



MSF Architecture for xDSL Broadband Access
Network Tile

MSFR4-ARCH-xDSL-FINAL

MultiService Forum Architectural Framework

Contribution Number: msf2007.154.03

Document Filename: MSFR4-ARCH-xDSL-FINAL

Working Group: Architecture

Title: MSF Architecture for xDSL Broadband Access Network Tile

Editor: Ian Jenkins
ian.wg.jenkins@bt.com

+44 1277 326676

Working Group Chairperson: Stuart Walker

Date: May 15th, 2008

Abstract:

The MultiService Forum (MSF) is responsible for developing Implementation Agreements or Architectural Frameworks which can be used by developers and network operators to ensure interoperability between components from different vendors. MSF Implementation Agreements are formally ratified via a Straw Ballot and then a Principal Member Ballot.

Draft MSF Implementation Agreements or Architectural Framework may be published before formal ratification via Straw or Principal Member Ballot. In order for this to take place, the MSF Technical Committee must formally agree that a draft Implementation Agreement or Architectural Framework should be progressed through the balloting process. A Draft MSF Implementation Agreement or Architectural Framework is given a document number in the same manner as an Implementation Agreement.

Draft Implementation Agreements may be revised before or during the full balloting process. The revised document is allocated a new major or minor number and is published. The original Draft Implementation Agreement or Architectural Framework remains published until the Technical Committee votes to withdraw it.

After being ratified by a Principal Member Ballot, the Draft Implementation Agreement or Architectural Framework becomes final. Earlier Draft Implementation Agreements or Architectural Frameworks remain published until the Technical Committee votes to withdraw them.

The use of capitalization of the key words "MUST", "SHALL", "REQUIRED", "MUST NOT", "SHOULD NOT", "SHOULD", "RECOMMENDED", "NOT RECOMMENDED", "MAY" or "OPTIONAL" is as described in section V-B of the MSF Technical Committee Operating Procedures.

The goal of the MSF is to promote multi-vendor interoperability as part of a drive to accelerate the deployment of next generation networks. To this end the MSF looks to adopt pragmatic solutions in order to maximize the chances for early deployment in real world networks.

To date the MSF has defined a number of detailed Implementation Agreements and detailed Test Plans for the signaling protocols between network components and is developing additional Implementation Agreements and Test Plans addressing some of the other technical issues such as QoS and Security to assist vendors and operators in deploying interoperable solutions.

The MSF welcomes feedback and comment and would encourage interested parties to get involved in this work program. Information about the MSF and membership options can be found on the MSF website <http://www.msforum.org/>

Note: Attention is called to the possibility that use or implementation of this MSF Implementation Agreement may require use of subject matter covered by intellectual property rights owned by parties who have not authorized such use. By publication of this Implementation Agreement, no position is taken by MSF as its Members with respect to the existence or validity of any intellectual property rights in connection therewith, nor does any warranty, express or implied, arise by reason of the publication by MSF of this Implementation Agreement. Moreover, the MSF shall not have any responsibility whatsoever for determining the existence of IPR for which a license may be required for the use or implementation of an MSF Implementation Agreement, or for conducting inquiries into the legal validity or scope of such IPR that is brought to its attention.

DISCLAIMER

The information in this publication is believed to be accurate as of its publication date. Such information is subject to change without notice and the MultiService Forum is not responsible for any errors or omissions. The MultiService Forum does not assume any responsibility to update or correct any information in this publication. Notwithstanding anything to the contrary, neither the MultiService Forum nor the publisher make any representation or warranty, expressed or implied, concerning the completeness, accuracy, or applicability of any information contained in this publication. No liability of any kind whether based on theories of tort, contract, strict liability or otherwise, shall be assumed or incurred by the MultiService Forum, its member companies, or the publisher as a result of reliance or use by any party upon any information contained in this publication. All liability for any implied or express warranty of merchantability or fitness for a particular purpose is hereby disclaimed.

The receipt or any use of this document or its contents does not in any way create by implication or otherwise:

Any express or implied license or right to or under any MultiService Forum member company's patent, copyright, trademark or trade secret rights which are or may be associated with the ideas, techniques, concepts or expressions contained herein; nor

Any warranty or representation that any MultiService Forum member companies will announce any product(s) and/or service(s) related thereto, or if such announcements are made, that such announced product(s) and/or service(s) embody any or all of the ideas, technologies, or concepts contained herein; nor

Any commitment by a MultiService Forum company to purchase or otherwise procure any product(s) and/or service(s) that embody any or all of the ideas, technologies, or concepts contained herein; nor

Any form of relationship between any MultiService Forum member companies and the recipient or user of this document.

Implementation or use of specific MultiService Forum Implementation Agreements, Architectural Frameworks or recommendations and MultiService Forum specifications will be voluntary, and no company shall agree or be obliged to implement them by virtue of participation in the MultiService Forum.

For addition information contact:

MultiService Forum
48377 Fremont Blvd., Suite 117
Fremont, CA 94538 USA
Phone: +1 510 492-4050
Fax: +1 510 492-4001
info@msforum.org
<http://www.msforum.org>

Table of Contents

1.	Introduction.....	8
1.1.	Scope.....	8
1.2.	Tile Prefix	8
1.3.	References.....	8
1.4.	Definitions and Abbreviations	8
1.4.1.	Definitions.....	8
1.4.2.	Abbreviations.....	10
2.	Overview of Relationship with the MSF Architectural Framework.....	11
3.	xDSL Broadband Access Tile Generic Architecture Overview	13
4.	Trust Boundaries.....	14
5.	Simplifications of the Generic Architecture	15
5.1.	CuANP and xNP are the Same Provider.....	15
5.2.	xNP and ISP are the Same Provider	15
5.3.	xNP, ISP and CoreSP are the Same Provider	16
6.	Element Definitions	16
6.1.	Digital Subscriber Line Access Multiplexer (DSLAM).....	16
6.2.	Backhaul & Aggregation Network	17
6.3.	Broadband Remote Access Server (BRAS).....	17
6.4.	RADIUS Server	17
6.5.	Access Location Server (ALS)	18
6.6.	Operational Support System (OSS)	18
6.7.	Service Policy Decision Server.....	18
6.8.	Access Resource and Admission Control Server (A-RACS)	19
7.	Principals of Operation	20
7.1.	Network Attachment.....	20
7.1.1.	ATM Backhaul.....	20
7.1.2.	Ethernet VLAN Backhaul.....	20
7.2.	Location Information Retrieval.....	21
7.3.	Data Stream QoS Management.....	21
7.3.1.	Generic Architecture.....	21
7.3.2.	Combined xNP and ISP Operator Architecture	22
7.3.3.	Combined xNP, ISP and MSF Core Operator Architecture	22
8.	External Interface Description and Reference	23
9.	Internal Interface Description and Reference	24

Table of Figures

Figure 1: Generic Relationship of the Access Domain within MSF Architectural Framework	12
Figure 2: xDSL Broadband Access Tile Architecture Generic Architecture	13
Figure 3: xDSL Broadband Access Tile Architecture for a Combined xDSL Network Operator and Internet Service Provider	15
Figure 4: xDSL Broadband Access Tile Architecture for a Combined xDSL Network Operator, Internet Service Provider and MSF Core Operator	16
Figure 5: SPDS in a Hybrid Network Provider Scenario	19

I. The MultiService Forum

The MultiService Forum (MSF) is a global association of service providers, system suppliers and other organizations committed to developing and promoting open-architecture, multiservice communication systems. Founded in 1998, the MSF is an open-membership organization comprised of the world's leading telecommunications companies.

The MSF's activities include developing implementation agreements, promoting worldwide compatibility and interoperability, and encouraging input to appropriate national and international standards bodies.

As part of MSF's effort to drive and promote interoperability, the MSF has created a number of programs geared toward accelerating real world network deployments:

1. Global MSF Interoperability (GMI) events. GMI events provide a real-world setting for vendors to test their solutions and provide evidence that vendor products meet the interoperability standards set forth by MSF Implementation Agreements. Each MSF GMI event is built around a set of capabilities defined for a given release of the MSF Architecture.
2. Next Generation Network (NGN) Test Bed. The NGN test bed provides a facility to enable carriers and vendors to perform in-depth testing of a specific interface as defined in a given release of the MSF architecture.
3. Certification Programs. For more mature technologies the MSF can provide Certification of compliance to a given Implementation Agreement where MSF members believe that it is of value to the industry to do so.

II. An introduction to MSF documentation and GMI 2008

This document is part of the MSF Release 4 set of architectural, protocol and test documentation.

The MSF Release 4 Architecture is a physical implementation of the functional architectures that have been proposed by the key Standards Development Organizations. As such the MSF Release 4 Architecture represents the current state of the industry and it identifies current open interfaces between physically separate network elements.

MSF Implementation Agreements define the protocols to be used over specific open interfaces. Where possible MSF Implementation Agreements are based on industry standard protocols augmented with additional information so as to ensure interoperability between communicating network elements. This level of interoperability is achieved by closing any gaps and tightening any optional capabilities in those industry standards to remove the danger of mutually incompatible selections by vendors. An MSF Implementation Agreement is targeted at a given release of the MSF architecture but can

be used in any circumstance where an operator wishes to deploy the open interface and its functionality within their own network.

The MSF Release 4 architecture and its associated implementation agreements are used as the basis for GMI 2008. GMI 2008 is a global test event executed to demonstrate multi-vendor, multi-service interoperability based around IMS and includes IPTV and web based services.

As part of GMI 2008 a number of detailed test scenarios have been developed and a number of test plans defined. Test plans contain the set of test cases required to demonstrate a given MSF Release 4 capability and serve to exercise and validate the set of Implementation Agreements required to realize the capability.

Following the completion of GMI 2008 the MSF Release 4 architecture and individual implementation agreements will be updated if the testing identifies any deficiencies in the documents.

For more information about the scope of GMI2008 please go to <http://www.msforum.org>

III. Impact on previously published MSF documents

< To contain either >

This is a new specification for MSF release 4 and GMI 2008.

< or >

This specification is for MSF release 4 and GMI 2008. It replaces the following earlier MSF documents

- <document name>
- <document name>

1. Introduction

1.1. Scope

This document defines the access tile architecture for Digital Subscriber Loop Broadband service. It includes the network attachment procedure for various access network configurations and the derivation of location information. It also includes bandwidth / QoS management of the media path.

1.2. Tile Prefix

The Tile Prefix for the Digital Subscriber Loop Broadband service access tile SHALL be “BR”

1.3. References

- [1] MSFR4-ARCH-OVERVIEW-FINAL, MSF Release 4 Architecture Overview
- [2] MSFR4-ARCH-CORE-FINAL, MSF Release 4 Core Architecture
- [3] MSFR4-ARCH-ACCESS-FINAL, MSF Release 4 Access Architectural Framework
- [4] TR-101, Rel 3, DSL Forum; Migration to Ethernet-Based Aggregation, April 2006
- [5] MSF-IA-XML.001-FINAL, MSF Implementation Agreement for Location Objects

1.4. Definitions and Abbreviations

1.4.1. Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", "OPTIONAL", "CONDITIONAL" and "IF" in this document are to be interpreted as described in the MSF Technical Committee Operating Procedures.

Access Network Domain	The part of the overall MSF architecture framework that generically represents an access network, independent of its technology
-----------------------	---

Access Network Tile	A specification of the architecture for a specific access network technology or a grouping of similar access technologies.
MSF Core Architecture Domain	The functionality contained in the Transport, Session and Common Blocks defined in the MSF Architecture [2]
Customer Domain	The part of the overall MSF architecture framework that represents equipment residing with the customer or end user.
Copper Access Network Provider	The business entity that wholesales the 'last mile' wire connection to the customer domain.
Internet Service Provider	The business entity that retails broadband service to the end customers.
Network Access Provider	The business entity that wholesales broadband service to ISPs.
MSF Core Service Provider	The business entity that provides the application and / or session connectivity to the user of the access.

1.4.2. Abbreviations

A-RACS	Access Resource & Admission Control Server
ADSL	Asymmetric Digital Subscriber Line
ALS	Access Location Server
ATM	Asynchronous Transfer Mode
BB	Broadband
BRAS	Broadband Remote Access Server
DSLAM	Digital Subscriber Line Access Multiplexer
F/W	Firewall
IP	Internet Protocol
ISP	Internet Service Provider
L2TP	Layer 2 Tunnel Protocol
LAC	L2TP Aggregation Controller
LNS	L2TP Network Server
N/W	Network
OSS	Operational Support System
PPP	Point to Point Protocol
PPPoA	Point to Point Protocol over ATM
PPPoE	Point to Point Protocol over ATM over Ethernet
PVC	ATM Permanent Virtual Connection
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
SDSL	Symmetric Digital Subscriber Line
SHDSL	Symmetric High-speed Digital Subscriber Line
SID	Subscriber Identity
SPDS	Service Policy Decision Server
S-VLAN	Static Virtual Local Area Network
VC	ATM Virtual Connection
VP	ATM Virtual Path
VDSL	Very high-speed Digital Subscriber Line
xDSL	one of the DSL technology types, i.e. ADSL, SDSL, SHDSL or VDSL
xNP	xDSL Network Provider

2. Overview of Relationship with the MSF Architectural Framework

The MSF Release 4 architecture [1] introduced an Access Network Domain into its architectural framework (see Figure 1). The Access Network Domain has a number of standard interfaces defined that are independent of the network access technology. This allows the architectural framework to define the interaction between the MSF core architecture domain and access network entities in order to support common capabilities such as extracting location information associated with access network attachment and managing access bandwidth allocation. As access technologies differ from one another, so do the mechanisms internal to that access network domain that support these interfaces. To accommodate this, a generic access domain is defined with the MSF architectural framework with common interfaces [3]. To facilitate adding different and multiple access networks to the overall architecture, each access network technology or group of similar technologies is defined in its own 'Access Network Tile' architecture that can be substituted for the generic access domain. Each Access Network Tile specifies how it operates internally and supports a sub-set of the common interfaces with the MSF Core Architecture Domain [2].

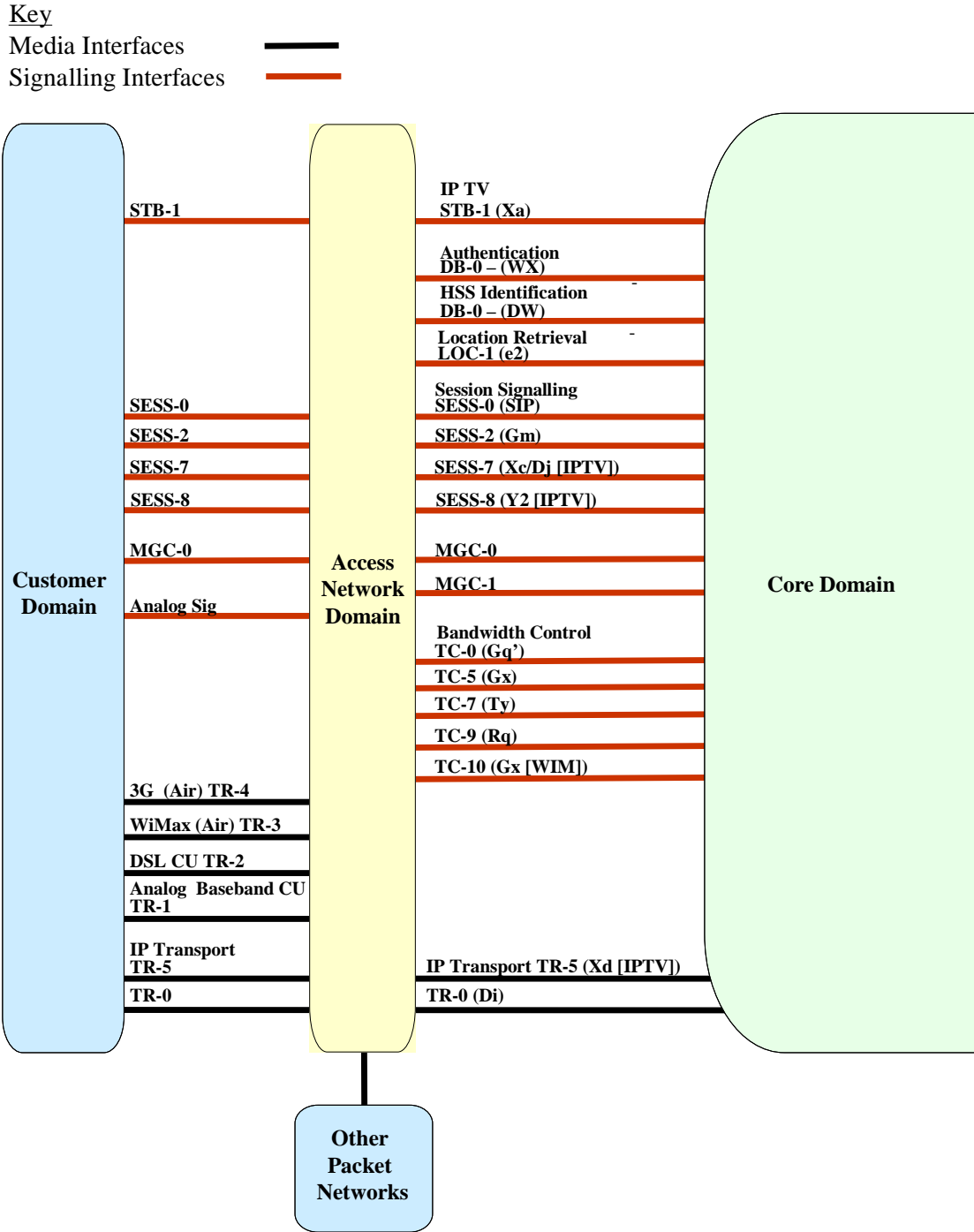


Figure 1: Generic Relationship of the Access Domain within MSF Architectural Framework

The common interfaces between the MSF Core Architecture Domain and the Access Block are for Location Retrieval (LOC-1), Bandwidth Control (TC-0) and IP transport (TR-0).

3. xDSL Broadband Access Tile Generic Architecture Overview

The Broadband Access Tile architecture is shown in Figure 2 and as is based on the principles defined in TR-101 [4]. Figure 2 depicts the generic scenario where the each part of the xDSL Access and the MSF Core is in a different trust domain

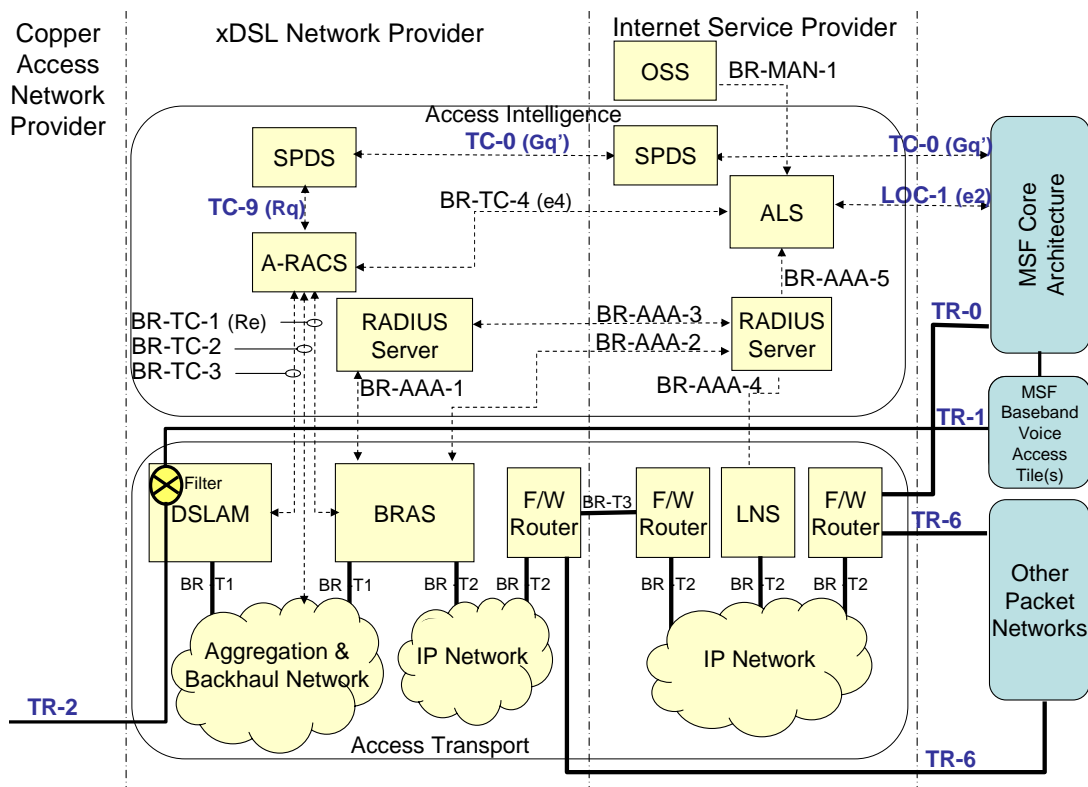


Figure 2: xDSL Broadband Access Tile Architecture Generic Architecture

For broadband service the copper pair (TR-2) is terminated on a DSLAM which supports one or more ATM virtual connections (VCs) to the subscriber via xDSL technology. The architecture shows the components grouped into those relating to intelligence and those related to transport of the data streams. The aggregation and backhaul network shown within the xDSL Network Provider Domain can be either ATM or Ethernet technology

For completeness, Figure 2 also shows the copper pair taken via a filter directly to the MSF Baseband Access Tile for telephony service via TR-1.

4. Trust Boundaries

The generic architecture in Figure 2 shows that there can be up to five separate trust boundaries. These are:-

- i) The Copper Pair Access Network Provider (CuANP)
- ii) The xDSL Network Provider (xNP)
- iii) The Internet Service Provider (ISP)
- iv) The MSF Operator of the core domain (CoreSP)
- v) An Internet exchange operator or other internet backbone peering operator.

5. Simplifications of the Generic Architecture

In many cases network operators will own and manage more than one on the domains shown separated by trust boundaries in the generic architecture. The following section describes how the generic architecture shown in Figure 2 can be simplified where the trust boundaries can be removed as the provider of the various domains is the same operator and can therefore be combined.

5.1. CuANP and xNP are the Same Provider

If the Copper Pair Access Network Provider and the xDSL Network Provider are the same provider this trust boundary can be removed without architectural impact in any of the other options for trust boundary removal described in this section.

5.2. xNP and ISP are the Same Provider

If the xDSL Network Provider and the Internet Service Provider are the same operator, the trust boundary between them can be removed to provide the architecture shown in Figure 3.

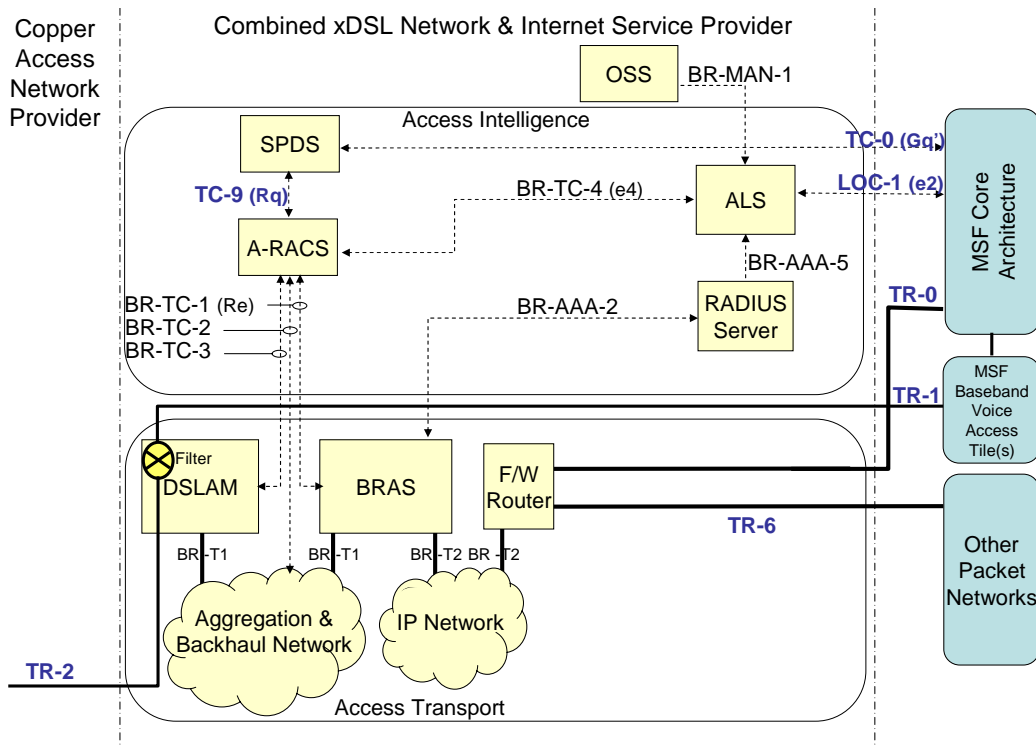


Figure 3: xDSL Broadband Access Tile Architecture for a Combined xDSL Network Operator and Internet Service Provider

This shows that the Radius servers can be combined to provide all of the functions as can the SPDSs be also combined. The firewall / BGP routers and between the xNP and ISP disappear.

5.3. xNP, ISP and CoreSP are the Same Provider

If the xDSL Network Provider, the Internet Service Provider and the MSF Core network are the same operator, the removal of the trust boundaries shown in the generic xDSL access architecture results in the architecture shown in Figure 4. In addition to the simplifications described in 5.2, Figure 4 shows the SPDS in the MSF core interfaces directly to the A-RACS.

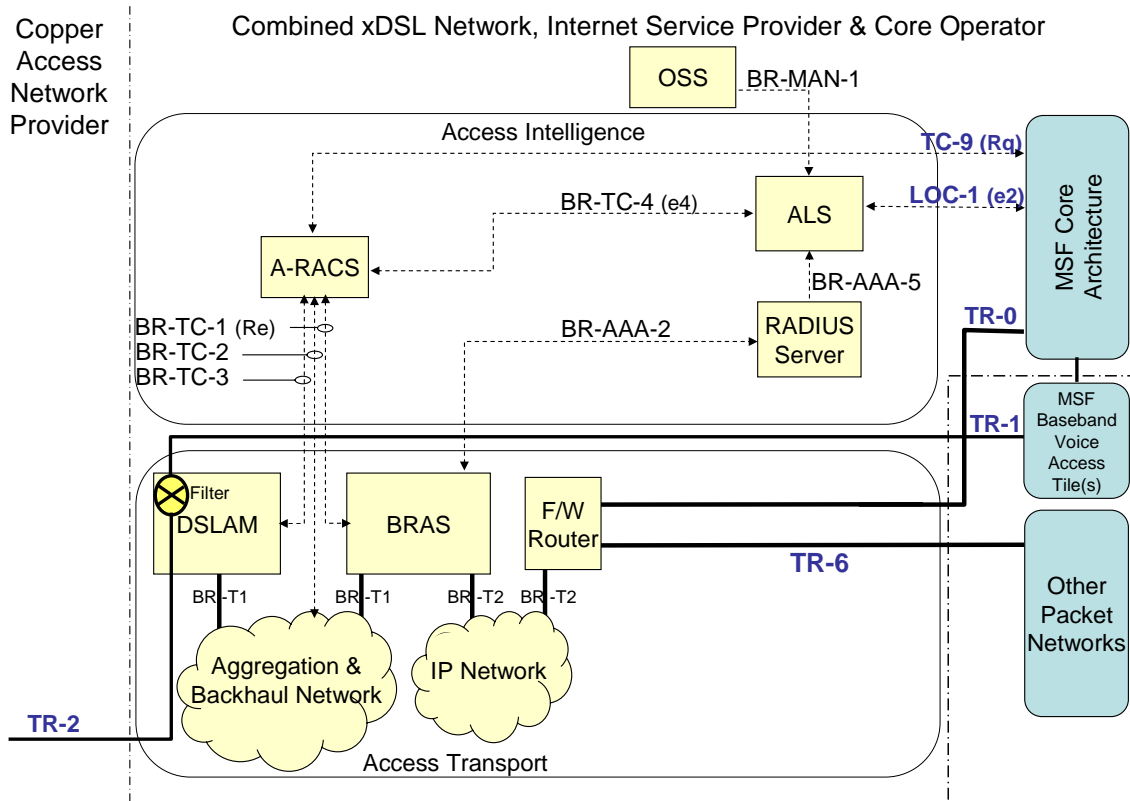


Figure 4: xDSL Broadband Access Tile Architecture for a Combined xDSL Network Operator, Internet Service Provider and MSF Core Operator

6. Element Definitions

6.1. Digital Subscriber Line Access Multiplexer (DSLAM)

The DSLAM multiplexes different customers ATM VCs onto the Aggregation and Backhaul network where each individual subscriber VC is either switched into an ATM PVP or mapped into an Ethernet VLAN depending on the backhaul network technology. Customer attachment and session access are established via PPPoA which the DSLAM switches transparently for ATM backhaul. If the backhaul network is using Ethernet VLANs then the DSLAM converts the PPPoA to PPPoE via an intermediate agent. In this case the intermediate agent MUST include an Agent Circuit Id as defined in TR-101

[4] which uniquely identifies the DSLAM, the card and physical port on which the copper access is terminated and the ATM PVC/VC identifiers to the subscriber.

6.2. Backhaul & Aggregation Network

The backhaul network aggregates and switches the subscriber connections to a BRAS. This network can use either ATM or Ethernet VLAN technology

6.3. Broadband Remote Access Server (BRAS)

The BRAS receives the network attachment requests that are signaled from either the subscriber's terminal or from the subscriber's DSL router gateway via PPPoA or PPPoE depending of the backhaul network technology.

The BRAS consists of a number of virtual instances that can be configured to meet an individual ISP's requirements. BRAS instances can be configured to provide a:-

- i) DHCP server with a range of IP address from which to allocate
- ii) PPP termination
- iii) L2TP Access Concentrator (LAC) to extend a PPP session via L2TP to the ISP
- iv) RADIUS server address for an 'instance specific' RADIUS server look-up

The BRAS communicates via BR-AAA-1 to the xNP RADIUS server and also, if configured, the ISP RADIUS server via BR-AAA-2 for authentication and the provision of accounting records.

The BRAS also provides bandwidth policy enforcement on data streams toward the DSLAM under the control of the A-RACS via BR-TC-1.

6.4. RADIUS Server

The RADIUS Server holds data for authenticating and authorizing the line access and subscriber access and providing accounting records.

The xNP RADIUS server validates that that the line is a valid BB line when requested by the BRAS via BR-AAA-1 and points the PPP session to the appropriate virtual BRAS instance. It can act as a proxy to the ISP RADIUS server via BR-AAA-3 for user authentication and also to forward accounting information.

The ISP RADIUS Server holds the subscriber authentication information and receives authentication requests and accounting information from the:-

- i) xNP Radius Server via BR-AAA-3
- or
- ii) BRAS via BR-AAA-2
- or
- iii) LNS via BR-AAA-4

On successful network attachment, the ISP RADIUS server sends the allocated IP address to a particular line to the ALS via BR-AAA-5 including any fixed IP address allocations.

6.5. Access Location Server (ALS)

The ALS is the system that allows location queries to be processed in real time, without reference to a chain of other non-real systems and thus avoids attendant performance issues. The ALS holds a table of information that is populated by the ISP OSS via BR-MAN-1 which includes the:-

- i) Line Id associated with a subscriber
- ii) geographic location information for that line termination (e.g. civic address)
- iii) privacy policy to be applied to that location information in order to restrict its release, in part or whole.

The ALS receives the allocation of IP address to the Line Id from the ISP RADIUS server via BR-AAA-5. Location Requests can be made from the MSF Core, referenced by the access IP address (i.e. that allocated in the access tile by the ISP) via interface LOC-1 which provides the location information and the associated privacy policy. The A-RACS can also make requests for the DSLAM line id that has been associated with the access IP address via interface BR-TC-02.

6.6. Operational Support System (OSS)

The ISP OSS holds all the subscriber details including the installation address for the broadband line, the line identifier values used with the xNP and any line associated privacy policy. It provides this information to the ALS as part of the provisioning and update process over BR-MAN-1.

6.7. Service Policy Decision Server

The SPDS receives service based QoS policy request for a data flow. It is the final policy decision point for requests within that provider's domain as it holds the service policy rules determined by that operator. The SPDS hides the underlying network topology of its own network or the use of other providers' networks and orchestrates what further requests need to be made, and to where, in order to fulfill the service request. The SPDS in the ISP domain selects which xNP to forward the service request from the MSF Core. If a service request can no longer be maintained the SPDS communicates the change back to the source of the service request.

Hybrid situations can occur where the ISP and xNP are combined for some subscribers but use a separate xNP operator for other subscribers (e.g. to cover different geographic areas). In this case the SPDS of the hybrid provider must decide whether to make requests to its own A-RACS or to the associated xNP operators SPDS (See Figure 5).

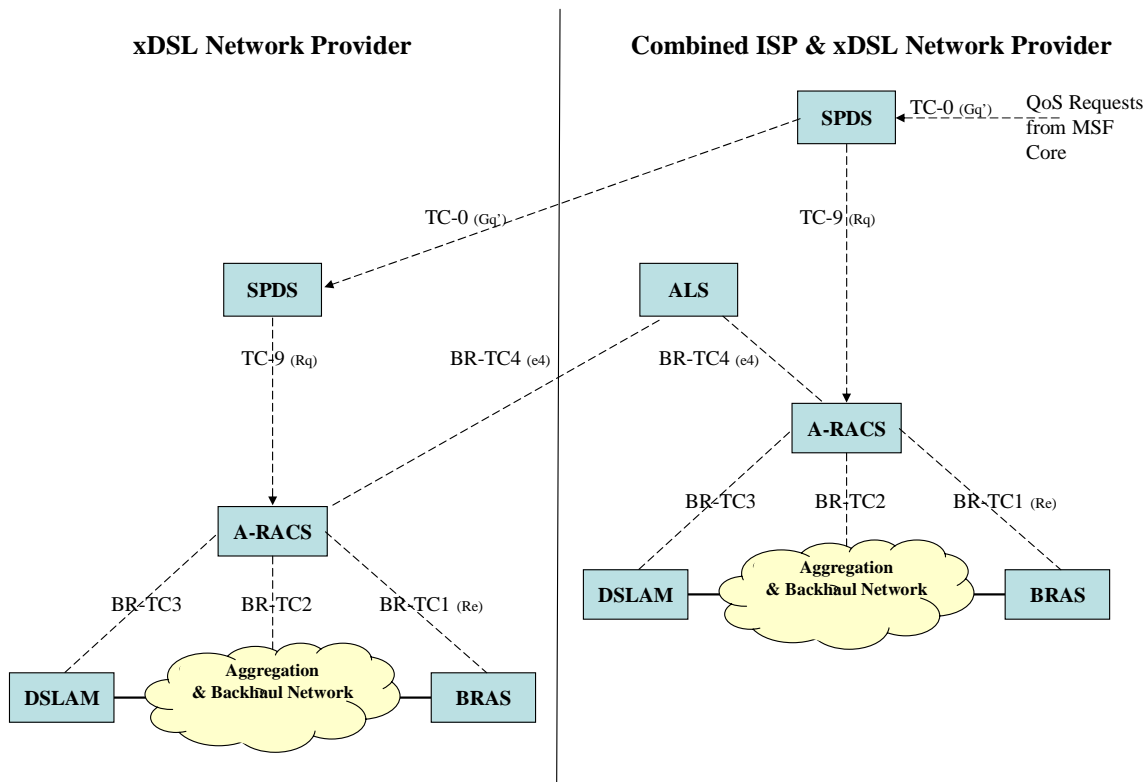


Figure 5: SPDS in a Hybrid Network Provider Scenario

6.8. Access Resource and Admission Control Server (A-RACS)

The A-RACS holds and maintains a model of the physical network components and their topology which it hides from the SPDS. It performs admission control for the access and aggregation segment of the access network which depends on the following checks:-

- Subscriber Access Profile Checking – i.e. is this line allowed to have this resource allocated to it?
- Resource Admission Control - i.e. are the resources available to fulfill the request?

The A-RACS monitors changes in the underlying resource availability, which can alter due to faults or maintenance actions, reporting any impact on existing policy commitments to the SPDS.

7. Principals of Operation

7.1. Network Attachment

There are two basic network attachment modes depending on whether the aggregation and backhaul network is using ATM or Ethernet VLANs.

7.1.1. ATM Backhaul

When the subscriber attaches to the network the BRAS passes the logon information received in PPPoA to the xNP Radius Server and the BRAS id/ATM port id/ VP/VC via BR-AAA-1. The xNP Radius Server uses the BRAS id/ATM port id/ VP/VC to derive a Line ID from the configuration of the ATM backhaul network. This Line Id indirectly relates to the copper access line that is terminated on the DSLAM and is agreed as part of the ISP / xNP provisioning process. The derived Line Id may be used by the xNP RADIUS server to validate that the attachment request is from a valid BB line. Once validated, the xNP RADIUS server either:-

- i) uses the realm information within the PPP login to proxy a subscriber authentication request to the associated ISP RADIUS server via BR-AAA-3 and if valid, to direct the attachment to an associated virtual BRAS instance which allocates an IP address and terminates the PPP session. The BRAS then sends an accounting record to xNP RADIUS server via BR-AAA-1 with the allocated IP address. The xNP RADIUS server subsequently sends accounting information to the ISP RADIUS server via BR-AAA-3 with the derived Line Id and the associated IP address. The subscriber is given IP access to the xNP & ISP's IP network or any other IP network that is interconnected to them.

or

- ii) uses the realm information within the PPP login and/or the Line Id to direct the network attachment to a virtual BRAS instance configured as a L2TP Aggregation Controller (LAC). The LAC will then extend the L2TP tunnel across the NP's IP network to the ISP's IP network where it is terminated on a LNS. The LNS also terminates the PPP session. The LNS extends the PPP logon information in an authentication request to the ISP's RADIUS server via BR-AAA-4 and the LNS is sent a response indicating if the request was valid or not. Either the ISP RADIUS server or the LNS can allocate the IP address. The LNS sends an accounting record to the ISP RADIUS server with the allocated IP address via BR-AAA-4. The subscriber is given IP access to the ISP's IP network or any other IP network that is interconnected to it.

7.1.2. Ethernet VLAN Backhaul

When the subscriber attaches to the network, the BRAS makes an authorization request to the xNP RADIUS server via BR-AAA-1, passing the Agent Circuit Id carried in the PPPoE as defined in TR-101 [4]. The Agent Circuit Id directly relates to the copper

access line that is terminated on the DLSAM and is effectively a Line Id. If the Agent Circuit Id is valid the xNP RADIUS server responds with information to direct the session to a BRAS virtual instance that is associated with the ISP who owns the subscriber for that BB line.

The BRAS virtual instance can be configured to terminate the PPP session and make a second authentication request to the ISP RADIUS server via BR-AAA-2, passing it the PPP logon information. Having validated the subscriber, the ISP RADIUS server responds to the BRAS virtual instance which allocates an IP address from a pre-configured range. The ISP RADIUS server can also supply an IP address to be used by the BRAS virtual instance instead of allocating one from its range. The BRAS sends an accounting record to the ISP RADIUS server with the allocated IP address and Agent Circuit Id via BR-AAA-2. Depending on the BRAS virtual instance configuration, the subscriber is given IP access either to the ISP's IP network via an Ethernet VLAN or to the xNP IP network and any other IP network that is interconnected to it.

7.2. Location Information Retrieval

During the provisioning process the xNP provides the ISP with a Line Id /Agent Circuit Id. The ISP's OSS in turn provisions into the ALS via BR-MAN-1 the Line Id /Agent Circuit Id with the associated subscriber civic address of the line termination and any subscriber's line specific privacy policy, in line with the information required for MSF Location Objects [5].

Subsequent to a successful network attachment as described above, the ISP Radius Server sends an accounting record to the ALS via BR-AAA-5 which indicates the start of the attachment and the allocation of IP address to Line Id / Agent Circuit Id. The ALS stores the IP address and its attachment status (indexed by Line Id / Agent Circuit Id) against the subscriber details. When the subscriber detaches from the network, the ISP RADIUS server sends an accounting record to indicate this so that the attachment status can be updated.

When a location request is made by the MSF core, the IP address of the terminal / home router is sent to the ALS via LOC-1. If there is a current network attachment associated with the IP address, the location information and any privacy policy is returned, else an error message is sent. If the MSF network requests updates, then the ALS will respond when the subscriber attachment status changes.

7.3. Data Stream QoS Management

Resource and data stream policy requests are received from the MSF Core Domain either via interface TC-0 or TC-9 depending on how the various provider trust boundaries map onto operators (see section 4, Trust Boundaries).

7.3.1. Generic Architecture

This architecture assumes that the ISP IP network is built to provide no bandwidth constraints on data flows that traverse it.

With reference to Figure 2, QoS service requests are made from the MSF Core network via interface TC-0 to the ISP's SPDS. The SPDS decides which xNP network is associated with the request and forwards the request to appropriate xNP's SPDS via the inter-domain interface, TC-0. The xNP's SPDS requests that the service policy be translated into the appropriate network policies by the A-RACS via interface TC-9. As IP addresses are usually dynamically allocated to subscribers, and as this request to the A-RACS is referenced by IP address, the A-RACS requests the mapping of IP address to line identifier from the ISP's ALS via interface BR-TC-2. This enables the A-RACS to establish which BRAS, DSLAM and aggregation and backhaul network resources are associated with the request. It can then establish if the required resources exist and if so to send the network policy to the BRAS for enforcement. The service request is then confirmed to the SPDS.

7.3.2. Combined xNP and ISP Operator Architecture

With reference to Figure 3, QoS service requests are made from the MSF Core network via interface TC-0 to the SPDS. The SPDS requests that the service policy be translated into the appropriate network policies by the A-RACS via interface TC-9. As IP addresses are usually dynamically allocated to subscribers, and as this request to the A-RACS is referenced by IP address, the A-RACS requests the mapping of IP address to line identifier from the ALS via interface BR-TC-2. This enables the A-RACS to establish which BRAS, DSLAM and aggregation and backhaul network resources are associated with the request. It can then establish if the requested resources exist and if so to send the network policy to the BRAS for enforcement. The service request is then confirmed to the SPDS.

7.3.3. Combined xNP, ISP and MSF Core Operator Architecture

With reference to Figure 4, QoS service requests are made from the MSF Core network via interface TC-9 directly from the SPDS in the MSF Core to the A-RACS. . As IP addresses are usually dynamically allocated to subscribers, and as this request to the A-RACS is referenced by IP address, the A-RACS requests the mapping of IP address to line identifier from the ALS via interface BR-TC-2. This enables the A-RACS to establish which BRAS, DSLAM and aggregation and backhaul network resources are associated with the request. It can then establish if the requested resources exist and if so to send the network policy to the BRAS for enforcement. The service request is then confirmed to the SPDS.

8. External Interface Description and Reference

The following are external interfaces between the xDSL Broadband Access Tile and other non-xDSL Broadband Domains.

Interface Designation	ETSI Ref Pt	Description	Protocol Type	MSF IA
Transport Interfaces				
TR-0	N/A	IP transport connection to/from the MSF core	IP	N/A
TR-1	N/A	Baseband voice over copper pair	N/A	N/A
TR-2	N/A	xDSL and Baseband voice over copper pair	N/A	N/A
BR-TR0	N/A	IP transport connection to/from other IP networks e.g. Internet	IP	N/A
Location Information				
LOC-1	e2	MSF Core to ALS	Diameter	MSF-IA-DIAMETR.008-FINAL
Bandwidth management				
TC-0	Gq'	MSF Core to ISP SPDS ISP SPDS to xNP SPDS	Diameter	MSF-IA-DIAMETER.004-FINAL
TC-9	Rq	MSF Core SPDS to A-RACS	Diameter	MSF-IA-DIAMTER.005-FINAL

9. Internal Interface Description and Reference

Interface Designation	SDO Ref Pt	Description	Protocol Type	MSF IA
Transport Interfaces				
BR-T1	N/A	Session setup over either:- i) ATM ii) Ethernet VLAN	PPPoA PPPoE	N/A N/A
BR-T2	N/A	IP network connection	IP	N/A
BR-T3	N/A	IP interconnect between xNP & ISP	IP	N/A
Authentication, Authorization and Accounting Interfaces				
BR-AAA-1	N/A	BRAS to xNP RADIUS Svr	RADIUS	N/A
BR-AAA-2	N/A	BRAS to ISP RADIUS Svr	RADIUS	N/A
BR-AAA-3	N/A	xNP RADIUS Proxy to ISP RADIUS Svr	RADIUS	N/A
BR-AAA-4	N/A	LNS to ISP RADIUS Svr	RADIUS	N/A
BR-AAA-5	N/A	ISP RADIUS Svr to ALS	Diameter	TBD
Bandwidth Management				
TC-0	Gq'	ISP SPDS to xNP SPDS	Diameter	MSF-IA-DIAMTER.005-FINAL
TC-9	Rq	MSF Core SPDS to A-RACS	Diameter	MSF-IA-DIAMTER.005-FINAL
BR-TC-0	Ri'		Diameter	N/A
BR-TC-1	Rq	Access N/W Provider SPDS to BRAS	Diameter	N/A
BR-TC-2	N/A	BB Access N/W Provider SPDS to BRAS		N/A
Service Management Interfaces				
BR-MAN-1	N/A	The interface carries subscriber provisioning and update information and will be operator depended.	Probably XML based	N/A

End of Document