributors	ALC, BT, FT, IFX, PT, SIE, TID
Editor(s)	Rainer Stademann
EU Project Officer	Pertti Jauhiainen
Keywords	service model, Ethernet service, IPv4, IPv6, circuit emulation, interaction, mapping, point-to-point, point-to-multipoint, multipoint
Abstract (for dissemination)	This deliverable outlines a service model for Ethernet, IPv4, IPv6 and circuit emulation targeted to the multi-service broadband access and aggregation network. Based on a set of reference applications it is shown that the application requirements defined by WP A1 can be mapped onto this service model.

DOCUMENT HISTORY

Version	Date	Comments and actions	Status
0.1	23.04.2004	First "straw man" with Introduction, Scope, Outline	Draft
0.2	10.05.2004	First merge of input for Network reference model, Ethernet and PPP service model, IPv4 service model and interaction of IP and Ethernet services.	Draft
0.3	12.05.2004	Add text for application mapping in the Ethernet service model chapter. Editorial comments to chapter 5 and 6.	Draft
0.4	14.05.2004	as V03 but with accepted revisions	Draft
0.5	19.05.2004	Revised text from contributors after phone conference 13.05.2004	Draft
0.6	28.05.2004	Consolidated version as input for MUSE internal review	Draft
1.0	11.06.2004	Final version after internal review	Reviewed
1.01	24.06.2004	Correction in list of main contributors	

TABLE OF CONTENTS

DOCUMENT INFORMATION	2
DOCUMENT HISTORY	3
TABLE OF CONTENTS	4
LIST OF FIGURES AND TABLES	5
ABBREVIATIONS	6
REFERENCES	8
EXECUTIVE SUMMARY	9
GLOSSARY	9
1 INTRODUCTION	10
2 SCOPE	12
3 BASIC PRINCIPLES	14
3.1 Network Reference Model	14
3.2 Basic Terminology	15
3.2.1 <i>Application Flow</i>	15
3.2.2 <i>Service Connection</i>	15
3.2.3 <i>Types of configuration</i>	16
3.2.4 <i>Basic services</i>	18
3.2.5 <i>Binding of application flows to service connections</i>	19
4 OUTLINE OF A SERVICE MODEL FOR ETHERNET AND PPP SERVICES IN THE BROADBAND ACCESS	20
4.1 The MEF Service Reference Model	20
4.2 Application of p-t-p EVCs	21
4.3 Application of Multipoint EVCs	22
4.4 Implementing the PPP service on top of a multi-point EVC	22
4.5 Ethernet Service Multiplexing	23
4.6 Mapping of Specific Applications	24
4.6.1 <i>High Speed Internet</i>	24
4.6.2 <i>VoD</i>	25
4.6.3 <i>VoIP</i>	25
4.6.4 <i>Peer-to-peer applications</i>	26
4.6.5 <i>Video Telephony / Conferencing</i>	26
4.6.6 <i>Multicast TV</i>	27
5 OUTLINE OF A MODEL FOR IPV4 SERVICES IN THE BROADBAND ACCESS	28
5.1 Introduction	28
5.2 General outline	28
5.2.1 <i>Network Reference Model</i>	28
5.2.2 <i>Types of configuratios for IP service connections</i>	30
5.2.3 <i>Security</i>	31
5.2.4 <i>Quality of Service</i>	31
5.2.5 <i>Service multiplexing</i>	32
5.3 Mapping of Specific Applications	33
5.3.1 <i>High Speed Internet</i>	33
5.3.2 <i>VoD</i>	33
5.3.3 <i>VoIP</i>	34
5.3.4 <i>Peer-to-peer applications</i>	35
5.3.5 <i>Broadcast or multicast television</i>	35

6	INTERACTION BETWEEN ETHERNET AND IP SERVICES	37
6.1	Introduction	37
6.2	The impact of multicast.....	37
6.2.1	<i>Multicast Ethernet MAC address and IP address mapping.....</i>	<i>38</i>
6.2.2	<i>Ethernet service model model applied to multicast.....</i>	<i>38</i>
7	CIRCUIT EMULATION SERVICE	40
7.1	Reference Models.....	40
7.1.1	<i>CES Point to Point Reference Model</i>	<i>40</i>
7.1.2	<i>CES Point to Multi-Point Reference Model</i>	<i>41</i>
7.2	CES Reference Model Scope.....	43
7.3	Operator CES requirements	43
8	THE IMPACT OF IPV6 ON THE SERVICE MODELS	44
8.1	Ethernet Encapsulation	44
8.2	Address Structures	44
8.3	Autoconfiguration.....	45
8.4	Quality of Service.....	46
8.5	Terminal Mobility.....	46
8.6	Peer-to-peer Services.....	47
8.7	Security.....	47

LIST OF FIGURES AND TABLES

Figure 1: Network Reference Model.....	14
Figure 2: The different roles a Network Access Provider can play in services delivery	16
Figure 3: Point-to-point service connections	17
Figure 4: Two examples of point-to-multipoint service connections.....	17
Figure 5: A multipoint-to-multipoint service connection.....	18
Figure 6: The MEF service reference model	20
Figure 7: Examples of MEF p-t-p EVCs used in a broadband access network.....	21
Figure 8: Example of an MEF multi-point EVC used in a broadband access network.....	22
Figure 9: Implementation of a p-t-p PPP service on top of a multi-point EVC.....	22
Figure 10: Ethernet Service Multiplexing.....	23
Figure 11: NAP supporting on demand access to multiple ISPs	24
Figure 12: Implementation of VoIP by the use of p-t-p EVC	26
Figure 13: Network scenario with an NAP providing IP service.	29
Figure 14: Different IP service connections between users and ASPs	30
Figure 15 : A best effort mp-t-mp IP service connection implementing the Internet service ..	31
Figure 16: IP service multiplexing based on destination IP address	32
Figure 17: Internet Access with individual p-t-p IP service connections.....	33
Figure 18: VoIP application using direct p-t-mp IP service connections	34
Figure 19 : VoIP using IP DSLAM with mp-t-mp service connection	35
Figure 20: Multicast example	37
Figure 21: A p-t-mp Ethernet service connection used for multicast.....	39
Figure 22: Point-to-point CES reference model	41
Figure 23: Point-to-multi-point CES reference model.....	42

ABBREVIATIONS

6INIT Ipv6 Internet Initiative
AAA Authentication, Authorisation, and Accounting
AAL ATM Adaptation Line
ADSL Asymmetric Digital Subscriber Line
ANSI American National Standards Institute
AON All Optical Network
API Application Programming Interface
APON ATM-based PON
ARP Address Resolution Protocol
ASIC Application Specific Integrated Circuit
ASP Application Service Provider
ATM Asynchronous Transfer Mode
BB Broadband
BER Bit Error Rate
BPON Broadband PON
BRAS Broadband Remote Access Server
CAPEX Capital Expenditure
CDN Content Distribution Network
CE Circuit Emulation
CMOS Complementary Metal Oxide Semiconductor
CO Central Office
CP(E) Customer Premises (Equipment)
CWDM Coarse Wavelength Division Multiplexing
DHCP Dynamic Host Configuration Protocol
DS Downstream
DSL Digital Subscriber Line
DSLAM Digital Subscriber Line Access Multiplexer
DVB Digital Video Broadcasting
DWDM Dense Wavelength Division Multiplexing
EFM Ethernet in the First Mile
EMAN Ethernet MAN
E/O Electro/Optical
EPON Ethernet PON
FPGA Field-Programmable Gate Array
FQDN Fully qualified domain name
FSAN Full Service Access Network
FWA Fixed Wireless Access
GigE Gigabit Ethernet
GoS Guarantee of Service
GSM Global System for Mobile communications
HW Hardware
IANA Internet Assigned Numbers Authority
IC Integrated Circuit
IEC International Electrotechnical Commission
IEEE Institute of Electrical and Electronics Engineers
IETF Internet Engineering Task Force
IF Intermediate Frequency
ILEC Incumbent Local Exchange Carrier

ILMI Interim Line Management Interface
IP Internet Protocol
ISP Internet Service Provider
ITU International Telecommunication Union
LAC L2TP Access Concentrator
LAN Local Area Network
(L/E-)LSP (Label-only-inferred-Per Hop Behaviour Scheduling Class / Experimental bits-inferred-Per Hop Behaviour Scheduling Class) Label Switched Path
LNS L2TP Network Server
LT Line Termination
MAC Medium Access Control
MAN Metropolitan Area Network
MEF Metro Ethernet Forum
MIB Mangement Information Base
MPEG Motion Picture Expert Group
(G)MPLS (Generalised) Multi Protocol Label Switching
MPLSF MPLS Forum
MTU Multi Tenant Unit
NAP Network Access Provider
NAT Network Address Translation
NNI Network to Network Interface
NSM Network & Service Management
NSP Network Service Provider
NT Network Termination
OAM Operations, Administration and Maintenance
OLT Optical Line Termination
ONT Optical Network Termination (for FTTH)
ONU Optical Network Unit
OPEX Operational Expenditure
P2P Point (Peer) to Point (Peer)
P2MP Point to Multi Point
PHY Physical Layer
PKI Public Key Infrastructure
PnP Plug and Play
PON Passive Optical Network
POS Packet Over SONET
POTS Plain Old Telephone System
PSTN Public Switched Telephone Network
PPP Point-to-Point Protocol
PPVPN Provider Provisioned VPN
PSN Packet Switched Network
PVC Permanent Virtual Channel
QAM Quadrature Amplitude Modulation
QoS Quality of Service
RTP Real-time Transport Protocol
RNP Regional Network Provider
SC Service Connection
SIP Session Initiation Protocol
SLA Service Level Agreement
SLS Service Level Specification

SME Small and Medium Enterprise
SOHO Small Office/Home Office
STM Synchronous Transfer Mode
SVC Switched Virtual Channel
SW Software
TDM Time Division Multiplexing
TF Task Force
TG Task Group
TVoIP TV over IP
UNI User to Network Interface
UPnP Universal Plug and Play
US Upstream
VDSL Very high speed Digital Subscriber Line
VLAN Virtual LAN
VoAAL2 Voice over ATM Adaptation Layer 2
VoIP Voice over IP
VoMPLS Voice over MPLS
VPLS Virtual Private LAN Services
VPN Virtual Private Network
(C/D)WDM (Coarse/Dense) Wavelength Division Multiplexing
WAN Wide Area Network
WLAN Wireless LAN
WP Work Package
WWI Wireless World Initiative (proposal for FP6 project)

REFERENCES

- [1] MEF Technical Specification 1.0, Ethernet Services Model, Phase 1, Aug. 25th 2003
- [2] Technical Report DSL-Forum TR-058, Multi-Service Architecture and Framework Requirements, September 2003
- [3] Technical Report DSL-Forum TR-059, DSL-Evolution - Architecture Requirements for QoS-enabled IP Services, September 2003
- [4] RFC 1661, "The Point-to-Point Protocol (PPP)", IETF, July 1994
- [5] RFC 2547, "BGP/MPLS VPNs", IETF, March 1999
- [6] RFC 2474, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers", IETF, December 1998
- [7] RFC 2475, "An Architecture for Differentiated Service.", IETF, December 1998

EXECUTIVE SUMMARY

This deliverable outlines a service model for Ethernet, IPv4, IPv6 and circuit emulation targeted to the multi-service broadband access and aggregation network. Based on a set of reference applications it is shown that the application requirements defined by WP A1 can be mapped onto this service model.

The service model results from a generalization of the Ethernet service model specified by the Metro Ethernet Forum. It is based on the concept of “service connections”. A service connection provides a layer 2 and/or layer 3 service with a specific set of service attributes, e.g. a QoS profile, between two or more interfaces of the multi-service broadband access network. Service connections must be engineered according to their specific service attributes and therefore represent a rather static network property.

However, traffic flows generated by applications in a multi-service broadband access network can be rather dynamic and transient. This aspect is covered by the service model through a dynamic binding of application flows to the service connections. This flexible binding between application flows and service connections must be performed by the nodes of the access and aggregation network itself and is an essential requirement to be fulfilled in the future multi-service broadband access network.

GLOSSARY

Service connection instance	A service connection instance is an instance of an association between two or more U and/or V interfaces. The service connection instance provides Layer 2 and/or Layer 3 services to one or more application instances .
Application flow	An application flow is a traffic flow in the access/aggregation network which is generated by a single application instance.
Binding	Binding is the means by which an application flow is assigned to a service connection instance so that it can make use of the provided service.
Basic service	A basic service is either an Ethernet, PPP, CE, IPv4 or IPv6 service.

1 INTRODUCTION

The most common broadband application in today's access networks is often simple internet access, characterized by

- best effort SLA
- single service connection per access port
- moderate bandwidth per access port.

Future applications are much more demanding in requiring a multi service broadband access network which supports, e.g.,

- multiple concurrent service connections per access to multiple network and application service providers
- direct and on-demand service connections between different accesses (peer-to-peer)
- guaranteed QoS and/or SLA
- on demand QoS per service connection
- multicast and broadcast
- rich content applications with high bandwidth requirements
- nomadic applications
- peer-to-peer applications
- highly reliable applications, like telephony
- Circuit Emulation services
- Metro Ethernet business services, like Virtual Private LAN Service or Virtual Private Wire Service.

At the same time Ethernet technology step by step is starting to complement or replace ATM in the first and second mile of carrier networks. This is mainly due to the Ethernet's superior price/performance caused by the economy of scale, which is being originated in the huge enterprise market.

In parallel, functionality developments are also being carried out in Ethernet products which were only available before in advanced IP routers, e.g., QoS support, complex frame/packet filtering functions, user authentication (based on 802.1x), etc. These developing functionalities will help to fulfil carrier specific requirements, e.g., concerning security, reliability, multi-service engineering, which were in so far not completely supported in Ethernet enterprise networks.

Consequently Ethernet services have been defined for carrier networks, the most advanced service model being specified by the Metro Ethernet Forum [1]. This model was developed with the focus on Ethernet business applications, because it is targeting Metro Ethernet networks. Ethernet business applications and therefore the service model of the MEF must also be supported by a future multi-service broadband access. However, additionally the much larger scale of demanding residential and business applications as investigated in WP A1 must be supported simultaneously by this access network.

Altogether it is envisioned that the future broadband access network must implement powerful service models, with a wide variety of service attributes, which are capable of supporting many different business and residential applications as well as the different business models of the network access providers. One potential service model, which can be taken as a basis, is that of the Metro Ethernet Forum [1]. However since this targets only a small set of Ethernet business services, the objective of this deliverable is to outline more generic service models for the future multi service broadband access.

2 SCOPE

Annex 1 of the MUSE contract describes the scope of this deliverable as follows:

“Roles of Ethernet, IPv4, IPv6 and CE services in the broadband access

The first task is a research activity whose aim is to revisit the roles and uses of Ethernet services, IPv4 services and IPv6 services in a multi-service broadband access. The idea is to investigate whether the mapping between an application and a Layer 2 or Layer 3 service can be optimised, with respect to the present situation. This task involves

- to investigate how Ethernet services as defined in the Metro Ethernet Forum can be used for residential broadband applications (e.g. peer-to-peer services) and define specific requirements and service attributes
- to determine the service requirements (QoS, configuration,..) for emerging IP services.
- to study the interaction between Ethernet and IP services (e.g. multicast)
- to define IPv6 services for multi-service broadband access and determine the possible role and requirements for IPv6 services in broadband applications
- to study the interaction between IPv6 services and Ethernet/IP services (including interaction between fixed and mobile services).

After three months a proposal for service roles will be presented to SP A (M A2.1) and will need to be agreed on. The proposal will further be consolidated into a deliverable (DA2.1). Both documents will be a basis for the research task on network architecture.”

WP A1 defines a shortlist of reference applications together with the respective application requirements.

In deliverable DA1.2 these application specific requirements are mapped into generic classes of network requirements for multi-service broadband access.

It is the objective of the present deliverable DA2.1 to outline how these network requirements can be further consolidated into service models for Ethernet, IPv4, IPv6 and CE services. These service models must be appropriate for the broadband access, and must allow as well for an optimized mapping of the business and residential applications.

The scope of the present deliverable encompasses:

- an investigation about if and how the service model specified by the MEF [1] can be re-used and mapped onto the most common reference applications defined by WP A1
- an investigation on a service model for IPv4 services applicable to the broadband access and which is supporting the most common reference applications

- an investigation on the interaction between Ethernet and IPv4 services, e.g., caused by multicast
- an investigation on the influence of IPv6 on the above mentioned service models for the broadband access
- an investigation on the interaction between IPv6 services with Ethernet and IPv4 services.

It is not in the scope of this deliverable to:

- specify application or network requirements (performed by WP A1)
- investigate how the service models can be implemented by a network and which functions are required on the network elements in order to fulfil the implementation (performed by WP A2.2, WP A2.3)
- specify service models which are relevant only for the network beyond the access edge nodes.

3 BASIC PRINCIPLES

3.1 Network Reference Model

The basic network model this document is referring to is shown in figure 1. This network model is based on the DSL-Forum network model as defined in [2] and [3], which mainly identifies five different sub-networks:

- the customer premise network (CPN)
- the access network operated by a network access provider (NAP)
- the regional network operated by a regional network provider (RNP)
- the network service provider (NSP) network
- the application service provider (ASP) network.

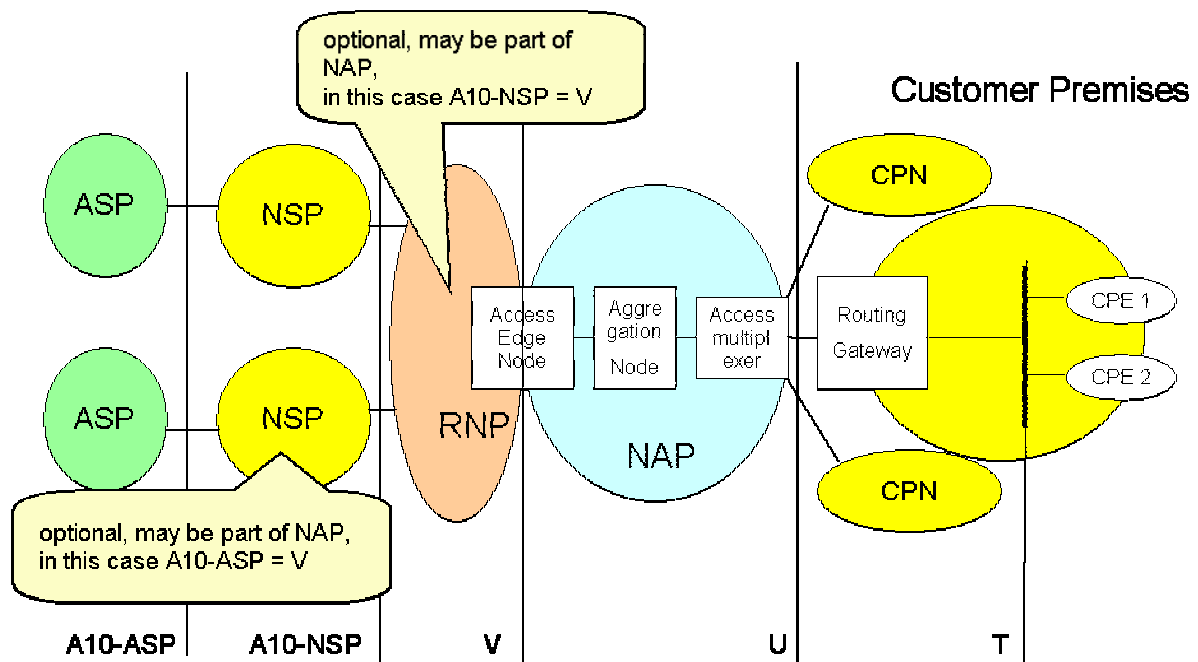


Figure 1: Network Reference Model

The customer premise network CPN is connected to the access network at reference point U. This corresponds to the interface between the routing gateway RG in the CPN and the access multiplexer of the NAP.

On its turn, the access network is connected to a regional network at reference point V, which corresponds to an interface of the access edge node. It is to be noted that the regional network in this definition does not offer itself IP services to the CPN, although it will often use IP networking to provide the connectivity between the access networks and the NSP network, e.g., by using L2TP tunnels.

This network service provider NSP offers an IP networking service to a CPN, e.g. it provides and manages IP addresses being visible at the U interface for customer premise networks. An NSP is interconnected to the regional network at reference point A10-NSP.

Finally, an application service provider ASP offers specific applications to application subscribers (e.g. gaming, video, content, IP telephony). For this purpose an ASP uses the IP networking service of an NSP. The ASP itself does not assign IP addresses to the application subscribers. An ASP network is connected to an NSP network at reference point A10-ASP.

Often the same organizational entity will operate more than one of the above sub-networks, e.g., the organizational entity operating the access network may also operate the regional network (NAP=RNP). In this case the V reference point equals the A10-NSP reference point. If additionally the same organizational entity takes over the role of a NSP (NAP=RNP=NSP) the V reference point becomes the A10-ASP reference point (compare also Figure 2).

3.2 Basic Terminology

3.2.1 Application Flow

An application flow is a traffic flow in the access and aggregation network which is generated by a single application instance.

An example of an application flow is the RTP stream of a single VoIP call instance in the access and aggregation network between a U interface, behind which the VoIP client is located, and a V interface where the media gateway of a VoIP provider is connected. It is to be noted that usually there are multiple application flows associated with one application instance, e.g., in the above example indicated there is another application flow which is a SIP or H.323 control stream.

3.2.2 Service Connection

The network access provider offers layer 2 and/or layer 3 services to network and application service providers, to regional network providers and to customer premises connected to its network. In this document, the basic means provided by the NAP to offer its service between a specific set of U and V reference points is designated by a “service connection”, see Figure 2. The service connection concept can be seen as a generalization of the concept of Ethernet Virtual Connections (EVC) defined by the Metro Ethernet Forum (MEF) [1].

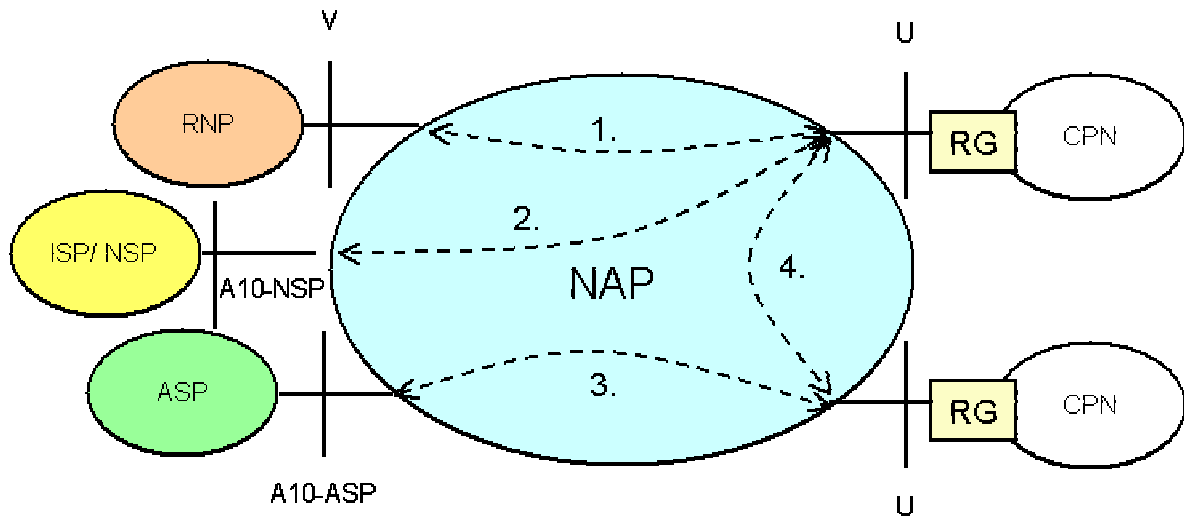


Figure 2: The different roles a Network Access Provider can play in services delivery

A service connection is an instance of an association between two or more U and/or V interfaces. These interfaces are said to be in the service connection or member of the service connection. Service frames/datagrams MUST NOT be delivered to interfaces which are not in the service connection. Service connections between U interfaces are known as peer-to-peer. There can be more than one service connection between the same set of U/V-interfaces.

Figure 2 shows additionally the different roles an NAP can have. The NAP can provide service connections to an Regional Network Provider RNP (1). The NAP can also be additionally an RNP and as such can offer service connections to an Internet or Network Service Provider ISP/NSP (2). Also the NAP can be an ISP/NSP and as such can offer service connections to an Application Service Provider ASP (3). Finally the NAP can provide peer-to-peer service connections to CPNs (4).

3.2.3 Types of configuration

In terms of types of configuration, service connections can be point-to-point (p-t-p), point-to-multipoint (p-t-mp) or multipoint-to-multipoint (mp-t-mp).

A point-to-point service connection is an instance of an association between a single U and a single V interface or between two U interfaces, see Figure 3.

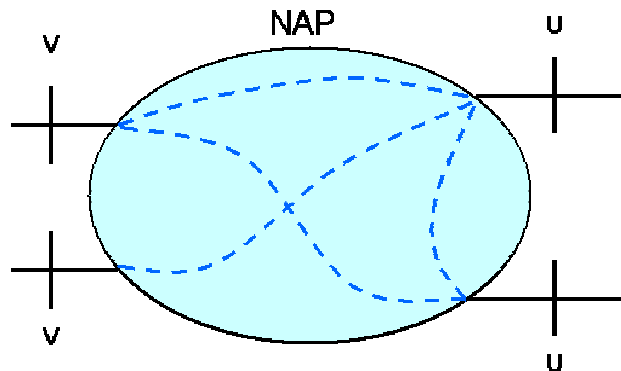


Figure 3: Point-to-point service connections

On its turn, a point-to-multipoint (p-t-mp) service connection is an instance of an association between a particular root interface U or V and a set of leaf or secondary U or V interfaces, see Figure 4. Service frames/datagrams are delivered between the root interface on one hand and the leaf interfaces on the other hand. Service frames/datagrams **MUST NOT** be delivered between two leaf interfaces.

Moreover, a p-t-mp service connection can serve multicast, broadcast, and also unicast application flows.

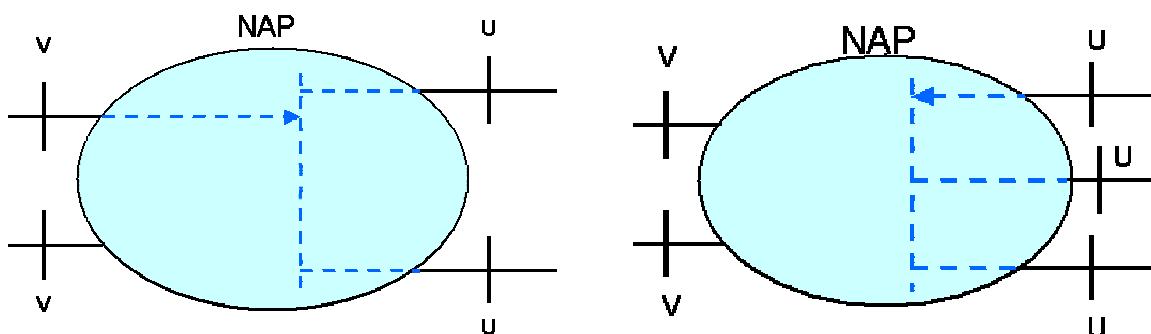


Figure 4: Two examples of point-to-multipoint service connections

Finally, a multipoint-to-multipoint service connection is an instance of an association between multiple U/V interfaces, see Figure 5. Service frames/datagrams can be delivered between all interfaces, which are in the service connection.

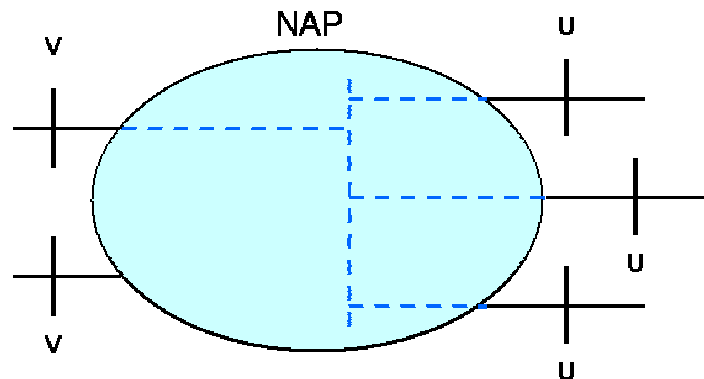


Figure 5: A multipoint-to-multipoint service connection

3.2.4 Basic services

A service connection can offer one of the following basic services:

- Ethernet service

This service delivers Ethernet frames between U/V-interfaces, and is based on an extension of the MEF service model [1]. It can be used to provide Ethernet bearer services to business customers or peer-to-peer Ethernet bearer services to residential customers. It may also be used for applications like high speed internet access or VoIP applications. The service can be offered via p-t-p, p-t-mp or mp-t-mp service connections.

- PPP service

This service conveys PPP frames between U/V interfaces, according to RFC 1661 [4]. It is often used to transport IP datagrams over the PPP connection, and is only applicable to p-t-p service connections. A PPP service can be provided over an Ethernet network using PPPoE, as well as over an IP network by using L2TP.

- IPv4 service

This service delivers IPv4 datagrams between the U/V interfaces of a service connection. The service includes the assignment of IP addresses or IP subnets to the involved U/V interfaces. Therefore a NAP can only offer this service if it is also a NSP.

- IPv6 service

This service delivers IPv6 datagrams between the U/V interfaces of a service connection. In this case, the NAP will also usually be an NSP.

- CE service

This service delivers service frames of the emulated circuit between the involved interfaces, e.g., for E1 emulation, each 125 microseconds a 256 bit frame should be delivered. Since CE is usually synchronous, strict requirements with respect to delay and jitter apply. These CE services are usually point-to-point.

3.2.5 Binding of application flows to service connections

A single service connection instance can support a flow of a single application instance, but usually flows of multiple application instances will be bound to the same service connection instance. Even flows of instances belonging to different applications can be bound to the same service connection instance, if these application flows have the same service requirements.

Multiple p-t-p flows between different pairs of U/V interfaces can also be bound to a single multipoint service connection instance, either p-t-mp or mp-t-mp.

While application flows themselves can be rather dynamic, service connections will often be rather static since they usually need provisioning effort by the NAP (e.g. by network engineering). For example, for a VoIP application a single p-t-mp service connection instance may be pre-provisioned by the NAP in an access network. For those customers which are subscribing to VoIP the respective U interface will become a member of this service connection instance. All application flows of the succeeding VoIP calls will be bound to this same service connection instance.

4 OUTLINE OF A SERVICE MODEL FOR ETHERNET AND PPP SERVICES IN THE BROADBAND ACCESS

4.1 The MEF Service Reference Model

In Figure 6 the basic MEF reference service model [1] is depicted. The MEF framework defines Ethernet service connections which are known by ‘Ethernet Virtual Connection’ (EVC). In the MEF model there are only p-t-p EVC and mp-t-mp EVC, i.e., there is no p-t-mp EVC defined. The reason for this is that the MEF is focused on Ethernet business services as a replacement of leased line service or FR and ATM services. In these kind of business services only user-network interfaces (UNI) are involved, i.e., in the MEF model there is no equivalent for the V interface acting as a NNI interface.

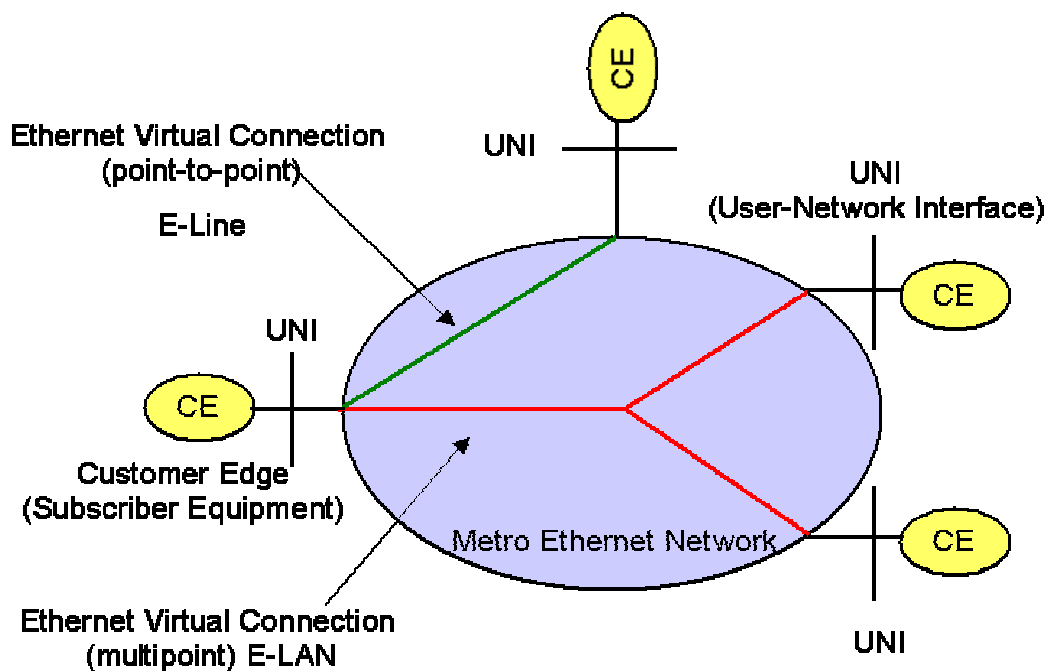


Figure 6: The MEF service reference model

Also the MEF model does not include a flexible binding mechanism between application flows and service connections.

In short, the MEF service model, as it is defined, can only be applied to a broadband access network either:

- for service connections with a static flow binding and where only U interfaces are involved, i.e., for static peer-to-peer business or residential services, or,

- for service connections with a static flow binding, that, from an Ethernet service point of view, are symmetric with respect to U and V interfaces.

As such, and in order to perform all the envisaged broadband applications in the access network, the basic principle that interfaces can act as U, V, A10-NSP, and A10-ASP interfaces must be assumed from the very beginning.

4.2 Application of p-t-p EVCs

Different examples for the use of p-t-p EVCs in a broadband access network are shown in Figure 7.

A p-t-p EVC can be used to implement an Ethernet virtual line between two U interfaces. If both U interfaces are connected to the same access network, this peer-to-peer service can be statically provisioned by the NAP

P-t-p EVCs can also be used to statically interconnect all U interfaces of an access network with a regional network in a point to point fashion. This results in a network architecture being similar to ATM based access networks, where PVCs for interconnecting U interfaces with the regional network are used.

A p-t-p EVC could also be provisioned to interconnect a U interface to a pre-selected NSP. In this case the NSP could offer directly IP service on top of the p-t-p EVC provided by the NAP, e.g. using a DHCP based solution.

It should be noted that an EVC cannot be used to interconnect to an ASP, since an ASP requires that an IP service is delivered to it by an NSP. However, an IP service cannot be provided only by an EVC.

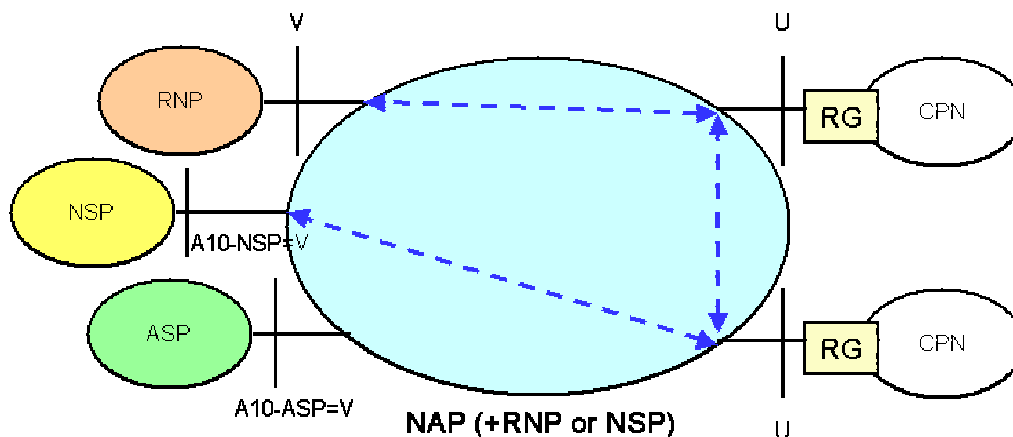


Figure 7: Examples of MEF p-t-p EVCs used in a broadband access network

4.3 Application of Multipoint EVCs

In Figure 8 an example illustrating the use of an MEF multipoint EVC for interconnecting all U interfaces of an access network to a regional network is shown. It should be noted that, due to the multipoint property of the EVC, peer-to-peer communication between the U-interfaces is not prevented in this case.

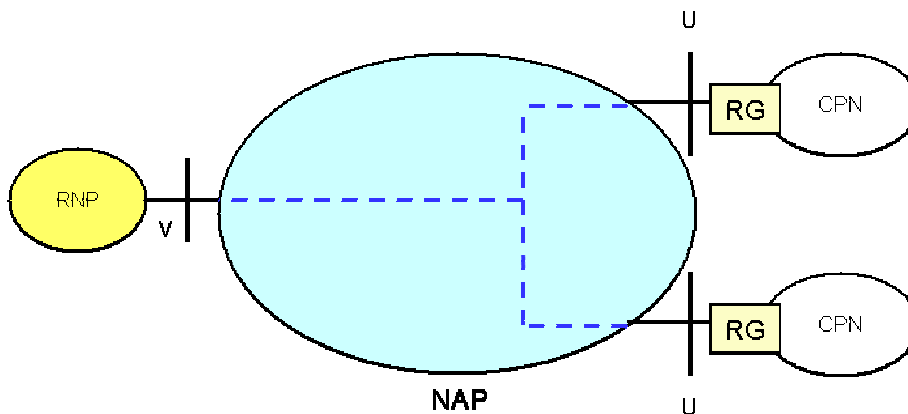


Figure 8: Example of an MEF multi-point EVC used in a broadband access network

4.4 Implementing the PPP service on top of a multi-point EVC

In Figure 9, a particular case of how a p-t-p PPP service can be provided on top of a multipoint EVC is shown. For this purpose, a special PPPoE service attribute can be introduced for the U interfaces. On a U interface where this attribute is set, only PPPoE client traffic that is destined for a PPPoE server behind a V interface will be accepted, and all other Ethernet frames are discarded. Thus, peer-to-peer traffic on the multipoint EVC can be prevented. However, it should be noted, that all PPPoE sessions share the same common EVC resource. The substantial functionality, which is required at the access network border for supporting this feature, is out of scope of this document.

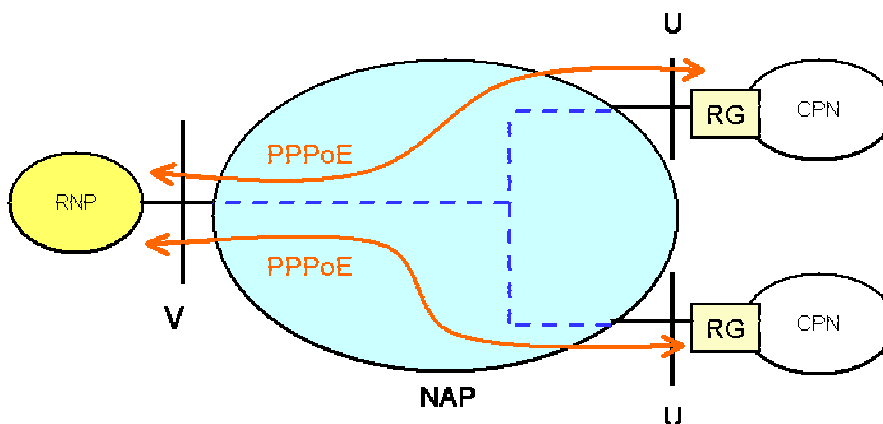


Figure 9: Implementation of a p-t-p PPP service on top of a multi-point EVC

4.5 Ethernet Service Multiplexing

Figure 10 shows how service multiplexing can be implemented at the U interface, in order to multiplex traffic between multiple Ethernet service connections and one physical U interface. The MEF service model [1] uses a Customer Edge (CE) VLAN tag-to-EVC map as a UNI service attribute to perform this multiplexing. This requires the administration of a fixed binding between EVCs and CE-VLAN tags. The disadvantage is that this binding must be adapted if new EVCs are introduced by the NAP.

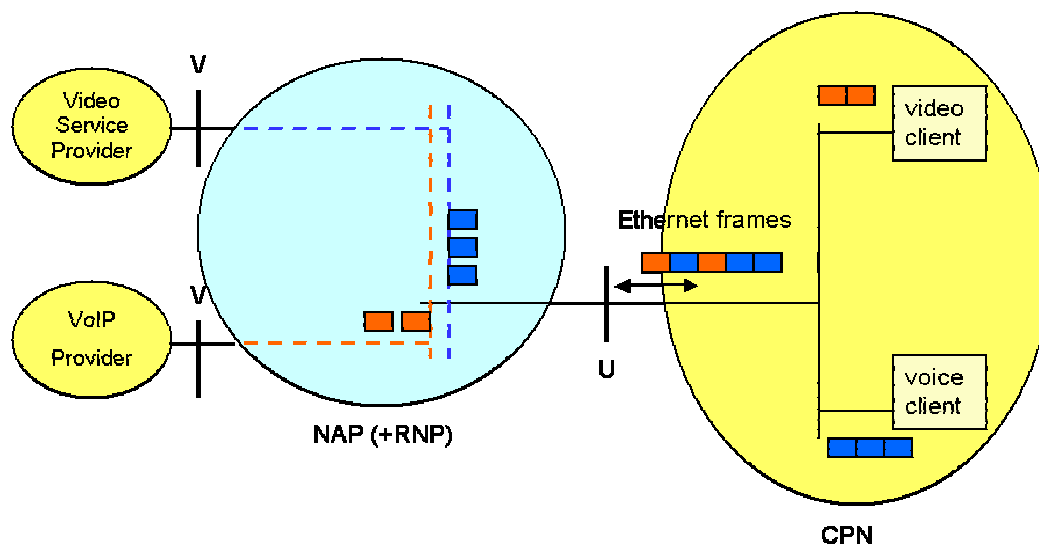


Figure 10: Ethernet Service Multiplexing

In the future, a more flexible approach could be followed in that the selection of the appropriate Ethernet service connection by a dynamic on-demand binding of the application flows to the service connection instance would be allowed, e.g., as part of the registration procedure of an application. The registration procedure would include a service selection phase during which the specific MAC address or CE-VLAN of the CPE would be bound to the selected service connection instance. Further on, the MAC address or CE-VLAN of the CPE would be used as criteria for the service multiplexing.

4.6 Mapping of Specific Applications

In the following, a mapping of some applications to a generic service model is investigated, taking the MEF service model [1] as a basis, and pointing out the necessary changes that should be performed in order to fulfil the specific requirements of those applications.

4.6.1 High Speed Internet

High speed Internet access is today often still based on the use of PPPoE in the access network as depicted in Figure 9. In this case the user selects the ISP during the authentication procedure based on a FQDN. However the use of PPP requires expensive PPP processing functionality within the IP network.

A more cost efficient solution can be achieved by directly using IP over Ethernet in the access network. However, in an unstructured Ethernet network without service connections, this means that only a single IP service can be provided, i.e., only one ISP can be supported.

Figure 11 shows how Ethernet service connections can help to allow also in this case for a dynamic on demand selection of ISPs.

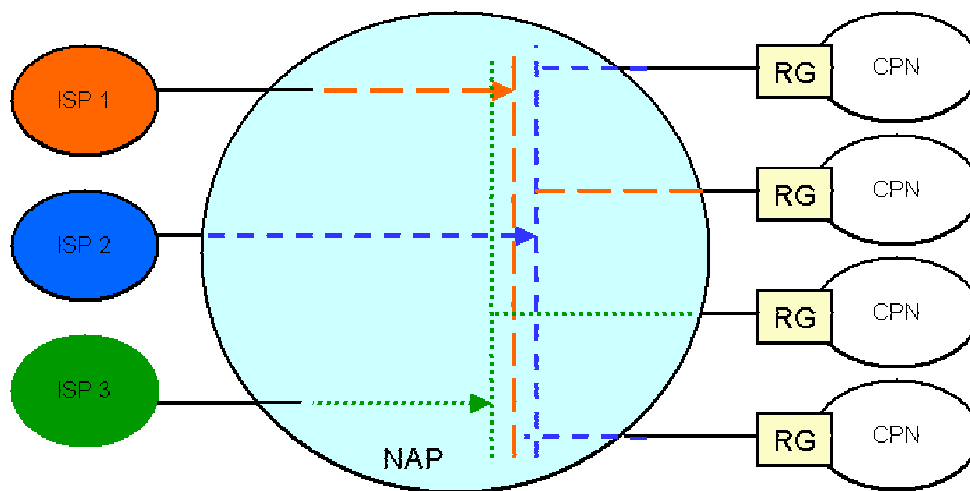


Figure 11: NAP supporting on demand access to multiple ISPs

For this purpose, and overtaking the p-t-mp EVC restriction of the MEF service model [1], each ISP could be assigned a p-t-mp Ethernet service connection by the NAP. The p-t-mp concept property prevents that the service connections are abused for peer-to-peer traffic. By using a service selection process, a user in the CPN can bind the flows of an Internet application to the appropriate service connection instance. Since each ISP has its own Ethernet service connection instance assigned, IP services can be delivered by the ISPs in a completely independent way from one another, e.g., with independent IP addressing.

Scalability is the main reason for the use of p-t-mp Ethernet service connections as opposed to a multitude of p-t-p Ethernet service connection instances. Indeed, a single p-t-mp service connection instance per ISP can serve all customer premises within an access and aggregation network, while otherwise for each combination of ISP and CPN a separate p-t-p Ethernet service connection instance would be required and provisioned.

It is to be noted that this concept also allows for a further differentiation of services, e.g., based on bandwidth profiles, which can be individually assigned to the different service connection instances.

Moreover, a U interface can be simultaneously present in two different service connection instances by using Ethernet service multiplexing.

4.6.2 VoD

For Video on Demand a similar service architecture as described above for high speed Internet access can be used. The Video on Demand provider would take over in addition the role of a NSP. A special p-t-mp Ethernet service connection is assigned to the VoD provider by the NAP. If necessary, a resource and admission control mechanism could be needed in addition, in order to prevent an overload of the service connection in occasional high demand situations.

4.6.3 VoIP

Again the service architecture described for High Speed Internet can be used also for VoIP application. In this case the VoIP provider takes over the role of an NSP and is represented in the Ethernet access network by a p-t-mp Ethernet service connection. During boot up/registration a VoIP client in the CPN initiates a service selection process by which the access network binds the client's application flows to the appropriate p-t-mp service connection.

An alternate solution based on a pre-selected VoIP provider is shown in Figure 12. In this case, p-t-p service connection instances are used to interconnect customer premises to a pre-selected VoIP network service provider. The VoIP service provider also assigns IP addresses to the voice clients in the customer premises. The service connection instances are pre-provisioned with the appropriate service attributes for the VoIP application, e.g. with respect to bandwidth profile, service availability, etc.

The example also shows how dual homing to two different V interfaces can be used to increase service availability.

4.6.6 Multicast TV

Video distribution applications can fully exploit the multicast capability of Ethernet service. The Ethernet service architecture can be based on a dedicated p-t-mp service connection, which is used for the distribution of all video channels. However, the member of U interfaces that belong to the multicast groups must be taken care of by the access network by, e.g., IGMP snooping or another control protocol. This is the reason why for multicast based TV applications additional service attributes describing this control function must be added to a pure Ethernet service connection. More details are discussed in chapter 6

5 OUTLINE OF A MODEL FOR IPV4 SERVICES IN THE BROADBAND ACCESS

5.1 Introduction

IP has become more and more the convergence layer for applications. The number of IP based applications and services and their importance to operators is increasing dramatically.

Currently two well known IP service models have evolved for the IP core, i.e., the best effort Internet service model, and the IP VPN service model based on RFC 2547 [5] BGP/MPLS VPNs. However, the future multi-service broadband access and aggregation network has different requirements, which are not fully addressed by these IP service models.

Therefore, and also taking the MEF Ethernet service model [1] as a working basis, this chapter outlines a more flexible IP service model targeted for the future multi-service broadband access and aggregation network. This chapter focuses on IPv4, while impacts of IPv6 on the service model are described in a separate chapter.

In the next paragraph, a general outline defining the model will be given. Next, some important service attributes will be discussed. Finally, the mapping of several important applications (as defined in MA1) onto the newly defined IP service model, will be analysed.

5.2 General outline

5.2.1 Network Reference Model

The same network reference model as for the layer 2 service model, see Figure 1, will be taken as a basis.

Also, the fundamental service concept outlined in chapter 3 to the IP network layer will apply, i.e., an IP service delivers IP datagrams between interfaces on the network layer. This is opposed to an Ethernet service as described in chapter 4, which delivers Ethernet frames between two or more interfaces at the link layer. Of course an IP service will itself make use of the services at the link layer, which leads to a dependency of the IP service from the implementation of the underlying Ethernet service model. This interaction between the Layer 2 and Layer 3 service models will be discussed in the next chapter.

IP datagrams can be delivered between U and V interfaces, or between two or more U interfaces, see Figure 2. For the IP service model to be applied, the NAP is required to be an NSP, since IP addresses/subnets must be managed by the NAP and assigned to the U/V interfaces. It is to be noted that, if the NAP is *not* also an NSP, and the aggregation network is based on layer 2, the IP datagrams are transported transparently through the NAP and the service provided by the access network relies on layer 2.

Therefore, in order to support the IP service model, a minimum of IP routing will have to be provided by the NAP network, as well as the support for IP QoS mechanisms.

In Figure 13, an example of a network scenario with an IP service provided by a NAP, is shown. In this example the NAP has opted for an IANA assigned address space (105.12.0.0/16), and has a peering point with another ISP to the Internet. Additionally the NAP provides IP services to a VoIP application service provider and a video on demand application service provider. The VoIP ASP was assigned an IP subnet of 105.12.16.0/20 by the NAP, while another 12 bit subnet is assigned to the VoD ASP. On its turn, U interfaces get assigned single host routes, e.g., by using DHCP).

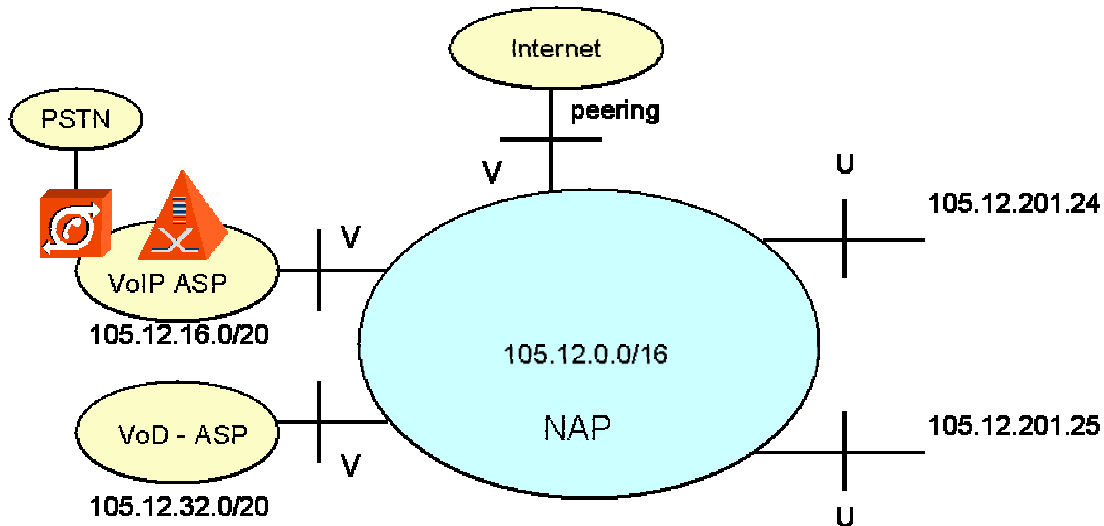


Figure 13: Network scenario with an NAP providing IP service.

In order to provide the appropriate QoS and bandwidth for the video and voice services the NAP allows for appropriate IP service connections. An example is shown in Figure 14, where a multipoint service connection (blue, short dashed) is used for the Internet access, another point-to-multipoint IP service connection (red, long dashed) is used for the VoIP service, while further p-t-p service connections (green, dotted) are used for access to the VoD applications. The Internet service connection is assigned with the best effort QoS class, while the other service connections are assigned according to the appropriate QoS profiles.

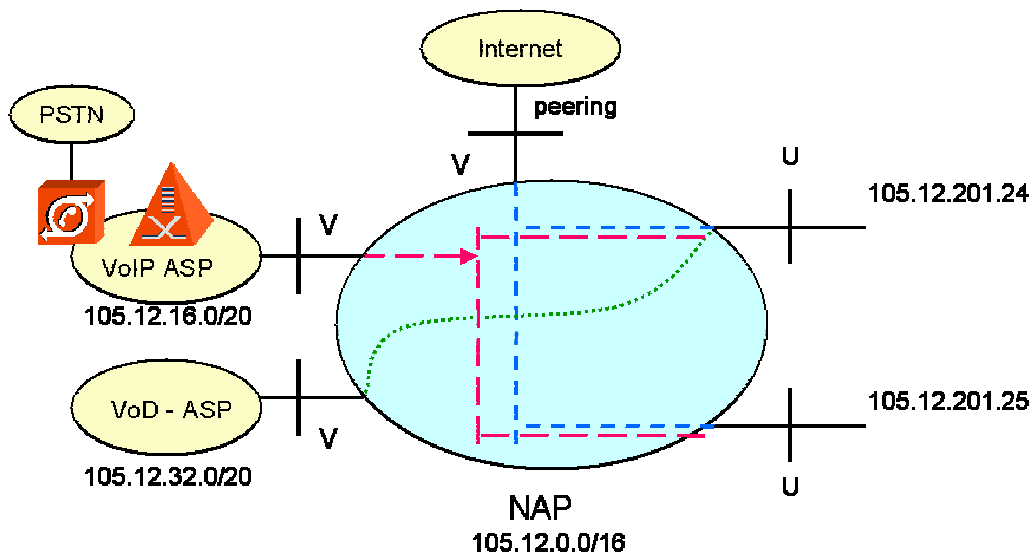


Figure 14: Different IP service connections between users and ASPs

5.2.2 Types of configurations for IP service connections

As already defined for the Ethernet service model [1], three types of configurations for IP service connections must be considered:

point-to-point : in this type, only two interfaces are involved, which can either be a V or a U interface, or two U interfaces. IP application flows which are bound to a p-t-p IP service connection enter the access network at one interface and leave the access network at the other interface of the p-t-p IP service connection. This could be achieved by the performance by the access network of an appropriate IP address filtering of the application flows at the interfaces, or by tunnelling. However, implementation details are outside of the scope of this deliverable.

The differences to p-t-p Ethernet service connection rely on the fact that the p-t-p IP service connection includes assignment of IP addresses/subnets to the interfaces, as well as that only appropriate IP datagrams will be delivered, and that binding of application flows is based on Layer 3 criteria, e.g., IP addresses, port numbers, DSCP bits, etc.

point-to-multipoint : in this type, characterised by a tree-like service topology that allows application flows either from a certain root or server interface (could be both a V or U interface) towards several other, secondary, interfaces (most probably U interfaces), or, in the other direction, where the application flows are from one of the secondary interfaces towards the root interface. There are no flows allowed between two of the secondary interfaces. Hence flows will always go through the root node. The traffic can either be multicast from the root to the secondary interfaces, or can be unicast traffic. Again, an implementation could be based on appropriate IP address filtering of the application flows at the interfaces.

multipoint-to-multipoint : in this type, several interfaces are involved, which could be both U and V interfaces. There are no restrictions with respect to traffic forwarding, and unicast, multicast and broadcast traffic are supported. By using this definition the current well-known Internet service model can be implemented by a NAP based on an overall multipoint-to-multipoint IP service connection. This type of service connection could also be restricted more specifically to single IP subnets, where the identification of the interfaces belonging to this particular IP service connection is based on their IP addresses.

In Figure 15 the subnet 105.12.201.0/24 including both U interfaces in the figure are part of the Internet, while the subnets 105.12.210.0/24 and 105.12.220.0/24 of the V interfaces are not in the Internet service connection. Therefore, these subnets are also not accessible from the Internet, i.e., traffic from the Internet with this destination addresses is discarded at the peering point.

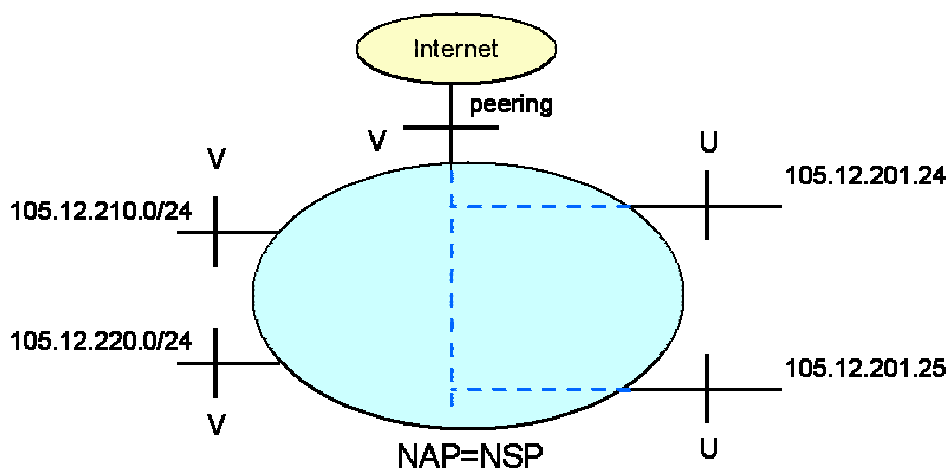


Figure 15 : A best effort mp-t-mp IP service connection implementing the Internet service

5.2.3 Security

Security is of course an essential requirement to be covered by any implementation of this service model. In this context, authentication MUST prevent un-authorized access to service connections, i.e., once a service connection is set up, no other interfaces but the interfaces who are a member of the connection, which is defined at provisioning-time or later on by an authentication procedure, can setup flows over the connection or send data over the connection. Additional security attributes could be considered, e.g., if strict security is required, the use of an encryption mechanism (e.g. IPSEC) can be introduced.

5.2.4 Quality of Service

A QoS profile is an essential IP service attribute that contains all relevant QoS parameters, e.g., bandwidth, delay, jitter, packet loss. A QoS profile can be assigned to an interface, independently from IP service connections, and/or to an interface per IP service connection instance, as already mentioned for the MEF service model [1].

It is to be noted that QoS engineering and SLA enforcement of point-to-point service connections is easier than for p-t-mp or even mp-to-mp service connections. This is because, in the latter cases, the application flow distribution is not completely pre-determined by the service connection itself. This must be taken into account, when specifying the QoS profiles for multipoint service connections.

QoS on demand is another application requirement, which must be taken into account. The current service model through, e.g., an on-demand re-binding of an application flow to a different service connection providing the required QoS profile can support this requirement.

5.2.5 Service multiplexing

An end-user can have several applications running at the same time, e.g., background “file-sharing” via a peer-to-peer application, some best effort Internet and listening to his or hers favourite radio station via streaming music. This shows how a single interface can have multiplexed several different application flows. It is necessary to be able to distinguish between the different application flows and to map them to the appropriate IP service connection.

Service multiplexing can be based on:

- source IP address
- destination IP address
- DSCP/TOS bits
- port numbers and combinations.

An example for IP service multiplexing based on destination IP address is shown in Figure 16.

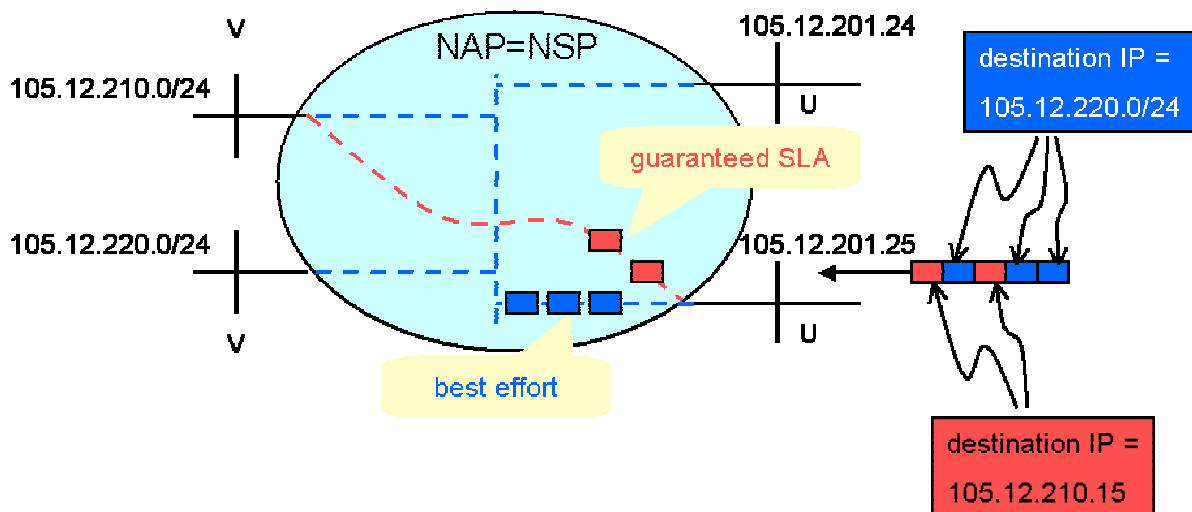


Figure 16: IP service multiplexing based on destination IP address

5.3 Mapping of Specific Applications

5.3.1 High Speed Internet

In order to support the High Speed Internet application, two different scenarios can be envisaged.

In the first scenario, initial setups of point-to-point IP service connections take place between end-users and a specific peering point to the Internet backbone. On the V interfaces, multiple point-to-point IP service connections, from different end-users are multiplexed. This approach will most likely be used for business users because it allows the assignment of guaranteed network resources to customers for accessing the Internet backbone.

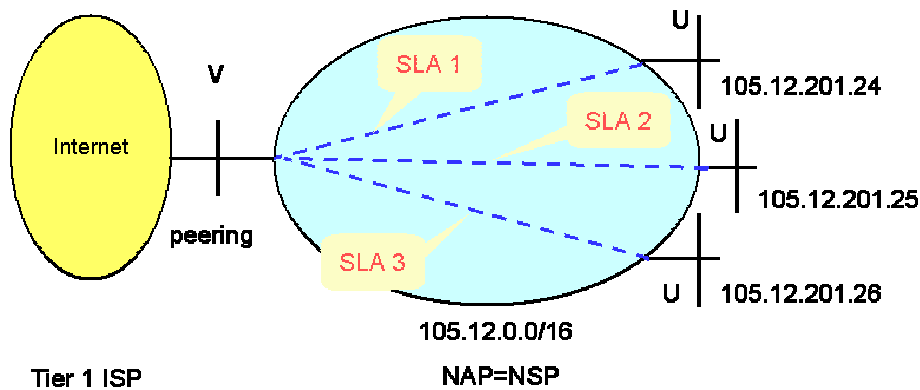


Figure 17: Internet Access with individual p-t-p IP service connections

In the second scenario, there is an initial setup of a mp-t-mp service connection (compare Figure 15). Since the traffic will be distinct towards the individual end-users, the reason for setting up a common service connection is related to a better scaling and a better usage of network resources due to multiplexing gains. On top of this, peer-to-peer applications for users with Premium High Speed Internet access can also be supported.

In order to distinguish High Speed Internet from the normal Best Effort internet, a separate multipoint-to-multipoint connection for Best Effort could be considered, whereas the High Speed Internet connections could be supported by either of the two methods described above, namely, either point-to-point or mp-t-mp, with an enhanced QoS profile. At multiplexed interfaces the IP service connection can be identified, e.g., by the destination IP address.

5.3.2 VoD

For the Video on Demand, a p-t-mp service connection between the ASP or content provider, which in this case is not the same as the NSP or NAP, and the end-users must also be considered. The QoS attributes on this p-t-mp connection will be strict, taking into account the nature of on-demand applications. There can be different parallel p-t-mp connections, with several participants, each with a different set of QoS parameters.

P-t-p application flows can be bound to this service connection(s). Multiple application flows are supported per CPN, e.g., multiple set top boxes per home. Also, as indicated for the Ethernet service model, if necessary, a resource and admission control mechanism could be needed in addition, in order to prevent an overload of the service connection in occasional high demand situations.

5.3.3 VoIP

In order to deploy this application, two different scenarios are considered, where, for each one, the location of the server node of the point-to-multipoint connection is not the same.

In the first scenario (see Figure 18), the ASP is considered to be a third party provider, independent from the NSP. In this case both the control and data plane will go transparently through the NSP network. This can be achieved by binding the VoIP application flows to a p-t-mp IP service connection. The ASP will process the control packets (e.g. SIP) and set up a VoIP call with the second end-user. All traffic will continue to flow through the ASP, for accounting, billing, security, etc. There is almost no interaction with the NSP, except maybe for setting QoS attributes in the network, if the static QoS attributes of the service connection are not sufficient. By configuring several parallel point-to-multipoint service connections, each with different QoS parameters, with the same participants, the interaction with the NSP is restricted to an absolute minimum. This case can also be applied if an ILEC is separated in distinct entities with one acting as a pure access provider, while another is a retailer service provider.

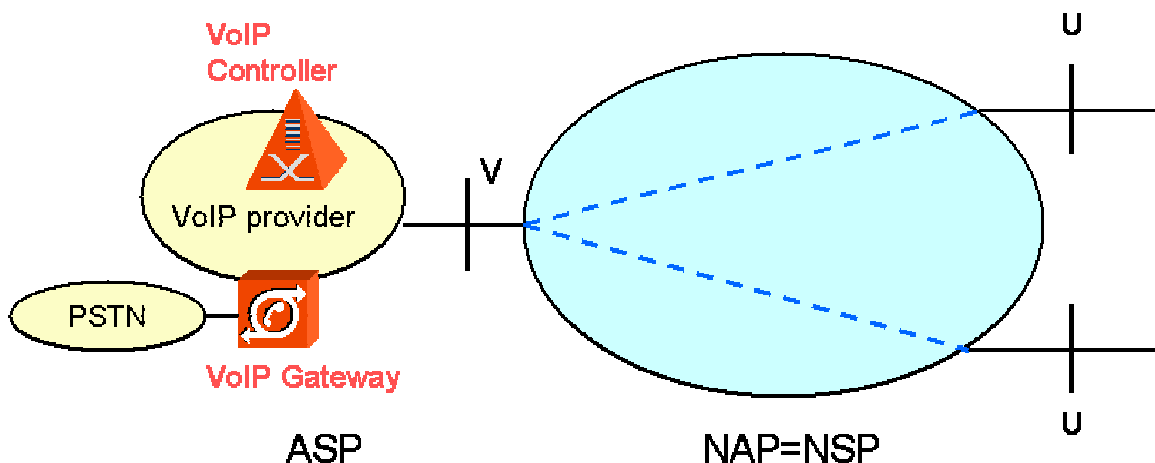


Figure 18: VoIP application using direct p-t-mp IP service connections

In the second scenario, the ASP is the same as the NSP or NAP. This makes it possible to optimize the routing of local calls by using a mp-t-mp IP service connection. It requires to include more functionalities, like accounting, or security, into the access network, closer to the end-user. This could for example be done in an IP DSLAM or a BRAS (or Edge Router) with SIP functionality.

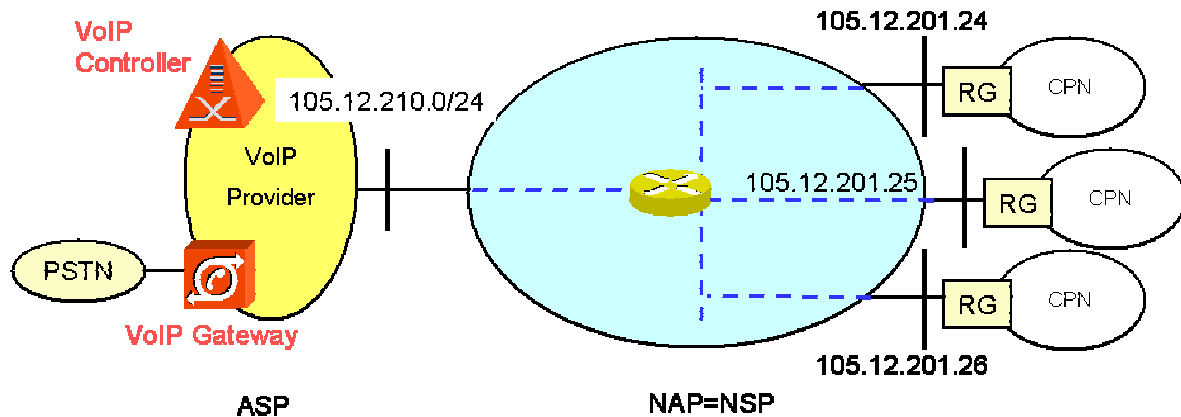


Figure 19 : VoIP using IP DSLAM with mp-t-mp service connection

5.3.4 Peer-to-peer applications

These applications are always between two or more U interfaces. To support peer-to-peer applications, two connections types are applicable. It is either possible to have a point-to-point connection between the two U interfaces or a multipoint-to-multipoint connection between the peers (more than two) that participate in the application. It is inherent to peer-to-peer applications that there is no V interface involved, since the whole application is end-user driven.

From a NSP/NAP point of view, there will have to be accounting functionality in the IP DSLAM, in order to be able to operate billing on the traffic generated by the peer-to-peer applications.

It is to be noted that, in the IP core, one instance of mp-t-mp IP service connections for peer-to-peer applications is today available, which is that related to the deployment of RFC 2547 [5] BGP/MPLS based VPNs. These VPNs support independent IP addressing for each service connection, i.e., VPN instance, and exchange routing information with the peers.

Of course for the broadband access more simple implementations of IP mp-t-mp service connections are more appropriate.

5.3.5 Broadcast or multicast television

It constitutes a standing fact that these type of applications are best mapped to a point-to-multipoint IP service connection, since the root interface will be the multicast source, providing the content to the other U interfaces or end-users. The biggest amount of traffic will be in the downstream direction, i.e., from the root interface towards end-users, whereas only some control traffic will go in the upstream direction.

For the purpose of controlling membership to multicast groups, specific service attributes must be added to a multicast capable IP service connection.

Again, multiple parallel point-to-multipoint service connections can be defined, each one dedicated to a specific channel or movie, or each one with a different set of QoS parameters.

6 INTERACTION BETWEEN ETHERNET AND IP SERVICES

6.1 Introduction

A network service makes use of services provided by the link layer. This can lead to an interworking scenario, where the IP service model can interact with the underlying Ethernet service model.

Since in some network scenarios, IP services and Ethernet services are offered by different network providers, a coordination of the service provisioning may be required.

This chapter investigates this interaction. Special care is given to services using multicast/broadcast, as the this IP service feature will rely on the multicast capability of Ethernet.

6.2 The impact of multicast

When discussing multicast, a clear definition should be given about the location where the copy of the multicast data is performed. The multicasting mechanism sends the same information only once and only to the intended end users. As such, the resulting bandwidth savings and scalability inherent in multicast provide a major benefit. The number of destination entities may be 0, all or any number in between, i.e., unicast (one entity) and broadcast (all reachable entities) are special cases of the multicast method. Data flows requiring multicast functions are unidirectional. Depending on applications, multicast flows are upstream or downstream, e.g., in the case of digital TV delivery, the flows coming from video head end are sent to end users connected to NAP, whereas for other applications, like teletraining, the flows could be provided from an end user server.

Having generically described the multicast mechanism, some specific characteristics are analysed in the following from the service model point of view, in order to identify issues to which a special attention must be paid.

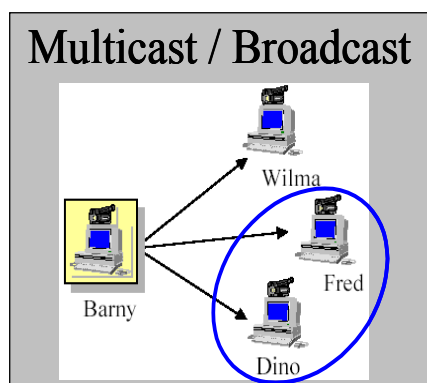


Figure 20: Multicast example

6.2.1 Multicast Ethernet MAC address and IP address mapping

In terms of defined addressing mapping, the IP addresses 224.0.0.0 through 239.255.255.255 (class D addresses) are reserved for multicast. Moreover, the IP multicast addressing extends down to the MAC addresses of "multicast aware" network interface devices, by using a reserved base Ethernet MAC address of 01:00:5E:00:00:00 and adding the last 23 bits of a multicast IP address that a group is listening to. With this address mapping, IP packets can be multicasted to a group of hosts over an Ethernet network.

However the default behaviour for an Ethernet switch is to forward all multicast traffic to every port that belongs to the destination LAN on the switch. IGMP snooping is one of the methods which efficiently allows to restrict IP multicast to a subset of Ethernet ports. Indeed, the IGMP function "snoops" layer 3 information in the IGMP packets sent between end users and the network node which terminates the IGMP flows. Also a table regularly updated by the switch enables to replicate flows already available at its level.

This is the reason why the multicast/broadcast functionality always affects both layer 2 and layer 3, i.e., the Ethernet as well as the IP layer. If the NAP is distinct from the NSP delivering the IP service, the NAP is nevertheless required to implement certain IP functionality, like IGMP snooping, in its network.

On the other hand, the provisioning model of multicast services considering an IPv4/IPv6 access network is based on multicast routing protocols like PIM-SM/D. However, it is also possible to keep the IGMP mechanism by using IGMP forwarding functionalities in the access network, allowing therefore to end IGMP messages further upstream in the network, even with an IP access node.

The NSP will be responsible for the authentication and authorization of the subscribers and also for the accounting process. In order to provide multicast services there will be a server (DHCP-type) connected to the NSP, managing and assigning dynamically the multicast addresses to be used in the multicast services. This will be done with a database containing several multicast address pools in the 224/8 range, for the multicast services. So every service, i.e., broadcast TV, PPV, and videoconference, has a different sub-range associated to it. The size of the address pools will be defined according to the characteristics of the service, i.e., so it will depend, for example, on the number of broadcast-TV channels or the number of simultaneous videoconference sessions allowed by the Service Provider.

6.2.2 Ethernet service model model applied to multicast

Figure 21 shows an example of how the concept of a p-t-mp Ethernet service connection can be used to support a multicast service with controlled membership to the multicast group. In this case, the membership to the multicast group is controlled by an on-demand binding of the multicast (sub-)flows to the service connection. This binding can be controlled via means like IGMP snooping or a specific Layer 2 control protocol (L2CP). Since these protocols are running at the IP layer an interworking between the Ethernet and the IP service layer will be needed. Any implementation MUST keep this interaction as small as possible.

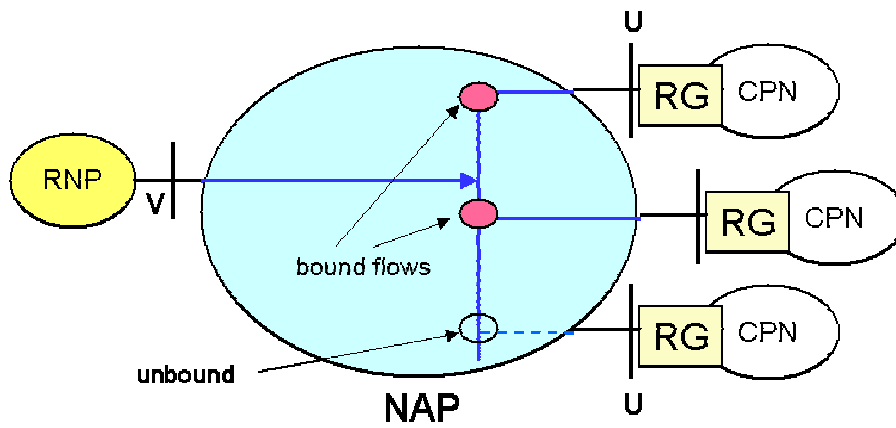


Figure 21: A p-t-mp Ethernet service connection used for multicast.

7 CIRCUIT EMULATION SERVICE

Circuit Emulation Service (CES) is currently used to enable various legacy PDH and SDH circuits to be transparently extended across ATM networks. Wherever Ethernet or IP networking evolves to replace ATM the same requirements for CES will be inherited. Work to specify circuit emulation requirements for Ethernet (CESoE) and IP (CESoP) networking is currently being actively progressed in groups such as the ITU, IETF, MEF and the MPLS Forum to support this.

In a heterogeneous network environment, some ATM circuit oriented services will in turn become legacy requirements for circuit emulation, which might be termed “virtual” CES, and will require inclusion in the scope of CES consideration. CES will be an essential mechanism for providing support of such ATM and TDM legacy services.

7.1 Reference Models

7.1.1 *CES Point to Point Reference Model*

The following reference models show the more complex CES requirements that can arise in a heterogeneous network. It is obvious that in a fully evolved pure packet network some of these options are not necessary. It is of note that ATM services could tunnel across the packet network either as native ATM in a Virtual Circuit emulation, as shown in the figure below, or packaged in a plesiochronous or synchronous structure in a TDM circuit emulation.

Point to Point CES Reference Model

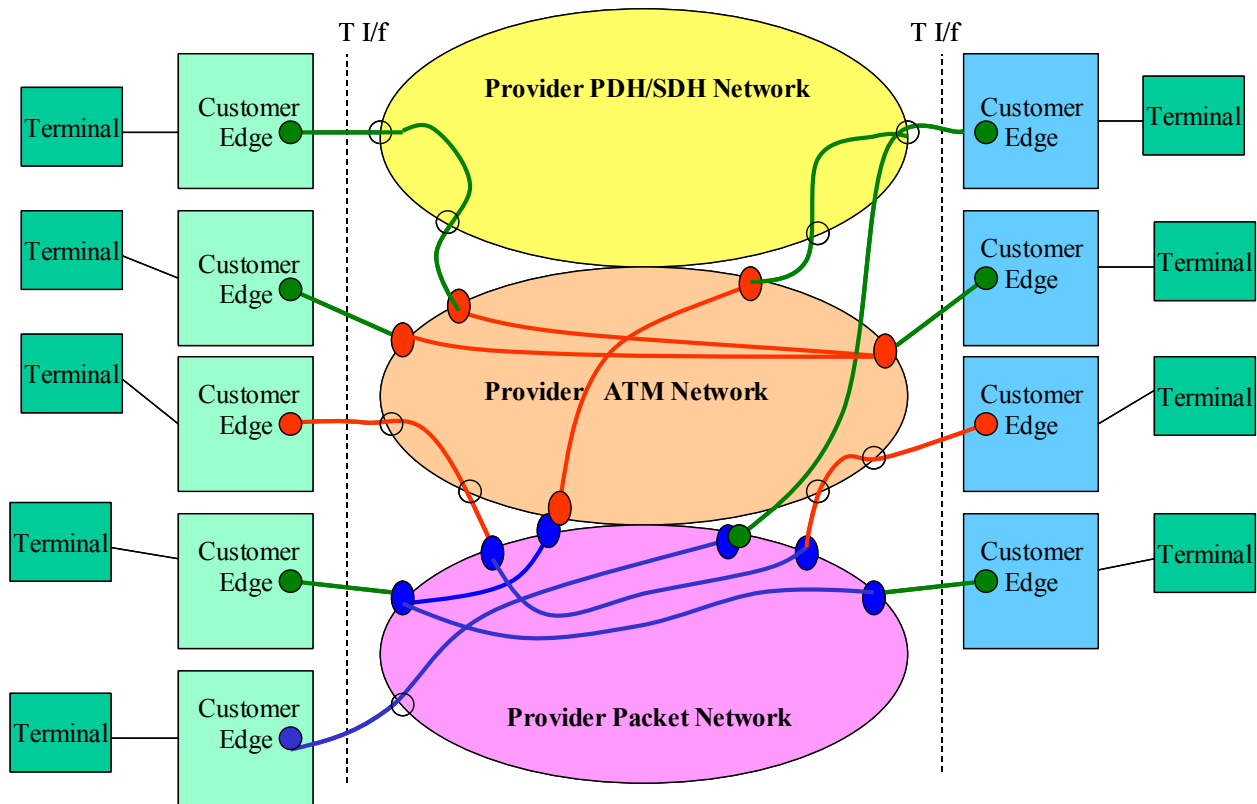


Figure 22: Point-to-point CES reference model

This shows Ethernet analogues for TDM over ATM CES requirements, and the possible need to tandem TDM - TDMoATM - TDMoPacket links. It also shows the possible tandeming of ATM links and ATMoPacket CES that could implement an end-to-end IPoPPPoATM service using a legacy DSLAM and BRAS.

7.1.2 CES Point to Multi-Point Reference Model

In the case of video broadcast streams for instance, there is a requirement to provide point to multipoint CES.

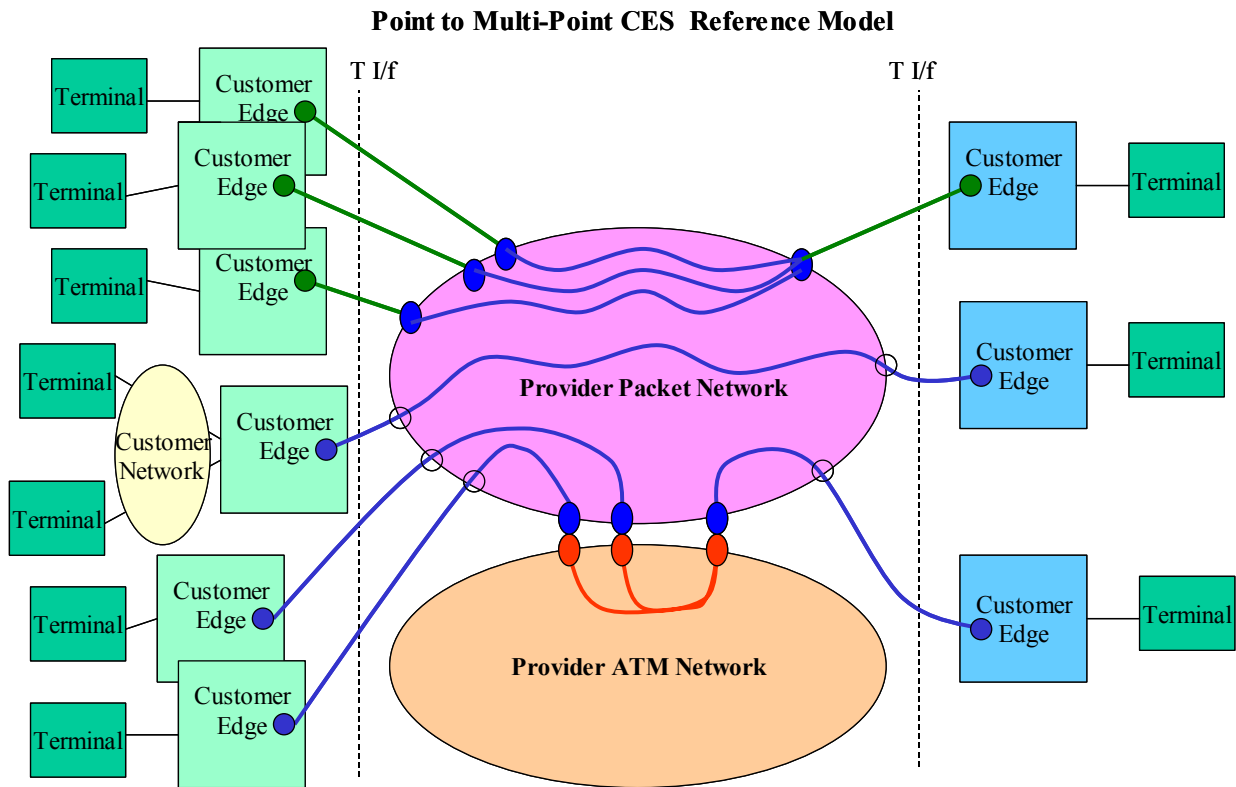


Figure 23: Point-to-multi-point CES reference model

Key to symbols

- Network Native circuit I/F
- Customer TDM, ATM or Packet Edge Function
- Provider ATM Network CES Edge Function
- Provider Packet Network CES Edge Function
- ATM Network circuit connection
- Packet Network circuit connection
- PDH/SDH Network circuit connection

A full consideration of the CES requirements should be understood in the context of functional models based on ITU recommendations G.805 and G.809. This should include consideration of the additional complexities associated with Ethernet and IPv6.

7.2 CES Reference Model Scope

The CES General Reference Model in Figure xx captures the requirement for CES to support the transport of TDM circuits across ATM and Ethernet/IP provider networks. Typically, CES is required to provide emulation of a specified TDM circuit type 'edge to edge' across a single type of provider network. However, the Reference Model also identifies the requirement for the case of end-to-end service requiring traversal of another provider network type.

CES originates and/or terminates at the Customer Edge, which is unaware whether it is using a circuit emulated rather than a native service. The customer edge is attached to the provider network using an Edge Function, which provides the appropriate service emulation mechanism to the customer edge to enable transport of the specified service across the provider network. The customer edge – provider network interconnection may be physical or virtual (eg an Ethernet port or an ATM VPI/VCI).

The CES Multi-point to Point Reference Model in Figure yy captures the requirements for CES support of Point to Multi-point operation. Two circuit emulation scenarios are shown. In one case the multiplexing function is provided within a single provider network, in the other case the multiplexing function is provided within a different provider network. The null CES case (where the multiplex function is performed externally) is also shown for completeness.

7.3 Operator CES requirements

Operator understanding of CES requirements is rapidly developing. It is essential that a small set of generic CES requirements is developed capable of supporting a wide variety of legacy services as well as those currently under development.

Packet network CES (as for ATM CES) requirements are derived from underlying SDH for QoS, GOS and OAM.

8 THE IMPACT OF IPV6 ON THE SERVICE MODELS

The service models outlined in chapter 4 and 5 for Ethernet and IPv4 are basically also fully applicable to IPv6. However, some important differences of IPv6 to IPv4 must be taken into account when specifying an IPv6 service model in detail. The main differences will be discussed in the following sub-chapters, where the protocol versions differences are resumed.

8.1 Ethernet Encapsulation

IPv6 is assigned the specific Ethertype 0x86DD while IPv4 has Ethertype 0x0800. Therefore IPv6 represents an independent network layer on top of an Ethernet link layer. As such IPv6 neither impacts the pure Ethernet service model nor the service model for IPv4. An Ethernet service connection must be able to convey IPv4 as well as IPv6 datagrams, and this even concurrently.

It is to be noted, however, that some Ethernet service implementations may allow to use service attributes to put restrictions on the Ethertype of the frames being conveyed.

Also specific attention must be given in the case that IP protocols requiring neighborhood detection are running over p-t-mp Ethernet service connections, e.g. as discussed below for stateless IPv6 autoconfiguration.

8.2 Address Structures

An important impact of IPv6 is seen with respect to IP addressing. Following address types are specified for IPv6:

- *Unicast addresses:*
 - *Internet Service Provider Unicast Address.* Designed specifically for use by Internet service providers (ISPs) to connect individual users to the Internet.
 - *Link Local Unicast addresses.* The Link-local address is for used on a single link, for purposes such as auto-address configuration, neighbour discovery, or when no routers are present.
 - *Site Local Unicast Address.* They may be used for sites or organizations that are not connected to the global Internet. They do not need to request or "steal" an address prefix from the global Internet address space. IPv6 Site-local addresses can be used instead.
 - *IPv6 Transitional Unicast Address Structures.* Two special IPv6 unicast addresses have been defined as transition mechanisms to allow hosts and routers to dynamically route IPv6 packets over an IPv4 network. infrastructure and vice versa, *IPv4-Compatible IPv6 Unicast Address* and *IPv4-Mapped IPv6 Unicast Address*.

- *Anycast addresses:*

The anycast address, introduced in IPv6, is a single value assigned to more than one interface. Typically, these interfaces belong to different devices. A packet sent to an anycast address is routed to only one device. It is sent to the "nearest" interface having that address, as defined by the routing protocols' measure of distance.

Anycast addresses are formed from the unicast address space and may take the form of any unicast address type. Anycast addresses are formed simply by assigning the same unicast address to more than one interface.

- **Multicast addresses:**
Multicasting was previously supported in IPv4, but required the use of obscure Class D addressing. IPv6 eliminates Class D addresses in favour of a new address format in the address range FF00::/8 that permits trillions of possible multicast group codes. Each group code identifies two or more packet recipients. The scope of a particular multicast address is flexible. Each address can be confined to a single system, restricted within a specific site, associated with a particular network link, or distributed globally. IPv6 multicast uses MLD (Multicast Listener Discovery) protocol instead of IGMP.
- **Broadcast addresses:** There is no explicit broadcast addressing in IPv6 because broadcast can easily be handled by the extended multicast capabilities of IPv6.

The structured 128 bit address space of IPv6 makes the implementation of independent IP service connections, which nevertheless use a coordinated ISP unicast addressing, much easier and much more useful than with IPv4. This simplifies implementation of IP service connections in a significant way, since a common routing table for different service connections can be used. The use of IPv6 ISP unicast addresses thus can avoid the complexity of learning private addresses and private routing tables within the access network as required for IPv4 VPNs.

It is to be noted however, that IPv6 also specifies private addresses called site local addresses, which may still require an IP VPN service model in analogy to that currently being implemented in the IPv4/MPLS core based on RFC 2547 [5].

8.3 Autoconfiguration

There are two types of autoconfiguration methods for IPv6 specified, that also can coexist:

- **Stateful** . The IPv6 equivalent of DHCP (DHCPv6). The DHCP server and the client must both maintain state information to keep addresses from conflicting, to handle leases, and to renew addresses over time.

- *Stateless*. A host gains an address via automatically "leasing" an interface address, without requiring a server to delve out address space. Stateless autoconfiguration allows a host to propose an address (based on the network prefix and its Ethernet MAC address). This address is checked by a neighbourhood detection protocol to be unique. Because no server has to approve the use of the address, or pass it out, stateless autoconfiguration is simpler. However, since still there is no mechanism (besides DHCP) to pass the DNS server address to the terminals, some degree of stateful configuration will often be needed.

The neighborhood detection of the stateless mode makes use of Layer 2 multicast capability. Therefore, each Ethernet service connection is seen as a separate link for the IPv6 network layer. It follows that special care must be taken for p-t-mp Ethernet service connections, since peer-to-peer traffic must be suppressed in this case while on the other hand the stateless auto-configuration of IPv6 addresses requires exchange of protocol datagrams between peers and must not be jeopardized.

8.4 Quality of Service

The *traffic class* and *flow label* fields in the IPv6 header can be used by the network for policing and scheduling purposes.

With respect to QoS, IPv6 does not provide any new mechanisms relatively to IPv4. Therefore the QoS techniques being specified for IPv4 such as *DiffServ* (RFC 2474 [6], RFC 2475 [7]) and the associated traffic engineering techniques are applicable also for IPv6.

The concept of a flow in IPv6 has no counterpart in IPv4. It could help in the access and aggregation network for an easier identification of packets belonging to the same application flow and may thus also substantially ease the task of application flow binding.

8.5 Terminal Mobility

Mainly due to the flexible and extended IPv6 addressing, terminal mobility is much easier to support in IPv6 than in IPv4. IPv6 allows a service provider to offer a mobility service to its customers in a much more flexible way. In fact there is no need of third parties to host a foreign agent for roaming IPv6 users on the destination network. This way, in principle any service provider wanting to offer an IPv6 mobility service only needs to have an IPv6 home agent at its premises and has to enable mobility for its customers' terminals.

However, a NAP will usually only grant access to his network to authenticated users. Therefore a visiting mobile IPv6 terminal on a foreign NAP requires means for authentication and authorization. This is especially true if broadband QoS services must be supported for the visiting terminal, since these can require substantial network resources.

8.6 Peer-to-peer Services

In terms of peer-to-peer services, since the IPv6 address space is large enough to allow each terminal to have its own unique address, this enables peer-to-peer services without the need for special service proxies elsewhere on the network. Any terminal may directly connect to any other terminal (according to established firewalls rules, what may prevent this kind of communications), enlarging the possibilities of new applications (especially multimedia) and certainly the amount and the pattern of the traffic on the network. This may have a big impact on the existing network service model, which is today, mostly asymmetric, and may tend to a more symmetric pattern in the future.

8.7 Security

IPv6 has an inbuilt mandatory security support, encompassing

- *IP Authentication Header* for integrity and authentication
- *IP Encapsulating Security Payload* for integrity and confidentiality.

It is foreseen that any IP service models in the broadband access needs service attributes addressing these security features. Moreover terminal mobility requires a security infrastructure which is interoperable between networks, as mentioned above. Therefore a common, standardized and interoperable security infrastructure, e.g. based on a public key infrastructure, is inevitable.