
White Paper
MUSE Business Model in BB Access

Identifier: White Paper Business Model
Class: Report
Version: 5
Version Date: 05/04/2007
Distribution: Public

EXECUTIVE SUMMARY

MUSE has developed a business model that allows to describe real life actors by a combination of different generic roles. The DSL Forum already defined the roles of a Network Access Provider, Regional Network Provider, Network Service Provider, and Application Provider. The MUSE model has a finer granularity than the one currently used by the DSL Forum in order to support further unbundling of the value chain, and has identified two new roles, the Packager and Connectivity Provider.

The present document gives the definition for each of these roles. It analyses the consequences for network configuration and scalability, as well as requirements for the definition of some new control and management interfaces. A detailed analysis is made of the technical responsibilities for the AAA architecture, IP address allocation, QoS framework and ACS.

TABLE OF CONTENTS

EXECUTIVE SUMMARY	2
TABLE OF CONTENTS	2
ABBREVIATIONS	3
REFERENCES	5
LIST OF CONTRIBUTORS	5
1 INTRODUCTION	6
2 BUSINESS ROLE MODEL	7
2.1 Definitions.....	7
2.2 Business Role Model.....	7
3 BUSINESS ROLES	8
3.1 Subscriber.....	8
3.2 Packager.....	9
3.3 Connectivity Provider (CP).....	10
3.4 Access and Regional Network Provider (NAP/RNP).....	13
3.5 Network and Application Service Provider (NSP/ASP).....	13
3.6 Multimedia Content Provider (MCP).....	14
4 RELATIONSHIPS AND INTERFACES	14
4.1 Relationships between roles.....	14
4.2 Interfaces between roles.....	14
4.3 Impact of multiple CP's per NAP.....	15
5 ARCHITECTURAL ANALYSIS OF RESPONSIBILITIES	15
5.1 Analysis of roles and responsibilities in AAA architecture.....	15
5.2 IP address allocation.....	17
5.3 Analysis of roles and responsibilities in QoS framework.....	17
5.4 Analysis of responsibilities to manage CPE (by means of ACS).....	19
6 SUMMARY RESPONSIBILITIES PER ROLE	21

ABBREVIATIONS

3GPP	3 rd Generation Partnership Project
AA	Authentication, Authorisation
AAA	Authentication, Authorisation, Accounting
ACS	Auto Configuration Server
AF	Application Function
AN	Access Node
ANP	Sometimes used for "Access Network Provider", however NAP "Network Access Provider" is the term consistently used in MUSE and DSL Forum.
ASP	Application Service Provider
BB	Broadband
BGF	Border Gateway Function
BNG	Broadband Network Gateway
BRAS	Broadband Remote Access Server
BW	BandWidth
CIR	Committed Information Rate
CP	Connectivity Provider
CPE	Customer Premise Equipment
CPN	Customer Premise Network
DHCP	Dynamic Host Configuration Protocol
DSL	Digital Subscriber Line
DSLIF	DSL Forum
EN	Edge Node
ETSI	European Telecommunications Standards Institute
GSB	Global System for Broadband communications
HGI	Home Gateway Initiative
HSI	High Speed Internet
IMS	IP Multimedia Subsystem
IP	Internet Protocol
ISP	Internet Service Provider
IST	Information Society Technologies
IWF	InterWorking Function
L2	Layer 2
L3	Layer 3
LAN	Local Area Network
MCP	Media Content Provider
MM	MultiMedia
NAP	Network Access Provider
NAPT	Network Address Port Translation
NASS	Network Attachment SubSystem
NAT	Network Address Translation
NGN	Next Generation Networks
NSP	Network Service Provider
OAM	Operations, Administration and Maintenance
OSS	Operations Support System
PC	Personal Computer
PDF	Policy Decision Function
PDG	Packet Data Gateway
PDP	Policy Decision Point
PE	Provider Edge
PIR	Peak Information Rate

QoS	Quality of Service
RACF	Resource and Admission Control Function
RACS	Resource and Admission Control Subsystem
RADIUS	Remote Authentication Dial-In User Service
RCEF	Resource Control Enforcement Function
RFC	Request For Comments
RGW	Residential Gateway
RNP	Regional Network Provider
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SP	Service Provider
SPDF	Service Policy Decision Function
SPM	Service Policy Management
STB	Set Top Box
TCP	Transport Control Protocol
TISPAN	Telecommunications and Internet converged Services and Protocols for Advanced Networks
TR	Technical Report
TS	Technical Specification
UDP	User Datagram Protocol
UE	User Equipment
VLAN	Virtual LAN
WT	Working Text

REFERENCES

- [1] MUSE deliverable DA2.4 “Network Architecture and Functional Specification for the Multi-Provider Access and Edge”, December 2005
- [2] MUSE deliverable DTF1.6 “Access network architecture III”, November 2006
- [3] DSL-Forum contribution dsl2005.556, “Role extensions to the TR-058 business model”, September 2005
- [4] ETSI ES 282 003 V1.6.8 Telecommunications and Internet converged Services and Protocols for Advanced Networks (TISPAN); “Resource and Admission Control Subsystem (RACS) Functional Architecture”

LIST OF CONTRIBUTORS

Peter Vetter (editor)	Alcatel-Lucent
François Fredricx	Alcatel-Lucent
Benoît De Vos	Alcatel-Lucent
Karsten Oberle	Alcatel-Lucent
Hans Mickelsson	Ericsson
Panagiotis Saltsidis	Ericsson
Govinda Rajan	Alcatel-Lucent
Harold Balemans	Alcatel-Lucent
Friedrich Armbruster	Siemens
Johannes Bergmann	Siemens
Alex De Smedt	Thomson
Dave Thorne	British Telecommunications
Peter Adams	British Telecommunications
Thomas Monath	T-Systems
Mario Kindt	T-Systems
Michel Borgne	France Telecom R&D
Christophe Alter	France Telecom R&D
Luc Le Beller	France Telecom R&D
António Gamelas	Portugal Telecom Inovação
Pieter Nooren	Netherlands Organisation for Applied Scientific Research (TNO)
Arnoud van Neerbos	TNO
Antonio J. Elizondo	Telefónica I+D
Enrique Areizaga	Robotiker

1 INTRODUCTION

One of the main goals of the MUSE project is to develop an access network architecture that is open to multiple services **and** multiple service providers. MUSE elaborated a business model in order to define requirements for a multi-service architecture that is open for multiple providers and flexible for different possible scenarios. The main objective of the present white paper is to give a complete survey of the work performed by MUSE on business models, which was reported in different deliverables [1][2] and contributions to standardisation (e.g.[3]).

In the DSL Forum TR-058 architecture, requirements have been formulated for a multi-service architecture and framework. Among the roles that have been defined are the Network Service Provider (NSP) and the Application Service Provider (ASP). The NSP is responsible for providing IP addresses for Internet access, or access to a corporate network and is also responsible for overall service assurance. An ASP/NSP may use wholesale services (AAA, connectivity, multicast etc.) from the Regional /Access Network Provider and have minimal operational dependencies on the Regional/Access Network Provider from whom they obtain services.

MUSE extends the model by adding 2 new roles: the Connectivity Provider and the Packager¹. The Packager takes responsibility for overall service delivery and assurance, and is the main point of contact for the Subscriber; the NSP role is then limited to providing access to the Internet or a corporate network. The Connectivity Provider acts as a kind of bandwidth broker that hides the technology from the Packager. Figure 1 shows various possible organized markets: vertically integrated, a horizontal separation of roles into separate roles and an unbundled value chain.

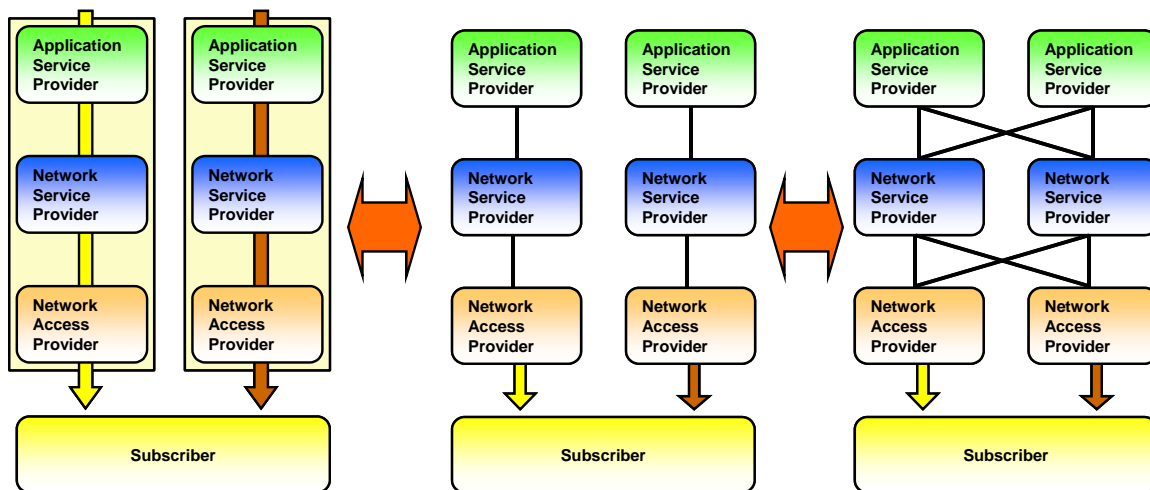


Figure 1: Possible organisation and evolutions of businesses: vertically integrated, horizontal separation, an unbundled value chain.

¹ In order to keep a clear distinction between roles and actors, the role names throughout the document are indicated with a capital. An actor is a business entity that takes on one or more roles.

2 BUSINESS ROLE MODEL

The roles have been defined as functionalities and/or responsibilities. The idea behind using a role model is that the responsibilities only need to be defined once, while the mapping to real business entities can be done differently for different business scenarios.

2.1 Definitions

"Role": A role is defined by a logical grouping of responsibilities. The idea is to provide a generic framework of atomic entities with appropriate granularity that allows for mapping the roles on different possible real-life actors. A single "role" can be a real life actor or multiple roles can be combined in one business actor. A role may have "business responsibilities" and/or "technical responsibilities".

"Business Actor" (also **"Player"**): A legal entity in real life that combines one or more roles, each of which must be instantiated as either a "business role" or a "technical role". A Business Actor must incorporate at least one business role (*this is required for the player to survive*). The combination of roles may vary in different countries or change in time (e.g. by acquisitions, divestments, or establishment of new roles).

"Technical Role" is a role that has only technical responsibilities. It only provides services to (an)other role(s) within the same player.

"Business Role" is a role that must have one or more specific business responsibilities and will in several cases also have technical responsibilities. That is the case when a role provides services to (an)other player(s) outside his organisation and hence also has a business relationship.

"Business responsibility": fulfilment of a service towards another player in accordance with a contract.

"Technical responsibility": technical tasks or functions to provide a service to another role; includes in general the responsibility for equipment.

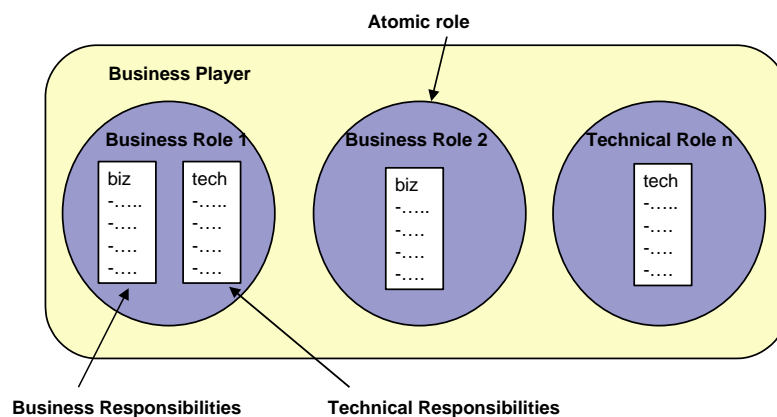


Figure 2: Definition of player, role, and responsibilities

2.2 Business Role Model

Figure 1 shows a generic business models with the different roles, which are described on the following sections. It also shows a generic representation of the relations between them. For instance, each of the n possible NAP can have up to m possible relations with m CP.

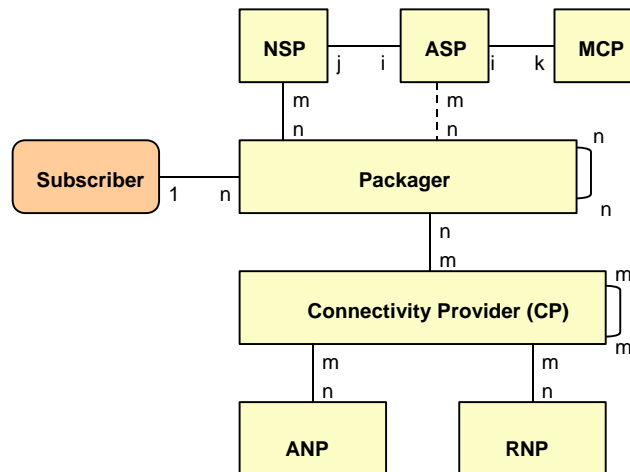


Figure 3: Business model and generic representation of the possible relationships

Remarks:

1. The model does not exclude further refinements. One example of a possible refinement is to make a distinction between an Access Network Provider and a Loop Provider, the latter just being responsible for the passive infrastructure of the network.

2. Depending on the real-life scenario (that is when we consider business actors), a role can be a business role or only a technical role. Consider e.g. the situation where a Connectivity Provider (CP) role is combined with an Application Service Provider (ASP) in one player (cf. definitions below). In case the Connectivity Provider provides the connectivity only for his own organisation, the Connectivity Provider is a technical role. If the Connectivity Provider also provides connectivity for another(s) player(s) (e.g. Application Service Provider), and hence has a business relation with this actor, the Connectivity Provider is also a business role.

MUSE mainly focuses on the technical responsibilities of a role.

3 BUSINESS ROLES

3.1 Subscriber

A **subscriber** is the business entity that subscribes for a service package. The subscriber signs a contract with a packager (or possibly several packagers) and pays for the access line, connectivity, and services. A subscriber is often also a **user**, but a user is not always a subscriber. A user is a pure technical role and uses the services, but is not always signing the contract or paying. There can be multiple users per subscriber line, e.g. a parent is the subscriber of a residential service package and the family members are the users, the owner of a company is the subscriber of a business service package and the employees are the users. There can be multiple subscribers per premises, e.g. a parent pays the contract for a basic service package and another family member subscribes to a specific service with a separate bill.

3.2 Packager

The Packager holds a trusted position with both network and service providers (note that a Service Provider can be an ASP or an NSP), as well as with the Subscriber, by means of SLA's. The Packager role avoids the Subscriber having to separately arrange agreements for each application service. The Packager links the services and applications with the required network service. The Packager is involved in AAA to the degree that it keeps (for its own use) the necessary credentials and profiles of the Subscriber.

The Packager is technology agnostic. All the technology related aspects of the contract with the Subscriber are placed as requirements to the technology specific Connectivity Provider or geographical NAP. As such, the Packager hides all the technology from the end user. "Technology agnostic means in this context that he does not deploy its own network technology. The Packager however provides the RGW, or advises the Subscriber which RGW is supported by the various network operators and Service Providers. (A possible consequence is that the RGW may have limitations to obtain services from providers that do not have agreements with the Packager). The packager may also give guidelines during configuration and installation or provide helpdesk services.

The Packager may also interface with other Packagers and Connectivity Providers in order to provide roaming for "nomadic" services. A subscriber can be connected to several Service Providers simultaneously as is already possible today. Due to the fact that different types of Service Provider (e.g. a VoIP Provider and a TV Provider) could have a relationship with different Packagers, it is desirable that the subscriber can choose from more than one Packager, but whether or not multiple Packagers per end-user can simultaneously be supported is still being studied.

Note that the subscriber himself may act as the Packager for some services and having direct contacts to ASP (when taking the responsibility for self-configuration), but there would be no overall QoS co-ordination function as a result.

A Packager's responsibilities are:

- Keeping subscriber profiles that describe how the network should handle the various sessions from different NSPs/ASP. If for example a subscriber uses several bandwidth consuming services simultaneously, these services may have an impact on each other, depending on the kind of QoS that is offered by the network. The subscriber's profile describes the desired policy in the event of a conflict. This kind of inter-service functionality can only be offered by a role that takes a central position with respect to Service and Network Providers.
- Receiving accounting information collected by the Connectivity Provider and sending bills to Subscribers.
- Supporting "nomadic" and "peer-to-peer" services by maintaining relations with several Connectivity Providers and maybe also business relationships with other Packagers.
- Providing a first line helpdesk to redirect Subscriber enquiries to the appropriate entity in charge of the maintenance wherever the problem occurred in the technical chain (CP, NSP, ASP).

A Packager may combine services from multiple NSP/ASPs to offer the Subscriber a complete service bundle. From a business point of view, it is beneficial to the Packager to enrich his offer with services from multiple Providers, and for Service Providers to have access to the subscribers of the Packager.

3.3 Connectivity Provider (CP)

The Connectivity Provider (CP) is responsible for implementing the network connectivity and resource between the Subscriber and the Service Providers as requested by the Packager. As such it must be able to check the resources used inside the network and take the appropriate measures (by imposing the corresponding requirements on the NAP²) to provide the corresponding technology-specific service bindings. While the Packager role is technology agnostic (hiding all technology related aspects from the subscriber), the CP role is technology specific. Further, the Connectivity Provider will assemble billing information from network services and provide this to the Packager. The CP also takes responsibility for providing the necessary means for AAA and legal intercept.

A Connectivity Provider may deal with multiple administrative network domains, e.g. combine one or more types of access network with a regional network in order to become more attractive to a Packager by offering true end to end connectivity. Multiple Connectivity Providers per administrative access network domain may be possible when appropriate separation is kept between those networks. In the case of Multiple CPs per administrative access network domain, each CP may want to manage the ACS. For practical reasons it would be reasonable to have a single physical ACS provided by the geographical NAP which is then divided into several virtual ACSs. Hence, fewer interconnection interfaces at the Edge Nodes will be required compared to an approach with separate physical ACS (one per CP).

The role of the Connectivity Provider needs rather more detailed examination and explanation, not just because it is new, but because there is also some apparent overlap with the role of the NAP; in some cases the NAP and the Connectivity Provider roles would be fulfilled by the same business entity.

A Connectivity Provider's responsibilities are:

- Providing end-to-end connectivity between the Subscriber and Application Service Provider, guaranteeing and monitoring the agreed end-to-end QoS and security characteristics. This includes (but is not limited to) the connectivity provided by the NAP and RNP,
- Adding value to the NAP access products in some way - e.g. by adding QoS, as discussed below,
- Management of the Auto-Configuration Server (ACS), while the Packager keeps the credentials and profiles of Subscriber,
- End user assignment (Authentication, Authorisation, and Accounting),
- Collecting accounting information from the network for the Packager,
- Remote management of the RGW at L2 (also L3 in case of retail service provisioning).
- Assignment of private IP address to retail users. Note that the assignment of public IP addresses is the responsibility of the NSP (which can be part of the same business player as the CP). The assignment of private IP addresses by the CP does not imply the provision of a "network service", but L3 connectivity in the realm of the CP to an NSP (then using NAT towards the Internet) or ASP (e.g. a local video server).

² Note that by defining CP as a separate role, the traditional NAP role as defined in DSLF TR-058 is now reduced to the entity that owns and manages the devices in the Access network but is no longer responsible for the end to end network connectivity.

Since the idea behind the CP is to add value in some way to the provision of basic access, it is appropriate to consider the various ways in which this can be done. Note that these are in addition to the basic CP role of combining Access and Regional Network connectivity. Value could be added in the following ways:

- **Scenario 1**
Buying Access across various geographies that had different NAPs, and then selling this on to a Packager, thereby reducing the number of business relationships the Packager has to maintain.
- **Scenario 2**
There is an increasing move towards running DSL lines at their maximum possible rate, and then imposing a lower service rate by other means. This provides an opportunity for a NAP to segment capacity on a given Access line which could then be sold to more than one CP. There would need to be hard L2 segmentation of some sort to allow this. Such an approach may also be relevant to higher bit-rate Access systems such as VDSL or fibre.
- **Scenario 3**
Buying a L2 Access product, but then adding some L2/L3 capability, e.g. PPP termination or IP address allocation.
- **Scenario 4**
Buying network products with a defined QoS value, which either individually or in combination allow the creation of a differentiated service. This might be done in addition to the provision of higher layer functionality.
- **Scenario 5**
Buying bulk interconnect at some point and then adding QoS by the introduction of a new network element, e.g. a box co-located with the BRAS for downstream QoS, or at each Access Node to allow upstream control. This could either be a traditional interconnection arrangement, where the backhaul then became the responsibility of the CP, or the traffic could be reinserted into a backhaul product bought from the NAP; this can be thought of as "interception" rather than interconnection.

The network impact of these possible approaches will now be considered. However before doing this it is necessary to consider the number of CPs there might be in any given Access network.

One possible view of the CP role is that there should be one and only one CP per NAP. This would obviously allow for the case where the CP was indeed the NAP, but also permit these roles to be separated. However the whole point of the CP is to add value. If there is a viable business model for a CP, then in many regulatory regimes it would be necessary to make this opportunity available to any CP; restricting this to one CP would not be allowed, unless it were technically impossible to have more than one.

Therefore the network impact of having multiple CPs in the various scenarios outlined above will now be assessed, along with its likely commercial benefit.

- **Scenario 1**
This is a pure business arrangement, it has no network impact. The benefit of this scenario is simply to reduce the number of business relationships a Packager has to maintain, but this would need to be balanced against the cost of segmenting the value chain.

- **Scenario 2**

This scenario is only relevant when there are indeed multiple CPs per NAP. To support it, both the Access Node and RGW need to be able to do hard L2 segmentation. Given that most DSL is currently ATM based, the obvious way to do this would be to have a separate VC for each CP. Note that these could then be mapped into separate VLANs in the case of Ethernet backhaul. There are some limits on the number of VCs that DSLAMs and RGWs can handle, but this is unlikely to be a practical constraint due to the fairly limited upstream bandwidth of the link, i.e. it does not make sense to divide this capacity up between a large number of CPs. For Ethernet-based access, the separation could be done by means of multiple VLANs across the Access link itself. Prior to this, the only network impact is the need to (continue to) support multiple VCs on the Access link, and specifying how they are mapped into VLANs.

There could however be more of an impact on the RGW, where there would be a need to map services to the appropriate VC/VLAN, and possibly also the need for segmentation of the RGW with regard to management and (QoS) configuration.

The value of this potential scenario would depend on the balance between the additional revenue potential versus the configuration complexity, and whether the hard separation between CPs could be achieved.

- **Scenario 3**

This is already an existing, deployed model. The only network impact might be a VLAN scaling issue. Apart from this, there is no problem with having multiple CPs in this scenario.

- **Scenario 4**

This is also an existing model. The network issues are the possible congestion with the consequent need to provide hard QoS over an Ethernet backhaul, and again the possible impact on VLAN scaling if multiple CPs were supported.

- **Scenario 5**

The network impact would be the need to be able to provide both physical and logical interconnection to a number of CPs; this could involve multiple network side interfaces on the Access Node, or the introduction of an Ethernet switch. This could have a significant impact on the VLAN architecture and scalability, and downstream QoS control.

An alternative approach to avoid this problem would be for each CP to be able to make QoS requests to the NAP, who brokered them and allocated Access Node resources accordingly. Note that the difference between this and Scenario 4 is that this is more dynamic. Scenario 4 involves buying network products, and so the AN can be configured by normal network management processes. In this scenario (which is actually something of a hybrid between 4 and 5) a rather more real-time resource allocation is required. There may be the need for a real-time interface between a number of CPs and the NAP to communicate these BW and QoS requests.

Therefore there are no overwhelming technical reasons why multiple CPs per NAP cannot be supported in any of the above scenarios, and there will be business and regulatory pressure to allow this multiplicity. A number of possible network impacts have been identified, which include scalability, interconnection points, forwarding behaviour, and the possible need for a new control interface.

3.4 Access and Regional Network Provider (NAP/RNP)

The NAP/RNP provides the physical network infrastructure. Several NAPs could exist in the same geographical area with each a separate L1 network infrastructure, e.g. as in a Local Loop Unbundling scenario, and then interconnect into one or more RNPs.

NAP and RNP responsibilities are:

- Transport and resource management between the RGW and the Edge Node with the QoS requested by the CP(s),
- Remote failure analysis of the RGW e.g. by means of loop-back measurements at L1,
- The RNP aggregates traffic from different Edge Nodes and delivers this to the appropriate service (or other) Edge Nodes,
- Implementation of service enabling functions like multicast, and QoS mechanisms including the setting of QoS related parameters (max. jitter, max. delay,...) in the access and edge nodes, and the monitoring and management of these parameters in the nodes against the overall QoS required by the CP,
- Implementation of auto-configuration (DHCP relays and/or servers) with mechanisms for the coexistence with PPP (e.g. PPP relays, L2TP),

3.5 Network and Application Service Provider (NSP/ASP)

NSP

The NSP role involves connecting Subscribers to the Internet backbone or a corporate network and has the responsibility for the assignment of (public) IP address. Some of the NSP tasks have been moved to the Packager role compared to the NSP role described in DSL Forum TR-058. NSPs and ASPs have a similar kind of relationship with the Packager and the Connectivity Provider.

ASP

The ASP offers application services, without providing basic network connectivity (e.g. the ASP will not be responsible for the assignment of IP-addresses). The ASP role mainly involves application service provisioning. The ASP manages services on top of the transport layer. ASPs may however also deploy their own network, apart from the NSP, to be able to provide the services with the required QoS. To enable services, the Application Service Provider may distribute software that has to be installed on the RGW.

An ASP has a business relationship with the Packager and a technical relationship with the CP. However, it could also offer its service directly to the end-user via the Internet without a relationship with either the Packager or the Connectivity Provider, and thus without any QoS guarantees.

ASPs may deliver their applications on top of an applications service platform (e.g. an OSGi service platform) running on the RGW, which could be delivered and managed by one "main" ASP.

Note: an ISP is a business player that combines the role of an NSP that provides public IP addresses with a specific ASP that provides basic Internet services (e.g. Web access, e-mail).

3.6 Multimedia Content Provider (MCP)

Multimedia Content Providers make content, e.g. movies or music, available to Application Service Providers. The ASP produces an end-user service with this content by means of a middleware platform which enables the Subscriber to listen to/watch the content from his end-user-device. A Multimedia Content Provider may have very stringent conditions regarding the security of his content before an Application Service Provider may use it (e.g. Digital Rights Management (DRM) may be required).

4 RELATIONSHIPS AND INTERFACES

4.1 Relationships between roles

The Figure 4 below shows how the various roles are related to each other. The lines between the roles represent the contractual relations. These relationships are of a business nature and do not reflect the underlying physical network architecture. As the figure clearly shows, the Packager(s) has a central position in this model. There can be one or more Packagers per access network.

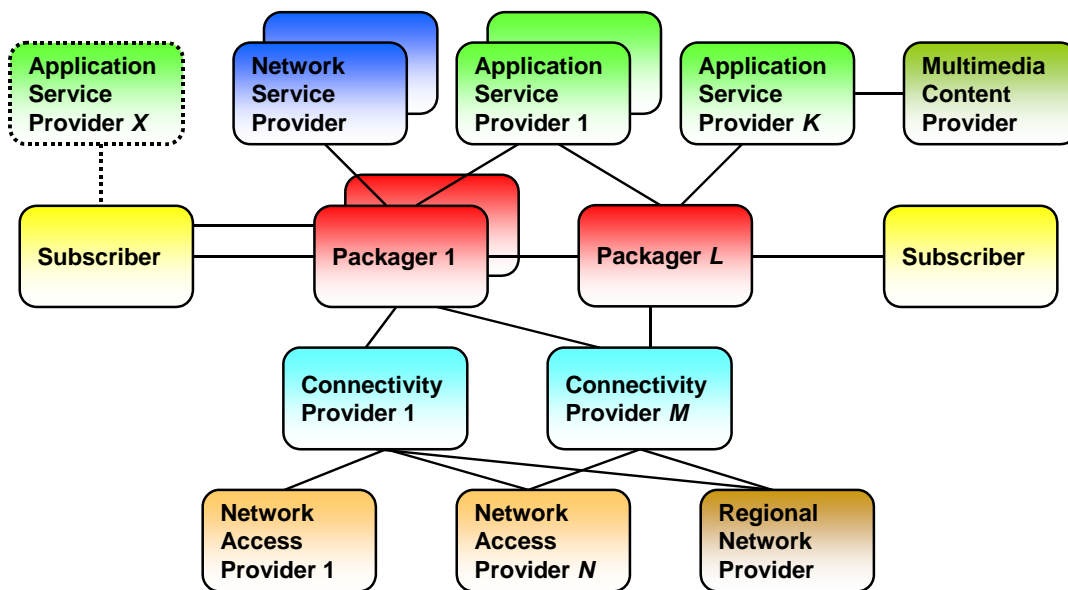


Figure 4: Proposed Muse role model indicating the basic relationships between the roles.

ASPs directly connected to the Internet, might also maintain a direct relationship with the Subscriber which is shown in the figure by a direct (dotted) line between the Subscriber and an ASP. For these ASPs, QoS cannot be guaranteed, since they do not have SLAs with a Packager who deals with the Connectivity Provider(s).

4.2 Interfaces between roles

The split between the Packager role and the NSP role and the introduction of the CP role makes the definition of extra interfaces necessary. These are:

Packager-NSP interface

- exchange of subscriber credentials for AAA purposes;

- exchange of information regarding nomadic services and QoS service profiles.

Packager-CP interface

- exchange of information regarding the different network locations between which connectivity is to be provided;
- exchange of information regarding levels of QoS to be provided in the NAP/RNP network;
- exchange of subscriber credentials for End-user assignment (AAA);
- exchange of subscriber accounting informations.

CP-NAP interface

- the CP needs to request network resources from the NAP.

4.3 Impact of multiple CP's per NAP

The major impact of having multiple CPs/NAP is the need for a resource reservation interface between the CP and NAP. The nature of these resource requests could be both flow and aggregate flow based (BW, QoS (PIR, CIR, etc)). They could either be subscription or session based. This is an important decision, as it dictates whether a non real-time (i.e. management plane) or real-time (control plane) mechanism is required.

Multiple CP's may want to manage the ACS. For practical reasons it would be reasonable to have a single physical ACS provided by the traditional NAP which is then divided into several virtual ACS.

5 ARCHITECTURAL ANALYSIS OF RESPONSIBILITIES

5.1 Analysis of roles and responsibilities in AAA architecture

The present section summarises the technical responsibilities of the different roles to support AAA. The details of the AAA architecture are explained in [1]. Here we consider the case without nomadism support. The study for nomadism is done in MUSE in the frame of activities on Fixed Mobile Convergence (FMC).

Figure 5 shows the AAA functions per role for the case of L2 pipes in the aggregation network (VLAN or PPP). The cases of L2 and L3 forwarding are very similar, whereby the AAA proxy function is accessed directly from the Access Node. Note that the AAA proxy function can be implemented as a stand-alone box or integrated in an Access Node or Edge Node.

Important requirements were the support of multiple CPs per NAP, as required by regulation, and multiple CPs per user, depending on the service he/she requests. The NAP therefore hosts an AAA proxy function to select the right CP. If the NAP is not a CP, then it only has the AAA proxy function, which selects the correct CP. If the NAP is also a CP, then the NAP has the AAA server and DHCP server associated with the CP role. There can still be multiple other external CPs for the NAP, where the AAA request can be sent.

Now, how can the NAP AAA proxy make the selection of CP? The Packager has this information, but only has a business relationship with the CP. Different solutions are possible. One solution is that the user device includes two identifiers in the credentials (credentials = username / password / domain) s/he sends to the network; one to identify the CP, and one to identify the (type of) service that is being requested. An alternative solutions is that one identifier (e.g. the Packager) identifies both the CP and Network Service Provider that is being requested. In both solutions, this is set by the Packager at service subscription time, and modified every time the user takes/leaves a service subscription from the Packager's offering. This interaction Subscriber-Packager happens transparently for the NAP, CP, SP and could be based on helpdesk/mail/web server/SIM card/other.

The next step is to forward the AAA request to the correct service provider. This is done by the CP based on the credentials; depending on the (type of) service it sends the AAA request either to its own AAA server (this is a service that will be offered by an ASP and for which the CP is responsible for AAA and IP address allocation), or to one of the NSPs, or to one of the ISPs.

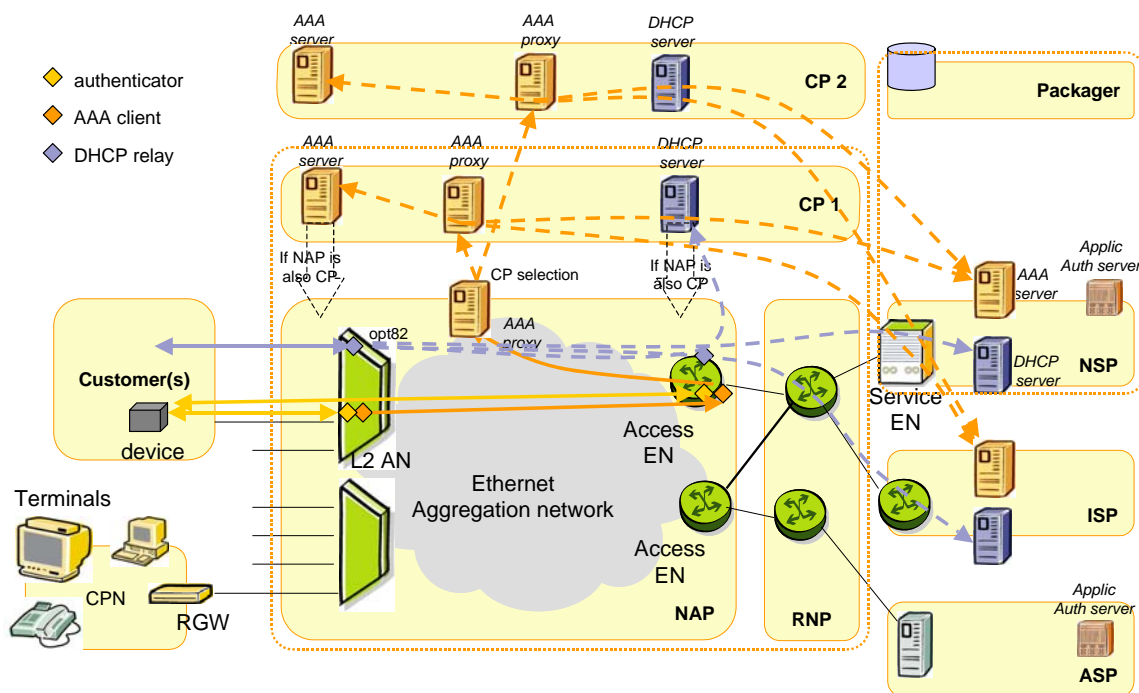


Figure 5: AAA functions and IP@ allocation functions per role

Although single sign-on is preferred by the end-user, there are several issues related with this, e.g. multiple CPs, lifetime of a service subscription, or failure of a specific authentication. The working assumption is that there is an authentication request per service request, which can be in push mode (CP replicates the authentication request to all SPs related to the user) or in pull mode (user requests service from a SP and then the SP contacts the CP to seek authentication).

On top of the described network-based AAA mechanism and transparently to it, there is application level authentication. This can be implemented either by means of web portal (manual log-in), or embedded in a device (e.g. SIP exchange).

5.2 IP address allocation

When different roles are involved in the business model, it is also important to reach the correct DHCP server. This can be based on the result of the authentication phase.

During authentication/authorization, the AAA server reply also includes the DHCP server of the corresponding SP (either by its name or by its IP address). The DHCP relays in the Access Node and Edge Node, snoops this reply from the AAA server and hence can forward the DHCP Discover message sent by the user device to the correct DHCP Server.

5.3 Analysis of roles and responsibilities in QoS framework

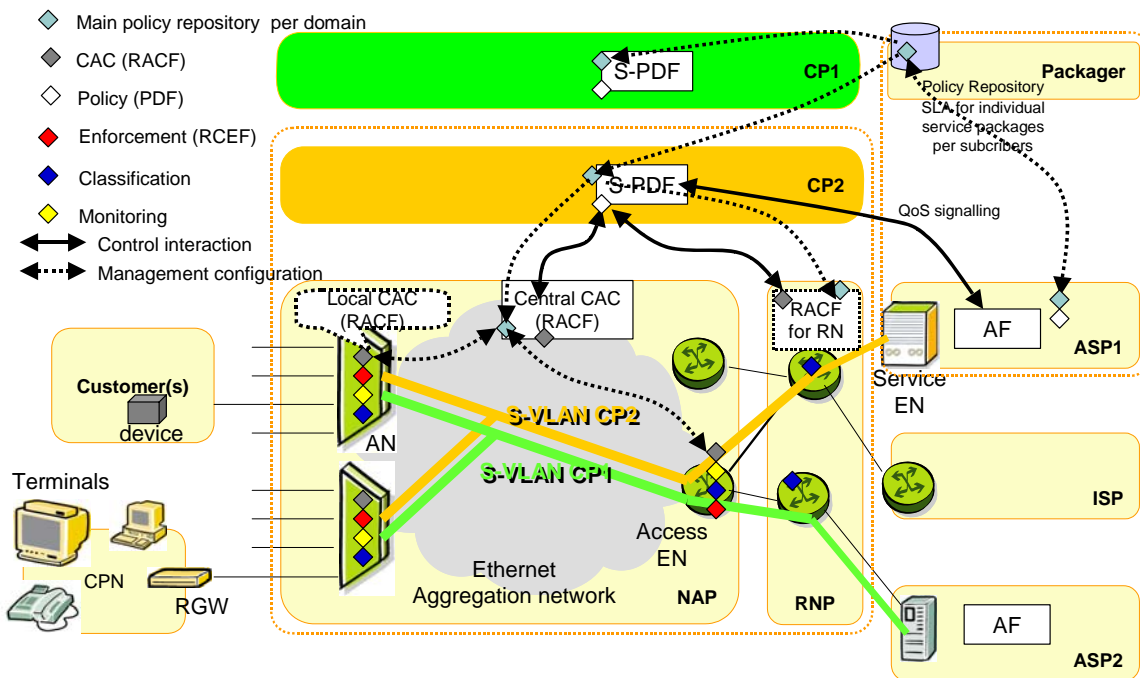


Figure 6: Technical responsibilities in QoS architecture

Figure 6 shows the responsibilities in the QoS architecture. The following responsibilities need to be allocated in the **management plane**:

There is a main **Policy Repository** for each administrative network domain (business role) which serves as a centralized database for the policy instances in their domain. (For more info on the MUSE QoS and Policy architecture, cf. [2].

The following main policy responsibilities can be distinguished per role:

- Packager: SLA for individual service packages per subscriber and for aggregate traffic per CP.
- ASP/NSP: Holds policy (or possibly even full SLA) per subscriber for a specific service.
- CP: Translates service policies into network policies per user for access network and regional network. The CP receives the connectivity related policies per subscriber from the packager, per line info from the NAP, and holds SLA between NSP/ASP and CP.

- NAP: Holds an SLA for the aggregate traffic for each CP that uses its infrastructure. The NAP will also hand specific management information on the individual subscriber lines to the CP, so that the CP can take them into account for policy decisions and control.

Each policy repository (except for the one with the packager) is associated with a **PDF (Policy Decision Function)** that consults the policy repository for the related policy decision when a session is set-up in the control plane (the terminology is aligned with ETSI TISPAN – cf. [4]).

It is possible that there are additional local policy repositories that contain copies of specific policy instances to speed up response times of policy decision functions. It is also possible that policy instances of one role are copied to another role to speed up the response time of a decision (e.g. the network policies per user from the CP are copied to the NAP to shorten the delay of the RACF).

In case of having multiple CP, the NAP statically partitions the resources per subscriber and aggregate resources per CP in the management plane. Dynamic provisioning of resources is realistic in a case where only one CP that carries priority traffic for e.g. voice, next to other CP that only provide best effort connectivity. Dynamic re-partitioning of resources among several CPs is considered too complex in the control plane.

The following responsibilities can be defined in the **control plane**:

The **AF** is located in the ASP. It receives the signalling for a service from the user. It verifies whether the requested service is in line with the SLA of the user and generates a QoS request to the CP. This QoS request contains QoS parameters (e.g. bandwidth, priority class). It waits for the response from the CP before granting or denying the service to the user.

The **SPDF** is located in the CP because it is responsible for the QoS of the connection. The SPDF verifies whether the QoS parameters requested by the AF are compliant with the SLA agreed between the CP and the ASP. It enforces priorities between competing services (from different ASP) per user, following settings received from the packager. The SPDF requests resources from the access network and the regional network and waits for a response before giving feedback to the AF.

The **RACF** is the responsibility of the NAP, because the NAP has the best view of the access network topology and resources offered to different CPs that use the access infrastructure. The NAP typically does not want to share this information with another business role, such as a CP. The RACF can hence not be part of the CP. There is also no open interface defined today between the CP and the resource database of the NAP. The RACF receives the resource request from the SPDF in the CP and returns a grant or denial for resources as feedback to the SPDF. The RACF can be implemented as a centralised RACF, as well as a local RACF on the AN or EN (cf. [2]). Whether the RACF for a specific service is local or centralised, RACF is a static configuration decided by the NAP. In order to improve the response it is possible that the PDF and AF are forwarded to the Access Node and configured in the management plane, but the related responsibilities respectively remain with the CP and ASP).

The NAP is also responsible for the policy enforcement (policing) at the ingress points of its network (**RCEF: Resource Control Enforcement Function**).

There may optionally also be a RACF and related policy enforcement function in the RNP. This is however only needed if congestion is expected on the aggregated connection between the NAP and the NSP or ASP.

The NAP is responsible for the QoS functions in the dataplane like **classification** and **monitoring**. Optionally, the RNP is responsible for these functions in his segment of the network.

The residential gateway will contain QoS classification functions. Optionally the residential gateway may also contain a policy decision, call admission control, enforcement, and monitoring function for the CPN. The complexity and necessity of these functions in the residential gateway however are for further study. There is also an issue with whether or not such functionality can be trusted in what may be a subscriber owned device.

5.4 Analysis of responsibilities to manage CPE (by means of ACS)

Several providers have a responsibility to manage functions in the CPE (Customer Premises Equipment) pertaining to their respective services. E.g., a Connectivity Provider needs to configure connection parameters, a service provider needs to configure service parameters or upload new versions of software modules, or a packager is interested in the outcome of diagnostics functions to fulfil its helpdesk responsibility. CPE can be a residential gateway or other type of terminal, such as a STB (Set Top Box). The management functions are performed by an ACS (Auto-Configuration Server). The DSLF TR-069 protocol is used to convey management messages between the ACS and the CPE. The questions addressed here are: who is responsible of the ACS and who is responsible for the mediation of agreements to avoid conflicting configurations by multiple providers?

MUSE TF3 has defined **three models for the management of the CPE** by multiple providers:

- *Model 1: Multiple ACS per CPE:* Each provider owns an ACS and manages its respective parameters in the CPE. A possible implementation is the use of virtual gateways in the RGW. A policy framework on the CPE enforces priorities in case of conflicting management actions. These policies can manually be pre-configured in the CPE or downloaded from a mediating ACS. This requires some adaptations of TR-069 and the related data model of the CPE (e.g. TR-098 for the RGW).
- *Model 2: Single ACS per CPE with multiple interfaces to different OSS:* Each provider communicates its management actions from its OSS to the single ACS via a so-called northbound interface. Mediation of conflicts is done by the ACS. This requires a standardised northbound interface to allow communication across provider domains, which is not available today.
- *Model 3: Single ACS with one northbound interface to one mediating OSS that communicates with the different OSS of each provider.* The ACS and mediating OSS are in the same provider domain. Conflicts are mediated at the level of the single ACS or the mediating OSS.

A single ACS per CPE model is more likely on the short term, until solutions for model 3 have been sufficiently matured. Model 3 is preferred as long as there is no standardised northbound interface required for Model 2. It is also possible that different CPE in the same household are managed by different ACS, which may result in conflicting settings in the home network. The current model assumes that all CPE are behind a RGW in order to have managed services.

The **Packager** has the business responsibility of defining priorities between providers to avoid conflicting configurations on the CPE, because it has the total view of the agreements with all involved providers and of the requirements of the service package of the subscriber. A majority of subscribers is expected to use a single packager for their services. The allocation of this responsibility to the Packager will hence be sufficient in most cases. A regulator is likely to require that a subscriber should be able to buy services from more than one Packager in order to prevent the first Packager locking out other service providers, and to accommodate the case where the required basket of services is not available from a single Packager. In the case of multiple Packagers, the subscriber either is sufficiently skilled to perform configurations of priorities himself (acts as "main" Packager) or selects a main Packager for this purpose.

Since the Packager is a pure business role and does not own network equipment, it has to rely on someone else to host the ACS and implement the policies used for mediation. In the case of a single ACS, the following scenarios are foreseen (only Model 3 is illustrated in Figure 7, Model 2 is however similar):

- Scenario of a single CP (Connectivity Provider), the CP is the most logical technical role to host the ACS, because the configuration of the connectivity parameters in the CPE is the most essential function to be performed by an ACS (option A in Figure 7).
- Scenario of multiple CPs, the Packager can either select a main CP (option A in Figure 7) or the NAP to host an ACS (option B in Figure 7).

In the case of multiple ACSs per residential gateway (Model 1), the responsibility of the mediating ACS could be assigned along the same guidelines as for a single ACS. More research is however required to understand the supporting technologies on the CPE and their cost impact. Hence the options in the business model are left open for further study.

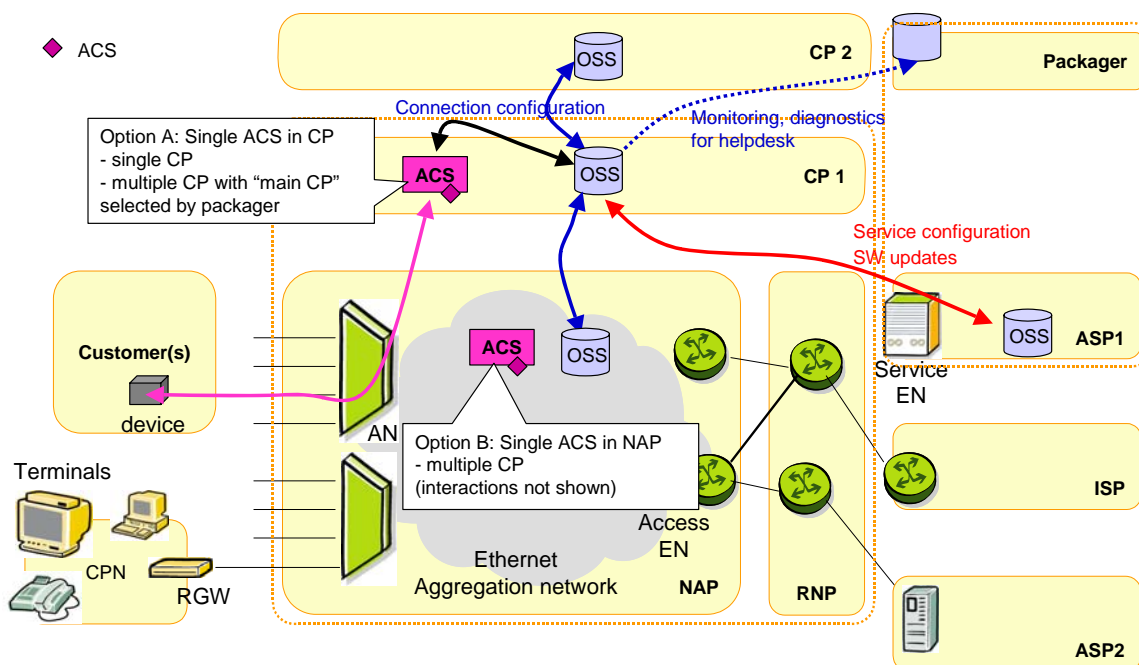


Figure 7: Responsibility in case of a single ACS (illustration for model 3, either option A or B applies)

6 SUMMARY RESPONSIBILITIES PER ROLE

MUSE has developed a business model that allows for describing real life actors by a combination of different generic roles. MUSE has analysed the business responsibilities and technical responsibilities for each role. The model is a tool to describe the network architectural requirements when unbundling the value chain.

Business responsibilities

Subscriber	<ul style="list-style-type: none"> • Signs a contract with Packager(s). • Agrees profiles with main Packager. • Pays the bill(s) (e.g. every month). • Contacts the main Packager in case of problems. • Chooses the main Packager, if appropriate.
Packager	<ul style="list-style-type: none"> • Contract (which contains profile and priorities) with subscriber and equipment (e.g. RGW) delivery to subscriber. • Installation and configuration (or guide to user). • SLAs to CP and different NSP/ASP, possibly to other Packagers • Helpdesk. • Collecting different technical data from providers (e.g. credentials, server URLs,...). • Exchange of technical data (e.g. user address, credentials, server URLs,...) to CP for configuration of control and management. • Assembles Accounting from different providers. • Billing to the Subscriber. • Selection of host for ACS in case of multiple CP (NAP or main CP).
NSP	<ul style="list-style-type: none"> • Signs SLA with Packager. • Provides technical user data (e.g. credentials, server URLs,...) to CP. • Provides network related settings to Packager.
ASP	<ul style="list-style-type: none"> • Signs SLA with Packager. • Provides technical user data (e.g. credentials, server and service URLs,...) to Packager on service activation, management and usage.
MCP	<ul style="list-style-type: none"> • Signs SLA with ASP. • Advertises content.
CP	<ul style="list-style-type: none"> • Signs SLA with Packager, NAP, and RNP. • Provides technical data (e.g. credentials, server URLs,...) to Packager.
NAP (also known as ANP)	<ul style="list-style-type: none"> • Signs SLA with CP. • Provider technical data (e.g. addresses, credentials, server URLs,...) to Packager.

RNP	<ul style="list-style-type: none"> • Signs SLA with CP.
-----	--

Technical responsibilities

Subscriber	<ul style="list-style-type: none"> • Has devices installed and starts provisioning procedures (e.g. installation of credentials into CPE).
User	<p>Makes an actual communication:</p> <ul style="list-style-type: none"> • Has devices powered on (= "Plug"), • Starts a service session (= "Play"), • Authenticates if needed, automatically or not.
Packager	<ul style="list-style-type: none"> • No technical equipment responsibilities. <p>But has technical responsibilities with regard to:</p> <ul style="list-style-type: none"> • Advice on purchase of RGW type if not delivered by Packager, installation and configuration of equipment, or installation guide, • Helpdesk, • Providing technical data (e.g. credentials, server URLs) to users (as far as this is not automated), • Holds a data base with policy profiles and possibly an SLA per subscriber.
NSP	<ul style="list-style-type: none"> • Provides the (network) functions for the Internet or corporate services. • Provides the credentials for a user to the Packager (for Internet account, for corporate network access, etc). • Checks the credentials in user request and deduces corresponding authorizations and accounting (AAA). • Assigns public IP addresses to the users. • Provides <u>Network</u> Access parameters (including credentials) and public IP addresses for User IP sessions to the CP, in case authorisation and address assignment for the network service is delegated to the CP.
ASP	<ul style="list-style-type: none"> • Provides the A10 functions for delivering and controlling the service. • Provides the credentials for a user to the Packager (for this service). • Holds the service policies per user.
MCP	<ul style="list-style-type: none"> • Makes the content in common formats. • Digital rights management. • Provides a <u>content</u> platform to offer the A11 functions for content provisioning.
CP	<ul style="list-style-type: none"> • Interprets those signalling messages that are necessary to determine the necessary connectivity means (data path) with involved networks (Internet, corporate, etc). Forwards initial signalling messages bound for ASPs that are in the same package to the appropriate server (e.g. AAA,

	<p>DHCP server).</p> <ul style="list-style-type: none"> • Setting up of semi-permanent and permanent connections with required QoS. • Holds SPDF (Performs policy decision whether requested QoS parameters received from the AF are compliant with the SLA between CP and ASP and sends resource request). • Optional signalling of QoS requests with core network to provide end-to-end QoS if congestion in core network is expected. • Hosts ACS in case of single CP or main CP selected by Packager. • On behalf of the ASP for retail users, checks the credentials in user request and deduces corresponding authorizations and accounting (AAA). • Assigns private IP addresses to retail users.
<p>NAP (also known as ANP)</p>	<ul style="list-style-type: none"> • Deals with connections in the access network – following requests received from CPs. • Enforces the authorizations resulting from subscriber profile. • Deals with management of residential gateway and home devices via the ACS and based on configuration data, profiles and priorities collected by main Packager. • Receives service requests from a home and distributes it to the appropriate serving entity(ies). • Performs admission control at resource level (A-RACF), resource reservation, and policy enforcement required to provide QoS in the access network. • Performs QoS classification, scheduling, shaping, and monitoring in the data plane of the access network. • Option to host ACS in case of multiple CPs.
<p>RNP</p>	<ul style="list-style-type: none"> • Provides connections in the regional network between the access edge and the service edge (border to the service networks) – following requests received from CPs. • Optionally performs resource admission control, resource reservation, and policy enforcement required to provide QoS in the regional network in case congestion is expected.

Note: contributions on business models to standardisation by MUSE partners

MUSE made various contributions to standardisation on business models.

- Contribution dsl2005.556.00 introduced the new business roles of Connectivity Provider and Packager to the DSLF. It also described the consequent shift of some of the responsibilities of existing roles to these new roles. The definitions were included in WT134 (the Policy Control Framework – PCF).
- Based on the MUSE results, BT introduced the Connectivity Provider concept to ETSI TISPAN by contribution ETSI_11bTD149 for consideration in TISPAN Release 2.

- MUSE presented the MUSE models in HGI (reference HGI00319). The HGI decided to proceed with a model that reflects vertical integration with two players. The NAP, RNP and CP are combined in an "Access Provider". The Packager, NSP, and ASP are combined in a "BB Service Provider".