TECHNICAL REPORT

TR-134
Broadband Policy Control Framework (BPCF)

Issue: 1 Corrigendum 1
Issue Date: January 2013

Notice

The Broadband Forum is a non-profit corporation organized to create guidelines for broadband network system development and deployment. This Broadband Forum Technical Report has been approved by members of the Forum. This Broadband Forum Technical Report is not binding on the Broadband Forum, any of its members, or any developer or service provider. This Broadband Forum Technical Report is subject to change, but only with approval of members of the Forum. This Technical Report is copyrighted by the Broadband Forum, and all rights are reserved. Portions of this Technical Report may be copyrighted by Broadband Forum members.

This Broadband Forum Technical Report is provided AS IS, WITH ALL FAULTS. ANY PERSON HOLDING A COPYRIGHT IN THIS BROADBAND FORUM TECHNICAL REPORT, OR ANY PORTION THEREOF, DISCLAIMS TO THE FULLEST EXTENT PERMITTED BY LAW ANY REPRESENTATION OR WARRANTY, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTY:

(A) OF ACCURACY, COMPLETENESS, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR TITLE;
(B) THAT THE CONTENTS OF THIS BROADBAND FORUM TECHNICAL REPORT ARE SUITABLE FOR ANY PURPOSE, EVEN IF THAT PURPOSE IS KNOWN TO THE COPYRIGHT HOLDER;
(C) THAT THE IMPLEMENTATION OF THE CONTENTS OF THE TECHNICAL REPORT WILL NOT INFRINGE ANY THIRD PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS.

By using this Broadband Forum Technical Report, users acknowledge that implementation may require licenses to patents. The Broadband Forum encourages but does not require its members to identify such patents. For a list of declarations made by Broadband Forum member companies, please see http://www.broadband-forum.org. No assurance is given that licenses to patents necessary to implement this Technical Report will be available for license at all or on reasonable and non-discriminatory terms.

ANY PERSON HOLDING A COPYRIGHT IN THIS BROADBAND FORUM TECHNICAL REPORT, OR ANY PORTION THEREOF, DISCLAIMS TO THE FULLEST EXTENT PERMITTED BY LAW (A) ANY LIABILITY (INCLUDING DIRECT, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES UNDER ANY LEGAL THEORY) ARISING FROM OR RELATED TO THE USE OF OR RELIANCE UPON THIS TECHNICAL REPORT; AND (B) ANY OBLIGATION TO UPDATE OR CORRECT THIS TECHNICAL REPORT.

Broadband Forum Technical Reports may be copied, downloaded, stored on a server or otherwise re-distributed in their entirety only, and may not be modified without the advance written permission of the Broadband Forum.

The text of this notice must be included in all copies of this Broadband Forum Technical Report.

TR Issue History

Issue Number	Approval Date	Publication Date	Issue Editors	Changes
1	2 July 2012	10 July 2012	Bill Welch, Juniper Networks Ezer Goshen, BandWD	Original
1 Corrigendum 1	January 2013	12 February 2013	Bill Welch, Juniper Networks Ezer Goshen, BandWD	7.1.4.2 – Changed duplicate R-76 to R-80 7.1.4.6 – Bolded text Figure 47 – deleted ‘)’

Comments or questions about this Broadband Forum Technical Report should be directed to info@broadband-forum.org.

Editor	Bill Welch Ezer Goshen	Juniper Networks BandWD
End-to-End Architecture WG Chairs	David Allan David Thorne	Ericsson BT
Vice Chair	Sven Ooghe	Alcatel- Lucent
Chief Editor	Michael Hanrahan	Huawei Technologies

TABLE OF CONTENTS

List of Tables

List of Figures

Executive Summary

TR-134 defines an architectural Framework to provide policy control of Broadband Multi-Service Networks. This Technical Report specifies business requirements, use cases, and a minimum set of Information Flows that facilitate the management and execution of policies.

1 Purpose and Scope

1.1 Purpose

The Broadband Policy Control Framework (BPC Framework) addresses the following:

- Providing Broadband network services based on Policies
- Dynamic and/or static activation and management of these Policies

These Broadband network capabilities are broadly aligned with the architectures, interfaces and protocols specified in generic NGN standards.

1.2 Background

Numerous Broadband Forum documents mention "Policies", "Policy Controllers" and "Policy Servers" as an architectural component. References exist in TR-058[1], TR-059[2], TR-092[4], TR-101[6], TR-102[7], TR-144[9] and TR-147[10], some of which have dedicated sections related to policy and policy management. Despite such common use of these concepts and high-level statements of requirements, the Broadband Forum has not agreed upon definitions for Policy or Policy Management.

Several SDO and industry initiatives have also been developing their own NGN architectures. A key feature of these architectures has been the development of policy and policy management architectures, interfaces and procedures. Such architectures include those from the ITU-T, ETSI TISPAN, ATIS, 3GPP and 3GPP2. Each of these architectures provides a different approach to the common goal of providing support for NGN applications over a broadband access network.

The Broadband Forum has not adopted any of these solutions as a preferred architecture, or offered its own contribution towards selecting, interoperating, augmenting, or replacing any of these architectures. Recent work often cites the need to align the Broadband Forum's standards with multiple 3rd party NGN standards (e.g. TR-144[9]). The Broadband Forum does maintain active liaison relationships with several of the above organizations with respect to policy management architecture. In particular the BBF is working jointly with 3GPP on requirements and an architectural Framework for fixed-mobile interworking.

1.3 Scope

TR-134 augments the Broadband Forum's Broadband Multi-Service architectures, including TRs 059, 101, 102, 147 and TR-144[9], with an integrated approach to policy management and control. It uses business requirements as a tool to identify the features of Broadband Multi-Service network architectures that it may be appropriate to control by means of policy, and provides a Framework and interfaces for such policy management and control. The relationship between the Broadband Forum approach and various external Standard Development Organizations (SDOs) policy and NGN efforts is also described, as is the integration of features to allow the broadband multiservice network to work with generic NGN architectures. These features are then exposed via a set of Information Flows. The ultimate goals are to develop an Information Model, based on existing standards, to provide any necessary extensions to address the aforementioned business requirements, and to define a general extensibility scheme to meet

future requirements. TR-134 is the first step in the development of a comprehensive information model for supporting policy based management and control

1.4 Relationship to other Broadband Forum Technical Reports

This Technical Report consolidates requirements from various existing Broadband Forum TRs to form an integrated view of current business and technical requirements for policy and policy management.

Specifically, this Technical Report builds on requirements from the following sources

- TR-058 – Multi-Service Architecture and Requirements
- TR-059 – Architectural Requirements for the support of QoS-Enabled IP services
- TR-092 – BRAS Requirements
- TR-101 – Migration to Ethernet DSL Aggregation
- TR-102 – Service Interface Requirements for TR-058 Architectures
- TR-144– Broadband Multi-Service Architecture & Framework Requirements
- TR-147 – Layer 2 Control Mechanism For Broadband Multi-Service Architectures

2 References and Terminology

2.1 Conventions

In this Technical Report, several words are used to signify the requirements of the specification. These words are always capitalized. More information can be found be in RFC 2119[14].

MUST	This word, or the term "REQUIRED", means that the definition is an absolute requirement of the specification.
MUST NOT	This phrase means that the definition is an absolute prohibition of the specification.
SHOULD	This word, or the term "RECOMMENDED", means that there could exist valid reasons in particular circumstances to ignore this item, but the full implications need to be understood and carefully weighed before choosing a different course.
SHOULD NOT	This phrase, or the phrase "NOT RECOMMENDED" means that there could exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications need to be understood and the case carefully weighed before implementing any behavior described with this label.
MAY	This word, or the term "OPTIONAL", means that this item is one of an allowed set of alternatives. An implementation that does not include this option MUST be prepared to inter-operate with another implementation that does include the option.

2.2 References

The following references are of relevance to this Technical Report. At the time of publication, the editions indicated were valid. All references are subject to revision; users of this Technical Report are therefore encouraged to investigate using the most recent edition of the references listed below.

A list of currently valid Broadband Forum Technical Reports is published at www.broadband-forum.org

Document		Title	Source	Year
[1]	TR-058	*Multi-Service Architecture and Framework Requirements*	BBF	2003
[2]	TR-059	*DSL Evolution – Architecture Requirements for the Support of QoS-Enabled IP Services*	BBF	2003
[3]	TR-069 Amendment 2	*CPE WAN Management Protocol v1.1*	BBF	2007
[4]	TR-092	*Broadband Remote Access Server (BRAS) Requirements Document*	BBF	2004

[5]	TR-098	*DSLHomeTM Gateway Device Version 1.1 Data Model for TR-069*	BBF	2008
[6]	TR-101	*Migration to Ethernet-Based DSL Aggregation*	BBF	2006
[7]	TR-102	*Service Interface Requirements for TR-058 Architectures*	BBF	2006
[8]	TR-124	*Functional Requirements for Broadband Residential Gateway*	BBF	2008
[9]	TR-144	*Broadband Multi-Service Architecture & Framework Requirements*	BBF	2007
[10]	TR-147	*Layer 2 Control Mechanism for Broadband Multi-Service Architectures*	BBF	2008
[11]	TR-181	*Device Data Model for TR-069*	BBF	2010
[12]	TR-181 Issue 1	*Device Data Model for TR-069*	BBF	2010
[13]	TR-181 Issue 2	*Device Data Model for TR-069*	BBF	2010
[14]	RFC 2119	*Key words for use in RFCs to Indicate Requirement Levels*	IETF	1997
[15]	RFC 2753	*A Framework for Policy-based Admission Control*	IETF	2000
[16]	RFC 2865	*Remote Authentication Dial In User Service (RADIUS)*	IETF	2000
[17]	RFC 2866	*RADIUS Accounting*	IETF	2000
[18]	RFC 3060	*Policy Core Information Model -- Version 1 Specification*	IETF	2001
[19]	RFC 3198	*Terminology for Policy-Based Management*	IETF	2001
[20]	RFC 3460	*Policy Core Information Model (PCIM) Extensions*	IETF	2003
[21]	RFC 3585	*IPSec Configuration Policy Information Model*	IETF	2003
[22]	RFC 3588	*Diameter Base Protocol*	IETF	2003
[23]	RFC 3644	*Policy Quality of Service (QoS) Information Model*	IETF	2003
[24]	RFC 3670	*Information Model for Describing Network Device QoS Datapath Mechanisms*	IETF	2004
[25]	RFC 5176	*Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)*	IETF	2008
[26]	RFC 6320	*Protocol for Access Node Control Mechanism in Broadband Networks*	IETF	2011
[27]	WT-145	*Multi Service Broadband Network Functional Modules and Architecture*	BBF	
[28]	WT-146	*IP Sessions*	BBF	
[29]	WT-178	*Multi-service Broadband Network Architecture and Nodal Requirements*	BBF	
[30]	WT-203	*Interworking between Next Generation Fixed and 3GPP Wireless Networks*	BBF	
[31]	TS 29.212	*Policy and Charging Control (PCC) over Gx/Sd*	3GGP	2012

		reference point		
[32]	TS 23.203	*3GPP Technical Specification Group Services and System Aspects, Policy and charging control architecture*	3GPP	2011
[33]	TR 182 031	*Telecommunications and Internet converged Services and. Protocols for Advanced Networking*	ETSI	2010
[34]	282 003	*Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control Sub-System (RACS): Functional Architecture*	ETSI	2009
[35]	Y.2001	*General overview of NGN*	ITU	2004
[36]	Y.2111	*Resource and admission control functions in next generation networks*	ITU	2012
[37]	Y.dpifr	*Framework for Deep Packet Inspection*	ITU	2011

2.3 Definitions

The following terminology is used throughout this Technical Report.

AAA Client function	A logical entity that sends authenticating, authorizing and accounting requests to an AAA Server function. An example of an AAA client function contained with a network node is a Network Access Server (NAS) as described in RFCs 2865[16] and 2866[17]. Examples of AAA client function in BBF TRs are the BRAS of TR-059[2] and the BNG of TR-101[6].
AAA Server function	A logical entity in the client-server relationship that replies to AAA Client Authentication, Authorization and Accounting requests. The AAA server function is typically responsible for receiving user connection requests, authenticating the user, and replying to the AAA Client function with an Accept or Deny response. The AAA Server function can return, as part of this reply, some or all of the configuration information necessary for the AAA client function to deliver service to the user. An AAA server function can act as a proxy client to other AAA server functions or other kinds of authentication servers. The AAA Server function does not contain any business logic other than basic authentication.
AAA Server	A physical device that contains an AAA Server functions.

AAA Protocol	A communications protocol that supports exchanges between AAA Client and Server functions. Examples of AAA protocols include RADIUS and DIAMETER.
Bandwidth on Demand	The ability to change the access bandwidth allocated in response to applications, specific network connectivity, or user request.
Broadband Network Gateway (BNG)	IP Edge Router where bandwidth and QoS policies may be applied. This term is used instead of BRAS to denote an Ethernet-centric IP edge node in this Technical Report(and in TR-101[6]).
BRAS	Broadband Remote Access Server is the aggregation point for user traffic. It provides aggregation capabilities (e.g. IP, PPP, and Ethernet) between the access network and the NSP or ASP. It can also support policy management and IP QoS in the access network.
Charging Key	A parameter used by the charging system to indicate the appropriate charging rate for a given flow.
Charging Control	The process of associating packets, belonging to a service data flow, with a charging key and applying online and/or offline charging, as appropriate.
Condition	A condition in its most general form is any expression that can evaluate to true or false. A condition is often referred to as a match criterion (i.e. if a specific criterion is met/matched, then the associated action(s) will execute).
Congestion Point	A physical or logical egress point in the network where the sum of aggregated ingress traffic can be larger than available physical or logical bandwidth. Physical congestion points include Ethernet ports and DSL local loops. Logical congestion points include ATM VCs, ATM VPs, Ethernet VLANs, Ethernet SVLANs and MPLS LSPs.
Control Policy	A type of policy for which the execution trigger is an explicit control-plane event (e.g. a signaling event, a timer expiry event), and for which the action(s) does not entail the processing of a forwarded data packet. A Control Policy is defined by both: • A set of conditions which describe the event which triggers the execution of the policy actions, and

- A set of actions to be applied when the conditions are met, including:
  - Terminate a session
  - Request a subscriber's re-authentication
  - Trigger the involvement of another PDP
  - Trigger the activation of other policies (either Traffic Policies or Control Policies)

Downstream	The direction of data transmission from the regional network to the Access Node and from the Access Node towards the end user.
Upstream	The direction of transmission from the end user to the Access Node and from the Access Node towards the regional network.
Dynamic Policy Rule	Policy rule for which the definition is provided from the PDP to the PEP
Event report	A notification message sent from the PEP to the PDP, which includes information on an event that has occurred that corresponded to an event trigger
Event Trigger	Specifies the event reporting behavior of PEP. Event triggers may be unconditionally reported to PDP, or subscribed to by the PDP.
Policy Decision Point (PDP)	A logical entity that makes policy decisions
Local Policy Decision Point (LPDP)	A logical entity that makes local policy decisions independently but may ask a higher level PDP for overriding policy decision (Source: RFC 2753[15])
Policy Server	A physical device that contains the PDP entity and typically serves a number of PEPs. This device is usually a network server with PDP software, and can be dedicated to the purposes of PDP entity, or generalized and used for other purposes.
Policy Controller	See Policy Server
Policy Enforcement Point (PEP)	A logical entity that enforces policy decisions.
Policy	A set of rules which governs the behavior of a system.

Policy Rule	The combination of a specific condition(s) and action(s). For example, in the case of a Traffic Policy, the Policy Rule will specify a particular Traffic Flow condition(s) which when matched, results in the execution of the action(s) specified within the Policy rule.
Static Policy Rule	Policy rule on the PEP predefined via some type of provisioning, CLI or NMS/OSS system. Static, predefined policy rules could be activated / deactivated on the PEP by a PDP request to the PEP
Quality of Service (QoS)	Quality of Service refers to the different types of traffic delivery provided, and is described by parameters such as achieved bandwidth, packet delay, and packet loss rates. Traditionally, the Internet has only offered a Best Effort delivery service, with available bandwidth and delay characteristics dependent on instantaneous load. There are two different types of QoS: **Relative QoS**: A traffic delivery service without absolute bounds on the achieved bandwidth, packet delay or packet loss rates. It can still be used to handle certain classes of traffic differently from others. **Guaranteed QoS**: A traffic delivery service with certain bounds on some or all of the QoS parameters. These bounds may be determined by mechanisms such as RSVP. Other sets of bounds may be contractual, such as those defined in service level agreements (SLAs).
QoS on Demand:	The ability to request the QoS capabilities in near real time.. This includes both relative and guaranteed QoS. **NOTE:** Within this Technical Report the generic terms "QoS" and " QoS on Demand" will be used to describe the general concept of differentiated traffic delivery implemented by means of traffic parameters, without regard to any specific parameter or bound / guarantee. Wherever possible, the qualifying adjectives "Relative" and "Guaranteed" will be used when describing the needs of a particular service.
Session	There are four types of session: • Access Session: this is where the access link comes up and is available for data transmission. In the DSL case, this start when the DSL modem has trained up with the

	DSLAM, and with ANCP the DSLAM would then transmit a Port Up message to BNG • Subscriber Session: Layer 2 ALA Sessions, PPP Sessions and IP Sessions as defined in WT-146[28]. • Traffic rule session: this type is an abstraction of a set of policy rules. This would be used with an identifier to allow an operator to know if a particular "set of Traffic rules" is enabled or not without needing to know the underlying rule details. For example, an http redirect service would be a set of rules that allowed DNS traffic to be transmitted, redirected http traffic to a web portal, and dropped all other traffic. • Application Session: for example a voice call, a VOD session, a gaming session or a P2P session.
Service Data Flow	An aggregate set of packet flows that matches a specific criterion
Subscriber ID	Used to identify a specific subscriber.
Traffic Flow Filter	A set of packet flow header parameter values/ranges used to identify one or more of the packet flows constituting a service data flow. These can include: • Physical interface • Ethertype • Ethernet VLAN-ID, ATM VPI/VCI, MPLS label • Source/destination MAC address • Source/destination IPv4 or IPv6 address • PPPoE Session ID • 802.1p, DSCP, MPLS EXP • Source/destination TCP/UDP ports • Protocol type from the IP header • Other information included in each packet Each packet carries sufficient information to allow the determination of whether or not it matches a given flow definition. Only in the case of application-level criteria, might it be necessary to consider the correlation between several packets.
Traffic Flow Identifier	A Traffic flow Identifier is a given combination of the following criteria: • Physical interface • Ethertype

- Ethernet VLAN-ID, ATM VPI/VCI, MPLS label
- Source/destination MAC address
- Source/destination IPv4 or IPv6 address
- PPPoE Session ID
- 802.1p, DSCP, MPLS EXP
- Source/destination TCP/UDP ports
- Protocol type from the IP header
- Other information included in each packet

A traffic flow identifier is one type of condition used in a traffic policy.

Traffic Policy

A type of policy for which the execution trigger is the arrival of a data packet matching a particular condition, for which the action(s) constitutes some form of processing of this packet before it is forwarded to another device.

A traffic policy is defined by both:
A set of conditions which describe what traffic the policy must be applied to.
A set of processing actions to be applied when the conditions are met (security rules like allow/block or QoS/bandwidth-management policy like prioritize, shape, rate limit etc.)

2.4 Abbreviations

3GPP	3rd Generation Partnership Project
AAA	Authentication, Authorization, and Accounting
ACF	Admission Control Function
ADSL	Asymmetric Digital Subscriber Line
API	Application Program Interface
A-RACF	access-resource and admission control function
ASP	Application Service Provider
ATIS	Alliance for Telecommunications Industry Solutions
ATM	Asynchronous Transfer Mode
BNG	Broadband Network Gateway
BPCF	Broadband Policy Control Framework
BRAS	Broadband Remote Access Server
CPE	Customer Premises Equipment
DHCP	Dynamic Host Configuration Protocol

Diffserv	Differentiated Services
DMTF	Distributed Management Task Force
DSCP	Differentiated Services (Diffserv) Code Point
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
ETSI	European Telecommunications Standards Institute
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPSec	Secure Internet Protocol
ISP	Internet Service Provider
ITU-T	International Télécommunications Union - Telecommunication Standardisation Sector
L2TP	Layer 2 Tunneling Protocol
LDAP	Lightweight Directory Access Protocol
LSP	Label Switched Path
MAC	Medium Access Control
MPLS	Multi-Protocol Label Switching
NAPT	Network Address Port Translation
NGN	Next Generation Network
NSP	Network Service Provider
PPP	Point-to-Point Protocol
PPPoE	Point-to-Point Protocol over Ethernet
QoS	Quality of Service
RACS	Resource and admission control subsystem
RADIUS	Remote Access Dial-In User Service
RFC	Request for Comments
RG	Routing Gateway or Residential Gateway
RSVP	Resource reservation Protocol
SIP	Session Initiation Protocol
TMF	Tele Management Forum
TR	Technical Report (Broadband Forum)
VC	Virtual Circuit

VLAN	Virtual Local Area Network
VoD	Video on Demand
VoIP	Voice over Internet Protocol
VP	Virtual Path
VPN	Virtual Private Network
WT	Working Text
XML	Extensible Markup Language

3 Technical Report Impact

3.1 Energy Efficiency

TR-134 has no direct impact on Energy Efficiency. However time of day policies can shift usage patterns so that power demand peaks are reduced.

3.2 IPv6

TR-134 is required to support both IPv4 and IPv6 networks, and so the generic term IP Address is normally used which applies equally to both these address types. There are a few high level IPv6 specific requirements in Section 4.8 to emphasize the need for equal IPv6 support. Any version specific IP attributes (e.g. DHCP Option) are called out explicitly.

An IPv6 network can allow each end device in the customer network to have its own address which can be directly visible to, and accessible from, the Internet, as opposed to being hidden behind the NAT in an RG. This raises general security and privacy issues which are not uniquely related to Policy, but still apply in the Policy context.

As some Policy mechanisms use the IP address in flow identification and/or enforcement, IPv6 allows more granular Policy, i.e. (end-user) device based.

3.3 Security

There are several aspects of Policy which are related to security. Policy can be used to enhance security by both helping to recognize network attacks, and then carrying out defined counter-measures, such as port blocking or rate limiting.

However a Policy system implementation is typically distributed, and in particular there are likely to be multiple places where traffic conditioning can be enforced (at the PEPs). This raises a security issue in that there are now more points in the network that could be attacked, for example by installing rogue policies, with the aim of traffic disruption. Authentication of devices that communicate policy information is therefore needed, and protection of the messaging.

Depending on the nature and location of the PDPs, there may be a wider distribution of customer information throughout the network, which is always a security (and privacy) concern.

Finally one aspect of Policy is more sophisticated charging, and so there needs to be security to prevent Policy related fraud.

3.4 Privacy

As noted above, Policy can involve the distribution of customer specific information to more network nodes than is currently the case, in particular the PDPs. This includes both allowed and actual activities and usage, i.e. configuration and metering. This information may be both sensitive and private, for example TV channels watched, time spent on gaming, etc. Therefore

the Policy Framework needs to provide enhanced privacy (and indeed security) mechanisms to ensure that customer data cannot be misappropriated.

4 Business Requirements for Policy

A large number of high level business requirements for policy have already been captured in existing Broadband Forum documents, in particular TR-058[1], TR-059[2], TR-092[4], TR-101[6], TR-102[7], TR-144[9] and TR-147[10]. This section references and re-affirms these existing requirements while introducing quite a few new ones.

Much of this section is concerned with sessions, and while this can imply highly dynamic behavior, some types of session, for example access sessions, can be very long-lived. While the session construct is still useful in this case, this is more aligned with a static, provisioned model.

In addition to sessions, this section includes requirements on admission control, QoS and bandwidth management, security, AAA and charging.

4.1 Session-Based Policies

R-1. The BPC Framework MUST support policies that are associated with the following session types: access, L2, subscriber, and application sessions.

R-2. The BPC Framework MUST support interaction with session establishment.

R-3. The BPC Framework MUST support Policy Change requests from Applications after session establishment.

R-4. The BPC Framework MUST support policies that apply to individual sessions

R-5. The BPC Framework MUST support policy evaluation that is triggered by a change in state of a session.

R-6. The BPC Framework MUST support policies that apply to aggregates of subscriber sessions sharing logical interfaces, and/or layer 2 interfaces, and/or a physical access e.g. DSL loop.

R-7. The BPC Framework MUST support policies that apply to logical interface/layer 2 interface based on individual subscriber session policies when multiple subscriber sessions share a logical interface, and/or layer 2 interfaces, and/or a physical access e.g. DSL loop.

4.2 Wholesale Sessions

TR-059[2] and TR-101[6] provide support for multiple backhaul (e.g. A-10 interface) architectures including

- ATM
- Ethernet
- L2TP
- IP

Depending on the wholesale model employed, the regional Broadband operator may have limited ability to control the characteristics of the user's connectivity.

R-8. The BPC Framework MUST support the application of policies to L2 access sessions.

R-9. The BPC Framework MUST support the application of policies to subscriber sessions.

R-10. The BPC Framework MUST support ASP/NSP application requests for policy changes and resources from the network, without any knowledge of network topology and network state.

R-11. The BPC Framework MUST support ASP/NSP applications querying the status of policy changes and resource requests without any knowledge of network topology and network state

R-12. The BPC Framework MUST allow secure and controlled access by NSPs and ASPs to the Policy Control infrastructure

R-13. The BPC Framework MUST support policies for traffic associated with a specific A10-NSP interface and the associated backhaul tunnel.

4.3 Application Admission Control

The BPC Framework enables applications to participate in the allocation of network resources through signaling. The BPC Framework enables the operator to control the acceptance of application traffic into the network based on policy rules. The decision criteria that lead to an admission control decision may include both network and business rules.

A key aspect of a network based decision is information regarding the allocation of network bandwidth in those parts of the network where congestion can occur. The BPC Framework must support the use of this network resource based view, and business rules to determine if a particular application request can be honored.

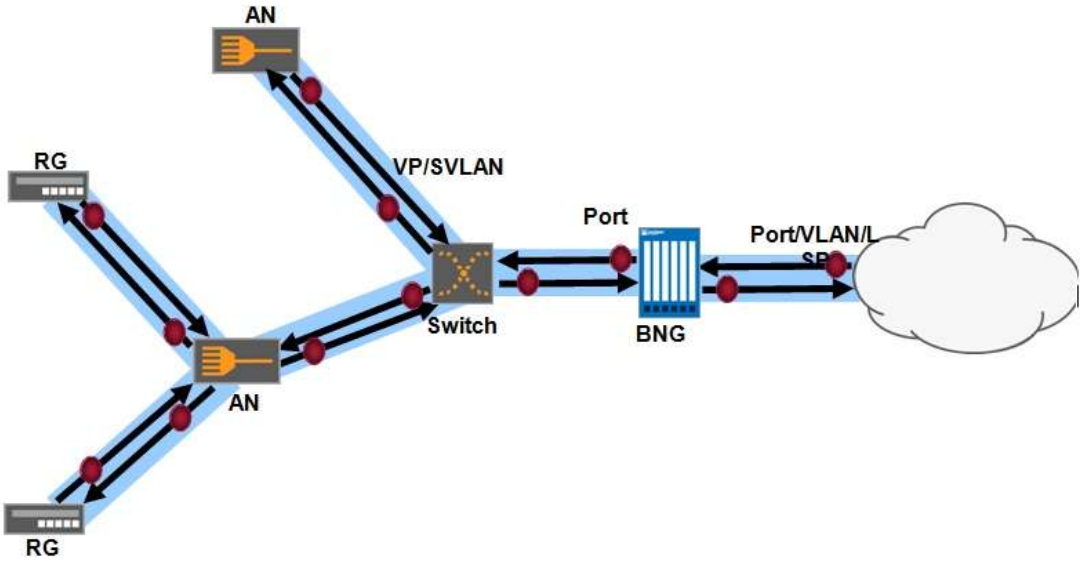


Figure 1 Application Admission Control

R-14. The BPC Framework MUST support policies that control traffic flows.

R-15. The BPC Framework MUST support network capacity admission control.

R-16. The BPC Framework MUST support pre-emption of existing reservations based on a priority scheme

R-17. The BPC Framework MUST support business authorization of application requests (time of day, group membership, etc.)

R-18. The BPC Framework MUST support activation of another policy as a condition of a first policy (e.g. in order to authorize a particular media flow, some charging policy must be activated). This is also known as nested policies.

R-19. The BPC Framework MUST support combining the following information when making admission control decisions for a new session:

- application requirements (e.g. bandwidth, QoS, etc.)
- available bandwidth for the subscriber based on the subscribers subscription
- current bandwidth usage
- network topology
- the available network capacity

Note: this does not necessarily imply real time measurement of network usage.

R-20. The BPC Framework MUST support a reservation model based on a provisioned, static view of the topology and bandwidth.

R-21. The BPC Framework MUST support a reservation model based on a dynamically learned view of the topology and bandwidth.

R-22. The BPC Framework MUST support bandwidth reservations in networks which have alternate traffic delivery paths (multipath).

R-23. The BPC Framework MUST support automatic re-establishment of bandwidth reservations impacted by network failure.

4.4 Session Resource Request initiation sources

R-24. The BPC Framework MUST supports any application type requesting policy changes and/or resources from the network.

R-25. The BPC Framework MUST be able to consider the status of available network resources.

R-26. The BPC Framework MUST support taking network events into account (e.g. events from Network elements).

R-27. The BPC Framework MUST support time of day and duration based policies and policy changes

4.5 Bandwidth

TR-059[2], TR-101[6] and WT-145[27] specify a variety of bandwidth management features. The BPC Framework enables policies to control the allocation of bandwidth resources in the access network.

R-28. The BPC Framework MUST support policies that control bandwidth allocation in TR-059[2], TR-101[6] and WT-145[27] based access network resources

4.6 QoS

TR-059[2], TR-101[6] and WT-145[27] specify a variety of L2 and L3 QoS features. The BPC Framework enables policies to allocate traffic flows to QoS classes in the access network, and supports the dynamic control of the set of active QoS policies.

R-29. The BPC Framework MUST support policies that control QoS in TR-059[2], TR-101[6] and WT-145[27] based access networks

4.7 Security

Broadband access normally includes network capabilities designed to protect the network from malicious users. The BPC Framework enables dynamic control over these features based on policies determined by the carrier.

4.8 IPv6 Support

The BPC Framework needs to be able to support the same traffic identification and filtering capabilities for IPv6 traffic as it does for IPv4.

R-30. The BPC Framework MUST support the use of IPv6 for communication between the various policy related network elements

R-31. The BPC Framework MUST support the use of the IPv6 header fields for the purposes of flow identification and policy enforcement.

R-32. The BPC Framework MUST support the use of IPv6 address management and allocation in the policy related nodes

4.9 Network Threat Detection

Policy may control the response of the network to threats such as flood attacks, security breaches or virus infection.

R-33. The BPC Framework MUST support policies that control response to any type of network intrusion event.

4.10 Multicast

Multicast is an important network capability which needs to be supported by the BPC Framework. Multicast replication policies, for example, are one way of allowing the carrier to specify how and where multicast replication will occur.

R-34. The BPC Framework MUST allow control over multicast replication for individual multicast groups

4.11 Routing

BBF TRs presume the existence of multiple network partners including retail service providers, network service providers, application service providers, as well as enterprise networks. The BPC Framework needs to allow control over the routing of access session traffic to and from each of these providers and networks.

R-35. The BPC Framework MUST support controlling routing policies for individual access sessions

4.12 Auditing, Service monitoring and Accounting

R-36. The BPC Framework MUST support logging of all transactions for the purposes of troubleshooting and security.

R-37. The BPC Framework MUST support the generation of Accounting information for the purposes of billing and non-repudiation

R-38. The BPC Framework MUST support the exchange of RADIUS and Diameter accounting messages with the AAA Server or network elements like the BNG.

Note: the BPC Framework could use the accounting start and stop radius messages as an

indication of subscriber log in and log out, and their binding to an IP address.

R-39. The BPC Framework MUST support the use of AAA RADIUS and Diameter attributes in the accounting messages for policy decisions.

The BPC Framework could use the AAA RADIUS or Diameter field attributes to identify the service attributes of each subscriber session, for example, 'Service-Type' Attribute.

4.13 Charging

There are several different charging models for service access. Support is needed for pre and post-paid services, as well as pay-per-use and subscription (flat-rate). This needs to address both the reporting of service utilization, and the enforcement of quotas related to time or volume.

R-40. The BPC Framework MUST support the use of the charging models defined in TR-058[1], TR-102[7] and TR-144[9].

R-41. The BPC Framework MUST support the use of charging models for the use cases in Section 5.4

R-42. The BPC Framework MUST support the identification of charging rules for the various charging models

For example, charging rules could be transmitted between functions to support charging for particular traffic flows.

4.14 Deep Packet Inspection

Broadband deployments increasingly include components that provide L4-7 deep packet inspection (DPI) so the BPC Framework needs to support this capability.

R-43. The BPC Framework MUST support interaction between DPI detection and enforcement functions.

R-44. The BPC Framework MUST support the use of L4-7 classifiers in defining traffic policy

5 Use Cases

This section contains seven high level use cases. The uses cases are used to describe the needs of Service providers and how they can be addressed using both provisioned and Policy based solutions. Most of the seven use cases contain a number of more specific sub uses cases. These sub use cases represent the originally contributed use cases, and they have been consolidated on the basis of the underlying network functions that are used to address them.

In this section, a TR-101[6] access network was used as the base architecture and is pictured below. Each node in this architecture has specific Policy Enforcement Point and QoS capabilities. The BRAS/BNG and RG are typically Layer 3 devices, and responsible for upstream and downstream QOS. The BRAS/ BNG and RG are also IP multicast replication points. The Access Node/DSLAM and Aggregation switch are layer 2 devices, but provide IP multicast replication points.

Please note the diagrams in this section show a nodal view with a Policy Server as the PDP. However the PDP could either be integrated into another network node, (for example, the BRAS/BNG, that may also contain a PEP function), or be a standalone function, in which case it is referred to as a Policy Server.

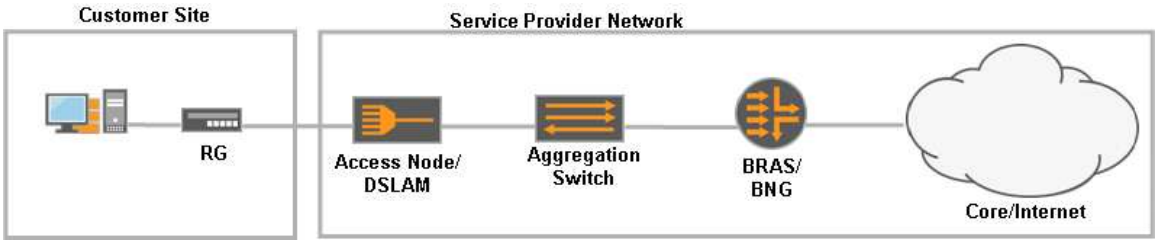


Figure 2 TR-101 Access Network topology

Each of the high level use cases has a range of possible solutions, and can be handled by using a range of static and dynamic methods for both provisioning and policy. The precise meaning of static and dynamic are defined in the context in each use case. Note that the use of these terms may or may not align with their use in other bodies.

5.1 Layer 1 – 4 and QoS based Policy

This use case encompasses the following more specific use cases:

- Bandwidth Boost for faster uploads or downloads
- QOS on Demand
- Applying Policy, QoS and session parameters via authentication
- Parental control or personal firewall
- Network infrastructure protection – denying access to particular parts of network (e.g. by filtering).
- Prioritization of particular traffic types into different traffic classes

5.1.1 Static Provisioning

In this approach, the Static Policy and or QOS configuration is provisioned locally using some type of Command line, or remotely using an NMS or OSS.

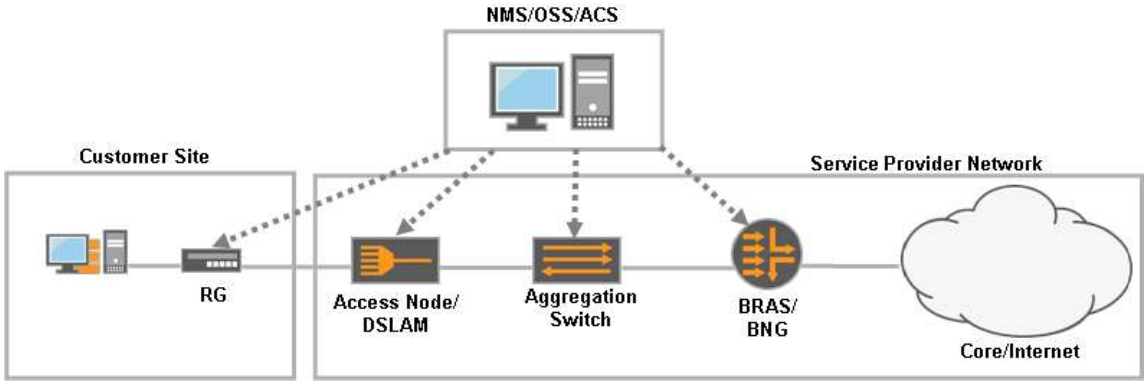


Figure 3 Layer 1 – 4 Policy and QoS using Static Provisioning

Table 1 Static Provisioning

Capabilities	All nodes are configured with a particular policy and QoS configuration which remains fixed until changed via an NMS, OSS or ACS. All necessary policy and QoS configuration attributes are held locally within the nodes. The approach is particularly efficient when there is no need for frequent or real time configuration changes
Limitations	Policy or QoS configurations cannot be changed in real time. The 'permanent' installation of a subscriber-specific Policy or QoS configuration (e.g. subscriber profile) into a Node makes it difficult to support nomadism and network rearrangement.

5.1.2 Static Pull from an AAA Server

Here a static Policy and QOS configuration is provisioned when a PPP or IPoE session is started on a BRAS/BNG. The Policy and QOS configuration is provided as part of the RADIUS Access accept message in response to a RADIUS Access Authentication Request message for that session.

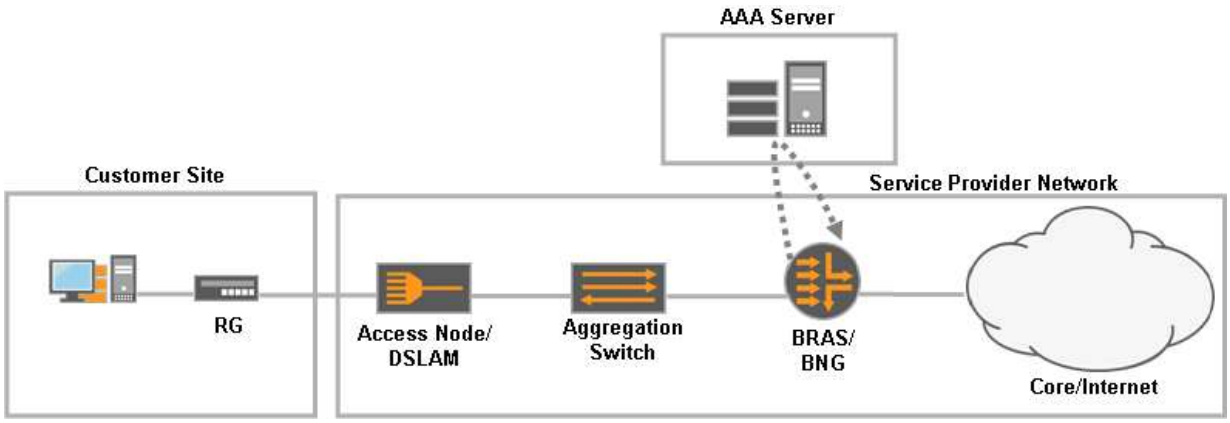


Figure 4 Layer1-4 Policy and QoS using Static Pull

In this example static Policy is provisioned on the access line on the AN/DSLAM via an ANCP (RFC 6320[26]) interaction with the BNG, and then an AAA interaction between the BRAS/BNG and AAA Server. As specified in TR-147[10], the BNG/BRAS sends a Port Configuration Request to an AN to configure the Multicast ACL Policy on the local loop access port. The BRAS/BNG is triggered to send the Port Configuration Request by the establishment of a PPP, PPPoE or IPoE session.

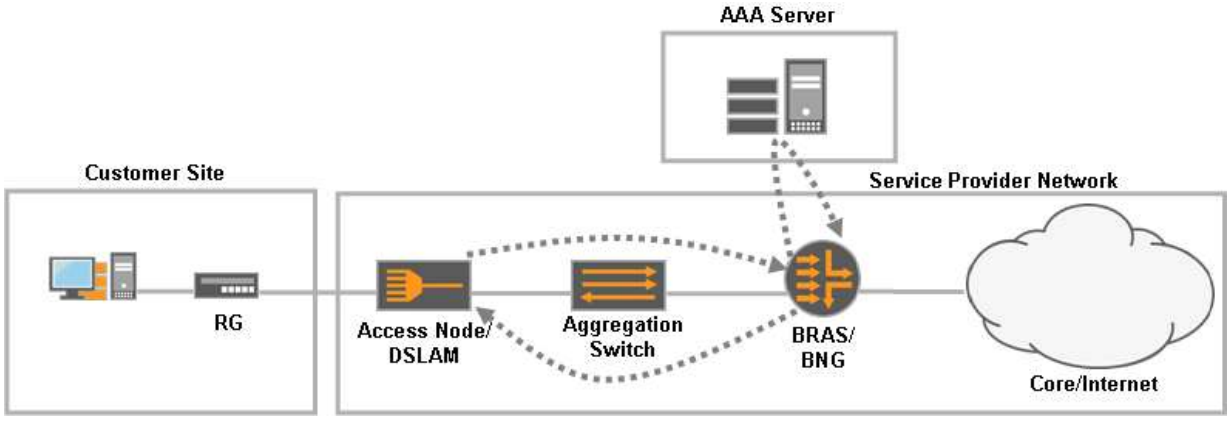


Figure 5 Layer1-4 Policy and QoS Static Policy provisioning on access line via ANCP

Table 2 Static Pull from AAA Server

Capabilities	Policy and QoS configuration are held in an AAA Server. Allows Policy and QoS configuration information to change as a result of events related to subscriber sessions: typically the start or end of a PPP or IP session, but also other events such as the change of DSL sync rate or a new multicast membership. This can be used in conjunction with Static Provisioning. This method can be used to overcome the limitations mentioned in Table 1.
Limitations	Where triggering a Policy or QoS update requires the session to be dropped

	and re-established, this can cause application communication issues. The addition of COA (RFC 5176[25]) capabilities would avoid a session drop and therefore overcome this limitation. See the PDP methods for RADIUS COA capabilities.

5.1.3 Dynamic Push from a Policy Decision Point

This is an example of a dynamic push from Policy Server. For example Radius COA messages use this type of push from the Policy Server to a BRAS/BNG.

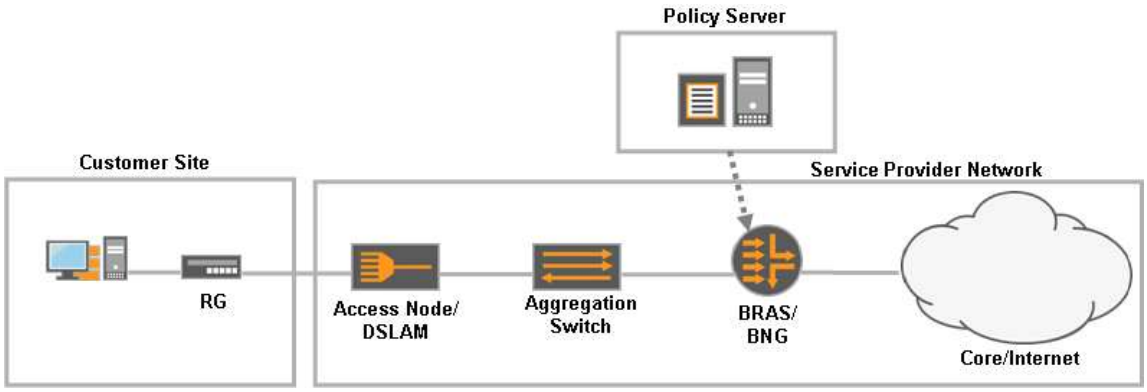


Figure 6 Layer1-4 Policy and QoS Dynamic Push

Table 3 Dynamic Push from a PDP

Capabilities	Allows applications and subscribers to interact directly or indirectly with Policy Decision Points to allow real time changes to be made; for example a subscriber could interact with a Web Portal and request additional bandwidth. There is no need for sessions to be dropped and re-established. This type of deployment can be used in conjunction with the Static Provisioning and/or Static Pull with AAA Server method
Limitations	Increases the complexity of a network as it requires the deployment of policy decision points, their interaction with other elements of the network (e.g. subscriber profile repository) and the support of control interfaces in the Network nodes.

5.1.4 Dynamic Pull from a Policy Decision Point

This is an example of a dynamic pull whereby the BNG retrieves Policy and QoS configuration information from a PDP, triggered by a network event.

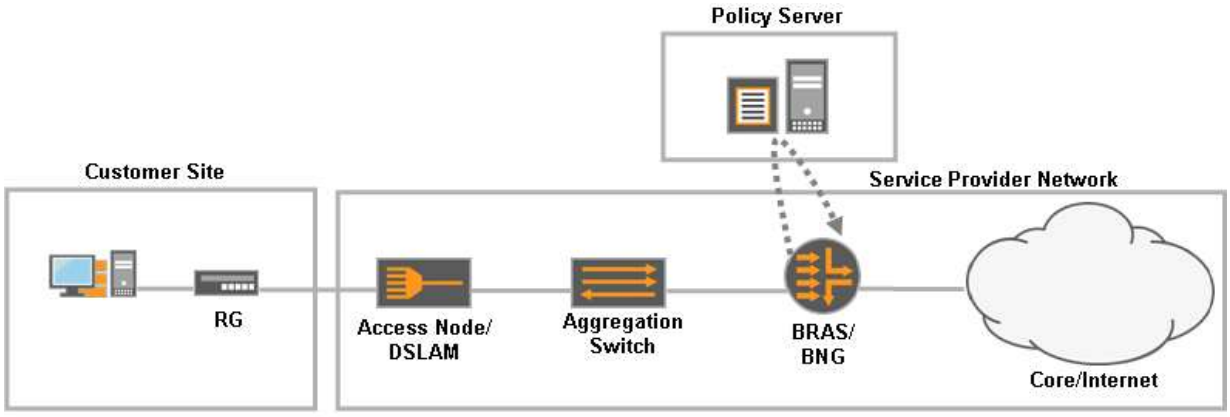


Figure 7 Layer1-4 Policy and QoS Dynamic Pull from PDP

Table 4 Dynamic Pull from PDP

Capabilities	Allows BRAS/BNG to pull the required Policy and QoS information dynamically from a Policy Decision Point in response to a network event such as a change on the local loop.
Limitations	Same as in Table 3

5.2 Layer 4 – 7 Traffic Policy

This high level use case encompasses the following more specific use cases:

- Associating video streaming over HTTP with a given QoS Class
- Redirecting HTTP traffic to provide Web based authentication
- Redirecting HTTP traffic to notify subscribers of service suspension due to non payment
- Redirecting HTTP traffic to provide self-service registration for new subscriptions
- Network based Web filtering to protect children from harmful or objectionable content

The TR-101[6] architecture does not define a node or function to prioritize or recognize application level traffic – it simply uses the traditional IP five tuple classification. Therefore a TR-101[6] BNG would not be able to distinguish between web page traffic transported over HTTP on TCP port 80, and Video traffic transported over HTTP on the same TCP port.

The diagrams below include this function as a separate node, but it could also be integrated into an existing network element such as a BNG or RG. This function will be referred to as deep packet inspection or DPI. Note that the DPI function could be integrated in a new network node, or added to an existing node e.g. the BRAS/BNG.

5.2.1 Static Provisioning

In this example the Static Policy and/or QOS configuration is provisioned locally using some type of Command line or remotely using some type of NMS or OSS system.

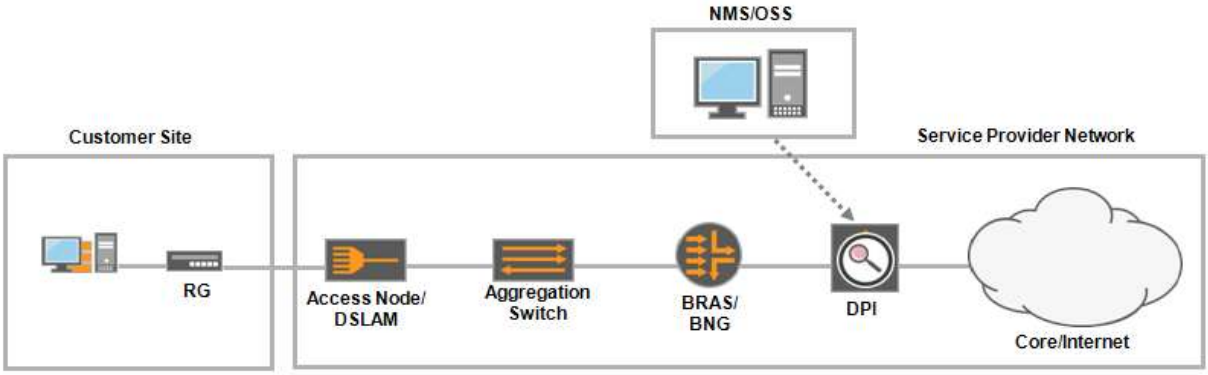


Figure 8 **Layer 4 – 7 Static Provisioning**

Table 5 Layer 4 – 7 Static Provisioning

Capabilities	DPI nodes are configured with a particular policy and QoS configuration and this configuration remains fixed until changed via an NMS, OSS or ACS. All necessary policy and QoS configuration attributes are held locally within the DPI nodes. The approach is particularly efficient when there is no need for frequent or real time configuration changes
Limitations	Policy or QoS configurations cannot be changed in real time. The HTTP Redirect to provide Web based authentication or self service registration cannot be achieved using this method due to their real time requirements. The 'permanent' installation of subscriber-specific Policy or QoS configuration (e.g.: subscriber profile) into a Node may make it difficult to support nomadism.

5.2.2 Static Pull from an AAA Server

In this example a static Policy and QoS configuration is provisioned when the DPI recognises a new application flow, or sees a new Source IP address. The Policy and QoS configuration is provided as part of the RADIUS Access Accept message in response to a RADIUS Access Request message.

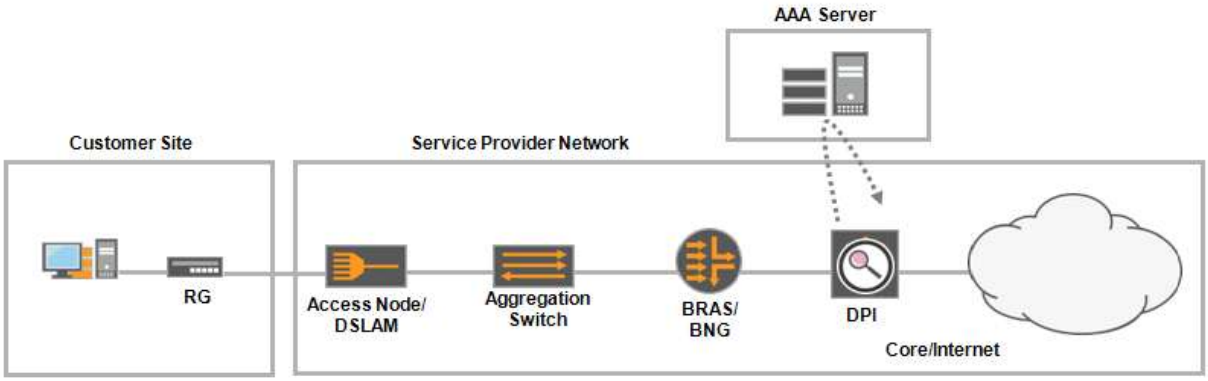


Figure 9 Layer 4 – 7 Traffic Policy Static pull from AAA Server

Table 6 Static Pull from AAA Server

Capabilities	The policy and QoS configuration are held in an AAA Server. Can support HTTP Redirect to provide Web based authentication and self service registration. Allows Policy and QoS configuration information to change as a result of application flow detection. Can be used in conjunction with Static Provisioning. Can be used to overcome nomadism limitations mentioned in Table 5.
Limitations	Unable to apply Policy or QoS changes without a DPI trigger, but the addition of COA capabilities would avoid this limitation. See the PDP methods for RADIUS COA capabilities.

5.2.3 Dynamic Push from PDP

This is an example of dynamic push from a PDP. For example Radius COA messages use this type of dynamic push from a PDP to a DPI function.

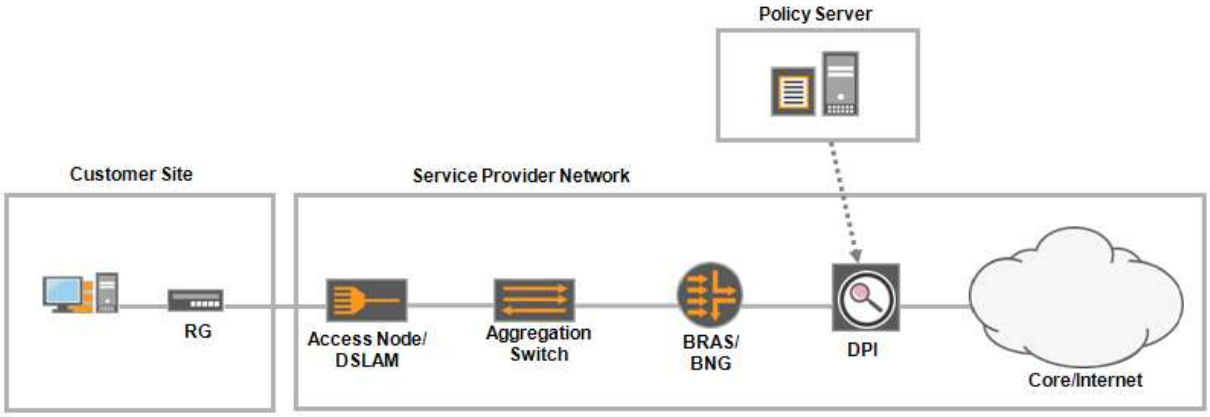


Figure 10 Layer 4 – 7 Traffic Policy using Dynamic Push from PDP

The capabilities and Limitations are exactly the same as in Table 3

5.3 Call Admission Control

This high level use case encompasses the following more specific use cases:

- Admission Control for Video on Demand
- Admission Control for unicast and multicast video on the access line
- Admission Control for unicast and multicast aggregates between the Access Node and BNG

The following diagrams show nodal views with the Admission Control Function (ACF) integrated into OSS/BSS, Policy Server, Access and BNG nodes.

The purpose of Admission Control is to protect the network from overload conditions by having application functions (and/or network triggers) request resources before the associated traffic flows begin. These requests are accepted, or denied, based on the available network resources, the status of such previous requests and operational parameters of the network operator.

The diagram below displays a number of potential congestions points in the network that the Admission Control Function could take into account (see Section 4.3and Figure 1). It is not expected that admission control would be needed on all links, rather only on those where congestion could occur.

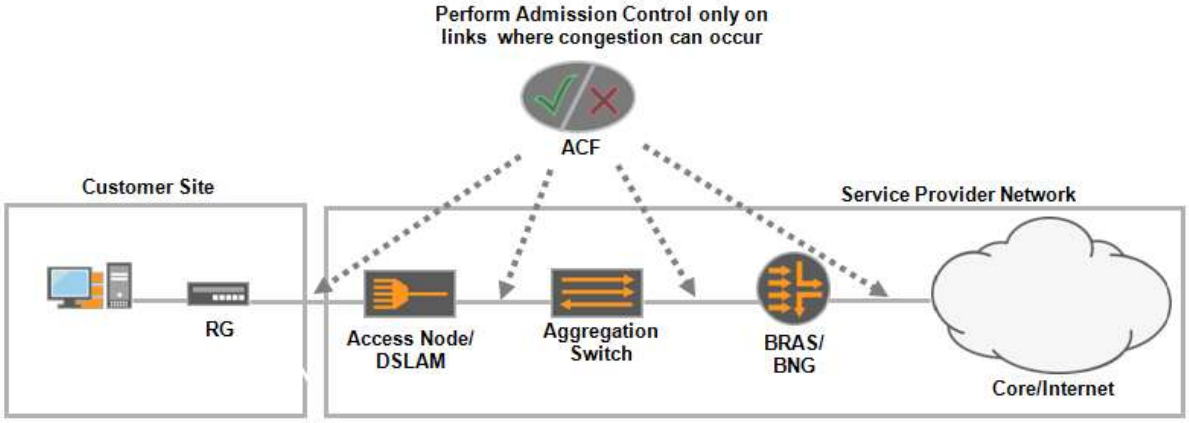


Figure 11 Call Admission Control Links

The TR-101[6] architecture does not define a node or function to perform Admission Control (for unicast or multicast traffic). Further, TR-101 does not define a particular Video or IPTV infrastructure. This use case assumes there is some type of Middleware or Application for Video on Demand.

There are various Admission Control deployment options.

5.3.1 Non-network based Admission Control

In this example, Admission Control is not performed by a Policy server, but by a support system, or the applications themselves. A BSS or OSS could perform Admission Control at the time of a service registration request by preventing a customer from subscribing to a service that their local access loop could not support – e.g. not being able to provide HD video over some ADSL1 loops.

An application or middleware can also implement an Admission Control function. For example, a Video on Demand server could simply keep track of the number of VOD sessions, and deny further sessions once a certain number had been reached, without any interaction with the network layer. In this case, network topology and bandwidth information could be provisioned into the VOD Server infrastructure and used in making the Admission Control decision.

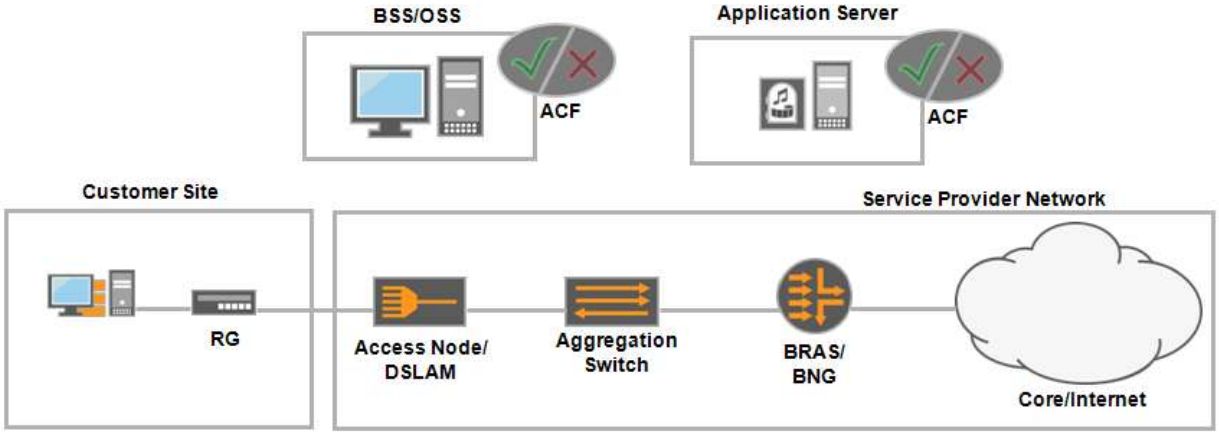


Figure 12 Application, middleware or BSS based Admission Control

Table 7 Application, middleware or BSS based Admission Control

Capabilities	Each application, middleware or BSS handles its own Admission Control without regard to the needs of other applications. Admission Control may or may not have awareness of network resources.
Limitations	Admission Control for multiple applications may not work without pre-partitioning bandwidth. Therefore it may lead to fragmentation of committed bandwidth.

5.3.2 Distributed Network based Admission Control

In this example, Admission Control requests for Unicast are handled by an Admission Control Function that is part of a Policy Server, whereas the Access Node handles Admission Control for Multicast.

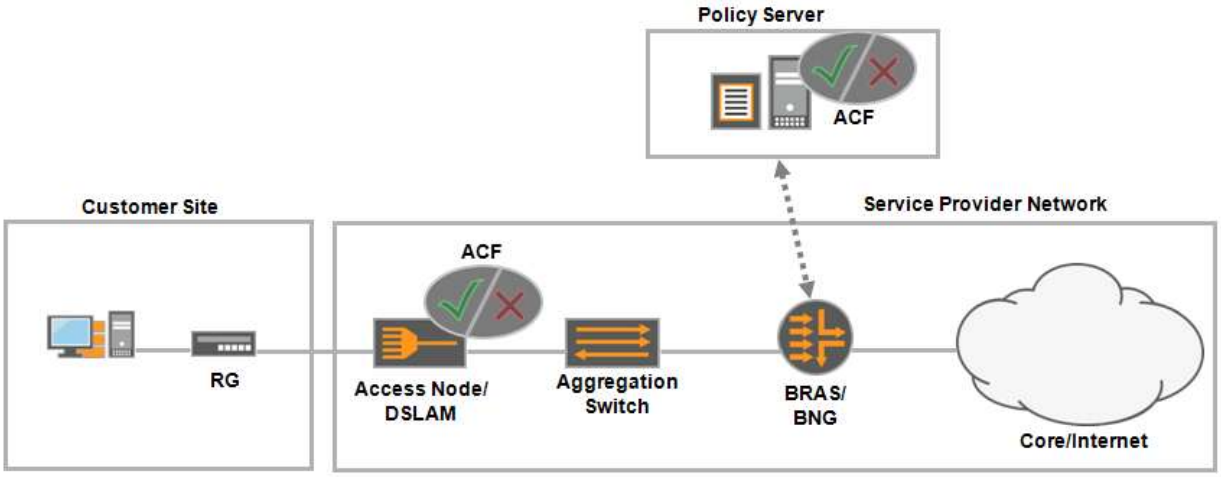


Figure 11 Distributed Network based Admission Control

Table 8 Distributed Network based Admission Control

Capabilities	This decoupling allows more sophisticated unicast admission control to be performed in the PDP, and multicast admission control to be done in the Access Node, thereby reducing multicast channel change latency.
Limitations	It is difficult to perform Admission Control for both Multicast and Unicast without signalling or partitioning bandwidth.

5.3.3 Coordinated Admission Control -

As in the above, multicast Admission Control is in the Access Node and unicast Admission Control is in the PDP However the two Admission Control functions are now coordinated. The below diagram shows two ways in which this could be achieved.

In the first, Admission Control functions on the Access Node and the Policy Server interact directly. In the second, these two functions communicate via the BNG.

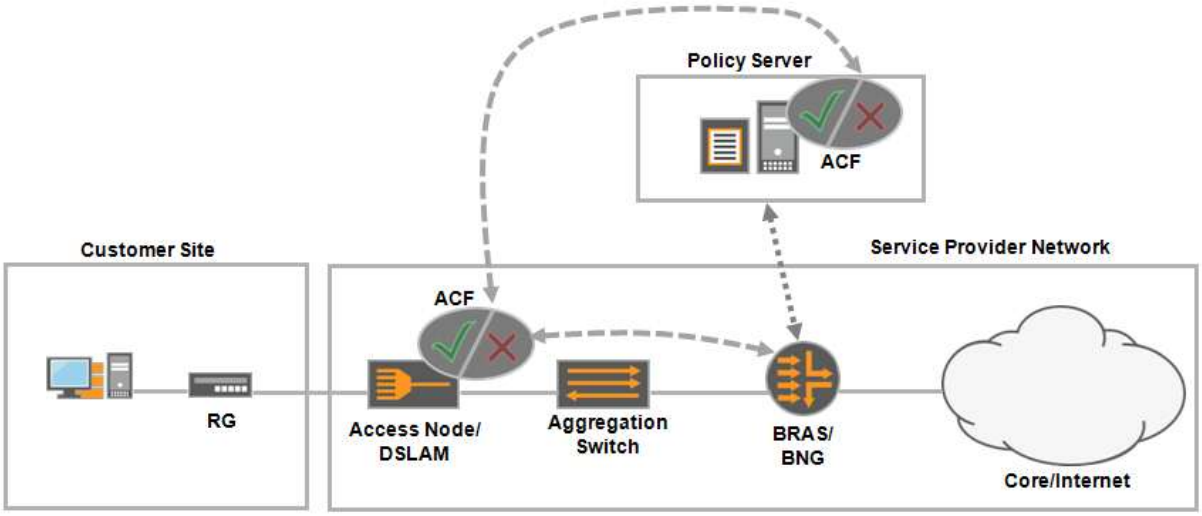


Figure 13 **Coordinated Admission Control**

Table 9 Coordinated Admission Control

Capabilities	Admission Control requests can be coordinated between ACFs and so avoid bandwidth partitioning. This allows a trade-off between bandwidth partitioning and the amount of signalling. Having Multicast Admission control in the Access node reduces channel change latency.
Limitations	Applications need to be able to send unicast requests to the Admission Control function on the PDP, and signalling between ACFs is required.

5.3.4 Admission Control for a Meshed Topology

In this example the Unicast Admission Control requests are again handled by the Admission Control Function that is part of the BNG with the Access Node handling Multicast Admission Control. However, the Access node and BNG are now connected over a more complex, meshed topology and it would be more difficult for the Policy Server to understand the available network resources. Admission control requests would be sent from the access network to the BNG via a network signalling protocol. It is expected that the on-path signalling would be hop-by-hop processed to handle this complex mesh topology.

In the diagram below the Admission Control functions on the Access Node and the Policy Server interact to eliminate the need to partition bandwidth.

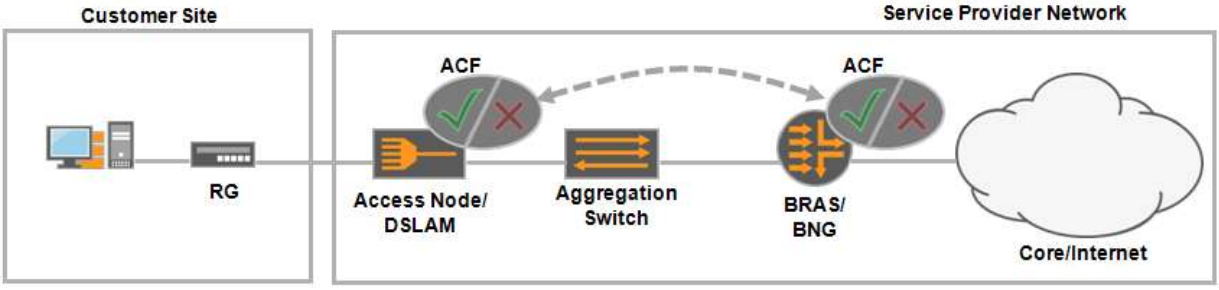


Figure 14 Meshed Topology Admission Control

Table 10 Meshed Topology Admission Control

Capabilities	All Unicast Admission Control requests can be handled and coordinated by the Admission Control function in the BNG. This type of deployment would allow for more complex meshed access networks to be used between the Access node and BNG. Additionally, the access network topology would not need to be provisioned into the Policy server, or learned via interaction with the BNG. Having Multicast Admission control in the Access node reduces the latency in making the resource decision.
Limitations	Applications behind the RG or the RG itself need to use a network signalling protocol to send resource requests to the access network. Coordinated communication between the ACF in BNG and ACF in the Access Node would be required to avoid bandwidth partitioning between unicast and multicast Admission Control

5.4 Authentication, Metering and Accounting Policy Use case

This general use case encompasses the following more specific ones:

- Traffic usage metering and accounting
- Traffic usage metering and accounting based on traffic destination
- Authentication policy that includes line authentication
- Bandwidth Fair Use policy
- QoS and accounting for Value added Services
- Volume Quota Control per subscriber

5.4.1 Static Provisioning

In this example, the Policy, QOS, session parameters, metering and accounting parameters are all provisioned locally using some type of Command line, or remotely using an NMS or OSS. All accounting data is sent to the AAA Server, typically using RADIUS accounting.

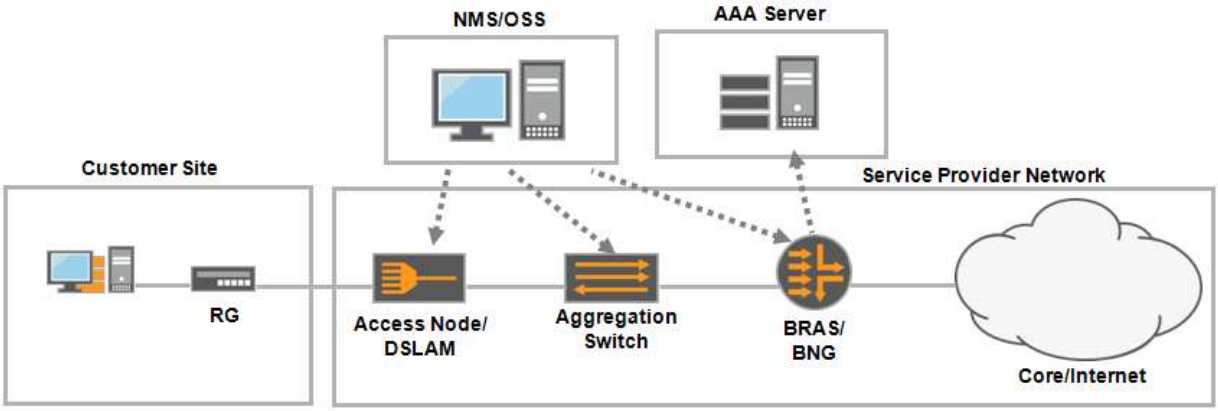


Figure 15 Authentication, Metering and Accounting Policy using Static Provisioning

The Capabilities and Limitations are the same as in Table 1, except that the Policy provisioning here includes the setting up of accounting tools.

5.4.2 Static Pull with an AAA Server

In this example Policy, QOS, session parameters, metering and accounting configuration are provisioned when a subscriber session starts on the BRAS/BNG. The configuration information is provided as part of the RADIUS Access Accept message in response to a RADIUS Access Request message for the subscriber session. All accounting data is sent to the AAA Server, usually in a RADIUS accounting message.

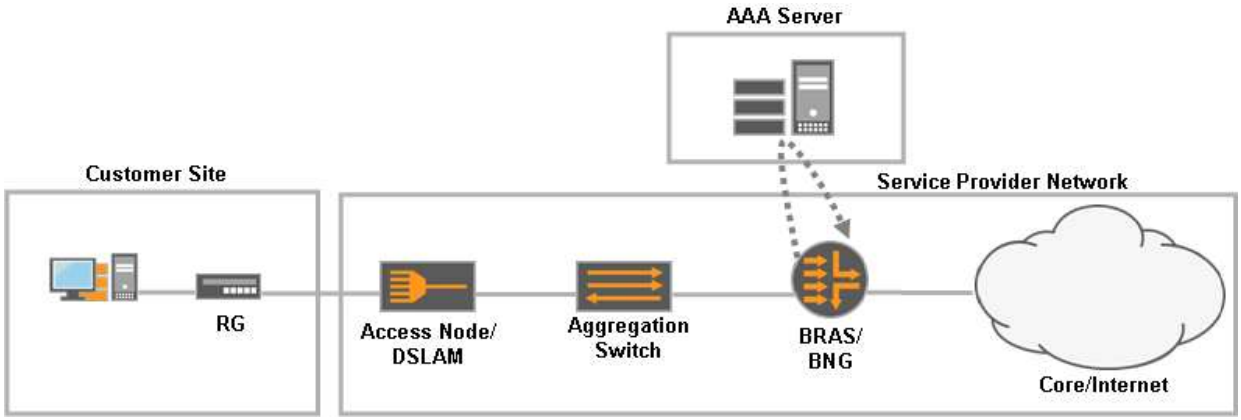


Figure 16 Authentication, Metering and Accounting Policy static pull with AAA Server

The Capabilities and Limitations are the same as in Table 2, except that Policy provisioning here includes the setting up of accounting tools.

5.4.3 Dynamic Push – With Policy Decision Point

This is an example of a dynamic push from a Policy Server. Radius COA messages are used for this type of dynamic push from a Policy Server to a BRAS/BNG.

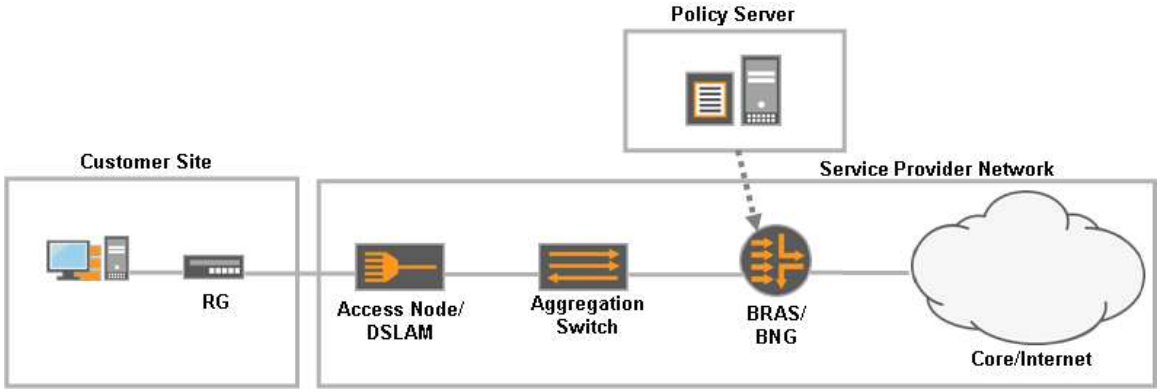


Figure 17 Authentication, Metering and Accounting Policy Dynamic push with PDP

Table 11 Dynamic Push with PDP

Dynamic Push with PDP	
Capabilities	Allows updates of Policy, QOS, session parameters, metering and accounting configuration information without requiring the subscriber session to be re-established. For example if a subscriber hit a particular meter limit, the PDP could push changes to Policy, QOS, session parameters, metering and accounting configuration. This could enable the subscriber to increase their subscription quota before continuing, or acknowledge an increase in charging. This type of deployment can be used in conjunction with Static Provisioning.
Limitations	Same as Table 3

5.4.4 Dynamic Pull with a PDP

This is an example of a dynamic pull from the service provider network.

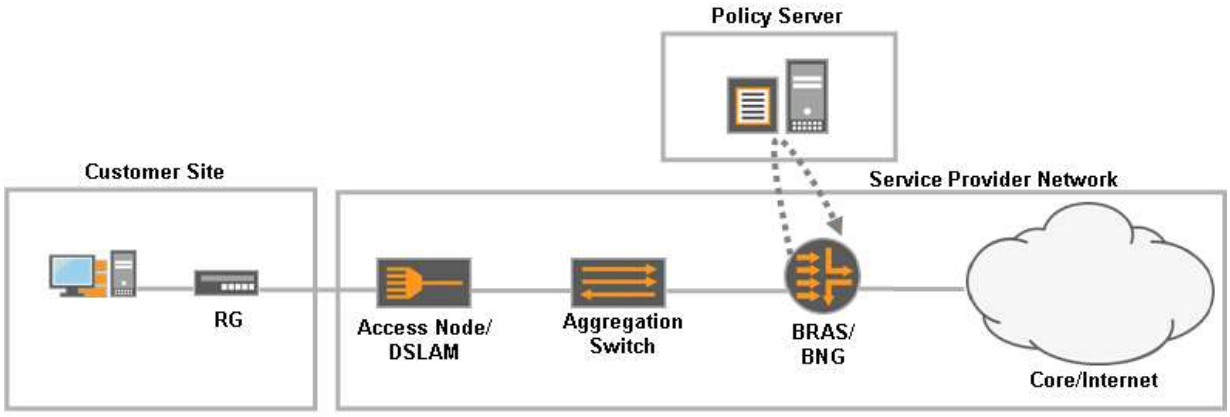


Figure 18 Authentication, Metering and Accounting Policy Dynamic Pull

Table 12 Dynamic Pull with PDP

Capabilities	Allows the BRAS/BNG to pull the required Policy and QoS information dynamically from a Policy Decision Point in response to an accounting event, such a subscriber reaching a usage threshold.
Limitations	Same as Table 4

5.5 Home Gateway use case

This high level use case covers changing upstream Policy and QoS on the RG WAN interface. TR-069[3] is used to push Policy and QoS configurations changes for the WAN interface of the Residential Gateway.

5.5.1 Static Provisioning on the home gateway

This is covered by the methods described in Section 5.1.1.

5.5.2 Dynamic Push – With PDP

In the figure below, the Policy Server interacts with the ACS as currently defined in TR-069[3] in order to make a Policy and/or QoS configuration change on the RG. The Policy Server and ACS can be separate devices as shown in the diagram, or integrated into a single network node.

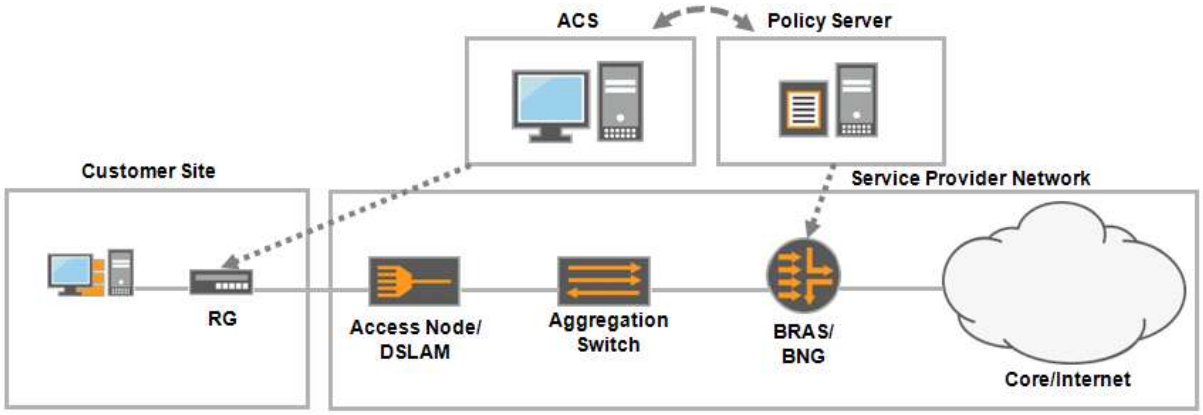


Figure 19 Home Gateway Use case With Policy Server and ACS

Table 13 Dynamic Push with PDP and ACS

Capabilities	Allows applications and subscribers to interact directly or indirectly with Policy Server to allow dynamic changes to be made for both upstream and downstream policy and QoS. For example a subscriber would interact with a game system and this game system would request additional bandwidth for a short period of time. There is no requirement for sessions to be dropped and re-established (or network-driver triggers to occur).
Limitations	Same Limitations as Layer1-4 Policy and QoS Dynamic Push with Table 3

5.6 Application Layer Policy

This high level use case covers Application Servers making Policy and QoS configuration requests as a result of subscriber interaction. Example applications include video streaming, gaming, video conferencing and VoIP.

The TR-101[6] architecture does not define an application server node or function that would interact with applications and then send requests to a Policy Server. This application server could for example be a Softswitch or Rich Communications Server.

TR-102 [7] does however provide a view of application interaction with TR-101 QoS capabilities, and while some details of these interactions may now be dated, Section 3/TR-102 (*Operational Application Framework Context),* remains a good introduction to access sessions,

business models, and flow classification capabilities. These concepts provide a valuable background for understanding TR-101 architecture QoS capabilities.

The diagrams below have added this server application function as a separate node, but it could also be integrated into existing network elements. This function will be referred to here as an Application Server or AS.

5.6.1 Static Provisioning

In this example the Static Policy and/or QOS configuration is provisioned locally using some type of command line or remotely using some type of NMS or OSS.

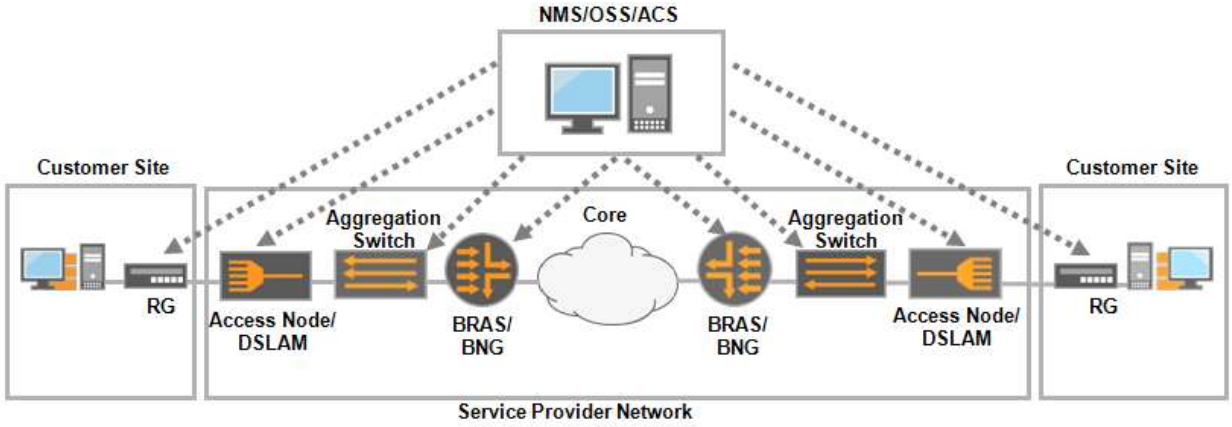


Figure 20 Application Layer with Static Provisioning

This model has the same Capabilities and Limitations as in Table 1

5.6.2 Dynamic Push with PDP

This is an example of a dynamic push from a Policy Server.

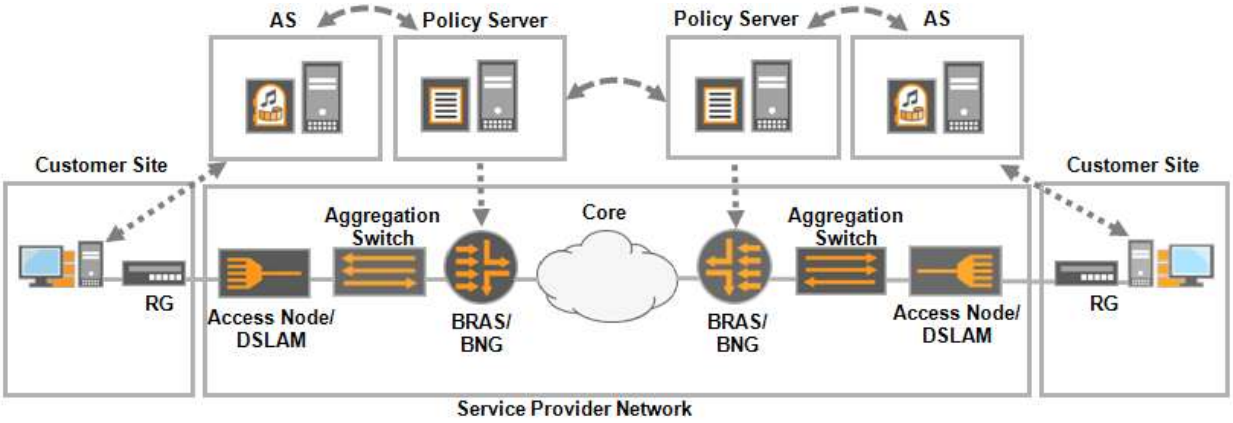


Figure 21 Application Layer Use Case with Dynamic Push from PDP

In this model, there can be a two-step Policy and QoS change. The first step would be reservation of the required resources (which may involve negotiation). In the second step, Policy and QoS parameters are installed before the application data flows start. This two-step process needs to happen at both ends of the connection, and the above picture illustrates this happening with two separate Application Servers and Policy Servers.

Also note that ANCP can be used to notify the BNG of the local loop bandwidth from the Access Node, and the BNG would then notify the Policy Server. This notification could be used when deciding how to handle Application Server Policy and/or QoS change requests.

This model has the same Capabilities and Limitations as in Table 3

5.7 Emergency Services Use Case

This high level use case encompasses the more specific use cases:

- National Emergency: A user has a device and is registered with an "early responder" profile. The user places an emergency call in situations where an early response is required, and is given the highest priority on the available resources.
- Local Emergency: An E911 user has a device and is registered with an "E911" profile. The user places an emergency call which is associated with a priority level just below a National Emergency user, but above everyone else

The TR-101[6] architecture does not provide a facility to identify and authenticate end devices. In particular, when end devices are behind a Layer 3 Residential Gateway, a TR-101 network is not capable of informing the service provider when a specific registered device joins or leaves the network. The ability to identify and authenticate end devices is assumed, but no solution to this requirement will be described. The service layer can provide the required information when devices register with the service.

5.7.1 Static Provisioning

This is covered by the methods described in Section 5.1.1.

5.7.2 Dynamic Push with PDP

This is an example of a dynamic push from a Policy Server. This is triggered by a device registering with an application function, for example a softswitch or IMS P-CSCF. This is covered by the methods described in Section 5.1.3.

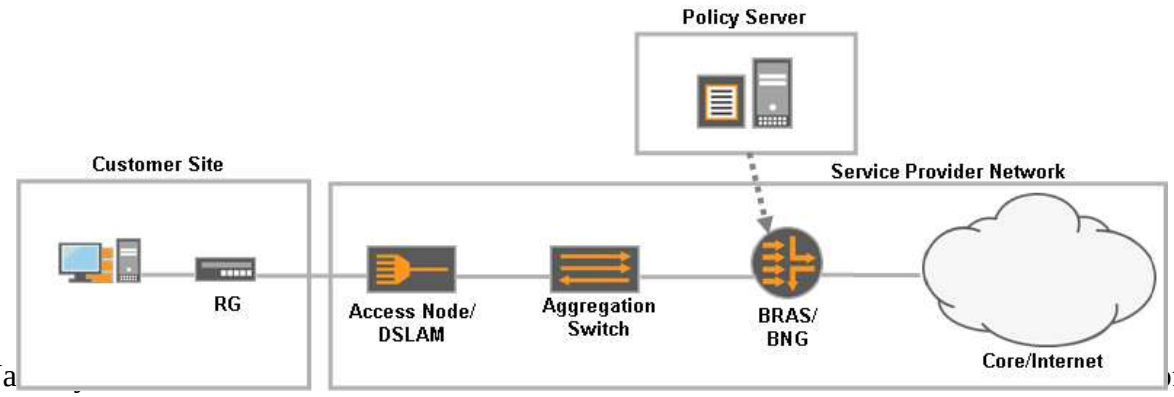


Figure 22 Emergency Services with Dynamic Push from PDP

This model has the same Capabilities and Limitations as with Table 3 Dynamic Push from a PDP

6 Functional Architecture elements

In TR-058[1], the Broadband Forum defined a three level logical and physical architecture to support advanced services. This architecture contains both mandatory and optional functionality that allows advanced QoS-enabled services. The three levels are the Application layer, the Common enabling Services layer and the Network layer.

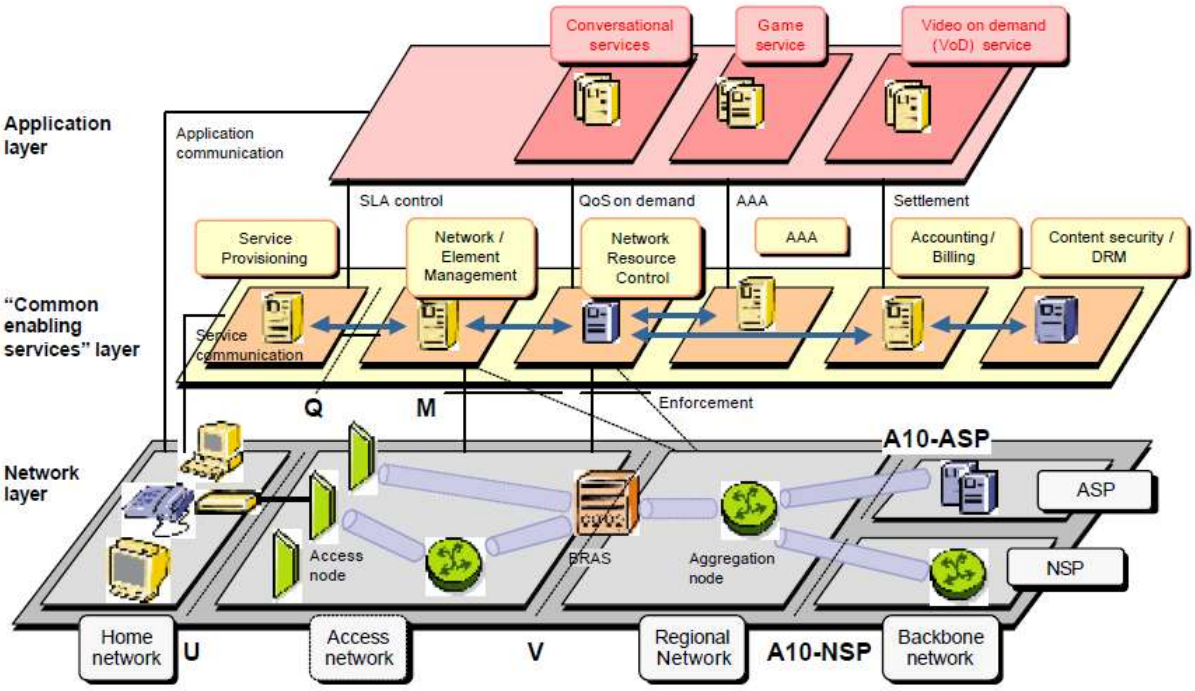


Figure 23 Source: Figure 4/TR-058

This high level physical and logical architecture is used as the backdrop for development of a logical policy architecture within this TR. A range of possible Policy architectures will be considered, but without defining a specific required architecture.

As a result of these considerations, normative requirements were defined for various functional entities. The section concludes by mapping this high level functional architecture onto the Physical architecture of TR-101[6], and the functional architecture of WT-145[27].

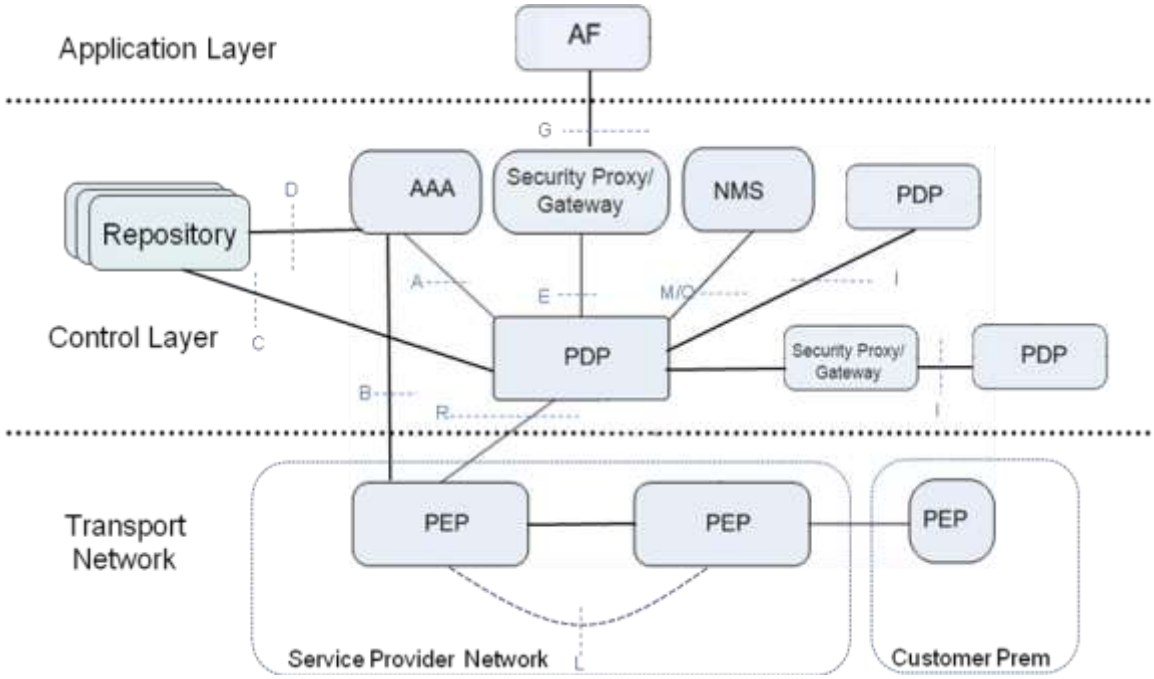


Figure 24 BPC Framework Interface Architecture

The logical interfaces and functional entities found in Figure 24 will be later defined and used in the sections below.

6.1 BPC Framework Functional Architecture

R-45. The BPC Framework MUST support architectures in which the PDP functionality can be centralized, or distributed in various physical and nodal locations.

R-46. The BPC Framework MUST support a centralized PDP functionality which sends policy enforcement commands to multiple Policy Enforcement Points.

The Centralized deployment functional architecture typically supports the situation where a single operator is responsible for providing both the Access Network and ISP services; this allows that operator to make all service policy based decisions.

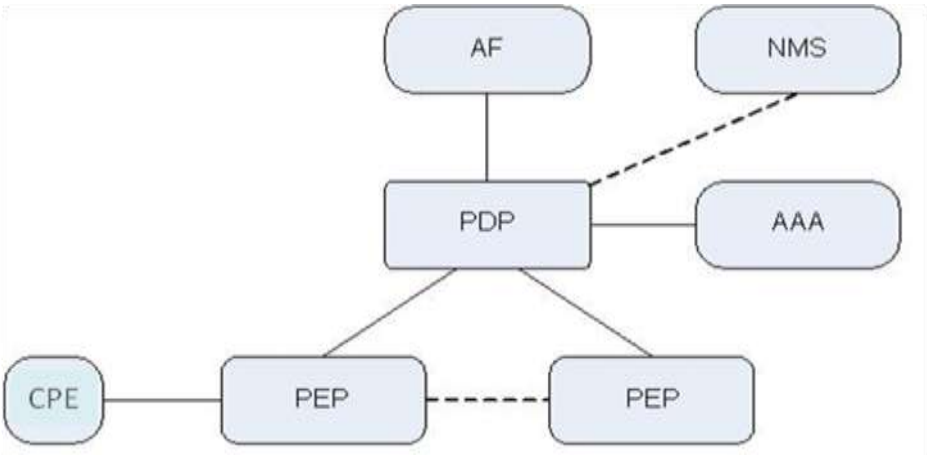


Figure 25 BPC Framework Centralized Deployment Functional Architecture

R-47. The PDPs MUST be able to interact to support end-to-end control for the purposes scaling and or spanning different network administration boundaries.

R-48. The BPC Framework MUST support multiple PDPs, where each PDP is responsible for making policy decisions for a predefined network domain (geographical, administrative wholesale, or retail).

R-49. The BPC Framework MUST support multiple PDPs, where each PDP is responsible for making policy decisions for different PEP types or PEP functions.

The interactions and relationships between multiple PDPs are for further study.

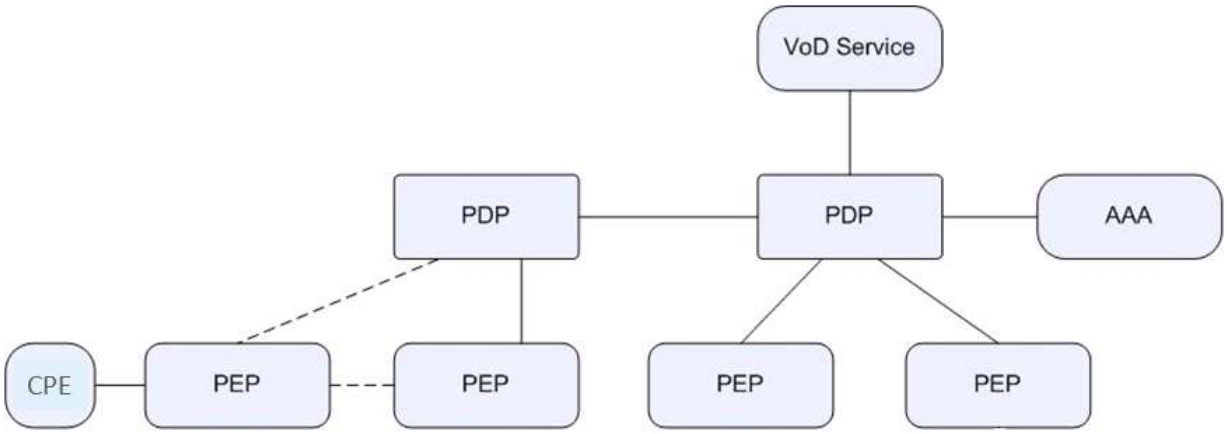


Figure 26 BPC Framework Distributed Deployment Functional Architecture

R-50. The BPC Framework MUST support the acceptance or rejection of requested policy changes.

R-51. The BPC Framework MUST support a single policy request being able to configure multiple individual sessions.

R-52. The BPC Framework MUST support a mechanism for communicating policy requests and decisions that is secure against spoofing, hijacking and DoS attacks.

R-53. The PDP logical entity SHOULD be able to interact with an Application Server to allow dynamic real-time changes of policy for both upstream and downstream traffic, e.g. a QoS change.

R-54. The PDP MUST be able to communicate with the NMS/OSS, AAA Server, AF, Repository and other PDP(s) to facilitate making policy decisions.

6.2 Policy Enforcement Point (PEP)

The Policy Enforcement Point (PEP) is a logical entity that enforces policy decisions. The Policy Enforcement Point is responsible for traffic policy enforcement of unicast and multicast traffic types. Policy Enforcement may be applied at an IP Session, IP Flow and aggregate level.

R-55. The BPC Framework MUST support policy enforcement for both downstream and upstream traffic.

R-56. The PEP logical entity MUST be able to enforce policy for unicast and multicast traffic

R-57. The PEP MUST be able to apply policy on Access Sessions, L2 Sessions, Subscriber Sessions and Traffic rule session.

R-58. The PEP MUST be able to receive policy information from the PDP over the R interface.

R-59. The PEP MUST be able to request policies from the PDP over the R interface.

R-60. The PEP MUST be able to be directed to receive/activate/modify/delete policies from the NMS/OSS over M/Q interface

R-61. The PEP MUST be able to be directed to receive/activate/modify/delete policies from AAA Server over the B interface.

6.3 Policy Decision Point (PDP)

The Policy Decision Point (PDP) is the logical entity that makes policy decisions The PDP makes decisions on subscriber policies on Access Sessions, L2 Sessions, Subscriber Sessions and Traffic Rule sessions. A PDP may manage multiple PEPs, coordinating what policies should be enforced at each PEP. The PEP may have static policies. The PDP may inform the PEP to apply a set of policies to a given session.

R-62. A PDP MUST be able to connect with another PDP(s) over the I interface. Examples of where this might be required include the case where multiple domains are involved, or when functionality is delegated from one PDP to another.

R-63. The PDP MUST be able to make policy decisions for Access Sessions, L2 Sessions, Subscriber Sessions and Traffic Rule session

R-64. The PDP MUST be able to provide policy decisions for multiple PEPs.

R-65. The PDP SHOULD be able to retrieve subscriber information from a Repository or AAA Server function

R-66. The PDP SHOULD be able to install/activate/deactivate/modify/remove Policies in the PEP, and allow dynamic changes of policy for both upstream and downstream traffic.

6.4 Admission Control Function (ACF)

The ACF performs an admission control and resource tracking procedure upon receipt of a specific request related to the network domain for which it is responsible. Such a request can be new, or to modify an existing reservation. The ACF performs this process based on its view of its network domain, and the resource usage therein. As a result, policies in PEPs may be installed, activated, de-activated, removed or modified. Prioritized applications, such as emergency calls, may require the ACF to pre-empt existing resource reservations.

The admission control process may or may not involve multiple network elements (Access Node, BNG, RG, Policy Server, etc), either in concert or independently

R-67. The ACF MUST be able to make admission decisions based upon network resources and business policies.

Note that the ACF is only shown in the use case section but no interfaces specific to this function are exposed.

6.5 Repository Function

The Repository Function is a data store, usually some type of database. This is used to store User profiles, subscriptions and policies, configuration information and network topology information, which is then used by PDP and AAA functions.

6.6 Security Proxy/Gateway function

Where service providers have different administrative domains, or interact with other NSP(s) and/or ASP(s), it is necessary to provide a control point where security features are used to control access to underlying Policy control and ultimately transport network resources. For example, the Security Proxy function would take care of the BPC Framework requirements R-10 – R-13.

6.7 Application Function(AF)

The Application Function provides a service that requires policy control.

6.8 AAA Server Function

The AAA Server function replies to AAA Client Authentication, Authorization and Accounting requests.

6.9 BPC Framework Policy Control Framework Interfaces

The interfaces shown in Figure 24 BPC Framework Interface Architecture are between:

A	The PDP and AAA Server function.
G	The AF and Security/ Proxy/Gateway Function.
E	The Security/Proxy/Gateway Function and PDP
I	PDPs in the same or in different network domains. Depending on the relationship between the operators controlling the PDPs and whether it is intra- or inter-domain, security/gateway functionality may be needed e.g. to hide topology.
R	a PDP and PEP. The detailed information model for the R Interface is in Section 7
C	The Repository function and a PDP.
D	The AAA Server function and Repository function.
M/Q	EMS/NMS and PDP and other network functions as defined in WT-145

6.10 BPC Framework PCF Deployment Functional Architecture Mapping onto TR-101 Functional Architecture

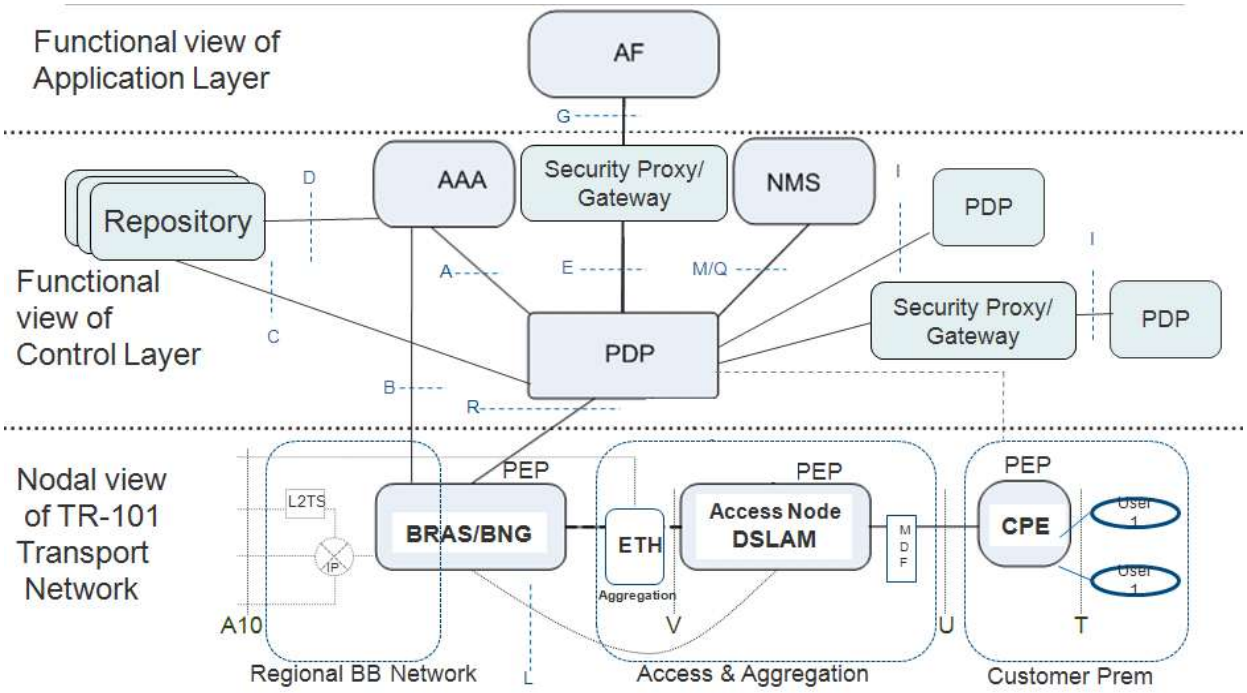


Figure 27 BPC Framework Interface Architecture mapping onto the TR101 Architecture

This figure shows the BPC Framework PCF Interface and functional distribution mapping onto the TR-101[6] Nodal Architecture. It illustrates which transport node elements in TR-101 could implement policy control elements such as the PEP and PDP.

6.10.1 BPC Framework Mapping onto WT-145 Functional Architecture

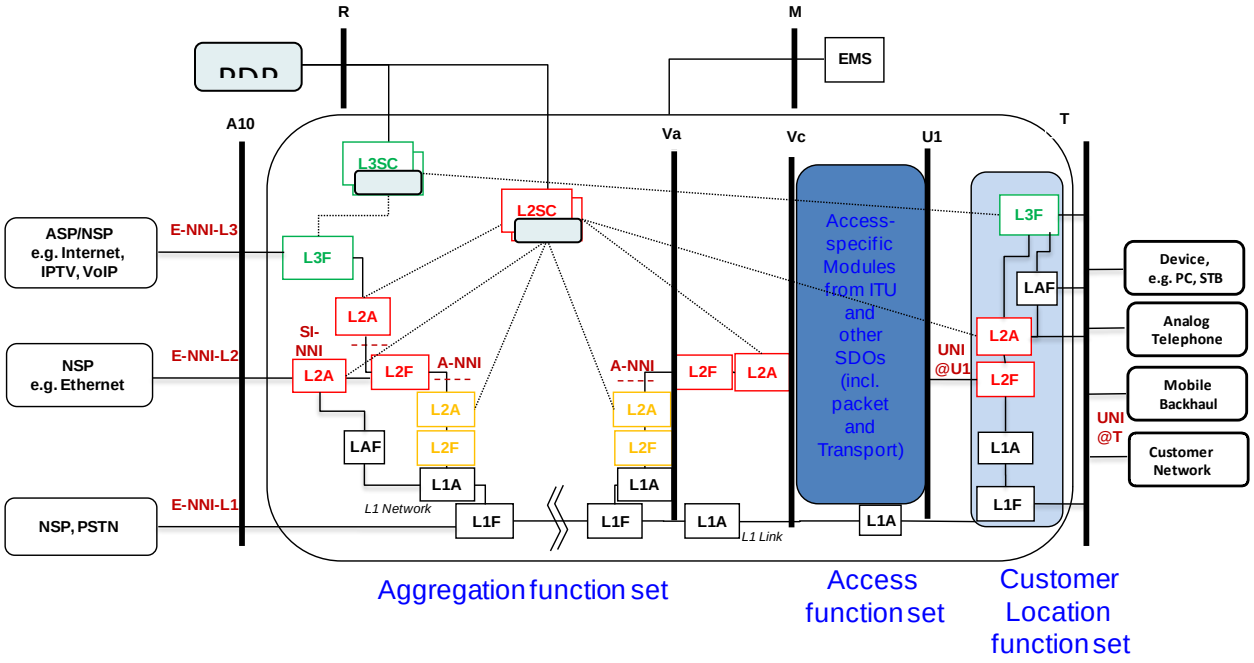


Figure 28 BPC Framework Mapping onto WT-145 Functional Architecture

Figures 28 show how the interfaces and functional entities of the BPC Framework are mapped onto the WT-145[27] functional architecture. Figure 28 also shows that the Policy PDP interacts with NSP's and ASPs through a Northbound interface (G), and interacts with Regional and Access networks through a Southbound interface (R).

6.11 Informative AAA implementation examples

6.11.1 Standalone AAA implementation

This example shows a standalone AAA Server that embodies the functions defined in RFCs 2865[16] and 2866[17]. Thus, in the language of RFC 2865, this is a RADIUS server example. This implementation does not include any integrated Policy Decision function. The AAA Server will accept, and reply to, RADIUS authentication, authorization and accounting requests. The AAA server function can act as a proxy client to other AAA server functions, or other kinds of authentication servers.

Note than an AAA Server could be a Diameter server (as per RFC 3588[22]).

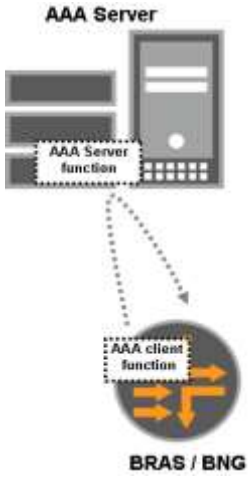


Figure 29 Standalone AAA implementation

6.11.2 Combined AAA/PDP implementation

This example shows a combined AAA Server and Policy Decision Point (PDP). This type of implementation is also known as a Policy server. When the AAA Server is processing authentication, authorization and account requests it will also apply additional business logic before responding to the AAA client function. Not authorizing a request at a particular time of day is one example of such business logic.

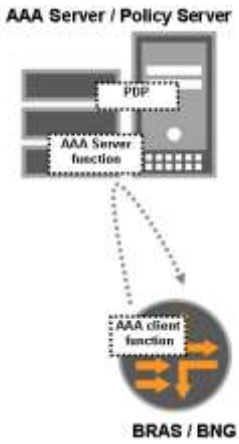


Figure 30 Combined AAA/PDP implementation

6.11.3 Interaction and flow possibilities between the BNG, AAA, PDP & repository functions

Here are two examples of how the BNG, PDP, repository of user data and AAA could interact to notify the PDP of a particular access session (IPoE or PPP) starting and stopping on the BNG.

Option 1: the AAA performs an AAA proxy function and forwards AAA accounting Start and Stop messages to the PDP.
Option 2: the PDP performs the AAA Accounting function itself; there is no separate AAA.

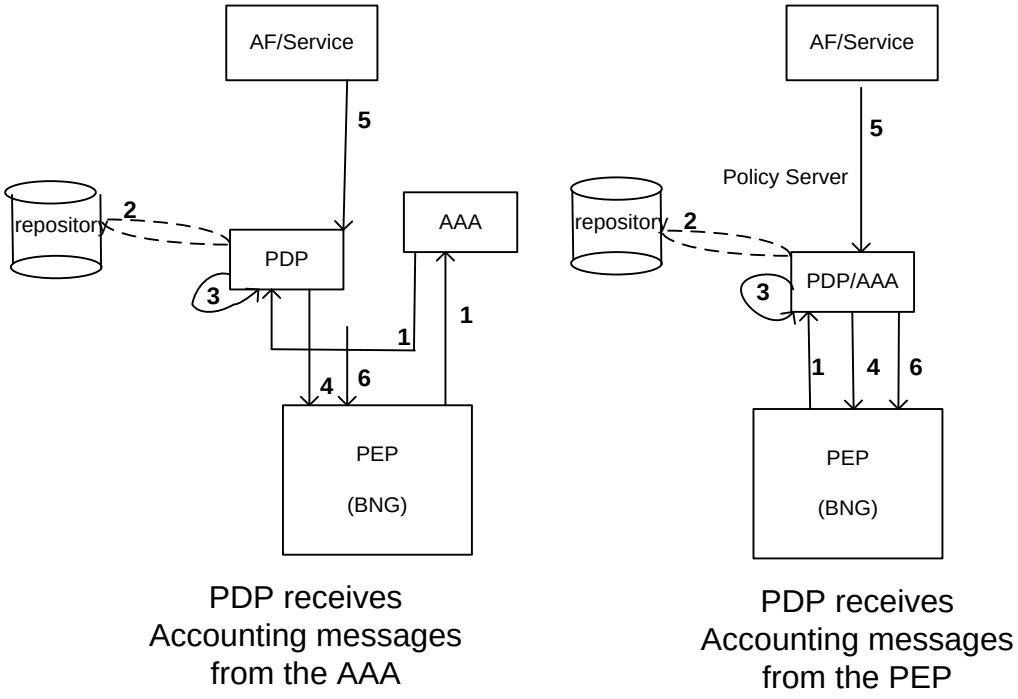


Figure 31 Interactions and flow possibilities between BNG, AAA, PDP & repository functions

Process description:

Login Session:

1) The BNG sends an accounting start message to the AAA, and then the AAA sends an accounting start message to the PDP. Alternatively, the BNG could send an accounting start message directly to the PDP

2) The PDP retrieve supplemental data from the repository (optional)

3) The PDP makes a login policy decision

4) The PDP sends an enforcement command to the BNG.

Service session:

5) The service request is sent from the Application Function to the Policy server PDP
6) PDP makes decision and send resource change command to the BNG enforcement point

6.12 Informative PEP/PDP implementation examples

6.12.1 Centralized Policy Implementation

In a Centralized Policy Deployment, there is one (or a small number of) policy server(s) that control and interact with multiple PEPs embedded in various network nodes.

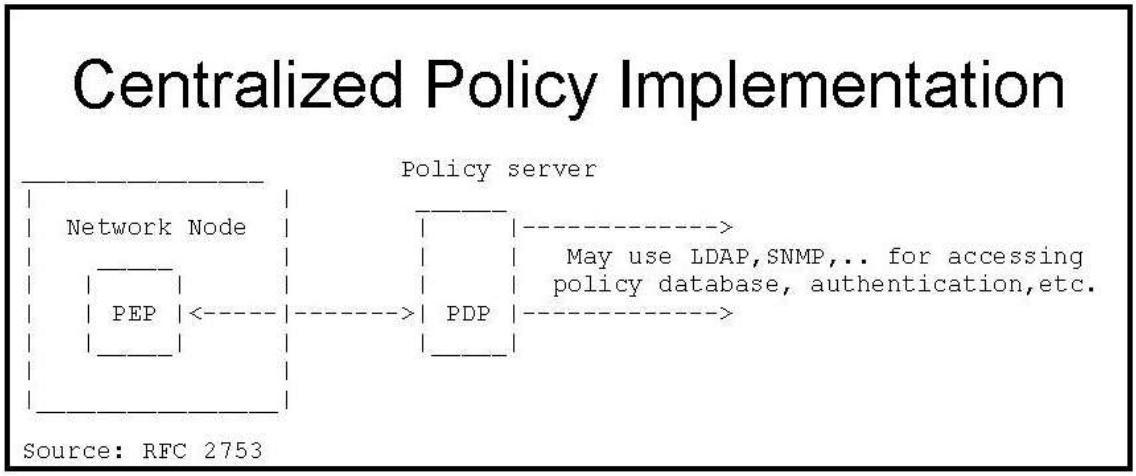


Figure 32 Centralized Policy Implementation

6.12.2 Integrated Policy Implementation

In this case, the PEP and PDP entities are located in same device e.g. a network node such as a BNG or Access node. This type of implementation allows network nodes to make policy decisions for themselves.

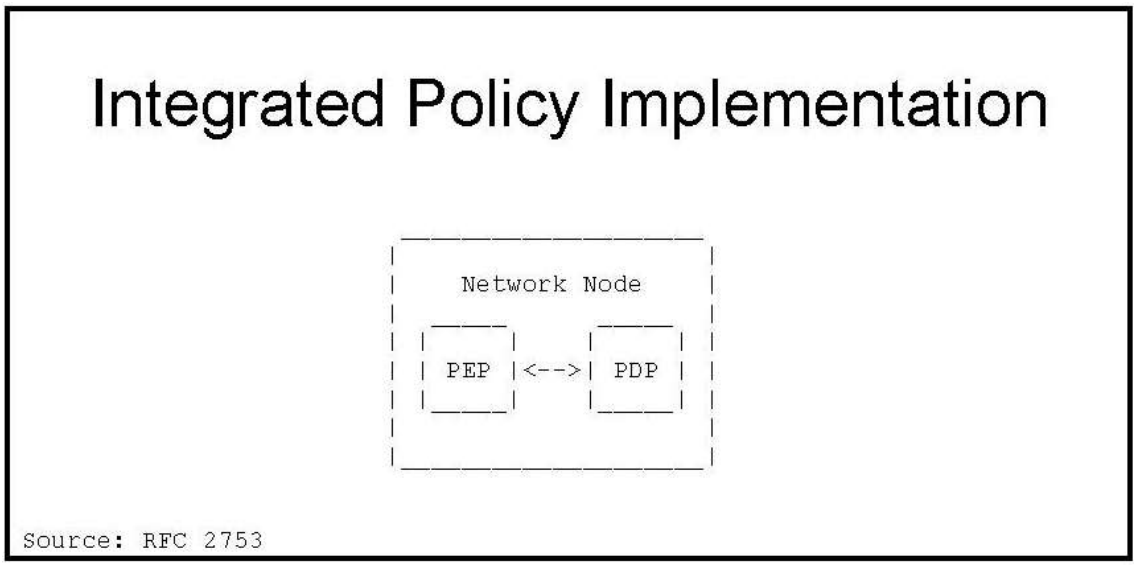


Figure 33 Integrated Policy Implementation

6.12.3 Distributed Policy Implementation

In this case, the Local PDP(LPDP) entity is introduced, as well as a more centralized PDP located on a Policy Server. The LPDP can make local decisions, or pass some of the decisions to a higher level PDP.

In the below diagram (reproduced unaltered from RFC 2753[15]), the LPDP and PDP do not communicate directly.

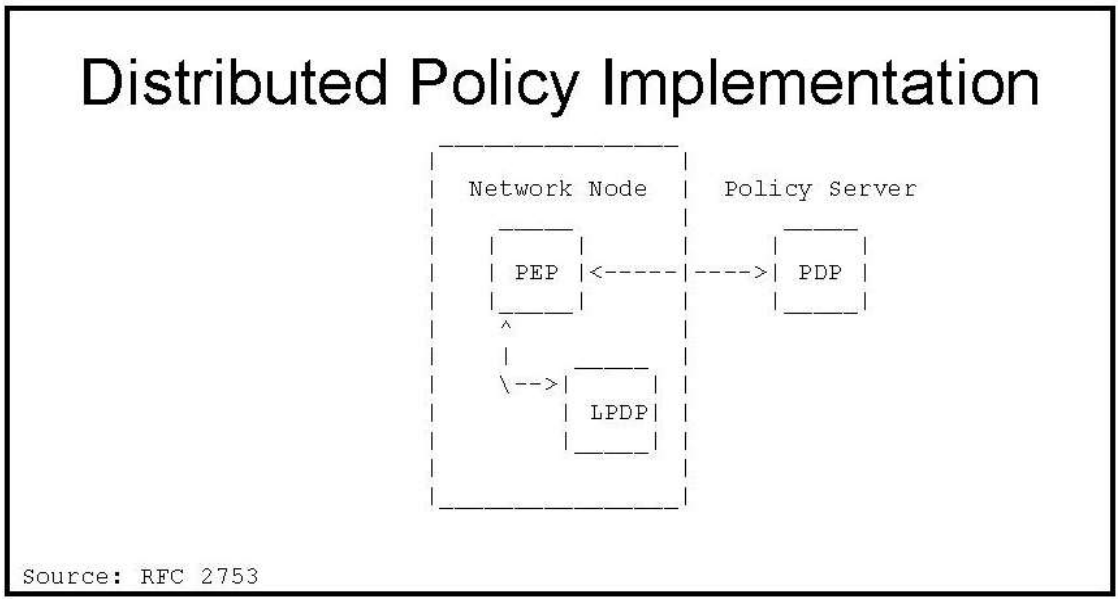


Figure 34 Distributed Policy Implementation

7 Policy Information Flows

This section describes information flows, and introduces a set of information elements that can be exchanged in these flows. Information Models are for further study (see Annexes).

7.1 Information Flow Objectives

The ultimate objective of the Policy Information Flow structure is to support the development of nodal requirements for individual functional elements in the Broadband Network Domain. Each functional element will need to support the receipt and processing of various types of policy information. This processing may or may not include admission control functionality

The identification of policy information flows and exchanges is vital to the development of functional element requirements. The policy information model and the resulting information flows must support the following:

- All identified Use Cases adopted by the Broadband Forum within this Technical Report, TR-144[9] and WT-145[27]
- All business requirements found in Section 4, and those in TR-144.

7.1.1 Policy Information Flow Structure

The Policy information flow structure is as follows. Each wireline Broadband Network Logical Function requires a set of information to perform its task. Each function receives information from one or more information sources. These sources could be signaling interfaces, including those that have been defined by other SDOs. They could also be other logical functions in the broadband network domain. These sources in turn provide information in the form of parameters/attributes to the logical functions. The information flow structure is as follows:

- Network Logical Function – Function responsible for implementing part of the policy of the wireline broadband network domain. The function will have defined characteristics such as:
  - Function Type – Policy Decision Point (PDP), Policy Enforcement Point (PEP) or other.
  - Function Hierarchy – Centralized or Distributed Policy Source (as per Section 6.1)
  - Location – Network element that could host the function. Note that any logical function could be hosted in different types of network elements.
- Information Source which can be:
  - A Logical Function in the Broadband Network Domain
  - An entity beyond the Broadband Network Domain that is reached via standardized signaling interfaces or other interfaces
  - A proprietary data source.

  Note that multiple Information Sources can feed information to any given Network Logical Function.

- Parameters/Attributes – Information that needs to be processed by the logical function for the application of the network policy. These parameters are transported to the Network Logical Function from the Information Source and have characteristics such as:
  - Category – the area of applicability of the parameter
    - Service Data Flow indicates that the parameter is only applicable to an identified Service data flow.
    - Session Identifiers
      - Access Session ID: local loop id/DSLAM ID
      - L2 Session ID: ALA
      - Subscriber Session ID: Subscriber ID/BNG ID
      - Service Session ID: Service Session ID/ PEP ID
      - Application Session ID: Application ID
    - Charging
    - QoS
    - Policy
  - Value Type – Enumerated, Octet String, Unsigned Integer, Address
    Note: The value type is provided for information and the specific format and encoding will be defined by protocol specification

  Note: The involvement of specific network functions and handling of specific parameters and attributes contained in this Framework may depend on the architectural-scenario and use case. It will be up to the architecture specifications to define the interpretation and/or actions related to those functions.

The basic information flow structure is shown schematically in Figure 35 Information Flow Structure.

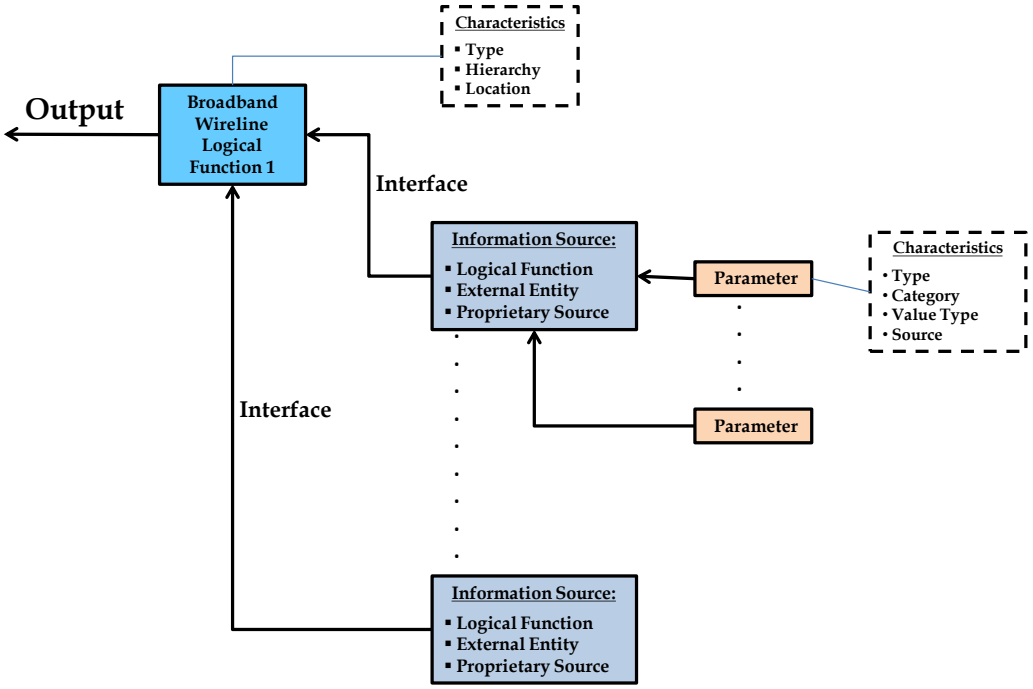


Figure 35 Information Flow Structure

Each [Network Logical Function – Information Source] combination is represented by a unique block of information {*Function, Source, Parameters*}. Note that outputs from any given logical function can serve as inputs to another logical function. Hence they will be represented in a separate block of information for the second logical function – the source in this case will be the first logical function and the parameters will be the output from the first function.

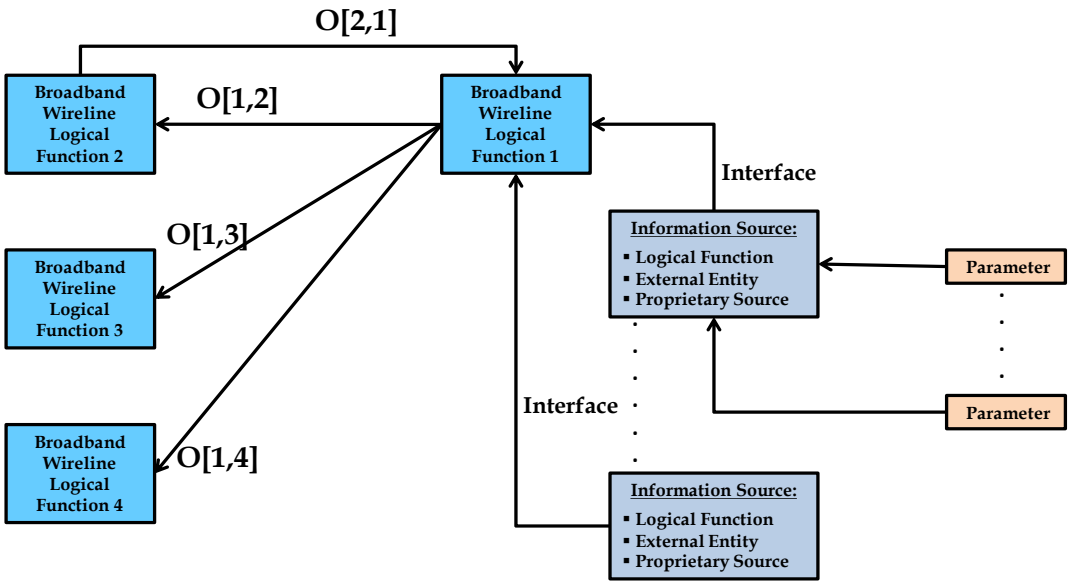
Figure 36 depicts the case where parameters from several information sources are input into Logical Function 1. Function 1 in turn produces a series of independent outputs which serve as inputs to Logical Functions 2, 3, and 4.

Figure 36 also shows the possibility of information flows in the reverse direction – Function 2 receives input from Function 1 and after processing, sends information back to Function 1. The output O[2,1] is depicted as yet another independent {Function, Source, Parameters} Information Block.

Thus the following independent information blocks are shown in Figure 36:

- {Logical Function = Function 2, Information Source = Function 1, Parameters = O[1,2]}
- {Logical Function = Function 3, Information Source = Function 1, Parameters = O[1,3]}
- {Logical Function = Function 4, Information Source = Function 1, Parameters = O[1,4]}

- {Logical Function = Function 1, Information Source = Function 2, Parameters = O[2,1]}



O[m,n]: Information Flow from Function m to Function n

Figure 36 Function Output as Information Source to Other Functions

7.1.2 Network Logical Functions

The purpose of the policy information flow structure is to drive the development of the necessary information flows between Network Logical Functions supporting policy objectives. These flows should be crafted to support all the use cases that have been adopted by the Broadband Forum. It is possible that each use case may be supported by multiple architectures. Hence, each architectural variation for all use cases may require a specific set of information flows.

The set of Network Logical Functions that require information flows for processing policy decisions and enforcement can be drawn from the Broadband Domain Elements and Interfaces shown in Figure 37.

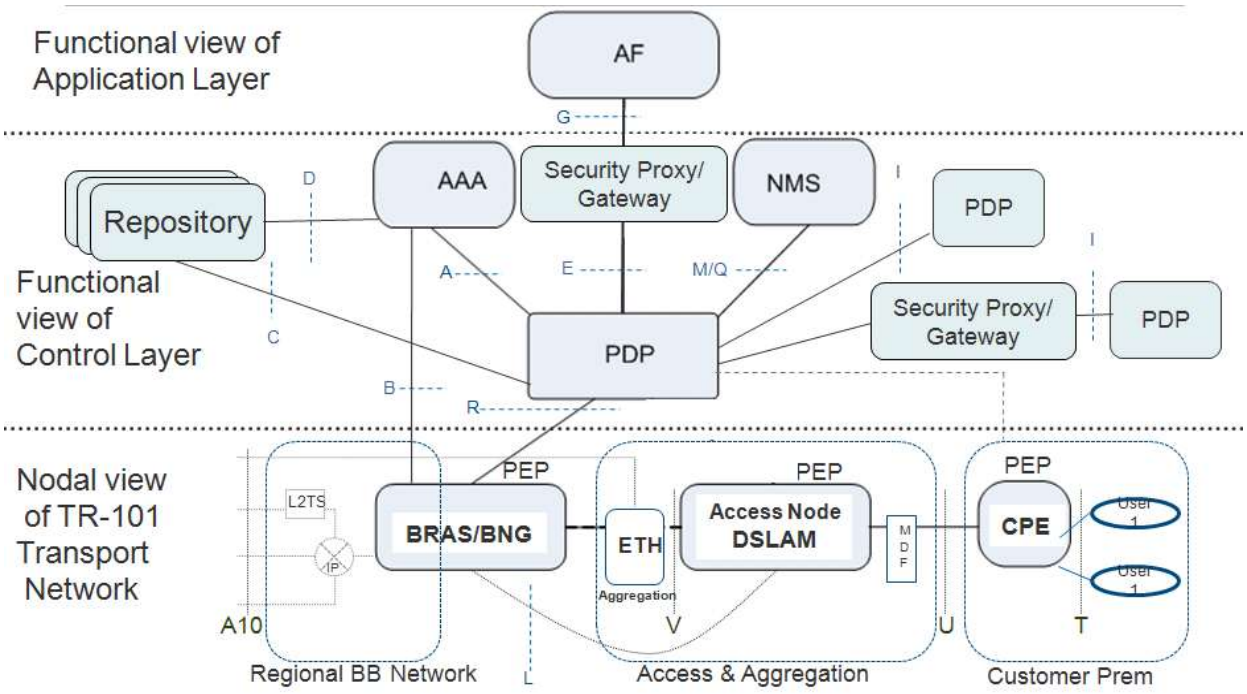


Figure 37 Broadband Domain Elements & Interfaces

The set of information exchanges with the appropriate [Logical Function, Source] combinations, is as follows.

a. [*Logical Function => PDP; Information Source => AF*] – Information on the incoming call/session from the BBF domain AF is conveyed to the PDP.

b. [*Logical Function => PDP; Information Source => AAA*] – Information on the authorization and authentication status is conveyed to the PDP.

c. [*Logical Function => PEP; Information Source => PDP*] – The PDP processes all incoming information and submits it to the PEP.

d. [*Logical Function => PDP; Information Source => PEP*] – The PEP submits the policy enforcement status back to the PDP or PEP requests policy decision from the PDP

e. [*Logical Function => AF; Information Source => PDP*] – The PDP responds back to the AF with information on acceptance or rejection of the incoming call/session.

f. [*Logical Function => PDP; Information Source => other PDP*] – The PDP receives information from the other PDP,.

g. [*Logical Function => other PDP; Information Source => PDP*] – The PDP sends information to the other PDP.

Flows (b), (c), and (d) are within the scope of TR-134 in that these flows support the development of nodal requirements for elements in the transport/nodal layer in Figure 37.
Flows (a) and (e) will need to be determined in conjunction with appropriate SDO's depending on the type of Application Layer functionality.
Flows (f) and (g) are in the out scope of TR-134 and for future study.

7.1.3 Policy Information Model Elements and requirements

R-68. The PDP MUST be able to add policy rules in the PEP via the R interface

R-69. The PDP MUST be able to modify policy rules in the PEP via the R interface

R-70. The PDP MUST be able to remove policy rules in the PEP via the R interface

R-71. The PDP MUST be able to activate policy rules in the PEP via the R interface

R-72. The PDP MUST be able to deactivate policy rules in the PEP via the R interface

R-73. The PEP MUST be able to respond to policy rules received from the PDP via the R interface indicating the result of the request

R-74. The PEP MUST be able to request policy rules from the PDP via the R interface

R-75. The communication between the PDP and the PEP MUST be reliable

R-76. The PDP MUST be able to respond to a policy request from the PEP via the R reference point accepting or rejecting the request

R-77. The protocol design for the R interface MUST support the exchange of Vendor-Specific Information.

R-78. The PDP SHOULD be able to submit the following message parameters to the PEP:
- Policy rule-set upon Subscriber session establishment
- Policy rule update during Subscriber session, upon session event and on termination
- Request for notification of specific events

R-79. PDP decisions MUST be able to be based on:
- Information obtained from the AF via the E/G interfaces (e.g. the session, media and subscriber related information).
- Information obtained from the PEP via the R interface (e.g. bearer attributes, request type and subscriber related information).
- Information obtained from the AAA Server via the A interface
- Information obtained from another PDP via the I interface.
- Information obtained from the repository via the C interface (e.g. subscriber and service related data)

7.1.4 Policy Information Model Messages between PDP and PEP over R Interface

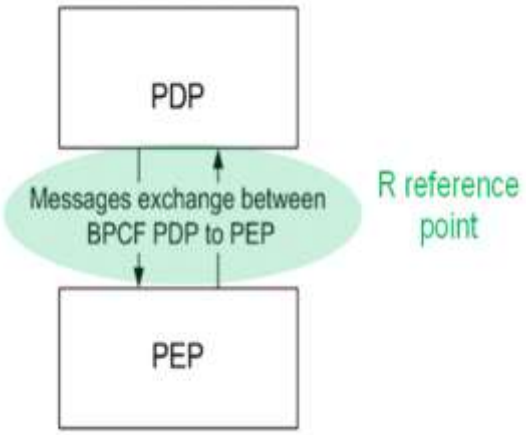


Figure 38 PIM Messages between PDP and PEP over R Interface

7.1.4.1 [Logical Function => PEP; Information Source => PDP]

Abstract Policy Information Elements – PDP ➔ PEP direction parameters submitted for policy

Table 14 PDP to PEP direction parameters

Parameter	Category	Type	Description
PDP ID	User Identification	Octet String	Identifies the PDP installing a Policy
Session ID	Identification	Unsigned Integer	The access session ID and / or application/flow session IDs Access session: unique value generated by the PEP and included in all message exchanges between the PEP and PDP. Application/Flow session: unique value generated by the PDP and included in all message exchanges between the PEP and PDP.
IP Address	User Identification	Octet String	IP Address associated with the subscriber line. Can have multiple occurrences e.g. in the case of a NAT in the data path ,or a mixed IPv4/IPv6 deployment. Can be optionally combined with a domain identifier indicating the area of validity
Policy Rule Request	Policy	Activate/ Deactivate/modify	Request towards the PEP for a policy installation/deactivation or modification.
Policy lifetime	Policy	Unsigned	Lifetime of the policy in seconds

		Integer	
Policy Rule Response	Policy	Activate/ Deactivate/modify	The response sent by the PDP to authorize the request and provide information to PEP in the policy pull mode.
QoS Parameter	QoS	NA	QoS Parameter/s setting Max-Requested-Bandwidth-UL,Max-Requested-Bandwidth-DL, Protocol, Reservation class, ToS traffic class, QoS Priority
Policy Rule ID	Policy	Octet String	Identifier for the policy rule activated at the PEP by the PDP
Policy Rule Group ID	Policy	Octet String	A predefined group of policy rules at the PEP
Policy Rule Precedence	Policy	Unsigned	The precedence of a Policy Rule in case of overlapping policy rules
Traffic actions	Policy	Enumerated	Indicates that the PEP Function must enforce the specified traffic action for the detected application traffic. Generic traffic actions include drop, forward, mark , policy route and rate limit
Application action	Policy	Octet String	Indicates that the PEP Function must enforce the redirection action for the detected application traffic Application actions include http redirect, TCP reset, DNS redirect
Traffic flow filter (IP 5-tuple)	Service Data Flow	NA	Consists of all or a subset of the following: source/destination IP@, port, protocol (above the IP layer)
Multicast ACL		NA	The multicast addresses/address ranges that specify the multicast groups a subscriber is allowed to join. Note: in the case of a multicast package ID, a pointer to this would be part of a policy rule
Quota	Charging	Set Quota/ Update Quota	User Allowed/remaining Quota. User Quota update per service list, session
Charging Mode	Charging	Enumerated	Online/Offline Charging (Pre-paid/Post-paid)
Rating-Group	Charging	Unsigned	The charging key for the policy rule used for rating purposes
Charging-Correlation ID	Charging	NA	Correlates charging records in the access with those in the AF/application domain
Policy Rule	Policy Charging	Set Policy rule/ Update Policy rule	Set Policy rule A Policy rule includes the rating group, QoS information (UL/DL BW, traffic class, priority), charging mode (online, offline) and precedence. For identification purposes a Policy rule is assigned a "policy rule id"
Policy Rule parameters	Policy	N/A	The information included in a Policy Rule regarding QoS and charging
Vendor-Id	Identification	String	Identify the PDP vendor. The PEP uses this when there are Vender specific differences at the PDP
Event Trigger	Policy	Add / remove	The list of events the PDP subscribes to. It includes the events the AF subscribes to

		subscription for event/ event list	
Default-Access Profile	Policy	NA	The QoS assigned to the broadband subscriber line at device attachment/Log-In time. The PDP may override the default QoS it receives from the PEP at device attach/log-in TIME. It includes the traffic Class, priority and pre-emption of the connection. The PDP may modify the default-access profile it receives from the PEP
Logical access ID	User identification	Octet String	The identity of the logical access to which the user device is connected. It is stored temporarily in the AAA function connected to PDP. This corresponds to the Agent ID in case of IPv4 and to THR Interface Id of DHCP option 82 for IPv6
Physical Access ID	User identification	UTF8String	The identity of the physical access to which the user device is connected. It is stored temporarily in the AAA function connected to the PDP. This corresponds to the Agent Remote ID
Globally Unique IP address	User Identification		The IP address of the User for which profile information is being pushed. The addressing domain in which the IP address is significant.
Subscriber ID	User identification	Octet String	Identity of the attached user. The Subscriber ID is stored permanently in the user profile data base and is stored temporarily in the AAA function connected to the PDP
HdrIpVersion	Service Data Flow	Octet String	Identifies the version of the IP addresses to be filtered on.
HdrSrcAddress	Service Data Flow	Octet String	A source IP address.
HdrSrcAddress EndOfRange	Service Data Flow	Octet String	The end of a range of source IP addresses (inclusive), where the start of the range is the HdrSrcAddress value.
HdrSrcMask	Service Data Flow	Octet String	A mask to be used in comparing the source address in the IP header with the value represented in the HdrSrcAddress property.
HdrDestAddres s	Service Data Flow	Octet String	A destination IP address.
HdrDestAddres sEndOfRange	Service Data Flow	Octet String	The end of a range of destination IP addresses (inclusive), where the start of the range is the HdrDestAddress value.
HdrDestMask	Service Data Flow	Octet String	A mask to be used in comparing the destination address in the IP header with the value in the HdrDestAddress
HdrProtocolID	Service Data Flow	Octet String or unsigned integer	8-bit unsigned integer, representing an IP protocol type. This value is compared with the Protocol field in the IP header.
HdrSrcPortStart	Service Data Flow	Octet String or unsigned integer	Represents the lower end of a range of UDP or TCP source ports. The upper end of the range is represented by the HdrSrcPortEnd property. The value of HdrSrcPortStart must be no greater than the value of HdrSrcPortEnd. A single port is indicated by equal values for HdrSrcPortStart and

			HdrSrcPortEnd.
HdrSrcPortEnd	Service Data Flow	OctetString or unsigned integer	Contains the upper end of a range of UDP or TCP source ports. The lower end of the range is represented by the HdrSrcPortStart property. The value of HdrSrcPortEnd must be no less than the value of HdrSrcPortStart. A single port is indicated by equal values for HdrSrcPortStart and HdrSrcPortEnd.
HdrDestPortStart	Service Data Flow	OctetString or unsigned integer	Provides the lower end of a range of UDP or TCP destination ports. The upper end of the range is represented by the HdrDestPortEnd property. The value of HdrDestPortStart must be no greater than the value of HdrDestPortEnd. A single port is indicated by equal values for HdrDestPortStart and HdrDestPortEnd.
HdrDestPortEnd	Service Data Flow	OctetString or unsigned integer	Provides the upper end of a range of UDP or TCP destination ports. The lower end of the range is represented by the HdrDestPortStart property. The value of HdrDestPortEnd must be no less than the value of HdrDestPortStart. A single port is indicated by equal values for HdrDestPortStart and HdrDestPortEnd.
HdrDSCP	Service Data Flow	OctetString or unsigned integer	HdrDSCP is defined as an array of uint8's, restricted to the range 0..63. Since DSCPs are defined as discrete code points, with no inherent structure, there is no semantically significant relationship between different DSCPs. Consequently, there is no provision for specifying a range of DSCPs in this property.
HdrFlowLabel	Service Data Flow	OctetString	The 20-bit Flow Label field in the IPv6 header may be used by a source to label sequences of packets for which it requests special handling by IPv6 devices, such as non-default quality of service or 'real-time' service.
QoSInformation	QoS	N/A	Defines the QoS information for resources requested by the IP session
QoS Information Identifier	QoS	enum	Identifies a set of specific QoS parameters that define the authorized QoS
8021 Source MAC address	Service Data Flow	MAC address	A 48-bit MAC address. This is compared with the SourceAddress field in the MAC header. If not present, then there is a match for all values. This parameters is used in 802.1 Filter rules
8021 Destination MAC Address	Service Data Flow	MAC address	A 48-bit MAC address. This value is compared with the Destination Address field in the MAC header. If not present, then there is a match for all values This parameters is used in 802.1 Filter rule
8021 Protocol ID	Service Data Flow	integer	This parameter represents an Ethernet protocol type. Its value is compared with the Ethernet Type field in the 802.3 MAC header. If no value for this parameter is provided, then it is not considered in selecting matching packets. This parameters is used in 802.1 Filter rules
8021 Priority Value	Service Data Flow	0 to 7	The 802.1Q priority. This value is compared with the Priority field in the 802.1Q header. Since the 802.1Q Priority field consists of 3 bits, the values for this property are limited to the range 0..7. If no value for this parameter is provided, then it is not considered in selecting matching packets.

			This parameters is used in 802 filtering rules and in QoS rules to indicating the value to be used for marking for traffic identified by the 802.1 filter
8021 VLAN ID	Service Data Flow	Value from 0 to 4095	An 802.1Q VLAN Identifier. This value is compared with the VLAN ID field in the 802.1Q header. Since the 802.1Q VLAN ID field consists of 12 bits, the values for this parameter are limited to the range 0..4095. If the value for this property is provided, then it is not considered in selecting matching packets. This parameters is used in 802.1 Filter rules

Note: The Value Type is provided for informational purposes only, and the specific format will be defined by protocol specification.

7.1.4.2 [Logical Function => PDP; Information Source =>PEP]

R-80. The PEP SHOULD be able to submit the following message parameters to the PDP during access session login and PEP initiated session modification. Req for Table 15

Abstract Policy Information Elements – PEP ➔ PDP direction parameters submitted during subscriber login

Table 15 PEP to PDP direction parameters

Parameter	**Category**	**Type**	Description
Vendor-Id	Identification	String	Identifies the PEP vendor. The PDP uses this when there are Vender specific differences at the PEP
Firmware revision	Identification	String	Identifies the software revision of the PEP. Different revisions can have different capabilities at the PEP
Policy Rule ID	Policy	Octet String	The Identifier for a policy rule activated at the PEP by the PDP
Subscriber ID	User Identification	Octet String	The identity used by subscriber to access the service. It is used by the PDP to access the subscriber's profile in the DB/AAA. It may also be used for session binding by the PDP. It is also used for authentication
IP Address	User Identification	NA	The IP@ (IPv4/v6) of the subscriber or end device allocated by the PDP, including the domain where it is valid.
Application / Traffic signature	Service Data Flow	Octet String	The application/ traffic signature for the Deep Packet Inspection Function (PEP) to detect.
Traffic flow	Service	NA	The IP 5-tuples of the application for the Deep Packet Inspection

filter (IP 5-tuple)	Data Flow		Function (PEP) to detect The PDP may make IP flow policies based on this parameter and push the policies to another PEP (e.g. BRAS/BNG)
Application/ traffic signature /session ID	Policy	Enumerated	The start/stop of the application/traffic signature for the Deep Packet Inspection Function (PEP) to detect.
Policy Rule Request	Policy	Activate/ Deactivate/ modify	Request towards the PDP for a decision for policy pull mode
Policy Rule Response	Policy	Activate/ Deactivate/ modify	The result of the policy activation/deactivation/modification performed by the PEP which was requested in the Policy Rule Request in response to push mode
Termination-Cause	Identification	Enumerated	Used to indicate the reason why a session was terminated by the PEP.
Policy lifetime	Policy	Unsigned Integer	In the case of a request towards the PDP, this contains the requested lifetime.
QoS Parameters	QoS	NA	Includes the traffic class for the service data flow, UL/DL BW for GBR connections, maximum BW for non-GBR connections and the priority of the connection
Session modification trigger	Policy	Enumerated	The specific event to be detected by the PEP that will trigger a session modification request to the PDP for rules re-authorization
Default-Access Profile	Policy	NA	The QoS assigned to the connection at device at attachment/log-In time. The PDP may override the default –connection QoS it receives from the PEP at device attach/log-in. It includes the traffic Class, priority and pre-emption of the connection
Interface Name	User Identification	Octet String	Commonly used to see if a customer logged in at their home, or in some other location The interface name may be sourced from common attributes such as NAS-PORT-ID or DHCP option 82
MAC Address	User Identification	Octet String	MAC address of the traffic from user
Access Loop Characteristics	QoS		Group of access loop attributes e.g. for UL and DL directions, min, max, attainable, actual data rates
Access Session ID	User Identification	Octet String	Identifier for the session associated with a local loop session. This is associated with an ANCP port up message
L2 Session ID	User Identification	Octet String	Identifier for a L2 session (e.g. as defined in WT-178 for ALA)
Subscriber Session ID	User Identification	Octet String	Identifier for a session associated with a PPP or IPoE subscriber session

Service Session ID	User Identification	Octet String	Identifier for a session associated with a traffic rule.
Application Session ID	User Identification	Octet String	Identifier for a session associated with an application.

Note: The Value Type is provided for informational purposes and the specific format will be defined by the protocol specification.

7.1.4.3 [Logical Function => PDP; Information Source =>PEP]

Access Port Configuration is typically used in a DSL environment. The Layer 2 Control Mechanism (as per Section 7.2/TR-147[10]) can be used to implement this function. Table 2/TR-147 provides a common set of parameters.

Table 16 Parameters from TR-147 Table 2

Parameter	Category	Type	Description
Actual data rate Upstream	QoS	Unsigned Integer	Actual data rate of an access loop
Actual data rate Downstream	QoS	Unsigned Integer	Actual data rate of an access loop
Minimum Data Rate Upstream	QoS	Unsigned Integer	Minimum data rate desired by the operator
Minimum Data Rate Downstream	QoS	Unsigned Integer	Minimum data rate desired by the operator
Attainable Data Rate Upstream	QoS	Unsigned Integer	Maximum data rate that can be achieved.
Attainable Data Rate Downstream	QoS	Unsigned Integer	Maximum data rate that can be achieved.
Maximum Data Rate Upstream	QoS	Unsigned Integer	Maximum data rate desired by the operator.
Maximum Data Rate Downstream	QoS	Unsigned Integer	Maximum data rate desired by the operator.
Minimum Data Rate Upstream in low power state	QoS	Unsigned Integer	Minimum data rate desired by the operator during the low power state (L1/L2).
Minimum Data	QoS	Unsigned	Minimum data rate desired by the operator during the low

Rate Downstream in low power state		Integer	power state (L1/L2).
Maximum Interleaving Delay Upstream	QoS	Unsigned Integer	Maximum one-way interleaving delay
Actual interleaving Delay Upstream	QoS	Unsigned Integer	Value in milliseconds which corresponds to the inter leaver setting.
Maximum Interleaving Delay Downstream	QoS	Unsigned Integer	Maximum one-way interleaving delay
Actual interleaving Delay Downstream	QoS	Unsigned Integer	Value in milliseconds which corresponds to the inter leaver setting.
Access loop encapsulation	QoS	Unsigned Integer	Encapsulation on the local loop
Interworking Function Session Flag	QoS	Unsigned Integer	Indication that the Access Node is performing Interworking between ATM based local loop and Ethernet based uplink
DSL Type	QoS	Unsigned Integer	The type of transmission system in use
DSL Port State	QoS	Unsigned Integer	The state of the DSL line (showtime, idle, silent)
DSL configuration profile name	QoS	String	Reference to a pre-configured DSL profile in the Access Node
Minimum Data Rate in low power state	QoS	Unsigned Integer	Minimum data rate desired by the operator during the low power state (L1/L2).
Port association to a multicast VLAN		Unsigned Integer	The association between an access port and a set of multicast VLANs
Multicast Access Control List	Service Data Flow	Address	A list of multicast groups/streams can be configured at the AN to specify which groups/streams are allowed/not allowed to be sent on that port
Max Simultaneous Streams		Unsigned Integer	The maximum number of authorized multicast flows which the Access port can join simultaneously
AdminStatus	Security	Enumerated	Used to block a suspect port after a security attack
Access Control List	Service Data Flow	Address	Access control lists for security purposes include: Source MAC address filter; Destination MAC address filter;

			Source IP address filter

7.1.4.4 [Physical Node => BRAS/BNG; Source Physical Node =>Access Node]

Access Resource Reporting is typically used in a DSL environment. Depending on the operational model various techniques such as DHCP Relay Agent (as per Section 3.9.4/TR-101[6]) or Layer 2 Control Mechanism (as per Section 7.2/TR-147[10]) can be used. The below table contain all the parameters from Table 3/TR-101, 4 /TR-101 and Table 1/TR-147. It is the operator's choice as to which set of parameters to use.

Table 17 parameters from tables 3 and 4 in TR-101 and Table 1/TR-147

Parameter	Category	Type	Description
Agent Circuit ID	User Identification	String	The Agent Circuit ID contains a locally administered ASCII string generated by the Access Node, representing the corresponding access loop logical port (U interface)
Agent Remote ID	User Identification	String	The Agent Remote ID contains an operator-configured string of 63 characters maximum that (at least) uniquely identifies the user on the associated access loop on the Access Node on which the DHCP discovery message was received.
Actual data rate Upstream	QoS	Unsigned Integer	Actual data rate of an access loop
Actual data rate Downstream	QoS	Unsigned Integer	Actual data rate of an access loop
Minimum Data Rate Upstream	QoS	Unsigned Integer	Minimum data rate desired by the operator
Minimum Data Rate Downstream	QoS	Unsigned Integer	Minimum data rate desired by the operator
Attainable Data Rate Upstream	QoS	Unsigned Integer	Maximum data rate that can be achieved.
Attainable Data Rate Downstream	QoS	Unsigned Integer	Maximum data rate that can be achieved.
Maximum Data Rate Upstream	QoS	Unsigned Integer	Maximum data rate desired by the operator.
Maximum Data Rate Downstream	QoS	Unsigned Integer	Maximum data rate desired by the operator.
Minimum Data Rate Upstream in low power state	QoS	Unsigned Integer	Minimum data rate desired by the operator during the low power state (L1/L2).
Minimum Data Rate Downstream in low power state	QoS	Unsigned Integer	Minimum data rate desired by the operator during the low power state (L1/L2).

Maximum Interleaving Delay Upstream	QoS	Unsigned Integer	Maximum one-way interleaving delay
Actual interleaving Delay Upstream	QoS	Unsigned Integer	Value in milliseconds which corresponds to the inter leaver setting.
Maximum Interleaving Delay Downstream	QoS	Unsigned Integer	Maximum one-way interleaving delay
Actual interleaving Delay Downstream	QoS	Unsigned Integer	Value in milliseconds which corresponds to the inter leaver setting.
Access Loop encapsulation	QoS	Unsigned Integer	Encapsulation on the local loop
Interworking Function Session Flag	QoS	Unsigned Integer	Indication that the Access Node is performing Interworking between an ATM based local loop and an Ethernet based uplink
DSL Type	QoS	Unsigned Integer	The type of transmission system in use
DSL Port State	QoS		The state of the DSL line (showtime, idle, silent)

7.1.4.5 [Logical Function => AAA; Source Physical Node =>BRAS/BNG]

Access Resource Reporting is typically used in a DSL environment. Dependent on the operational model, various techniques such as DHCP Relay Agent or Layer 2 Control Mechanism can be used. Tables 3 and 4 in TR-101[6] and Table 1 in TR-147[10] give a common set of parameters. It is the operator's choice which set of parameters to be used.

Table 18 Parameters from Tables 3 and 4 in TR-101 and Table 1/TR-147

Parameter	**Category**	**Type**	Description
Agent Circuit ID	User Identification	String	The Agent Circuit ID contains a locally administered ASCII string generated by the Access Node, representing the corresponding access loop logical port (U interface)
Agent Remote ID	User Identification	String	The Agent Remote ID contains an operator-configured string of 63 characters maximum that (at least) uniquely identifies the user on the associated access loop on the Access Node on which the DHCP discovery message was received.
Actual data rate Upstream	QoS	Unsigned Integer	Actual data rate of an access loop
Actual data rate Downstream	QoS	Unsigned Integer	Actual data rate of an access loop

Minimum Data Rate Upstream	QoS	Unsigned Integer	Minimum data rate desired by the operator
Minimum Data Rate Downstream	QoS	Unsigned Integer	Minimum data rate /desired by the operator
Attainable Data Rate Upstream	QoS	Unsigned Integer	Maximum data rate that can be achieved.
Attainable Data Rate Downstream	QoS	Unsigned Integer	Maximum data rate that can be achieved.
Maximum Data Rate Upstream	QoS	Unsigned Integer	Maximum data rate desired by the operator.
Maximum Data Rate Downstream	QoS	Unsigned Integer	Maximum data rate desired by the operator.
Minimum Data Rate Upstream in low power state	QoS	Unsigned Integer	Minimum data rate desired by the operator during the low power state (L1/L2).
Minimum Data Rate Downstream in low power state	QoS	Unsigned Integer	Minimum data rate desired by the operator during the low power state (L1/L2).
Maximum Interleaving Delay Upstream	QoS	Unsigned Integer	Maximum one-way interleaving delay
Actual interleaving Delay Upstream	QoS	Unsigned Integer	Value in milliseconds which corresponds to the inter leaver setting.
Maximum Interleaving Delay Downstream	QoS	Unsigned Integer	Maximum one-way interleaving delay
Actual interleaving Delay Downstream	QoS	Unsigned Integer	Value in milliseconds which corresponds to the inter leaver setting.
Access loop encapsulation	QoS	Unsigned Integer	Encapsulation found on local loop
Interworking Function Session Flag	QoS	Unsigned Integer	Indication that Access Node is performing Interworking between ATM based local loop and Ethernet based uplink
DSL Type	QoS	Unsigned Integer	The type of transmission system in use
DSL Port State	QoS	Unsigned Integer	The state of the DSL line (showtime, idle, silent)

7.1.4.6 [Logical Function => PDP; Information Source =>AAA]

Table 19 **Abstract Policy Information Elements – AAA ➔ PDP direction parameters submitted for policy**

Table 19 AAA to PDP direction parameters

Parameter	Category	Type	Description
Globally Unique IP address	User Identification		The IP address of the User for which profile information is being pushed. The addressing domain in which the IP address is significant.
Logical access ID	User identification	Octet String	The identity of the logical access to which the user device is connected. This corresponds to the Agent ID in the case of IPv4 and to Interface Id of DHCP option 82 for IPv6
8021 VLAN ID	Service Data Flow	Value from 0 to 4095	An 802.1Q VLAN Identifier. This value is compared with the VLAN ID field in the 802.1Q header. Since the 802.1Q VLAN ID field consists of 12 bits, the values for this parameter are limited to the range 0..4095. If no value for this property is provided, then it is not considered in selecting matching packets. This parameter is used in 802.1 Filter rules

7.1.4.7 [Logical Function => AAA; Information Source =>PDP]

Table 20 Abstract Policy Information Elements – PDP ➔ AAA direction parameters submitted for policy

Table 20 PDP to AAA direction parameters

Parameter	Category	Type	Description
PDP Id	User identification	Octet String	Identifies the PDP requesting profile information.
Globally Unique IP address	User Identification		The IP address of the User for which profile information is being pushed. The addressing domain in which the IP address is significant.
Push Result	-	Unsigned32	Result of the request

7.1.5 Vendor proprietary extensions

Most systems (Access Node, BNG, and AAA) support Vendor-Proprietary Extensions in their informational model. The aim is to implement operator-specific functions that are not supported by Broadband Forum specifications. This is handled through the usage of Vendor-Specific Attributes (VSAs). For instance, TR-101[6] (R-114) requires support of the insertion of vendor specific information by the Access Node DHCP relay agent.

By means of VSAs for Policy Control, the IM can be extended and adapted, enabling quick deployments, and allowing customization of services for the Service Providers and Policy Control Vendors alike.

Appendix I. Relationship to other Broadband Technical Reports

I.1 TR-059

TR-059 [2] is entitled "*DSL Evolution – Architecture Requirements for the Support of QoS-Enabled IP Services*". This outlined an evolution of mass market DSL services to deliver multiple levels of QoS-enabled IP services from one or more service providers.

The DSL architecture and requirements in TR-059 document enable the product and service enhancements described in TR-058 [1] including Bandwidth on Demand, QoS, QoS on Demand, Many-to-Many Access and Content Distribution.

TR-059 has a two-phase QoS Architecture:

1. Phase 1 is characterized by Diffserv provided through static provisioning.
2. Phase 2 has a dynamic mechanism for changing the Diffserv QoS parameters through the use of policy-based networking.

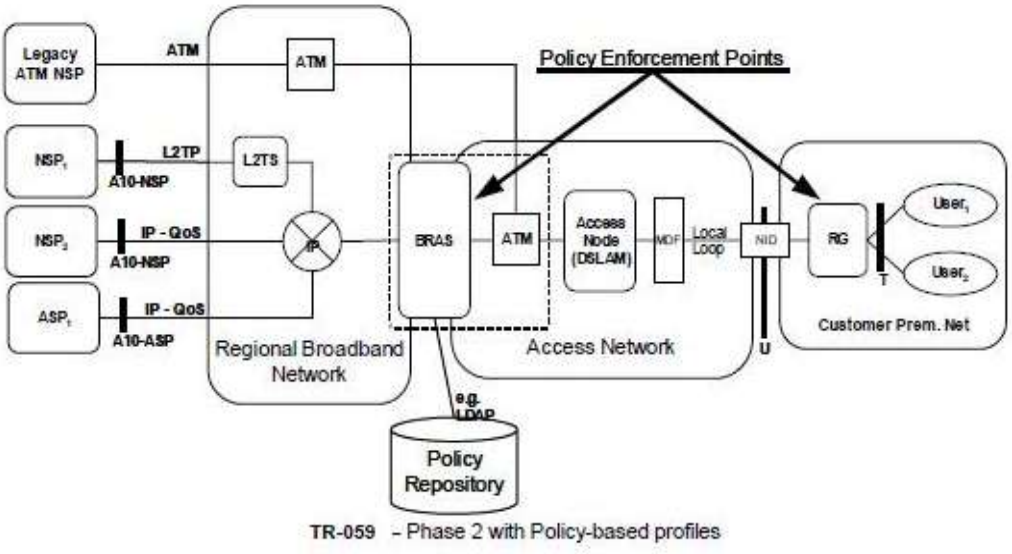


Figure 39 BPC Framework Relation to Broadband Forum Standard TR-059

TR-134 includes some requirements taken from TR-059.
TR-134 enables the PDP (Policy Decision Point) entity to control policy-based QoS by interfacing and interacting with the BRAS PEP over the R interface and allows (but does not specify in detail) the option to control a PEP in the RG at the customer premises.

I.2 TR-069

TR-069 [3] specifies a protocol for communication between CPE and an Auto-Configuration Server (ACS) that encompasses secure auto-configuration as well as other CPE management functions.

TR-069 provides the transport, method calls, and a common Framework to communicate with CPE. TR-098[5] contains the InternetGatewayDevice (IGD) root data model, and TR-181 [11]describes the Device data model, with TR-181 Issue 1[12] defining version 1(Device:1) and TR-181 Issue 2 defining version 2 [13](Device:2) which can be used for static configuration of Policy and QoS with TR-069 managed devices. The TR-098 and TR-181 data models include support for classification, tagging, shaping, queuing, and policing. This is consistent with the TR-134 architecture that allows for static configuration of Policy and QoS on an RG. The requirements for these Policy and QoS data model elements are found in TR-124 [8].

I.3 TR-101

TR-101 describes how an ATM aggregation network can be migrated to an Ethernet based one. It has a number of requirements relevant to the BPC Framework, in particular packet classification, scheduling and forwarding, VLAN support, policing and QoS.

The BPC Framework will support the exchange of sufficient information over the R-interface to manipulate a TR-101 [6] based access network in these areas.

I.4 TR-144

TR-144[9] describes the business requirements for a Multi-Service Architecture & Framework. These requirements include the need for network interconnection standards for broadband access, QoS support and Bandwidth on demand, increased overall bandwidth and higher network reliability and availability. The scope of TR-144 includes a generic converged Broadband Multi-Service network architecture. This converged architecture supports a wide range of services, including both emerging and legacy services, with an extension to add a degree of nomadism support. It covers market segments in addition to the residential and retail focus of TR-101, in particular the business and wholesale markets TR-144 also includes services like IPTV that require end to end Quality of Service, and business VPN services that may drive the need for higher network reliability and availability.

Figure 40 depicts the TR-144 broadband multi-service reference model, supporting policy control and management functionality. TR-144 states that in order to support new services and their underlying network features, the management of the Broadband Multi-Service architecture is extended to include policy management and control. In TR-144 this is only defined at a high level as dynamic configuration based on a set of inputs and/or stimuli plus the ability to resolve the outcome based on a set of rules. The broadband multi-service reference model includes a Policy Controller that interacts with the network by means of an interface to one or more of the network elements. Two types of policy control interface are indicated in the TR-144 reference model. The interface between the network element(s) and the Policy Controller is denoted by the R interface. The other interface to the Policy Controller, over which policy inputs are made, is denoted by the G interface. These policy control and management interfaces provide the intelligence to facilitate the orderly delivery of the services.

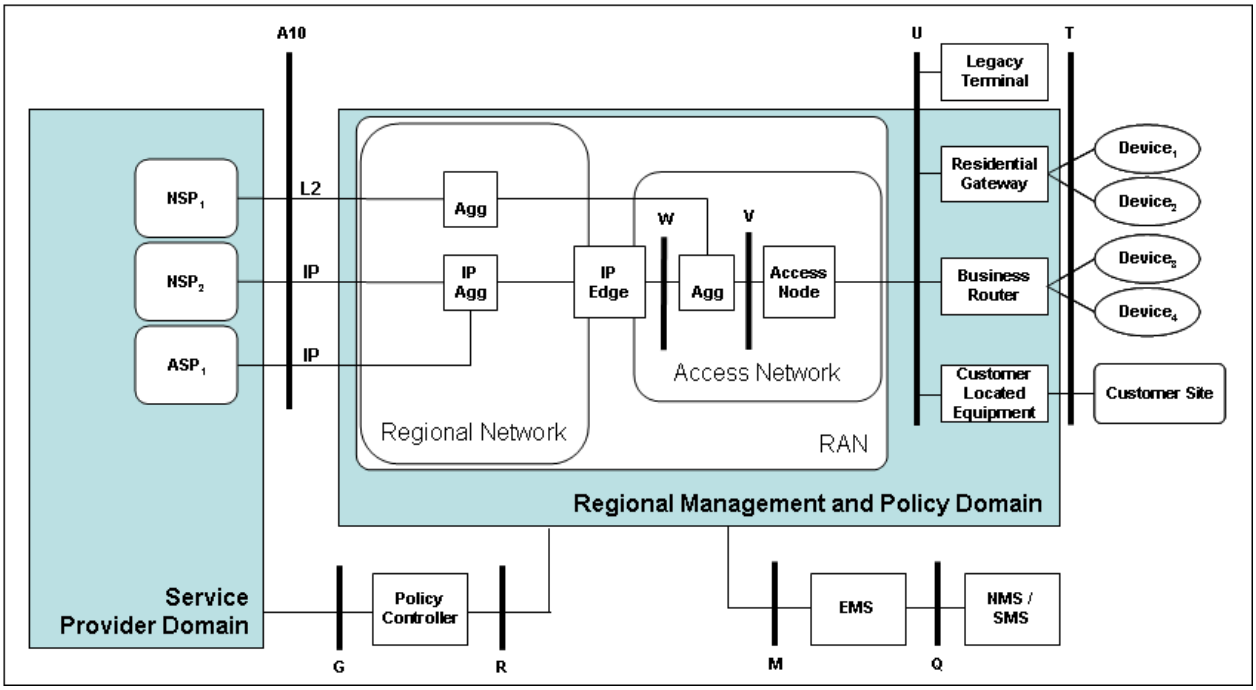


Figure 40 Broadband Multi-service Reference Model

I.4.1 Overview of TR-144 requirements related to the BPC Framework

The following subsections summarize the requirements from TR-144[9] that are relevant to TR-134.

I.4.1.1 Guaranteed and relative QoS

In TR-144[9], the generic terms "QoS" and "QoS on Demand" are used to describe the general concept of differentiated traffic delivery. Wherever possible, the qualifying adjectives "Relative" and "Guaranteed" should be used when describing the needs of a particular service. Where appropriate, the definition of the QoS requirements of an application or service should include various parameters (priority, delay, jitter, etc), any limits and the type of limits (engineered or contractual) involved.

The term "relative QoS" is used to refer to a traffic delivery service without absolute bounds on the achieved bandwidth, packet delay or packet loss rates. It is used to handle certain classes of traffic differently from other classes.

The term "guaranteed QoS" is used to refer to a traffic delivery service with certain bounds on some or all of the QoS parameters. These bounds may be hard ones, such as those implemented mechanisms as RSVP. Other sets of bounds may be contractual, such as those defined in service level agreements (SLAs).

I.4.1.2 Static and signaled/dynamic QoS

TR-144[9] defines the concepts of "bandwidth on demand" and "QoS on demand". The former is the ability to change the access bandwidth allocated in response to applications, specific network connectivity, or the user's desire to upgrade his/her bandwidth, while the latter is the ability to request the QoS capabilities described above in an on-demand fashion.

TR-144 specifies that the Broadband Multi-Service architecture must support both signaled and pre-provisioned QoS.

I.4.1.3 Service-related information for classification, admission control and scheduling purposes

Each service provider connection can have a fixed set of service parameters that are implemented at session startup such as bandwidth and default QoS. Each session may also take advantage of dynamic network features such as Bandwidth on Demand and QoS on Demand. The Broadband Multi-Service architecture supports the ability to reserve (or deny) the bandwidth requested for a session or flow.

I.4.1.4 QOS attributes

Network QoS and QoS related parameters specified in TR-144[9]include bandwidth, packet transfer delay, packet transfer delay variation, bit error rate and lost packet rate. Support of QoS can be achieved at network level, flow level, and packet level. At the network level, all customer traffic in the network is affected. At the flow level, only certain customer flows are affected. At the packet level, the QoS treatment is supported at a packet-by-packet granularity.

I.4.1.5 Service based accounting

TR-144 states that it is expected that some services will be offered for a fixed fee, no matter how long the service duration or how many times the service is used in a month (or other fixed timeframe), while other services will be charged on a "per hour" or "per usage" basis. The Broadband Multi-Service architecture must be able to provide service based accounting on the basis of both time and volume.

I.4.1.6 Wholesale support

TR-144 specifies that the Broadband Multi-Service architecture must support wholesale access connectivity. This will allow access providers to offer services to network providers based on wholesale relationships that are both mandated and freely contracted, as well as being able to continue to offer some legacy services over the newly deployed infrastructure

I.4.2 Summary

TR-144[9] specifies that the Broadband Multi-Service architecture must support policy control and management, which is to provide dynamic configuration based on a set of inputs and/or stimulus plus the ability to resolve the outcome based on the application of a set of rules. In this regard the TR-144 reference model includes a policy controller as well as the G and R interfaces. These interfaces correspond to the G and R interfaces that are incorporated into TR-134. With respect to policy and control, TR-144 specifies that the Broadband Multi-service networks support an information model that abstracts network instantiations from the application layer. TR-134 includes a policy information model to address this requirement.

I.5 TR-147

TR-147[10] provides a Framework for the Layer 2 Control Mechanism and identifies a number of use cases. The Layer 2 Control Mechanism runs directly between a BNG and an Access Node, and is used to perform QoS-related, service-related and subscriber-related operations. TR-147 allows access link related operations to be performed within those network elements, while avoiding any impact on existing management systems.

TR-147 defines the network element requirements and describes information flows and the protocol requirements for the following use cases:

- Reporting the characteristics of the access links and general Access Node capabilities to a BNG that uses this information for QoS purposes;
- Configuration of service parameters on selected access ports. This may include physical layer service parameters (e.g. DSL maximum net data rate) or network layer service parameters (e.g. 802.1p scheduling configuration on the access link);
- Triggering a point-to-point OAM mechanism on selected access links. This may include ATM OAM in the case of ATM-Ethernet interworking (cf. TR-101[6]), or Ethernet OAM in the case of an end-to-end Ethernet network;
- Communicating multicast related information between a BNG and an Access Node in order to configure, for example, multicast Access Control Lists.

TR-147[8] provides a mechanism to share local loop, service and QOS related parameters between the BNG and the Access node. TR-147 mentions interaction with RADIUS based AAA and/or a Policy Server when doing Access port Discovery, Port Configuration and Multicast control.

The information flows and parameters found in TR-147 and TR-101 have been incorporated into TR-134 as Policy information Objects and Policy Information flows. The L interface found in TR-134 is a direct consequence of the communication channel of TR-147. The B reference interface for AAA interaction found in TR-134 and its related RADIUS attributes are directly imported from TR-101, but some new extensions have been added

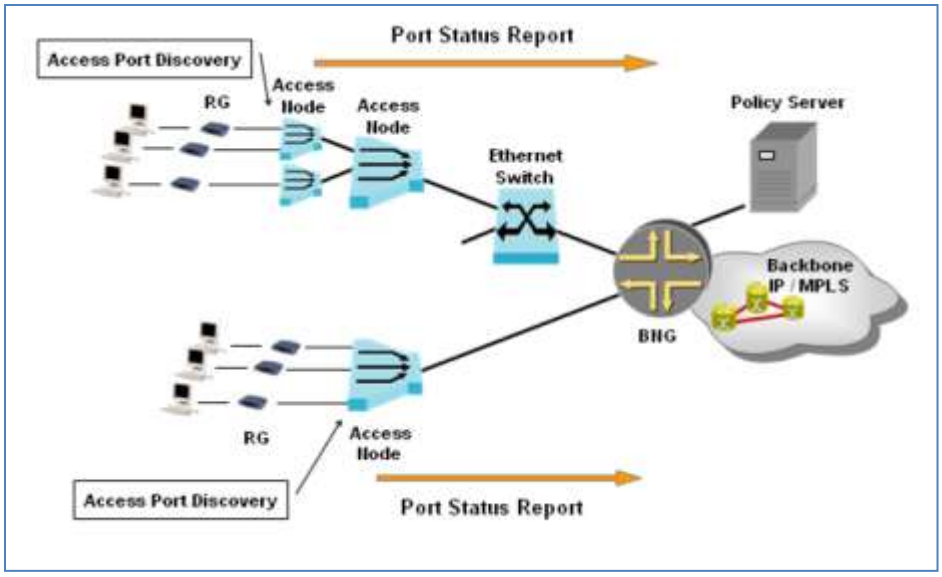


Figure 41 Sourced from TR-147

Appendix II. Relationships with other Policy Control Standards

II.1 ETSI TISPAN RACS

II.1.1 Overview

The Resource and Admission Control Subsystem (RACS) provides support for policy-based resource reservation and admission control and for managing traffic policies. It also plays a role in controlling Network Address Translation (NAT) at the edge of network segments and for assisting in remote NAT traversal for which it can control a BGF (Border Gateway Function).

The RACS architecture (Figure 42) is defined in ETSI ES 282 003[34]. It has two primary functional entities: the Service-based Policy Decision Function (SPDF) and the Resource and Admission Control Function (x-RACF). The SPDF is the single point of contact for Application Functions (AFs) to request resources. Each x-RACF is responsible for performing admission control for the resources under its responsibility. The resources are mainly transport resources but other types (e.g. processing resources) may also be taken into account. An SPDF communicates with one or more x-RACFs via the Rq reference point. The RACS can also export charging information at the Rf reference point.

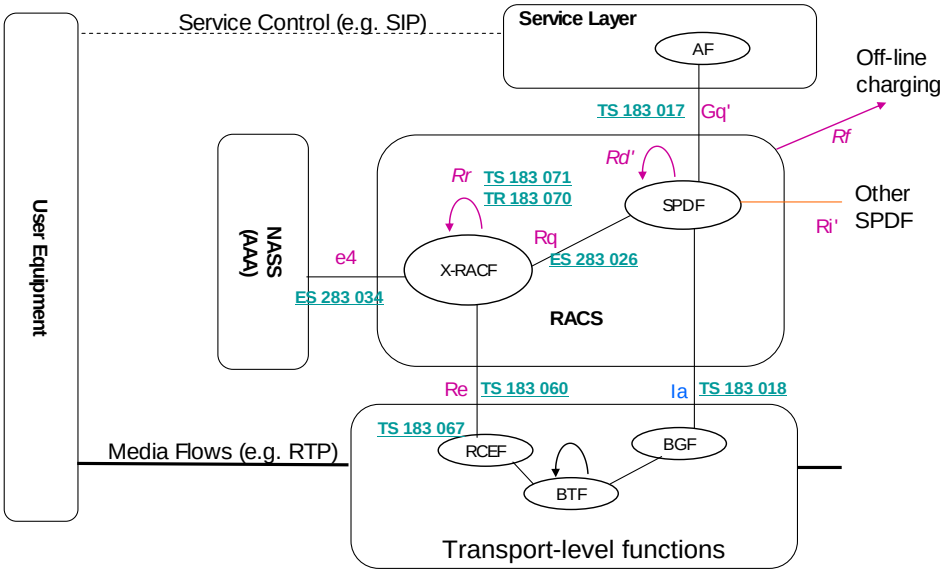


Figure 42 Relations to Other NGN standards- RACS Functional Architecture

Requests for resources are issued by Application Functions via the Gq' reference point. Resources can be related to a unicast or multicast session. The decisions that the SPDF makes are based on policies that are said to be “service-based” as they depend on the type of application and class of service requested. There are scenarios where an SPDF needs to forward a request to another SPDF. This occurs via the Rd' or Ri' reference point depending on whether or not they belong to the same administrative domain.

Two functional elements of the x-RACF (generic Resource Admission Control Function) have been defined: the A-RACF, which deals with resources in access networks, and the C-RACF, which deals with resources in core networks. Each x-RACF may receive requests from an SPDF, from a transport-level network element or from another x-RACF located in the same operator's domain. Based on these requests and available policy information, an x-RACF accepts or rejects reservation requests for the transport resources under its control. An x-RACF having granted resources to an application may set or modify traffic policies in some of the transport nodes that will be involved in processing the associated media streams using the Re reference point.

The RACS is defined as a purely functional architecture not mandating where functional entities are to be implemented. DIAMETER is used as the protocol apart from at the Ia reference point.

II.1.2 Admission Control

One of the primary functions of the x-RACF is to perform admission control for the resources it is responsible for. An x-RACF receiving an admission control request sees if the requested resources are available. Admission control requires the x-RACF to be able to retrieve topology and resource information from any combination of local configurations, external systems and network entities. This implies knowledge of the topology (including congestion point(s) and the current reservations) of a segment. In the case of a DSL-based access network, this verification will typically involve checking transport resources in the access segment (e.g. bandwidth allocated to an ATM VC) and in the aggregation segment (e.g. bandwidth allocated to a VLAN or an ATM VP). The admission control logic in an A-RACF may, depending on the operator's policy, include an additional step for checking that the amount of requested bandwidth is compatible with the subscriber's access profile (received via the e4 reference point) taking into account the amount of bandwidth being used by existing reservations.

The RACS specifications allow for multiple x-RACF instances in the same transport segment. An x-RACF may be implemented as a standalone platform or embedded in another transport network elements such as an AN or BNG. Co-ordination of admission control is achieved via the Rr reference point between x-RACF instances. This co-ordination may be needed to avoid uncontrolled overbooking (in case more than one x-RACF is entitled to admit traffic over the same resources) or to reserve resources spanning multiple transport segments each of which is under the control of a different x-RACF.

Coordination between x-RACF instances may be performed on a per-request or aggregated basis as follows:

- per-request coordination, which is coupled to reservation requests arriving over Rq or Re, and is only applicable to a unicast service, not to the multicast service
- bulk (or aggregated) coordination which is decoupled from reservation requests arriving over Rq or Re. Aggregate level delegation requests are independent of application triggers although they may result from processing of the application level requests.

The bulk resource coordination approach is used when an x-RACF makes resource admission control decisions independently without consulting other x-RACFs on a per-request basis and multiple x-RACFs are managing the same resources. This requires the x-RACF to have been delegated decision criteria (bandwidth, traffic properties, forwarding behavior…) for accepting or rejecting a request autonomously. The delegation of the responsibility for performing admission control can be initiated either by the x-RACF to which this responsibility is delegated, or by the x-RACF that delegates the responsibility.

Multicast IPTV traffic is a typical case where a two-level structure may be used. This involves an Access Node with an embedded x-RACF and a multicast router supporting IGMP/MLD. The embedded x-RACF is delegated an amount of bandwidth enabling it to autonomously accept a certain amount of traffic. This is intended to reduce zapping delays.

The RACS is able split the resource reservation and policy installation procedures into two steps. Whether the single (implicit commit) or two stage (separate reserve and commit steps) procedure is deployed depends on the operator's use cases. As an example, the SIP/SDP based offer/answer model may require a two stage procedure.

II.1.3 Traffic Policies

The RACS provides transport- nodes with traffic policies to be enforced. Within these network nodes, the function that is responsible for enforcing traffic policies is known as the Resource Control Enforcement Function (RCEF). Traffic policies to be enforced by an RCEF can either be provisioned directly or received from the RACS. Policy information is transmitted to the RCEF via the Re reference point and includes one or more of the following elements:

- Flow description indicating whether packets sent to/from a particular address/port and related to a particular protocol are permitted to enter/leave the network node where the RCEF resides.
- QoS-Information: Maximum bandwidth, maximum burst size, committed data rate, committed burst size and excess burst size in the uplink and downlink direction.
- Class of service to be mapped to a DiffServ code point and or a Layer 2 marking.

Communication between a RACS and an RCEF can use a policy push and/or pull model:

- With the "Push" Model", the RACS "pushes" traffic policies to the transport functions to enforce its policy decisions. The "push" occurs on receipt of a path-decoupled request for resource authorization and/or reservation from an Application Function (AF) or from an interconnected RACS entity.

- With the "Pull" Model", transport processing functions "pull" traffic policies from the RACS on receipt of a path-coupled request coming from user equipment and/or other transport network elements (e.g. RSVP or IGMP messages).

II.1.4 Support of architectural requirements

Architecture requirements and implementation examples described in Section 6 are supported by the RACS. The RACS architecture is a functional architecture, enabling both centralized and

distributed deployment options. The SPDF is the central contact point and delegates decisions to x-RACFs. x-RACF instances install policies on RCEFs (i.e. PEPs). SPDF instances may also interact with each other. x-RACF instances can be co-located with a PEP, implemented in standalone equipment or co-located with an SPDF.

Figure 43 provides a mapping on to the TR-101[6] architecture. The G interface maps to the RACS Gq' reference point. The R interface maps to the RACS Re reference point.

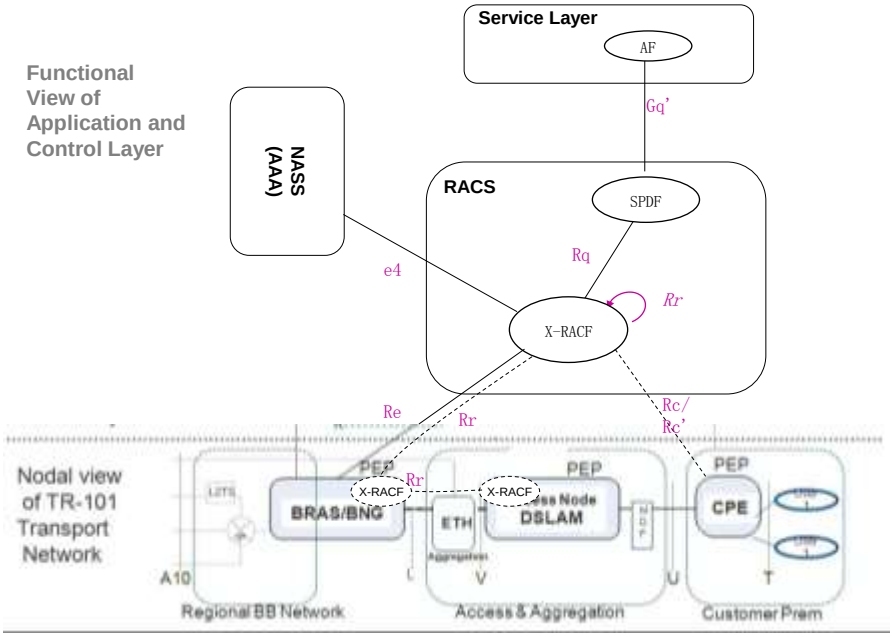


Figure 43 Mapping RACS on the TR101 architecture

The interaction with the CPE has been studied within RACS Release 3 covering two modes, the CPE as a PEP and as a PDP (proposed reference points named Rc / Rc', see ETSI TR 182 031[33])).

II.2 ITU-T NGN

The ITU-T Resource and Admission Control Functions(RACF) model encompasses access as well as core networks, and is intended to apply to a variety of network technologies including fixed and mobile transport as well as core transport (e.g. MPLS). The RACF model decouples service provisioning from the specifics of the network transport facilities, including not only the transport technology but also transport topology and QoS mechanisms. The RACF model supports dynamic management of a variety of resources across varied transport networks—different technologies, administrative domains, ownerships—to achieve end-to-end QoS and provide border control.

II.2.1 Overview

In the context of the ITU-T NGN architecture ITU-T Y.2001[35], the resource and admission control functions (RACF) defined in ITU-T Y.2111[36] serve to arbitrate between the service control functions (upper portion of Figure 44) and transport functions (lower portion of Figure 44), to control transport resources related to QoS, in access and core networks.

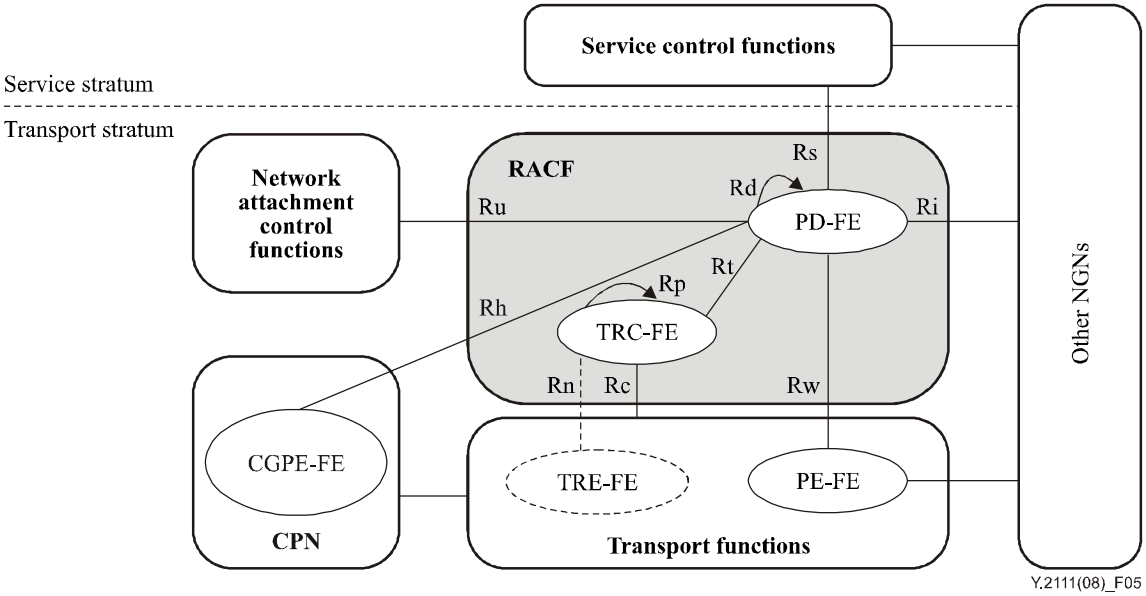


Figure 44 Relations to Other NGN standards- ITU-T RACF Architecture

The RACF functional architecture executes policy-based transport resource control upon the request of the SCF, determines transport resource availability, makes admission decisions, and applies controls to transport functions for enforcing the policy decisions. The RACF interacts with transport functions for the purpose of controlling one or more of the following functions in the transport stratum: bandwidth reservation and allocation, packet filtering; traffic classification, marking, policing, and priority handling; network address and port translation; firewall. The RACF functional architecture supports both "push" and "pull" modes for resource control.

As indicated in Y.2111[36], functions supported by the RACF architecture include:

- Controlling the QoS-related transport resources within packet networks and at the network boundaries in accordance with their capabilities.
- Support for different access and core transport technologies (e.g. xDSL, UMTS, CDMA2000, cable, LAN, WLAN, Ethernet, MPLS, IP, and ATM), while hiding network technology and administrative details (e.g. network topology, connectivity, control mechanisms) from the SCF.
- Support for resource and admission control within a single administrative domain and between administrative domains.
- Resource and admission control for multicast in support of e.g. IPTV.
- Resource and admission control in support of nomadicity.

The RACF functional architecture may support the following optional functions:

- The export of information to support charging based on resource usage and/or QoS treatments.
- Access to and use of information provided by network management on performance monitoring to assist in making resource-based admission decisions.
- Support of path selection between ingress and egress points within a single domain to satisfy QoS resource requirements.

The ITU-T RACF architecture gives an operator the option to deploy static and/or dynamic policy enforcement rules. The static rules are pre-defined by network operators. Static policy rules are not affected by individual service requests. The dynamic rules are a set of policy conditions and actions for enforcing resource control on a per-flow basis, based on requests from the SCF. Dynamic policy decisions may be modified during the lifetime of a resource control session.

The RACF architecture may control the resources for aggregated or individual flows. In the former case, the resources controlled at the aggregate flow level are not dependent on the beginning or end of an application session and may carry multiple application sessions. In the latter case the resources may be controlled at the individual flow level, e.g. in support of media flows.

II.2.2 Architecture Summary

The RACF functional architecture consists of two types of resource and admission control functional entities as shown in Figure 44: the PD-FE (Policy decision functional entity) and the TRC-FE (Transport resource control functional entity). This decomposition of PD-FE and TRC-FE enables the RACF to support a variety of access and core networks (e.g. fixed and mobile access networks) within a general resource control Framework. The PD-FE, via the Rw interface, communicates with the PE-FE (Policy Enforcement Functional Entity) that enforces policy in the transport plane. Functions performed by these three entities include the following:

PD-FE – Policy Decision Functional Entity

- Applies network policies to resource management requests from Service Control Functions
- Given an IP address pair and required BW, determines if the given flow can be supported in the network
- Manages resources along the flow path including NAPT Transversal and Gate Control
- TRC-FE – Transport Resource Control Functional Entity
- Performs “Connection Admission Control”
- Monitors network resource utilization and network topology to manage path bandwidth availability (reservation and/or monitor)
- Performs mapping from network QoS parameters received from the PD-FE via the Rt reference point to transport (technology dependent) QoS parameters based on specific transport policy rules.

PE-FE – Policy Enforcement Functional Entity

- Per flow policing, filtering, QoS-marking and metering

- NAPT translation and Transversal
- Lawful Intercept
- Can provide congestion/capacity information to Service Control

Information exchanged over some key interfaces in the RACF model includes:

- Rs: PD-FE－SCFs
  - For SCFs to request transport resource authorization and control
  - Information exchanged: *session ID, media descriptor, application QoS requirements, priority, gate or NAPT control policy, authorization token*, etc.
- Rw: PD-FE－PE-FE
  - For PD-FE to apply controls to PE-FE concerning NAPT, hosted NAT traversal, gating, bandwidth, packet marking, etc.
  - Information exchanged: *media descriptor, DSCP value, bandwidth committed, bandwidth authorized, authorization token, gate control command, NAPT control command, usage information,* etc.
- Rt: PD-FE－TRC-FE
  - For PD-FE to request resource availability check by TRC-FE
  - Information exchanged: *media descriptor, bandwidth, other network QoS requirements, network path,* etc.

The capability of the RACF model to support multiple administrative domains is illustrated below in Figure 45. As indicated in Y.2111[36], at least one PD-FE is required to be deployed in each network administrative domain (e.g. access network domain and/or core network domain) with associated PE-FEs and TRC-FEs. The RACF may be present in an access network domain or core network domain, or may be present in both access and core network domains. The implementation and physical configuration of the PD-FE and TRC-FE are flexible; they can be distributed or centralized, and may be a stand-alone device or part of an integrated device.
*NOTE: The objective of the Ri interface is to support nomadicity.

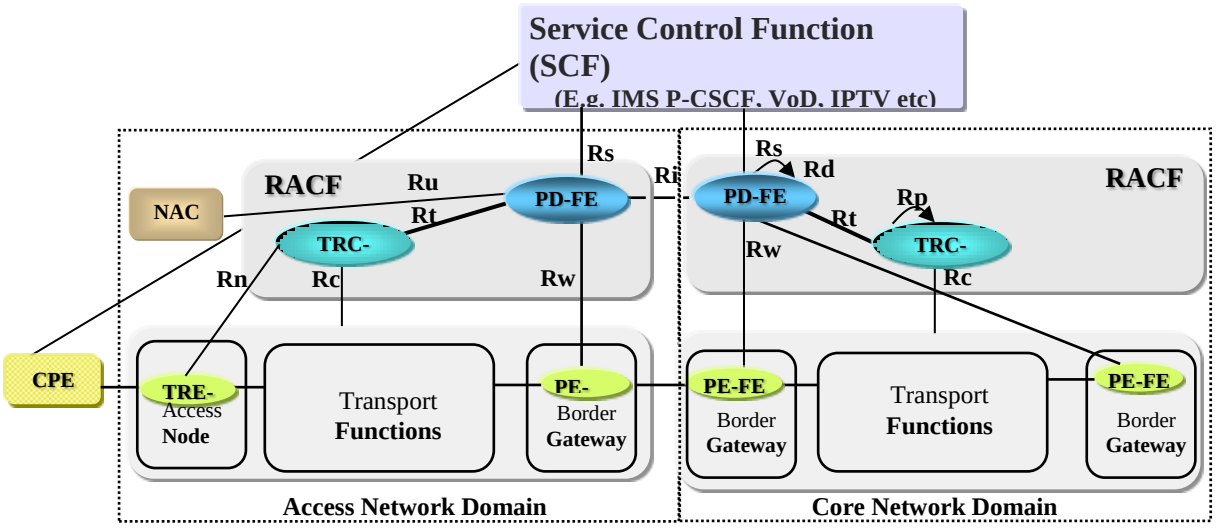


Figure 45 RACF Example Implementation Architecture

- Each operator administrative domain should have its own PD-FE for policy control
- Multiple PD-FE and TRC-FE instances are allowed in the same domain
- PD-FE and TRC-FE can be centralized or distributed, can be a standalone device or Each TRC-FE may control the TRE_EE for aggregation transport QoS
- Each operator administrative domain should have its own PD-FE for policy control
- Multiple PD-FE and TRC-FE instances are allowed in the same domain
- PD-FE and TRC-FE can be centralized or distributed, can be a standalone device or integrated with other network devices

II.2.3 Support of architectural requirements

Architecture requirements and implementation examples described in Section 6 are supported by the RACF. The RACF architecture is a functional architecture, enabling both centralized and distributed deployment options. The PD-FE makes the final decision regarding network resource and admission control based on network policy rules, SLAs, service information provided by the SCF, transport subscription information provided by the NACF in access networks, and resource-based admission decision results provided by TRC-FE. The PD-FE instances install policies on PE-FE (i.e. PEPs). The TRC-FE deals with the diversity of underlying transport technologies and provides the resource-based admission control decision results to the PD-FE. The TRC-FE instances can be implemented in standalone equipment units or co-located with a

PD-FE. The Rc reference point may be connected to any instances of the transport functions as needed to obtain the pertinent information.

Figure 46 provides a mapping on the TR-101[6] architecture. The G interface maps to the ITU-T RACF Rs reference point. The R interface maps to the RACF Rw reference point.

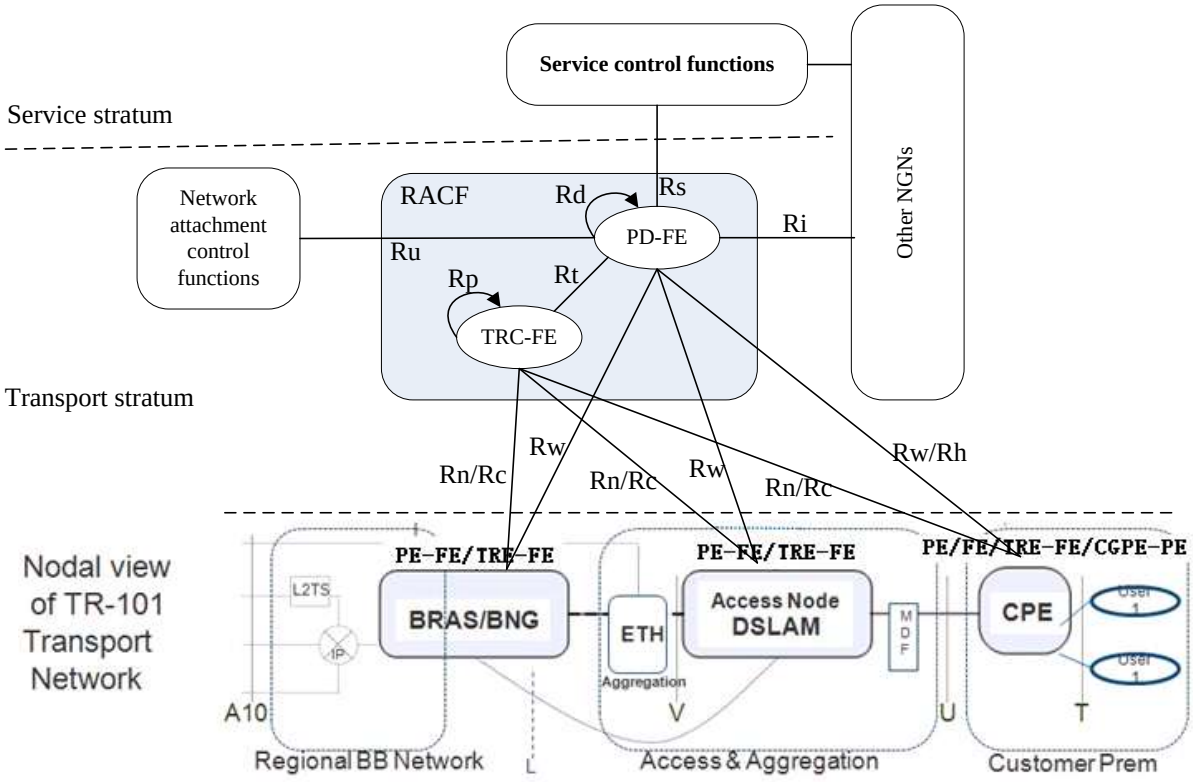


Figure 46 Mapping of ITU-T RACF to TR-101 architecture

The BRAS/BNG and DSLAM acts as the PE-FE and TRE-FE. And the CPE acts as the PE-FE and TRE-FE or CGPE-FE.

II.2.4 ITU-T Y.DPIFR (DPI Framework)

The use cases in TR-134 indicate a need for applications or subscribers (including NSPs/ASPs) to modify Policy or QoS configurations for ongoing sessions, as well as use cases that support configuration changes independent of sessions. While TR-134 does not primarily focus on DPI, ITU-T Y.DPIFR (or just Y.DPIFR) [37] describes how policy can be applied to control planes and management planes. In addition, the specification provides a set of policy mechanisms and terminology complementary to that commonly adopted in policy literature (e.g. IETF RFC 3198 [19]) that can be adopted in a broadband network to support these two categories of use cases. This section provides a mapping of these mechanisms to a BNG/BRAS. (Note that ITU-T document has not (yet) selected any specific protocols.)

Y.DPIFR[37] recognizes that policies can be shared with network elements via a control plane interface and/or a management plane interface. The document specifically describes a hybrid

(control and management plane) and a management plane only solution, as shown in the following figures.

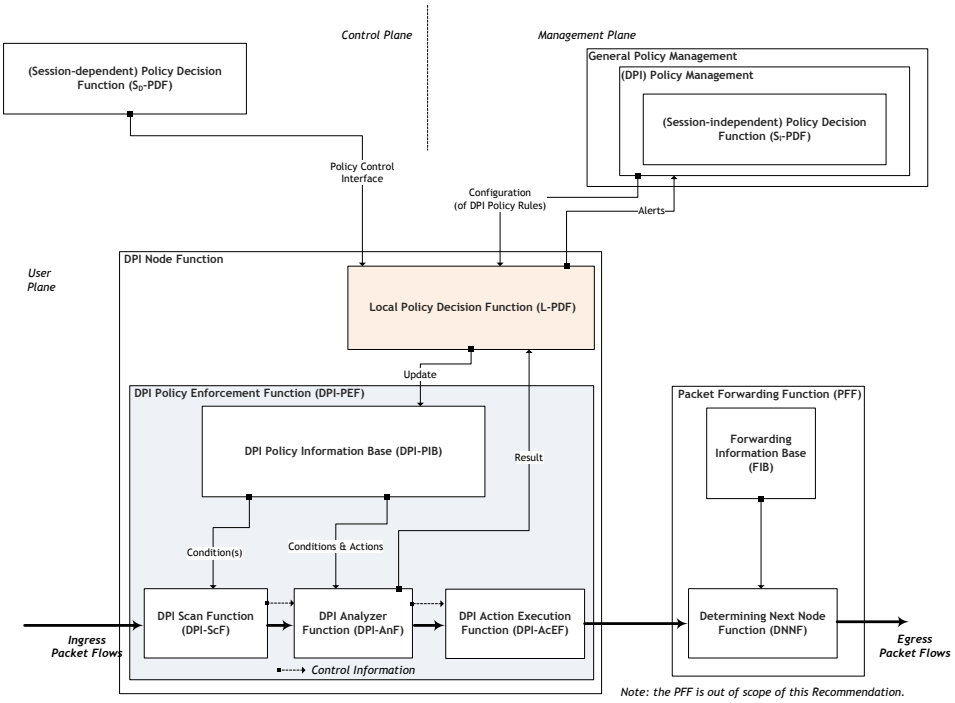


Figure 47 DPI models
"Modifying the DPI Policy Information Base via Control and Management Plane"

Note: the PFF is only present for *In-Path DPI* mode [Source: Figure 7-4/Y.DPIFR[37]]

II.3 3GPP

II.3.1 Overview

3GPP recognized the importance and benefits of standardized service based Policy and Charging Control (PCC) both to end users and to operators in the early days of the IP multimedia subsystem (IMS) standardization process. 3GPP PCC gives an operator static and/or dynamic admission, traffic and charging control via QoS and PCC rules. This PCC toolbox provides control of subscriber sessions on a service level, ensuring, for example, that a subscriber is allocated the required transport characteristics (e.g. guaranteed bit rate, minimum packet delay) for each of his services and is charged per service.

II.3.2 PCC ARCHITECTURE from 3GPP Rel-8 onwards

The policy and charging control PCC comprises the PCEF, BBERF, PCRF, AF, OCS, OFCS and SPR. From the policy and charging control perspective there are different architectural cases that depend on the protocol used between the Serving Gateway (SGW) and the Packet Data Network Gateway (PGW), whether the UE is roaming or in the home network and whether home routing or local breakout is applied to the traffic in the roaming case.

The PCC architecture for a non-roaming case is presented in Figure 48 below.

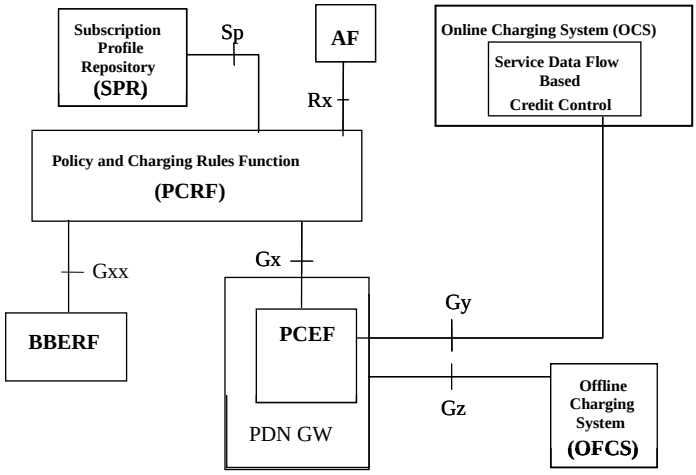


Figure 48 Relations to Other NGN standards PCC architecture for a non-roaming case

The PCC architecture for a home routed roaming case is presented in Figure 49 below:

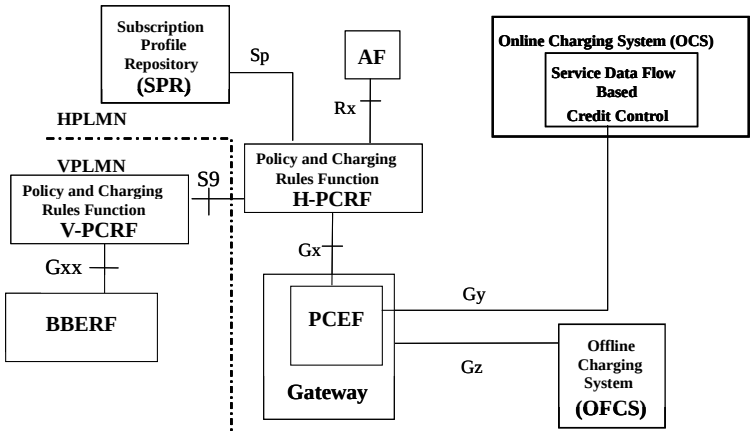


Figure 49 Relations to Other NGN standards PCC architecture for home routed roaming

The heart of the PCC architecture is the PCRF where service-session level policy decisions are taken based on PCC and QoS rules generated in the PCRF. These PCC rules are created based on operator configuration, session information received from the AF, and information received from the access network and the SPR (described below). Policy decisions are forwarded to the relevant Policy and Charging Enforcement Point or PCEF (located in the PDN-GW). Dynamic PCC rules are provisioned by the PCRF, while pre-defined/static PCC rules are provisioned directly in the PCEF.

The PCEF enforces PCRF gating requests, i.e. to control IP packet flow of a service session associated to a given PCC rule, and ensures that the service session does not exceed its

authorized QoS. In the case of On-line charging, the PCEF may deny access based on credit status provided by OCS.

The AF (Application Function) interacts with applications or services that request dynamic PCC. For example, a given application may require a certain minimum bandwidth and packet delay budget for the service to be delivered with an acceptable end-user experience. This information is provided to the PCRF (see below), which decides if this request can be fulfilled. The AF can also ask the PCRF for information on traffic-level events which occur in the network relevant to the service being delivered (decrease in bandwidth availability, changes in access type).
Subscription information related to IP-CAN transport level policies is stored in the SPR. The SPR can dynamically notify the PCRF of relevant changes to subscription information.
OCS allows online credit control for service data flow based charging (i.e. pre-paid), while OFCS provides a repository for offline charging (i.e. post-paid) and generates charging data records to be post-processed by the billing system.

The BBERF is applicable when a Mobile IP based mobility protocol is used towards the PDN GW. The BBERF is, if applicable, located in the serving gateway (SGW) or in access network gateway AGW for non-3GPP accesses. The main functions of the BBERF are to bind IP flows to "QoS bearers" in the access network with appropriate QoS and to report bearer level events to the PCRF. The BBERF is connected to the PCRF via a Diameter based Gx interface which is a kind of a QoS related subset of the QoS and charging control related Gx interface between the PCRF and the PCEF (TS 29.212[31]).

All interfaces shown are based on the Diameter protocol, except the Sp interface, for which no protocol has been specified in 3GPP.

II.3.3 Support of architectural requirements

The 3GPP PCC maps to the TR-101[6] architecture in the following way:

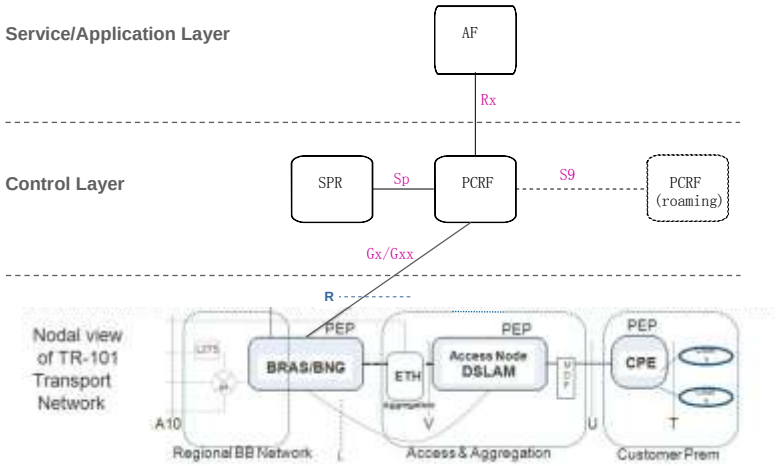


Figure 50 Mapping of 3GPP PCC to TR-101 architecture

The Service/Application Layer as well as Control Layer are already defined in 3GPP.
In this application the PCRF acts as the PDP. It serves the R interface by Diameter based Gx/Gxx resp.

II.3.4 Policy Information Model Overview

An information model (IM) is an abstraction and representation of the entities in a managed environment, their properties, attributes and operations, and the way that they relate to each other. It sspecifies a common description (syntactically and semantically) of the information that needs to be exchanged between various systems. It is independent of any specific repository, software usage, protocol, or platform; in other words, it is a technology neutral and implementation agnostic specification. Thus, an IM itself does not imply any specific architecture and as a result it also does not focus on any specific architectural mechanism (e.g. any form of provisioning or information exchange and coordination). However, the IM will serve as input to the architecture and implementation related specifications.
The value of such a specification is acknowledged across the industry as witnessed in DMTF, IETF, and TMF. This work is making inroads to become an important additional artifact before the specification of requirements for and development of a functional architecture. The DMTF CIM, IETF Policy, and TMF have defined various information models.
The intent of the IM is to support a variety of architectures. Hence, the IM should support architectures that:

- Manage network assets and resources by using a Network Management Systems (NMS) for example.
- Use policy-enabled solutions based on policy rules dynamically communicated via protocols (e.g., Diameter-based protocols) for wireline broadband applications and enforcing these rules as needed in individual network elements (NE).

IMs are typically described in the form of Object Oriented designs – as an example, UML is a popular "language" to describe the objects and relationships between these objects.

For example DMTF specifies a Policy IM (PIM). The PIM specifies a common description of policies, their conditions, actions, policy sets, etc. The PIM interacts with the other specified information models. Thus, typically, IMs are maintained as various subject specific IMs (and separate but related specifications).

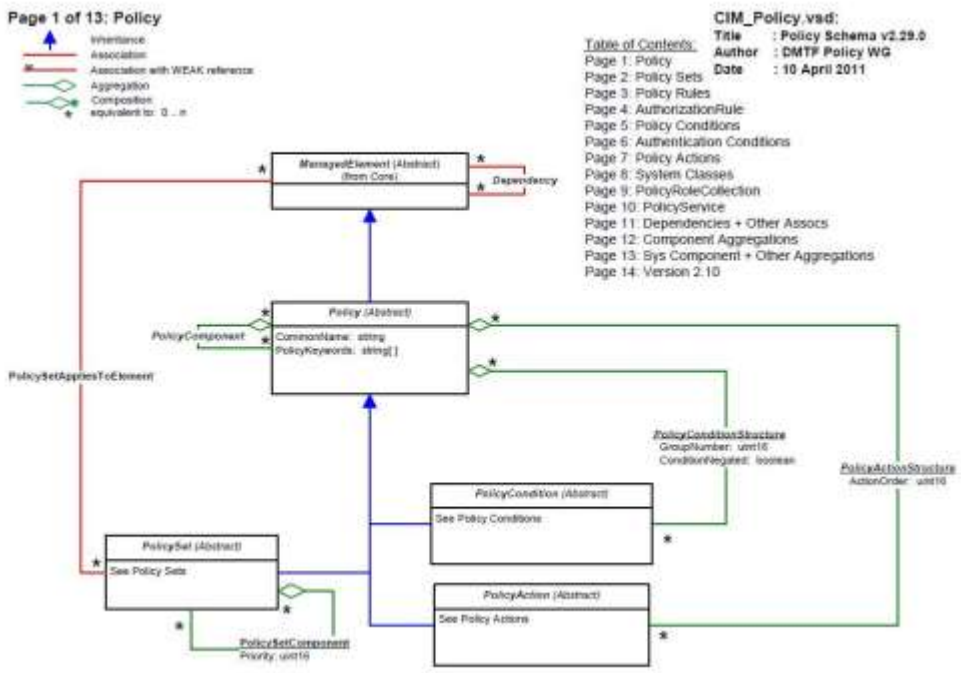


Figure 51 First page of the DMTF CIM Policy Information Model

Figure 51 shows the first page of the DMTF CIM defined PIM. DMTF CIM also has information models for QoS. An information model is technology neutral. In other words, it does not dictate any architectural mechanisms, however, an information model does need to support all the information that those mechanisms need to support.

Whereas typically information models are considered to support design of OSS, NMS, and EMS including their interfaces, they can be applied as a generic technique supporting any system including system interfaces. E.g. IETF RFC 3585[21] suggests that information models provide "…an on-the-wire representation over a transport protocol…"

Specific policy IMs have been developed in the IETF based on the DMTF CIM Common Schema – see RFC 3060[18], RFC 3460[20], RFC 3644[23], and RFC 3670[24]. These are extensions of the base DMTF CIM models.
Note that the information modeling approaches (e.g., formalism based on IETF RFCs) adopted in this annex are solely intended to aid the identification of the policy/QoS related information models and do not enforce any schema, protocols or implementation specification in any manner. When a technology neutral and agnostic IM specification, exists and with the use cases that need to be supported, one can make a variety of implementation technology choices, but is not limited to any specific choice. For example, typically, information models are mapped to data models that are technology specific, e.g. a specific directory schema such as the Lightweight Directory Access Protocol (LDAP) directory specification, or an XML Schema Definition (XSD) for an interface. Moreover, an IM can also be used as the foundation for the design of specific protocols (e.g. RFC 3585). Thus, a protocol and technology neutral IM specification allows the actual implementation to be realized in a variety of manners.

As mentioned earlier, architectures and architectural mechanisms implement the information model. Two examples of typical desirable architectural mechanisms are:

- Provisioned Execution Model RFC 3198[19]: This is an execution model where network elements are preconfigured, prior to and independent of events resulting from live traffic flows. Instructions are pushed to the network element, e.g. based on time of day or at time of booting the device. When a network element recognizes a certain event (e.g., as a result of traffic flows), it uses these downloaded (pre-provisioned) instructions. In other words, it does not hold up the traffic flow in any way and would not have to consult another entity.

- Signaled Policy Control Model: In this execution model, a dynamic policy control mechanism is used to identify and enforce the rules (e.g., for a given service, subscriber/subscriber group, etc.). A centralized component evaluates the conditions for the application of specific policies and communicates the results to a network element. Alternately, a network element may issue a query to the centralized component to obtain a policy. The interaction between the network elements depends on the architecture, and may be realized by means of a variety of mechanisms, including but not limited to APIs, signaling protocols (e.g., Diameter), etc.

"Signaled Policy Control" is contrasted with "Provisioned", but they are not mutually exclusive and operational systems MAY support both execution models for different types of policies.

These architectural mechanisms indicate what parts of the Information Model need to be implemented by the specific components that issue/receive/process requests. This makes intuitive sense, as the components that exchange information with each other will have the same semantic understanding of the managed entities that need to be processed.

II.4 Relationship between Information Flows, Policy Objects, and other Broadband Forum Technical Reports

The TR-134 IM supports both static and dynamic policies. For the broadband wireline domain, session information will be signaled between the Policy Decision Point (PDP) and the Policy Enforcement Point (PEP) (via the R interface as per the normative section of TR-134). The information flow over this interface will trigger the action of appropriate policy rules that are encapsulated within the IM objects embedded within the PDP and the PEP. The definition and development of appropriate information flows is thus an important part of the IM usage along with the associated IM objects.

II.4.1 Policy Information Model relationship to other Technical reports

The following diagrams show how this policy information model relates to other BBF Architectures and technical reports.

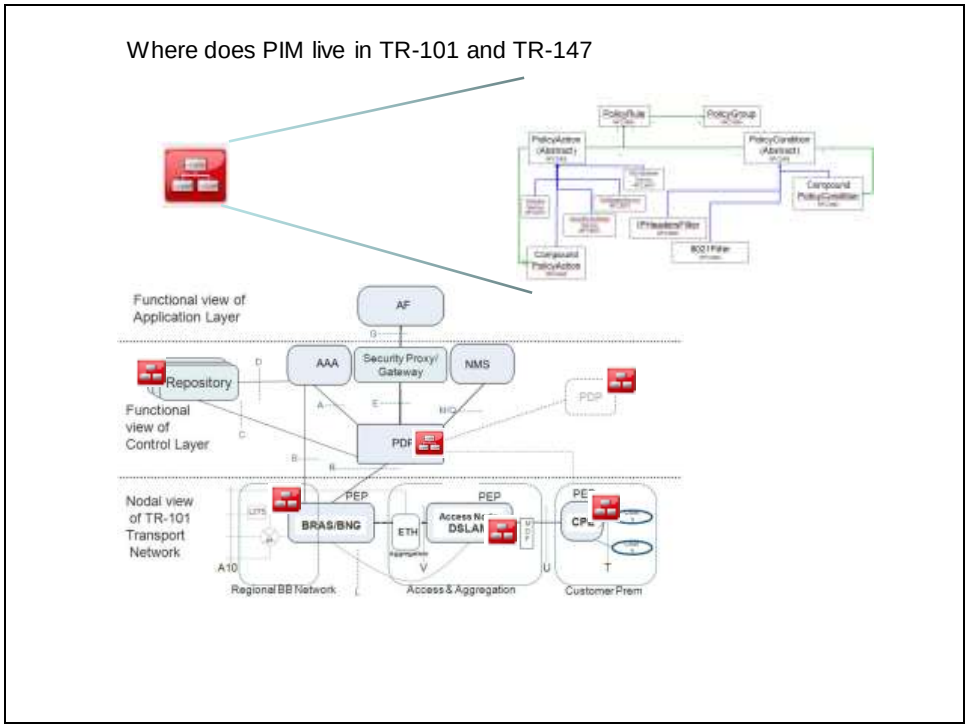


Figure 52 PIM relationships to TR-101 & TR-147

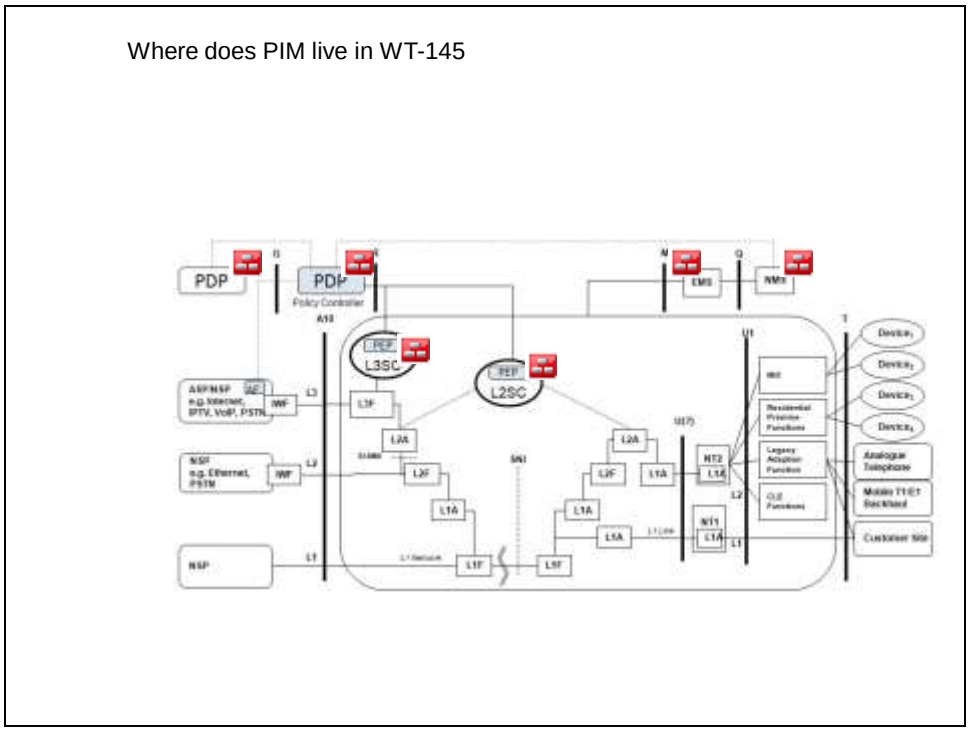


Figure 53 PIM relationships to WT-145

Appendix III. Policy Information Objects Definitions

This section provides a preliminary view of some of the objects selected from the IETF RFC Policy related IMs to support the use cases specified in the normative sections of TR-134. Additional selection is expected in future work.

III.1 Policy Information Objects Definitions

III.1.1 Policy Information Model Objects, Associations and Aggregations Definitions from RFC 3460

The following Table defines which object types definitions are utilized and referenced from RFC 3460[20] and included in the TR-134 PIM

Table 21 Object types referenced from RFC3460

Section	Object Name	Description from RFC
6.20	8021Filter	This concrete class allows 802.1 source and destination MAC addresses , 802.1 protocol ID, priority and VLAN identifier fields to be addressed
6.19	IPHeadersFilter	This concrete class contains the most commonly required properties for performing filtering on IP, TCP or UDP headers. Properties not present in an instance of IPHeadersFilter are treated as 'all values'.

III.1.2 Policy Information Model Objects, Associations and Aggregations Definitions from RFC 3670

The following normative Table defines which object type's definitions are utilized and referenced from RFC 3670[24] and are included in TR-134 PIM

Table 22 Object types referenced from RFC3670

Section	Object Name	Description from RFC
4.3.11	TokenBucketMeterService	A concrete class classifying admitted traffic with respect to a token bucket. Either two or three levels of conformance can be defined Additional cross references: TokenBucketMeterService refers to RFC 3290 "An Informal Management Model for DiffServ Routers" RFC 3290 refers to RFC 2697 "A Single Rate Three Color Marker" RFC 3290 refers to RFC 2698 "A Two Rate Three Color Marker"
4.3.16	8021QMarkerService	This is a concrete class that represents the marking of the user priority field defined in the IEEE 802.1Q specification.
4.3.15	DSCPMarkerService	This is a concrete class that represents the marking of the differentiated services codepoint (DSCP) within the DS field in

		the IPv4 and IPv6 packet headers, as defined in [R2474].

III.1.3 Policy Information Model Objects

The following information model objects below are provided with a different format and level of detail.

Table 23 Information model objects- Queuing

parameter	Parameter Type	Category	Value type	Description
QoS Queuing profile		QoS	String	This object identifies the QoS queuing (scheduling) policy that the BNG shall apply to the IP session

Table 24 Information model objects- Multicast

Name	Description	Derived From	Type	Abstract	Properties
MulticastFilter	A class that allows source and/or Multicast Address in IGMP message to be expressed in a single object	FilterEntry Base (referenced from RFC 3460[20])	Concrete	False	MulticastSrcAddress MulticastSrcAddressEndOfRange MulticastSrcMask MulticastGroupAddress MulticastGroupAddressEndOfRange MulticastGroupMask
Property	Description				
MulticastSrcAddress	This property is an OctetString representing a source IP address. When there is no MulticastAddressEndOfRange value, this value is compared to the source address in the IGMPV3 Membership Report Message, subject to the mask represented in the MulticastSrcMask property. (Note that the mask is ANDed with the address.) When there is a MulticastSrcAddressEndOfRange value, this value is the start of the specified range (i.e., the MulticastSrcAddress is lower than the HdrSrcAddressEndOfRange) that is compared to the source address in the IGMPV3 Membership Report Message and matches on any value in the range. If not present matches for all values				
Property	Description				
MulticastSrcAddressEndOfRange	This property is an OctetString representing the end of a range of source IP addresses (inclusive), where the start of the range is the MulticastSrcAddress property value. If a value for MulticastSrcAddress is not provided, then this property also MUST NOT be provided. If a value for this property is provided, then MulticastSrcMask must not be provided				

Property	Description
MulticastSrcMask	This property is an OctetString representing a mask to be used in comparing the source address in the IGMPV3 Membership Report Message with the value represented in the MulticastSrcAddress property. If a value for this property is not provided, then the filter does not consider MulticastSrcMask in selecting matching packets, i.e., the value of MulticastSrcAddress or the source address range must match the source address in the IGMPV3 Membership Report Message exactly. If a value for this property is provided, then MulticastSrcAddressEndOfRange must not be provided
Property	Description
MulticastGroupAddress	This property is an OctetString representing a mulitcast group address. When there is no MulticasGrouptAddressEndOfRange value, this value is compared to the multicast address in the IGMP Membership Report Message, subject to the mask represented in the MulticastGroupMask property. (Note that the mask is ANDed with the address.) When there is a MulticastGroupAddressEndOfRange value, this value is the start of the specified range (i.e., the MulticastGroupAddress is lower than the MulticastGroupAddressEndOfRange) that is compared to the multicast address in the IGMP Membership Report Message and matches on any value in the range.
Property	Description
MulticastGroupeAddressEndOfRange	This property is an OctetString representing the end of a range of multicast group addresses (inclusive), where the start of the range is the MulticastGroupAddress property value. If a value for this property is provided, then MulticastGroupMask must not be provided
Property	Description
MulticastGroupMask	This property is an OctetString representing a mask to be used in comparing the multicast address in the IGMP Membership Report Message with the value represented in the MulticastGroupAddress property. If a value for this property is not provided, then the filter does not consider MulticastSrcMask in selecting matching packets, i.e., the value of MulticastSrcAddress or the source address range must match the source address in the IGMP Membership Report Message exactly. If a value for this property is provided, then MulticastGroupAddressEndOfRange must not be provided

Name	Description	Derived From	Type	Abstract	Properties
MulticastControl Servcie	A class to define how IGMP message and Multicast duplication are processed in the data forwarding path of network device	ConditioningService(referenced from RFC 3670[24]	Concrete	False	MulitcastAssociateMVlan MulitcastProcess
Property	Description				

MulitcastAssociate MVlan	This property is a OctetString represents an multicast VLAN Identifier to be used for associating a IGMP message to a specific multicast domain
MulitcastProcess	This property is an enumerated 16-bit unsigned integer that is used to specify the IGMP message and Multicast duplication process represented by an instance of MulticastControlServcie 1 – Create MAC-level Group Filter entries in a multicast VLAN based on multicast group address in IGMP message and forward the IGMP message within a multicast VLAN. The multicast VLAN is specified by MulitcastAssociateMVlan property; 2- Dropped the IGMP message; 3- forward the IGMP message as user data

End of Broadband Forum Technical Report TR-134

