Policy Management Focus Group (PM-FG)

Assessment and Recommendations

June 2010
FINAL

ATIS is a technical planning and standards development organization that is committed to rapidly developing and promoting technical and operations standards for the communications and related information technologies industry worldwide using a pragmatic, flexible and open approach. Over 1,100 participants from more than 350 communications companies are active in ATIS' 22 industry committees, and its Incubator Solutions Program.

< http://www.atis.org/ >

The ATIS Policy Management Focus Group (PM-FG), Assessment and Recommendations is an ***ATIS Work Plan*** developed for the **TOPS Council**.

This document is subject to change. This document is a product of the PM-FG, and represents the consensus view of the PM-FG members. However, nothing contained herein is attributable to any particular member of the PM-FG.

Published by
Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

Table of Contents

EXECUTIVE SUMMARY

1.1 Problem Statement

As network resources are increasingly stretched by unprecedented growth in data traffic, Policy management is becoming an important industry topic. Many service providers are concluding that it is unrealistic to continue deploying additional capacity at the problem indefinitely. Policy management is emerging as a potential tool to get more capacity out of installed networks. Network policies are rules that are defined by the service provider to control and charge for the resources used for communication between end-points. Policies can also be used to bind the appropriate bandwidth, and Quality of Service (QoS) to a given application or subscriber. Policies can thus be used to control and better ensure the user's experience in utilizing a service or application, wherever the service is accessed. For example, a user streaming a video from a video service can be guaranteed a high quality viewing experience whether they are viewing the video on a smart phone or a High Definition TV.

Service convergence has been a vision of the communications industry for years, and recent deployment has begun to translate this vision into reality. Users can have a single contact number that will terminate on their landline phone, mobile phone, or computer, depending upon their needs. A given service can be accessed from a home network, a 3G network halfway around the world, or from a WiFi hotspot at the coffee shop around the corner. All of this demonstrates that service convergence is quickly becoming a practical reality, but only at the basic connectivity level. In most cases, once a user leaves their local service provider network they are limited to best effort. In many cases today, that is good enough, and the popularity of these services is growing exponentially. Growth at this level, especially from smart phones and netbooks, is already beginning to strain some networks, and it will only increase over time.

1.2 Policy Management as a Solution

Policy management can play a critical role in completing service convergence by making it transparent to the end-user. It can also be an important tool in helping service providers to effectively monetize resources. As already noted, policy affects all portions of the telecom ecosystem, but some areas are covered more effectively than others. In particular, the ability to accurately, consistently, and efficiently collect revenues from advanced services lags behind the ability for those services to be offered by providers.

Policy management is relatively well understood today within a single service domain, which in commercial deployments is typically limited to a single access technology. However, most interesting service convergence scenarios involve devices in multiple service domains, across different access technologies. Coordination of policy across these disparate domains with distinct access technologies is just now beginning to be addressed in standards, and still has significant standards gaps. Resolution of these gaps via a harmonized policy framework is needed for service providers to realize capital expenditures (CAPEX) and operational expenditures (OPEX) savings.

1.3 Scope of Effort

The initial scope of the Policy Management Focus Group (PM-FG) was network policy in the service provider network. However, at the request of the Technical and Operations (TOPS) Council, this scope was expanded to consider the application of policy to the network inside a

user's home (i.e., the home network (HNET)). This analysis was also driven by a series of cases based on scenarios where a service provider managed a user's HNET. In these use cases, management of a user's HNET was an optional capability offered by the service provider. The assumption is that this would require the user to opt-in, or subscribe to this additional service. The user would also have an ability to input their policy preferences, which would be combined with the network policy rules for traffic within the HNET and for upstream traffic from the HNET into the network. Policy management in the HNET is independent of policy management in the service provider network; when the service provider is not managing the HNET, all other aspects of policy management must continue to function normally. It was recognized that inside the HNET, there may be traffic from sources other than the service provider's network. Traffic that is completely within the HNET, such as video between a home video recorder and a television in another room, could potentially cause QoS disruptions if not managed properly. Addressing such traffic from other than the service provider's network was deemed out of scope for this analysis.

1.4 Assessment and Conclusions

The analysis conducted by this focus group was based on realistic end-user centric use cases contributed by service provider members. These use cases focused on capabilities providing concrete value to subscribers, with real revenue potential. The use cases were then analyzed to identify a number of requirements that applied to service provider networks, and by extension, to the standards these networks are based on. The analysis identified policy interworking between domains as the number one policy related standards priority. The group also agreed that policy interworking should be based on 3rd Generation Partnership Project (3GPP) Policy and Charging Control (PCC) S9 interface, with the specification of the required interworking to broadband networks. Although interworking is based on PCC S9 interface, this does not necessarily mean that the S9 interface must be used in its current form. If functions are required that are not supported by the S9 interface then it is recommended that 3GPP consider extensions to the PCC S9 interface to incorporate specific policy functions that are required for broadband networks. Policy interworking between domains is a necessary capability for service providers to offer consistent service capabilities to users independent of the access technology, or the service provider.

The PM-FG also concluded there is a business driver for developing a converged policy architecture. This is driven largely by operational expense reduction for service providers, but also has potential product consolidation value for vendors. There was general agreement that this work should take 3GPP PCC as the starting point for convergence, and enhance PCC where necessary. However, there was no consensus on the timing for convergence, or how far it should be taken. Some service providers also felt that the PCC architecture should not be the sole policy framework for all wireline networks. In part these different views are because the value of converged policy depends on each service provider's business model.

Finally, the PM-FG identified a number of specific requirements related to policy management. In general, these were not viewed as immediate, or even near term gaps. These were longer-term requirements that should be progressed in the context of ongoing standards work. There was a strong consensus that these items should not be allowed to distract attention from higher priority work on policy interworking or policy convergence. Nevertheless these are important requirements that should not be forgotten. The requirements that fell into this category include user privacy policies in the context of packet processing, application-aware content filtering

(e.g., parental controls), group subscriptions, policy support for multicast video in fixed networks, and interworking with Technical Report (TR-69) dynamic QoS for broadband networks.

1.5 Recommendations

The recommendations in this report fall into three broad categories:

- **Interworking** was identified as the top priority, and it was noted that 3GPP and Broadband Forum (BBF) are actively working to define policy interworking between wireless and broadband networks. To ensure maximum impact and business relevance, the members of this focus group have been actively contributing to this work in 3GPP and BBF based on the working conclusions of the focus group.
- **Convergence** was identified as an important objective that needs to be studied in more detail. Some SDOs are proposing to study aspects of policy management convergence, although it is not clear if they are considering all aspects as identified by this focus group. This report will be sent to the Alliance for Telecommunications Industry Solutions (ATIS) Packet Technologies and Systems Committee (PTSC) in the hope that it may help facilitate their analysis. It is expected that PTSC will continue to liaise with both 3GPP and BBF and share the results of their ongoing analysis to avoid duplication of effort between Standards Development Organizations (SDOs).
- **Other requirements** were identified and a plan proposed for how these should be addressed in standards. A point of contact was assigned for each item to ensure the recommendations in this report will continue to be addressed in standards after the focus group concludes.

It is important to note that this report focuses on policy from a network perspective. As a result, the recommendations in this report are restricted to requirements and standards for network-resource policy. Although policy can also be applied from other perspectives (e.g., applications) these are out of scope for this report. Future work may analyze policy requirements from this broader perspective, including the needs for 3rd party applications.

2 INTRODUCTION

Policy Management is becoming an important industry topic as a result of the deployment of new services over Internet Protocol (IP)-based, evolving fixed and mobile networks. Network policies are rules that are defined by the service provider to control the resources used for communication between end-points. Policies are used in effect to "compose" multiple services (e.g., charging services, location services, privacy/security services, or interaction with a 3rd party service provider) into a more complex service. Application of policies can be used to control the user experience as a subscriber is utilizing a service or application so, for example, a user streaming a video from a video service can be guaranteed a high quality viewing experience.

Policy affects all portions of the telecom ecosystem, but some areas are covered more effectively than others. In particular, the ability to accurately, consistently, and efficiently collect revenues from advanced services lags behind the ability for those services to be offered by providers.

There is also a recognized industry need to understand how to best allocate network resources; primarily network bandwidth, and security, according to defined business policies. A significant amount of work appears to be ongoing in the industry pertaining to policy management, although it is very disjointed. In order to assess the extent and complexity of the issues faced by service providers with respect to policy management, the ATIS TOPS Council formed a focus group to conduct an assessment of policy management from a network perspective. Specifically, this assessment included: 1) performing an inventory of policy management standards activities ongoing in the industry; 2) addressing specific issues related to packet processing, convergence and policy charging control; and 3) addressing any other issues that have been identified in the ATIS Next Generation Networks (NGN), Convergence, and Service Oriented Networks (SON) efforts, but are not within the purview of established ATIS committees or forums. It has also been recognized that standardized interfaces are needed to accurately and efficiently exchange policy-related signaling between networks for the purposes of policy decision making and enforcement.

The Pm-FG recognizes that the following organizations are addressing certain aspects of Policy Management: 3GPP/3GPP2, Internet Engineering Task Force (IETF), BBF, TeleManagement Forum (TMF), European Telecommunications Standards Institute (ETSI) Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN), International Telecommunications Union- Telecommunication (ITU-T), ATIS IPTV Interoperability Forum (IIF), ATIS PTSC, and ATIS SON Forum. However, given the importance of this topic to the continued development of NGN and convergence, there is a need to clarify the landscape of policy management standards activities. In addition, the areas of packet processing, convergence and policy-based charging control have been identified as pressing industry issues that need further assessment.

With this report, the industry will benefit from an inventory assessment of policy management standards from a network perspective and a gap analysis with recommendations for issues related to packet processing, convergence and policy charging control.

It is important to note that this report is focused on policy from a network perspective. As a result, the recommendations in this report will be restricted to requirements and standards for network-resource policy. Although policy can also be applied from other perspectives (e.g., applications) they are not within scope for this report.

3 METHODOLOGY

3.1 Overview of Initial Methodology

At the onset of this initiative, a roadmap was developed to provide structure for the PM-FG's assessment and assist in identifying milestones. The following is a graphical depiction of the roadmap. The accompanying text describes each of the phases in more detail.

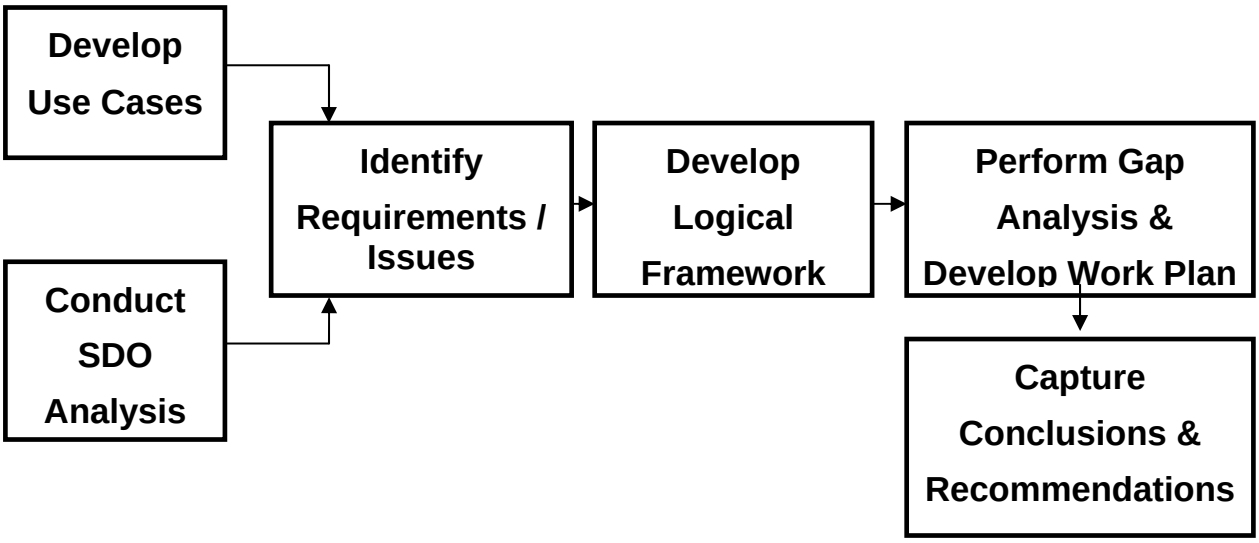


Figure 3.1 – Policy Management Focus Group Roadmap

Use Cases: starting from a core set of use cases input from the BBF, a set of policy management use cases were assembled from contributions provided by service providers. The use cases were grouped, and where appropriate combined into consolidated use cases that combined all relevant capabilities. The use cases were used to identify requirements that were directly linked to each use case.

SDO Analysis: an overview of the policy management related work being done in the key SDOs was assembled to provide a starting point for subsequent gap analysis.

Service Provider Requirements: the requirements that were directly linked to each use case were correlated. This allowed duplicate requirements to be eliminated, and allowed related requirements to be grouped together and consolidated. In some cases the focus group also identified "derived requirements" that were not directly linked to any single use case, but which could be inferred by considering the combination of several individual requirements.

Logical Framework: in order to identify standards gaps, and especially to determine the best place to address these gaps, a logical framework for policy management was required. The framework draws heavily on the partial frameworks currently used by 3GPP, BBF, and ATIS technical committees.

Gap Analysis: the service provider requirements, derived from use cases, were analyzed in the context of the logical framework, and compared against work already underway in other SDOs to identify gaps. When gaps were identified, the group considered the best forum to address the gap.

Conclusions & Recommendations: the output of the gap analysis was captured in the conclusions, along with recommendations on how these gaps can best be addressed.

4 USE CASES

The use cases in this document are typically based on a specific access technology, but generally are also applicable to a range of access technologies. Unless otherwise stated in the use cases, they should be viewed as independent of access technology.

4.1 Fixed Mobile Convergence (FMC)

4.1.1 Residential FMC

A family has purchased a family subscription plan that is independent of access (e.g., fixed or wireless) and location (e.g., both when at home and away from home). The subscription contains at least the following components:

- Internet access: includes service provider specific service such as firewall and content filtering (parental control) independent of access for selected devices within the family. The service is available at home, within the home mobile network and when roaming to a visited mobile network.
- Voice/Multimedia: QoS is provided for all access types, and mobility is available between the home Wireless Local Area Networks (WLAN) and Long Term Evolution (LTE) when outside the home. Roaming to another service provider's LTE network is also supported.
- Video: Premium Video on Demand Service including guaranteed bandwidth and QoS regardless of the access network (subject to the limitations of specific access networks).
- Flexible charging schemes are supported, depending on access type, user preferences and location.

4.1.1.1 Internet Access with Parental Control and Personal Firewall (UC1)

The kids leave their house and take a bus to their grandparents' house. The service provider specific services, like parental control and personal firewall, that were invoked for specific users and terminals, are provided in the home network, and continue to be provided in a consistent manner from the home network (fixed and mobile) and from any visited networks (fixed or mobile). This allows the kids to get the same service and filtering inside their home, in the bus going to the grandparents and at the grandparents' home. In this use case the grandparents have a different service provider than the family but the services will still be provided by the service provider where the family has a subscription, although access may be provided over the visited access network.

4.1.1.2 Voice/Multimedia and Charging (UC2)

The father travels home after work while talking on the phone with his colleague. The ongoing voice/multimedia call between the father and his colleague is maintained while switching over between LTE wide area network and residential fixed broadband WLAN network. Once the call switches over to WLAN, the charging changes, so that it is based on the home-based access. Bandwidth and QoS is maintained for the duration of the call,

independent of access, (subject to the limitations of specific access technologies) to guarantee the subscribed service delivery.

4.1.2 Video (UC3)

The kids in the backseat of the car are watching an Internet TV show on their laptop using LTE while being driven home from their grandparent's house. The TV show is sent from an Internet TV provider. Once they arrive at home, the terminal detects indoor WLAN coverage where the subscriber has a WLAN residential gateway connected to his fixed broadband network. The user or the terminal can then automatically select to switch the IP connection to the wireline broadband connection and the user can resume watching the same TV show on the same laptop, over the WLAN connection. It may be possible for the user to have a better quality picture over the WLAN connection, depending on the available bandwidth, user-specific policy, network policy and QoS setting.

4.1.3 Enterprise FMC

An Enterprise has purchased a subscription plan that is independent of access (e.g., fixed or wireless) and location (e.g., both when at work and away from the office). The subscription contains at least the following components:

- Internet Access: Includes specific services, customized for enterprise or personal roles, including firewall and content filtering independent of access for devices associated with the enterprise. The service may be user-selectable such that either work or personal role controls and services will be applied for internet traffic routed through the enterprise network. Users may be able to select roles on a per session basis; however the impact enterprise FMC is out of scope for this effort.

  NOTE: This does not preclude that the enterprise user remotely accesses the enterprise network e.g. from their home or via WiFi hotspot or macro-cellular coverage.

- Voice/Multimedia: Consistent QoS will be provided, with mobility between all access network types.
- Video: Premium Video on Demand Service, including guaranteed bandwidth and QoS regardless of access network (subject to the limitations of specific access networks).
- Flexible charging schemes can be applied, depending on access type, work/personal role selection, user or enterprise preferences, and location.

An enterprise may compose an "enterprise network" and its related applications/services from any combination of in-house or outsourced networking and application resources. It is for further study to identify which compositions are most likely and of those compositions what are the impacts on policy architecture of service providers offering subscriptions to the enterprise and to other users and interconnect and routing to other service providers (the so called "public network operators").

4.1.3.1 Internet Access with Enterprise Control / Firewall (UC4)

The enterprise user leaves the office and heads home from work. The enterprise internet access service is invoked for specific users and terminals from within the enterprise network. This service continues to be applied from the enterprise network as the enterprise user accesses the internet via cellular access and via the WiFi network in their home, allowing them to get the same services and performance anywhere (subject to the

limitations of specific access networks). In this use case, the Internet access service is provided to the enterprise user by the enterprise network with the enterprise network itself composed of any combination of in-house and outsourced networking and application resources including at least (for this use case), IP connectivity to the enterprise network via the cellular network for enterprise users outside the office and connectivity to the Public Internet from office sites. Filtering, firewall and charging/accounting aspects of the service may be provided by a combination of in-house and/or outsourcing to a service provider subject to appropriate commercial arrangements.

4.1.3.2 Voice/Multimedia and Charging (UC5)

The enterprise user travels home after work while talking on the phone with his colleague. The ongoing Voice/Multimedia call between the enterprise user and his colleague is maintained while switching over between LTE and residential fixed broadband WLAN network. The requested bandwidth and QoS is maintained for the duration of the call (subject to the limitations of specific access networks) to guarantee the same service delivery. Charging may vary as the call is handed off between the various access networks. Users may be able to select roles on a per call basis; however the impact enterprise FMC is out of scope for this effort.

4.1.3.3 Video (UC6)

The executive in the backseat of the car is watching an Internet TV live meeting on her laptop using LTE while riding to the office. The TV feed is sent from an enterprise site. Once in the office, the terminal detects indoor WLAN coverage from the enterprise WiFi network. A policy can be set on the terminal to automatically switch the IP connection to the wireline broadband connection (WiFi) and enable the user to resume watching the same Internet TV live meeting on the same laptop. Alternatively the user can manually switch from LTE to WiFi coverage. Accessing the broadcast over the WLAN may make it possible to support a better quality picture depending on the available bandwidth, user-specific policy, network policy and QoS setting.

4.1.4 Femtocell

4.1.4.1 Residential Femtocell (UC7)

A subscriber desires to improve coverage and access speed for their mobile device in their home. They purchase and install a Home eNodeB (Femtocell AP) device for their home which attaches to the home LAN and establishes a connection back to the subscriber's mobility service provider network. Real time coordination may occur between the mobility provider and the broadband access provider to deliver proper bandwidth and QoS to support a good QoE for calls and data sessions made within the home that access services from the mobility network. The Femtocell may allow some types of data traffic to be shared with the home LAN, including traffic for Internet applications. Local traffic can be discerned and accounted for differently than traffic that is carried on the mobile network.

4.1.4.2 Enterprise Femtocell (UC8)

An enterprise desires to improve coverage and access speed for their mobile devices in their office. They purchase and install one or more enterprise femtocell devices for their office which attaches to the enterprise Local Area Network (LAN) and establishes a connection

back to the enterprise's mobility service provider network. Real-time coordination may occur between the mobility provider and the enterprise and the enterprise's broadband access provider to ensure appropriate resources to support a good QoE for calls and data sessions made within the office that access services from the mobility network. The femtocell may allow some types of data traffic to be shared with the enterprise LAN, including traffic for Internet/enterprise applications. Local traffic can be discerned and accounted for differently than traffic that is carried on the mobile network.

4.2 Applications

4.2.1 Application Mobility

4.2.1.1 Subscriber/Application Mobility (UC9)

A subscriber is in a multimedia call on their mobile device, and then wishes to change the device they are using to a fixed, residential network attached device (in this case a set top box / TV). Following a command by the subscriber the multimedia call is transferred to a STB with a large screen display. The subscriber resumes the call on the set-top box / TV. Bandwidth and QoS are adjusted as required for the large screen experience to be meaningful. Accounting and settlement is supported among the application and network service providers, and reflects the changes to the access technology and required bandwidth.

4.2.1.2 Enterprise/Application Mobility (UC10)

A subscriber is using an application on their mobile device, and then wishes to change the device they are using to a fixed, enterprise network attached device. The multimedia call is handed over from the mobility macro network to an enterprise network, but instead of remaining on the same device, the employee chooses to transfer the multimedia call to a teleconference controller with a large screen display and resumes the call on that device. Bandwidth and QoS are adjusted as required for the large screen experience to be meaningful. Accounting and settlement is supported among the application and network service providers, and reflects the changes to the access technology and required bandwidth.

4.2.2 Application Interface (UC11)

A service provider is supporting a large number of applications, including carrier-hosted services (e.g., IP Multimedia Subsystem (IMS)) as well as 3rd party applications, and needs to provide this in a cost-efficient way. To reduce operational expenses the service provider wants a consistent, simplified policy interface to access network resource policy capabilities. This interface will be accessible either directly or indirectly (depending upon trust relationships) by all applications. A single point of admin / policy decision is required for policy requests from applications.

4.2.3 Application Service Systems ANI (UC12)

A network service provider supports access to a large number of applications, including 3rd party application providers. Application providers have the ability to request that policy rules be applied to the network via a consistent Applications Network Interface (ANI). Policy rules

can also be requested by the end user, across the User Network Interface (UNI), and these could potentially be in conflict with the request from the application provider, across the ANI. The network service provider has a mechanism for defining how these conflicts will be resolved, based on preferences and commercial agreements with the user and the application provider. Charging is based on a number of criteria, including which policy is given precedence. This use case implies:

- Application of policy rules according to the application server ANI
- Resolution of policy rule conflicts between application server ANI and application subscriber UNI
- Authorization to allow application server policy requests to override end user subscriber policy rules
- Charging function applied to application server ANI when app server policy rules override application subscriber UNI policy rules
- Negotiation of policy rules between subscriber home network and application service network

4.2.4 Flexible Application Policy (UC13)

Joe subscribes to high-speed Internet and voice service from his local service provider. He also subscribes to a 3rd party application package that includes online video games, karaoke on demand, and an electronic newspaper service. Joe wants to receive consistent QoS across the various applications except for the electronic newspaper, which is best effort. He also has a number of policies that he wants applied to his services. He is competing in the international karaoke championships, so he has defined a policy that ensures he is not disturbed when he is practicing his karaoke. This policy automatically diverts all calls to voice mail while he is using the karaoke on demand, except for calls from Lisa, his karaoke coach.

4.3 Nomadicity

4.3.1 Nomadic Customer Use Case Context

A business customer has subscribed to a service that is independent of location. The service includes both voice and multi-media, with QoS provided on the home Wide Area Network (WAN) as well as on the visited WAN. Depending on the service contract, the request for QoS on the visited network could come from the home network, or directly from the user. The charging schemes for this service are connected to the access type, user preferences, and location. This service also provides full support for emergency service requests, including providing location information for 911 and other citizen to authority services when using a visited network.

4.3.1.1 Nomadic Business Use Case (UC14)

A road warrior travels to a different city and establishes an extended stay location on a visited network. He uses a Voice over Internet Protocol (VoIP) soft client or WLAN-phone at the extended stay location. QoS agreements based on the home network subscription are applied to visited network. Charging functions may apply to use and QoS establishment between networks. This use case introduces:

- Recognition of multiple sessions and session types on a specific access and enforcement of policy control limiting to subscribed bandwidth for the aggregate transport.
- Enforcement of session limits within the subscribed parameters for specific session type. For example, subscription of a customer may limit the number of voice sessions to "n" and the number of video sessions to "y" on the aggregate service transport (UNI or Network-to-Network Interface (NNI)).

4.3.1.2 Nomadic User (UC15)

Same as previous use case, except that the home network provider has a wholesale arrangement with the access network provider, so that it appears to the customer as if the access network is owned by the home service provider. However, this introduces additional inter-provider policy requirements. These inter-provider policies could be applied to the individual user on a per session basis, or the policies might be applied to the aggregate traffic between the access network provider and the home network provider. This use case introduces:

- Ability for target network to receive a policy request (e.g., the serving access network) and to evaluate the policy request in the context of its own policies to determine whether or not the request should be granted. The "inputs" to this policy decision include factors such as whether accepting this request would violate the Service Level Agreement (SLA) between the service provider and the serving access network provider, and the availability of resources in the serving access network.
- Ability to account for aggregate resources used as a result of policy requests admitted under a particular SLA.

4.3.1.3 Nomadic User Establishes Location for Emergency Services (UC16)

A nomadic user has established a temporary visited location. The user registers with their home network. An emergency service address is established for the user's temporary location. The user makes an emergency call/session request (911) and the request is forwarded, along with the correct location information, to the appropriate responder location based on the user's temporary address and the policies established (implicitly or explicitly) during registration. This use case introduces:

- The ability to over ride pre-subscribed policy limits for specific secured and authorized access.
- Ability for a visited network to be informed of an emergency service request by a nomadic user.
- Ability for a visited network to automatically identify the service request point/location of the nomadic user requesting an emergency service.
- Ability for a visited network to establish guaranteed QoS parameters for a nomadic user requesting emergency service.
- A mechanism where the home network may request back to the visited network a QoS matching the requirements of the nomadic users. The ability of the home network to communicate the location and session attributes of the nomadic user and the appropriate session attributes.

- A mechanism where the nomadic user can request a specific level of QoS from the visited network for the specific session requested.
- A charging mechanism for the visited network to charge for specific policy enforcement request to meet a guaranteed QoS. A charge back to the home network to be applied to a specified Nomadic user.

4.3.2 Network Interface (UC17)

A service provider is supporting coordinated policy requests for services that span multiple service providers. To reduce operational expenses, it requires a consistent NNI/ANI policy interface to all other carriers, whether they are wireline, wireless or transport providers.

- Reduce operating expenses by simplifying policy interfaces from other networks.
  - Single point of admin / policy decision for policy requests from other networks.
  - Many existing interfaces exist. Develop standard interconnect interface that also meets additional service requirements enumerated in this Use case register.

4.4 Aggregate Policy Controls

4.4.1 Media Session Aggregation (UC18)

A subscription includes a range of media types, including voice, video, and Internet access. All media types in a given session are aggregated over a common transport interface UNI. (In the case of large enterprises, this interface may be treated as an NNI, but for the purposes of this use case, it is called a UNI.) The subscriber could be a residential user, a small business, or a large enterprise. Based on the defined policies, as specified by the user and the service provider, each service receives an agreed QoS and bandwidth over the shared access link. If any traffic involves multiple service providers, the agreed QoS and bandwidth will be maintained across the NNI. This use case introduces:

- Session management within subscribed policy limits on aggregate transport
  - Recognition of multiple sessions and session types on a specific access and enforcement of policy control limiting to subscribed bandwidth for the aggregate transport.
  - Enforcement of session limits within the subscribed parameters for specific session type. E.g., subscription of customer may limit the number of voice sessions to "n" and the number of video sessions to "y" on the aggregate service transport (UNI or NNI).

4.4.2 Session Establishment Beyond Pre-subscribed Limits (UC19)

A business user subscription includes access to a priority non-emergency override service (i.e., neither 911, Government Emergency Telecommunications Service (GETS), Wireless Priority Service (WPS), National Security/Emergency Preparedness (NS/EP), nor other government emergency services). This service allows the user to override the established traffic limits, and allow more traffic. This would be subject to availability of aggregate subscribed resources, and typically for a higher fee. This use case introduces:

- Session establishment beyond pre-subscribed limits

  - Allows override of pre-subscribed policy limits by specific secured and authorized access.

4.4.3 Network Operations (UC20)

A service provider wants to ensure that traffic from network operations staff receives priority treatment to ensure that the network performance is optimized. This includes prioritization of standard network operations traffic, as well as prioritization of elevated activity network operations traffic (e.g., outage scenario, public emergency scenario, etc.). This use case introduces:

- Application of a QoS level to service provider traffic for the daily operation of the network.
- Authentication and authorization of service provider for QoS level application.
- Application of a QoS level to service provider specific to elevated activity level.

4.4.4 Dual Carrier Network Service Subscription (UC21)

A large national or multi-national enterprise customer has multiple sites geographically dispersed. The enterprise customer subscribes to multiple service providers for network access based on physical office location. The enterprise customer requires consistent policy rules across all locations and service providers. This use case introduces:

- Policy management coordination across multiple access carriers.
  - Application of common QoS level to services for enterprise users when the enterprise network utilizes multiple carrier networks.

4.4.5 Priority User Override (UC22)

An executive or high-ranking official within an organization requires an immediate session and the access network has reached the limits of its service level agreement. The executive chooses to invoke an override and may temporarily expand the policy or pre-empt a lower priority session from within the organization. This use case could apply to private enterprises as well as government organizations. This use case introduces:

- Session establishment beyond pre-subscribed limits
  - Allows over ride of lower priority sessions from within the same organization when IP-Connectivity Access Network (CAN) does not support additional sessions.
  - Authentication and authorization of priority user.
  - Allow temporary expansion of policy or SLA if physical limits allow.
  - Charge notification for business priority override.
  - Charge acceptance for business priority override.

4.5 Miscellaneous

4.5.1 Emergency Services (UC24)

During a major disaster, the network is overloaded with traffic between emergency responders inside the disaster zone, outbound traffic from the emergency responders, inbound traffic to the emergency responders, citizen to authority traffic, and general traffic. Correct prioritization of these traffic types must be maintained. This use case introduces the need to provide:

- Priority of emergency responder inside disaster zone
  - After recognition of a disaster, the application of priority QoS level to emergency responder traffic within the disaster zone
- Disaster area emergency responder outbound priority
  - After recognition of a localized disaster, the application of priority QoS level to emergency responder traffic exiting the disaster zone
- Disaster area emergency responder inbound priority
  - After recognition of a localized disaster, the application of priority QoS level to emergency responder traffic entering the disaster zone
- Disaster area general use outbound prioritized over inbound
  - After recognition of a localized disaster, the application of priority QoS level to general traffic exiting the disaster zone

4.5.2 Time- and Location-Sensitive Billing (UC25)

Jane, a self-employed consultant, has a home office but spends most of her working time at her customers' places of business around the country. Having been incented by the "home zone" provisions of her cell phone company's nationwide data service plan, she recently purchased a 4G data card for her laptop & replaced her Digital Subscriber Line (DSL) service. While at her home waiting for a taxi to take her to the airport on Monday morning, she joins one of her customer's webinars. The taxi soon arrives, and she continues viewing the webinar in the taxi. As the taxi leaves her "home zone" area, the volume-based billing rate for the webinar traffic changes. She later visits a customer that day in another city, and catches up on email that evening at the hotel on her laptop. Internet access is not free at the hotel, so she uses her data card instead. Since she is outside her "home zone," time-based provisions of her data service plan apply, and the volume-based billing rate applied to her traffic changes as the weekday data busy-hour approaches. Jane's subscription includes Advice of Charge. Thus, she may check at any time an estimate of charges for an in-progress session; moreover, at the start of each data session and when the charging rate changes mid-session, she is advised of the rate at which the session is being charged.

4.6 HNET Use Cases

The following use cases were analyzed as part of the Policy Management Focus Group HNET sub team.

4.6.1 User Exceeds Authorized Bandwidth (UC26)

While a user is watching a high definition quality video on demand using the maximum subscribed bandwidth, he/she receives a video call. During the video conversation, the quality of the video may deteriorate, if allowed by the policy control.

4.6.2 Authorizing Maximum Bandwidth (UC27)

A user has subscribed to a multicast/linear-Internet Protocol Television (IPTV) service package, which includes channels A, B, C, & D. The user wishes to view the program shown on channel A. The user presses the remote control, which signals the set top box to initiate a request to the network for the multicast service. The network provides the set top box information on the

bandwidth requirements for the service package, which includes the maximum bandwidth required for any of the channels in the service package plus other services such as re-transmission. The set top box calculates the total bandwidth required for the user to view any of the channels in the service package. The set top box sends a request to the network for the allocation of the total bandwidth. The network allocates the total bandwidth. User moves between the channels A, B, C, & D to view different programs. The set top box makes no further request to the network for bandwidth de-allocation and re-allocation. When the user has finished using the service the set top box releases the network resources.

4.6.3 Home Network Traffic (UC28)

Several household members watch a downloaded movie to a storage device from different rooms using different end-user devices (e.g., set top box/"big screen", mobile device, laptop), while one household member wishes to view a program shown on a multicast/linear-IPTV channel and initiates the request for this via a set top box.

4.6.4 HNET and Roaming (UC29)

A mobile user with a subscription to "mobile service provider A" (SP-A) attaches to a femtocell associated with "mobile service provider B" (SP-B) in a friend's home-based network that has fixed broadband access from "service provider C" (SP-C). In this use case, SP-A and SP-B have a roaming agreement that specifies the charging policies. In this scenario, there are two policies that apply: policy determined by service provider B and a femtocell subscription, and policies authorized by SP-A for QoS to the mobile user. In general, the home node B (femtocell) policies will take precedence. Depending upon configuration, the mobile user could access services from SP-A (home network services) or from SP-B (visited network services). Charges for services used while attached to the femtocell may be billed to the mobile user, through the subscription with SP-A. The friend would not see any incremental charges at all, either for the use of the femtocell, or for broadband network usage.

4.6.5 3rd Party Pre-scheduled and/or On-demand Download Service (UC30)

A user with a high-speed connection subscribes to a 3rd party provider, with a business relationship with the service provider, for pre-scheduled and/or on-demand video download through the 3rd party supplied device (e.g., Digital Video Recorder (DVR)). The 3rd party provider may have pre-agreed [static] QoS arrangement with the user's access provider for streaming service. Alternatively, the 3rd party may request a one time bandwidth increase for faster video download (especially on-demand subscription), if the capability is supported by the access provider.

5 SDO ANALYSIS

SDOs are currently working both independently and in conjunction in order to address many different aspects of network policy management standards. In some circumstances, standards are being developed without harmonization, therefore creating some overlapping work and leaving some key areas uncovered. Thus, in order to identify the amount of overlapping work and gaps that require immediate attention, a high-level examination of the current state of standards defined by the following industry organizations; ITU-T, ETSI TISPAN, 3GPP, 3GPP2 and BBF is required.

The analysis of policy management standards delineated in this section identifies several aspects that are common to multiple SDOs and are relevant to packet processing, convergence and policy charging control principles stated in the scope of this Focus Group. Appendix G provides a more detailed overview of individual, ongoing policy management standardization activities from a network perspective (e.g., access, aggregation, core network, and peer network), as defined in the industry.

5.1 Functional Roles in Policy Frameworks

Policy management standards for wireless and wireline networks define the following functional entities to process incoming session initiation prior to formal admission into the underlying network, as well also to provide interconnection processing between network domains in end-to-end sessions.

- ***Policy Decision Function (PDF)***: Responsible for evaluating policy rules when interacting with the application and enforcement points to determine the resource requirements of the incoming session considering policy functions such as:
  - Application of charging rules
  - Resource allocation / reservation
  - QoS / priority
  - Network Address Port Translation (NAPT) / Network Address Port Translation – Protocol Translation (NAPT-PT)
  - Gate Control
  - Usage metering
  - Transcoding
  - NAT traversal
  - Traffic policing
  - Traffic shaping, rate limiting

  The scope of policy rules may include the following:

  - Per network
  - Per application
  - Per subscriber group
  - Per subscriber
  - Per device
- ***Policy Enforcement:*** Based on policies defined by policy decision functions, the policy enforcement function is responsible for realizing the resource requirements in the

underlying transport layer, along with admission or denial of the session (e.g., packet policing, packet marking, QoS and priority support).

5.2 Distinguishing Aspects of Policy Framework

This analysis considers distinctive aspects of the Policy Framework development such as the following:

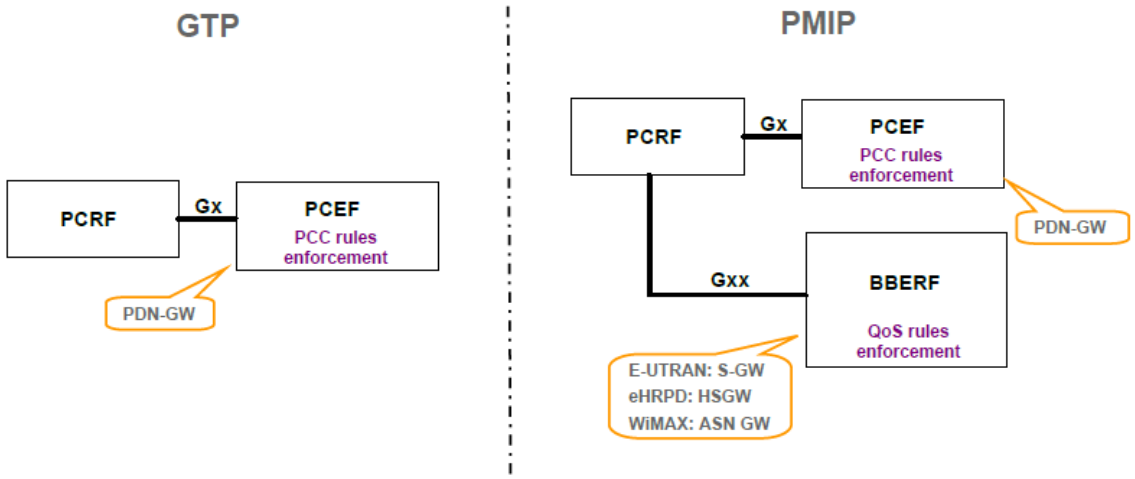
- Coordinated control over multiple policy enforcement points
- Policy repository for subscriber and/or network policies
- Inter-working with "Packet Processing"
- Home network control over roaming, mobile subscribers
- Charging control (specified by 3GPP & 3GPP2)
- Border Policy Control

While wireless, 3GPP and 3GPP2 policy standards include charging rules in their purview, wireline, ITU-T RACF and ETSI TISPAN Resource and Admission Control Subsystem (RACS) standards do not address charging. Wireline, RACF and RACS specifications integrate access and border policy controls. 3GPP and 3GPP2 have specified access policy controls only, and a Release 10 study item related to 3GPP TR 23.848 has introduced IMS border policy control that is distinct from the access-associated, Policy and Charging Control (PCC) framework.

5.2.1 Coordinated Control Over Multiple Policy Enforcement Points

The 3GPP Release 8 Policy Framework (TS 23.203) defines the control over the following policy enforcement points:

- The Policy Charging Enforcement Function (PCEF), such as the 3GPP Packet Data Network Gateway terminates the Gx interface for PCC rules provisioning.
- The Bearer Binding and Event Reporting Function (BBERF) such as the Serving Gateway (S-GW), terminates the Gxx interface for QoS rules provisioning, as well as detecting and reporting events.



REL-8 3GPP PCC Architecture (non-Roaming)

Figure 5.2.1-1 – REL-8 3GPP PCC Architecture (non-Roaming)

The adoption of a reference model for cdma2000 systems according to the 3GPP PCC architecture in the draft X.P0062 specification proposes the following non-roaming cases.

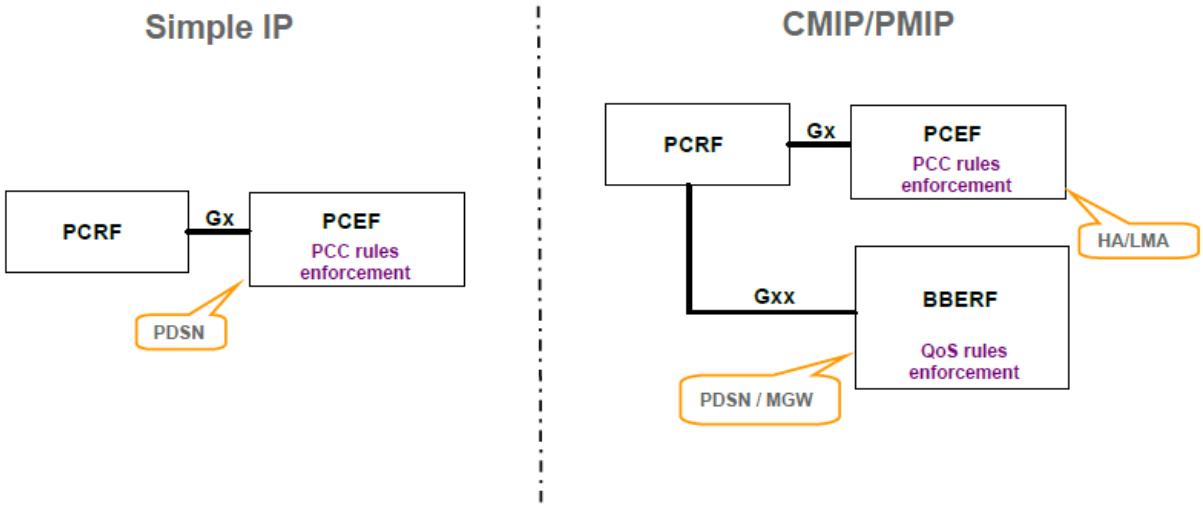
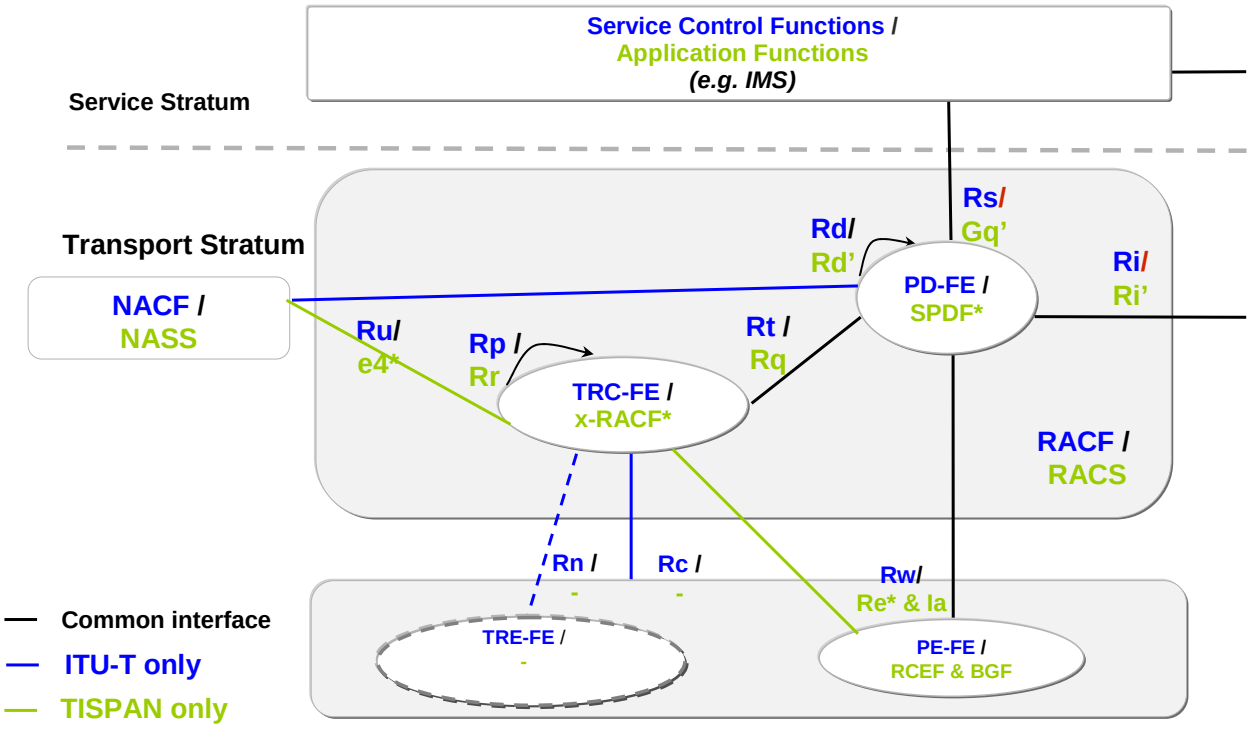


Figure 5.2.1-2 – 3GPP2 PCC Architecture for cdma 2000 (non-Roaming)

Both ITU-T RACF (Y.2111) and ETSI TISPAN RACS (ETSI ES 282 003) standards define the control over the following policy enforcement points:

- Gateways (e.g. BNG, edge router, SBC/BGF)
- Access node (e.g. DSLAM, OLT)
- L2 aggregation node

The following diagram maps ITU-T RACF and TISPAN RACS functional architectures, and corresponding network entities and interfaces.



*: The transport subscription profile checking is performed by A-RACF in TISPAN

Figure 5.2.1-3 – ITU-T RACF & TISPAN Function Architectures

The above diagram provides an approximate mapping between ITU-T RACF and TISPAN RACS. In fact the distribution of functions between the functional entities is not a one to one mapping. As shown in the table below the "Policy Decision Function" in TISPAN is distributed across two functional entities – the Service-based Policy Decision Function (SPDF) and the x-RACF. In other words the SPDF and X-RACF both contain elements of the ITU-T Policy Decision Functional Entity (PD-FE). This split of policy decision functionality between the SPDF and x-RACF is also reflected in the fact that in the ITU-T architecture the network attachment information is uploaded to the PD-FE (via the Ru interface) whereas in the TISPAN architecture similar information is uploaded to the x-RACF (via the e4 interface). The network attachment information includes the user QoS profile that the policy decision function (x-RACF in TISPAN, PD-FE in ITU-T) then uses to apply subscriber specific policies.

FEs	ITU-T	ETSI
Policy Decision Function	PD-FE	SPDF*+X-RACF
Policy Enforcement Function	PE-FE	BGF/RCEF
Resource Control Function	TRC-FE	X-RACF*

Interfaces	ITU-T	ETSI
Rs	Diameter	(Gq') Diameter
Rw	H.248/COPS/ Diameter	(Ia) H.248 (Re) Diameter
Ri	Diameter	(Ri') Diameter
Rc	COPS/SNMP	–
Rd	Diameter	(Rd) Diameter
Rn	TBD	-
Rp	RCIP (new), ANCP	(Rr) Diameter
Rt	Diameter	(Rq) Diameter
	Diameter	(e4) Diameter

Figure 5.2.1-4 – FEs for ITU-T and ETSI

The following chart compares ETSI TISPAN and 3GPP network attachment procedures.

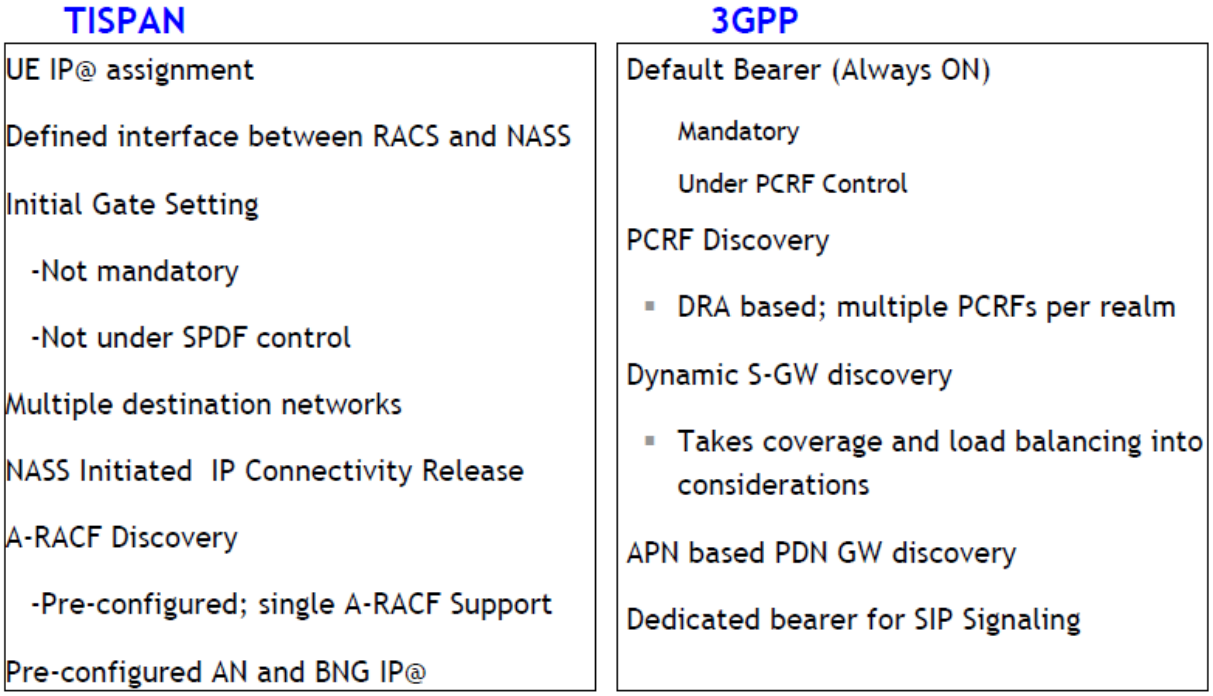


Figure 5.2.1-4 – ETSI TISPAN and 3GPP Network Attachment Procedures

There are obvious differences between the 3GPP/3GPP2 and ETSI TISPAN/ITU-T approaches concerning the control over the following policy enforcement points. The PCRF has been generally adopted for policy control by a range of SDOs, including the ATIS NGN Architecture. Since standardized PCRFs have enjoyed broader deployment and standardized wireline policy servers, emphasis should be given to PCRF-based control of policy enforcement points in a converged environment.

5.2.2 Policy Repository for Subscriber and/or Network Policies

The following depicts 3GPP's and 3GPP2's Policy Management functional models. The Subscription Profile Repository (SPR) in the 3GPP PCC architecture and Subscriber Policy Repository in the 3GPP2 Service Based Bearer Control (SBBC), stores subscription information related to the IP-CAN transport level policies needed for definition of PCC rules by the PCRF. There is one significant difference between the 3GPP and 3GPP2 functional models; 3GPP2 includes the ability to store service provider network policies in the SBBC policy repository, while the 3GPP policy model does not include equivalent functionality. Network policies define how network resources are generally to be utilized, and may be of higher or lower priority to a particular subscriber priority, as defined by the service provider. Furthermore, network policies provide centralized control over the network and specify service provider rules across multiple subscribers. Although 3GPP2 has identified a Network Policy Resource (NPR) function, it has not defined the specific operation policy rules for that function. 3GPP does not include a separate NPR function at all. In addition, the NPR function has not been implemented by any vendors. Therefore, the separate NPR function is not considered as a gap.

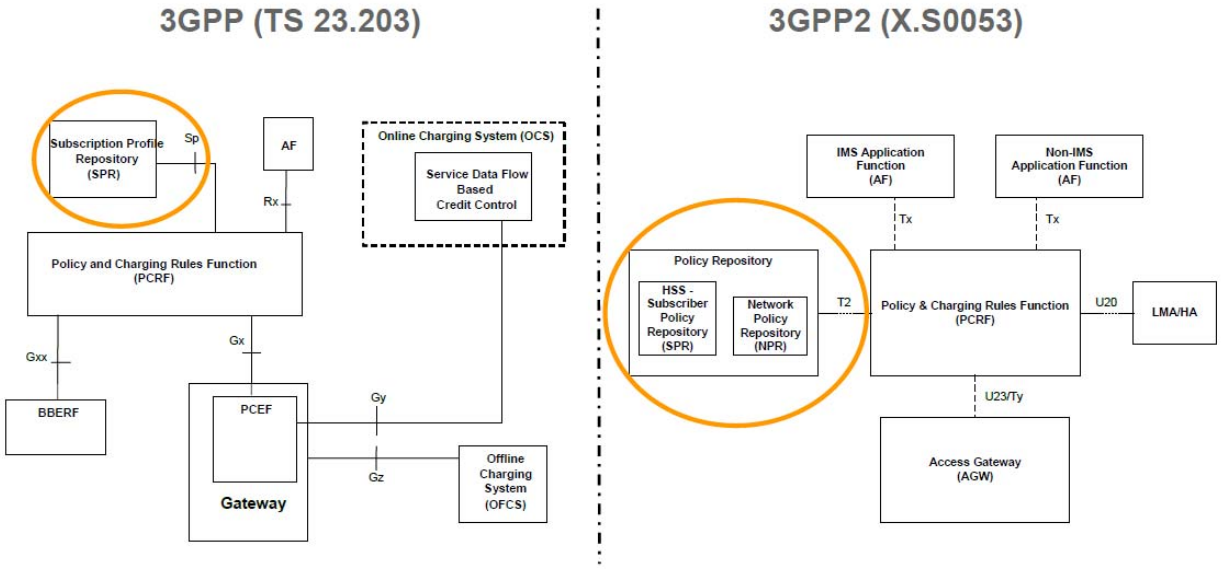


Figure 5.2.2-1 – 3GPP (TS 23.203) & 3GPP2 (X.S0053)

It must be noted that ETSI TISPAN ES 282 004 defines the Profile Data Base Function (PDBF) as the functional entity in the (NASS) that contains the user network profile as part of the NASS user authentication data. The user network profile includes QoS Profile Information element required for network access configuration. The QoS profile information defines subscribed transport service class and application class, i.e. maximum amount of bandwidth subscribed by the attached user in uplink and downlink directions, and maximum priority allowed for any reservation. According to ETSI TISPAN ES 283 034 the QoS Profile Information is transferred by the NASS to RACS as part of the NASS user profile information sent over the e4 interface.

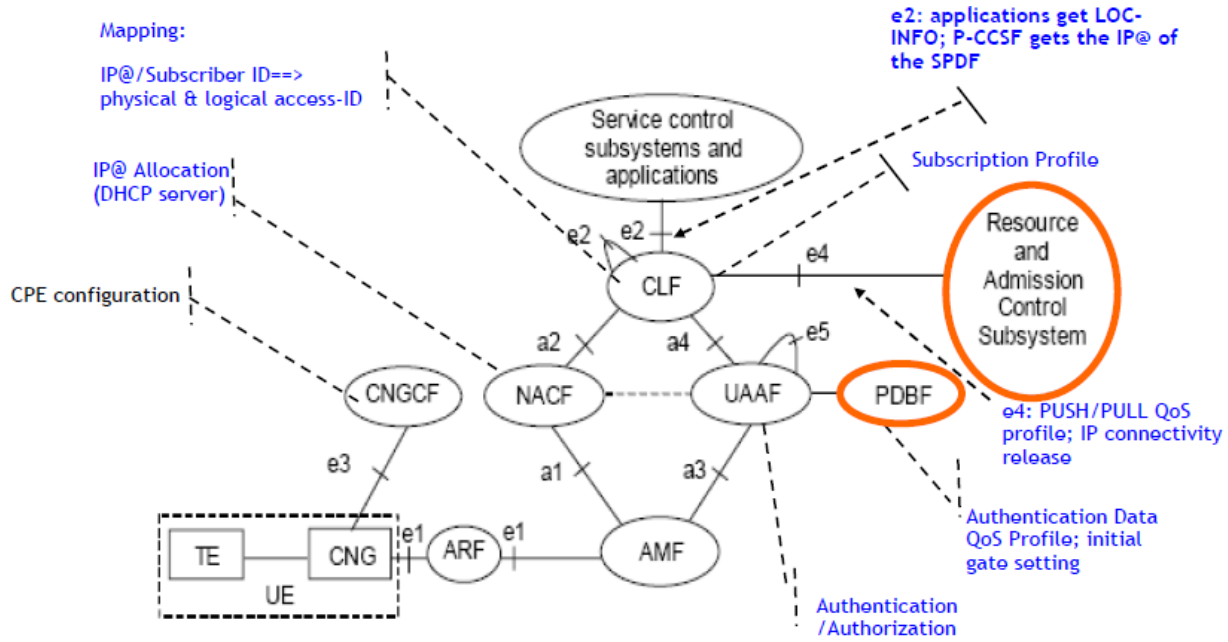


Figure 5.2.2-2 – ETSI TIPSPAN ES 283 034

5.2.3 Inter-working with "Packet Processing"

3GPP2's Packet Flow Optimization (PFO) management, as delineated in Appendix F, enables the network to filter IP flows under policy. PFO functionality defines policy rules to detect applications by examining the data part of the packets in the IP flow, and how to act upon their detection. PFO functionality resides in the Access Gateway (AGW) or as a separate functional entity in the traffic plane. As such the inspection point may be in the serving network, the home network or both.

Reference should be made to TR 23.813 (related to R10 Study Item SP-090361) which borrows from this aspect of 3GPP2 policy architecture described in X.S0053 for Traffic Detection Function (TDF) for service awareness in the network and the implementation of service specific policies. It should be also noted that PFO is not known to have been implemented in any 3GPP2 network and usage scenarios for TDF in 3GPP networks need to be investigated once a decision has been reached on possible normative work in the Rel-11 time frame.

5.2.4 Home Network Control Over Roaming, Mobile Subscribers

Although 3GPP2 SBBC Framework specifications have been mapped to corresponding 3GPP standards as part of common IMS efforts, there are some aspects like the definition of Network Policy Repository and Packet Flow Optimization that have not been considered in the 3GPP PCC Framework yet. In turn, the 3GPP2 policy architecture enhancements defined in X.S0053 only consider a generic roaming case with services provided by the home network.

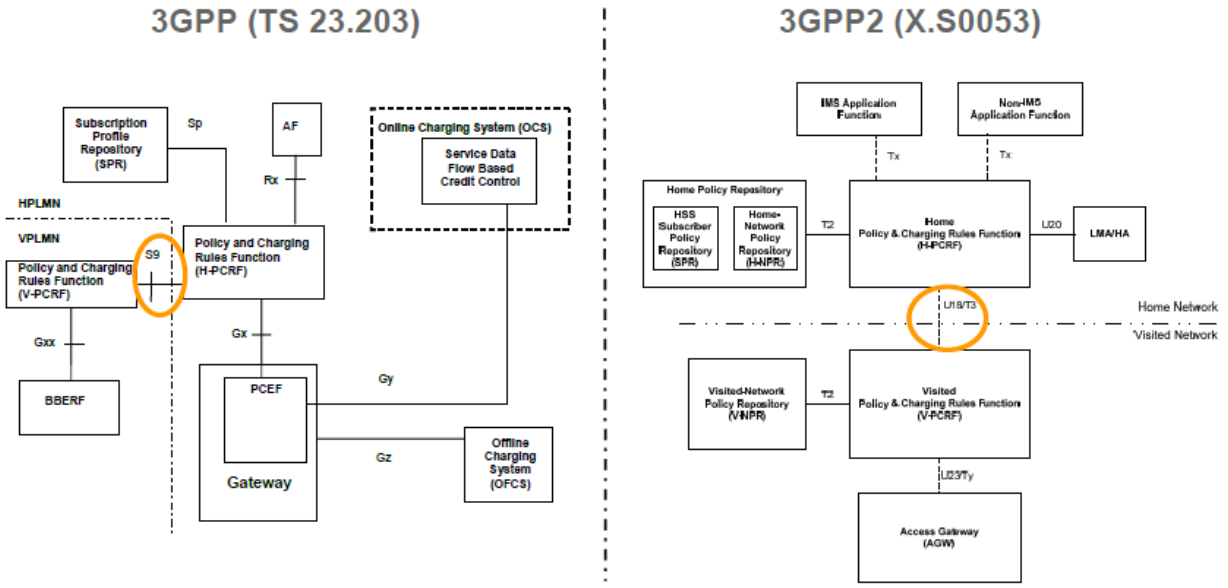


Figure 5.2.4 – 3GPP (TS 23.203) & 3GPP2 (X.S0053)

The adoption of a reference model for cdma2000 systems according to the 3GPP PCC architecture as proposed in the 3GPP2 draft X.P0062 specification distinguishes roaming cases for home routed traffic and local breakout.

S9 has been generally adopted by a range of SDOs as the basis of policy interworking between domains.

5.2.5 Charging Control (specified by 3GPP & 3GPP2)

As ITU-T RACF and ETSI TISPAN RACS standards do not address charging, the assessment is limited to Policy based charging control in the 3GPP PCC and 3GPP2 SBBC frameworks.

Both 3GPP and 3GPP2 charging models are identical. The 3GPP policy and charging control rule operations consist of activation, modification and de-activation of dynamic (via rule information) and or predefined (via relevant identifier) PCC rules in the PCEF by the PCRF via the Gx reference point. Predefined PCC rules not known in the PCRF may be implemented by the PCEF based on service provider policy. In a similar way, the 3GPP2 functional charging control model implies that the Traffic Plane Function (TPF) or Bearer Management Function (BMF) in the AGW implements statically provisioned charging rules or dynamical charging rules provided by the Charging Rules Function (CRF) in the PCRF for the purposes of offline and/or online charging.

Architectural differences between the charging control implementations in 3GPP PCC and 3GPP2, are currently being addressed with the adoption of the reference model for cdma2000 systems according to the 3GPP PCC architecture, as proposed in the 3GPP2 draft X.P0062 specification.

5.2.6 Border Policy Control

Generally, border policy relates to aggregate traffic and does not require dynamic interaction with the policy framework. However, some services, such as those offered with IMS may require dynamic border policies, which have been addressed by TISPAN and ITU-T and are currently under study in 3GPP. The following details the IMS work that is ongoing in these SDOs.

Although border functions (e.g., TISPAN Interconnect Border Gateway Function (I-BGF) and 3GPP Transition Gateway (TrGW)) at the Network-to-Network Interface (NNI) are harmonized in 3GPP Rel-9, additional work is required to harmonize the IMS AGW and the TrGW border functions in 3GPP. Furthermore, TS 23.228 indicates the IMS AGW does not have any policy functions, and it is for further study if the Iq reference point between the Proxy Call Session Control Function (P-CSCF) and the IMS AGW can be merged with the Rx+ reference point for this purpose.

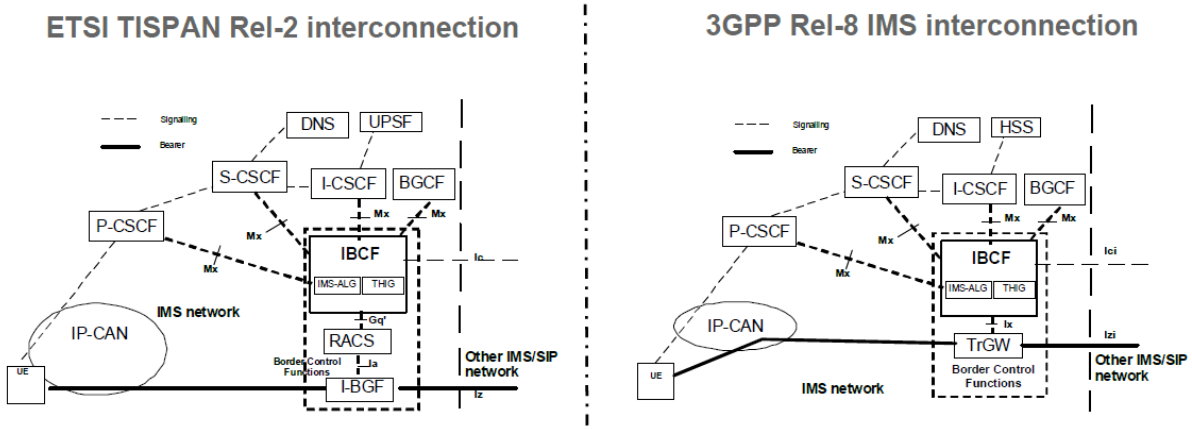


Figure 5.2.6 – ETSI TIPSPAN Rel-2 & 3GPP Rel-8 IMS Interconnection

The effort to define requirements and capabilities for both access and border interconnect Gateways (GWs) is documented in 3GPP study item SP-080559 related to TR 23.848. The study item investigates the definition of the limited policy control functionality for border functions or Interconnection Border Policy Control Function (IBPCF), as well the equivalence between TrGW and IMS AGW, and related equivalence between the Ix reference point and Iq reference point.

6 SERVICE PROVIDER REQUIREMENTS

6.1 Vertical Coordination between Architectural Layers

(R1) A given application requesting or authorizing use of network resources shall signal to at most one PDF using a uniform, access- and transport-network-independent protocol.

Rationale: The goal is to reduce OPEX for policy enablement of applications.

(R2) The protocol of R1 shall account for the requirements of all network access types (e.g., fixed broadband, cellular, WLAN, and cable network service providers).

Rationale: The goal is to reduce OPEX for policy enablement of applications by allowing applications to use a common interface for all access types.

(R3) The protocol of R1 shall allow the application to be advised of the underlying access type or its capabilities.

Rationale: Wireless networks have been asserted to need greater policy control than fixed networks. By allowing the application to be advised of the underlying access network capabilities, the application can then account for access-network limitations using access-agnostic capabilities.

(R4) Network infrastructure shall be able to apply policy control to applications without policy signaling from the corresponding Application Function (AF).

Rationale: Policy may be applied to policy-unaware applications in a number of scenarios. For example, service providers could monetize QoS enablement for 3rd party applications. Service provider offered or 3rd party services could also be deployed initially without policy-awareness, to accelerate time-to-market. In all cases, there is a need for some other mechanism, such as packet processing, to correlate the appropriate policy with each policy-unaware application.

(R5) For network service providers supporting both wireless and fixed broadband access networks, it shall be possible for a single PDF to control network resources related to multiple access types, while accounting for access-specific differences in such resources.

Rationale: Goal is to reduce OPEX for policy enablement.

(R6) The PDF of R5 shall control, via a single protocol, subtending Policy Enforcement Points (PEPs) associated with different access types.

Rationale: Convergence for interfaces both northbound and southbound from the PDF has been identified as a requirement by participating service providers.

6.2 Horizontal Coordination between Network Domains

Policy-controlled network domains, in this context, could include distinct network segments operated by a single service provider, and/or network segments under the control of different service providers. The network segments could provide access, aggregation, or backbone network transport services, or some combination thereof.

(R7) To accommodate FMC, roaming, wholesale and nomadic scenarios involving two network domains, an interface between the respective policy systems of these domains shall enable the two domains to exchange policy information necessary to achieve dynamic and consistent policy control.

Rationale: Consistent policy for FMC, roaming, wholesale and nomadic scenarios.

(R8) The inter-domain interface of R7 shall enable the home domain to request installation of policies in the serving domain, so that the serving domain may provide appropriate QoS for the user's session.

Rationale: Consistent policy for FMC, roaming, wholesale and nomadic scenarios. Other functions besides QoS support are also necessary, but QoS has been specifically highlighted in use-case analysis.

(R9) Regardless of the home and serving domains' policy systems being interworked, the inter-domain interface of R7 shall employ a uniform control protocol and set of information elements.

Rationale: ATIS EGC Report and Recommendations specified that this interface shall be consistent to the extent possible, regardless of whether the signaling service providers support fixed, wireless, or transport services.

(R10) The inter-domain protocol of R9 shall allow the PDF of the home domain to be advised of the underlying access type in the serving domain or of the serving domain's capabilities.

Rationale: Service providers identified a need to allow the functional scope of policy in the inter-worked domains to be different. Some would assert that wireless networks need greater policy control than fixed networks. By allowing the home-domain PDF to be advised of the underlying serving domain capabilities in the serving network, the home-domain PDF can then account for serving-domain limitations in its signaling.

(R11) The inter-domain protocol of R9 shall allow semantic expression that is at least equivalent to the application-PDF protocol of R1.

Rationale: This is the minimum capability to ensure consistent policy between domains. The inter-domain protocol may allow semantic expression that goes beyond that of the application-PDF protocol.

(R12) The inter-domain protocol of R9 shall allow access- and transport-network-independent semantic expressions.

Rationale: derived from R11 and R1.

(R13) It shall be possible for one or more transit domains to support transport of policy signaling between the home and serving domains with QoS that is appropriate for that signaling.

Rationale: Traffic between networks may traverse a transit network.

(R14) The serving domain shall support dynamic discovery of the home-domain PDF, in order to enable cross-domain policy signaling. Alternatively the serving domain PDF shall be provisioned with the address of the home domain PDF.

Rationale: implied by R15, and confirmed by service providers. Possibilities include Domain Name System (DNS) or Diameter proxy routing.

(R15) It shall be possible for the home domain to direct policy requests from serving domains to an appropriate PDF.

Rationale: Policy requests between domains are possible.

(R16) Using its own policies, including relevant SLAs, the serving domain shall be able to evaluate policy requests from the home domain, to determine how the request should be handled.

Rationale: The owner of the network resources being used always has the final say on whether a policy request should be granted. The serving domain's policy decision may be informed by availability of resources in the serving domain, serving domain policies, the SLA with the requesting home domain, and the resources already allocated on behalf of this domain.

(R17) For nomadic or roaming users, policy infrastructure shall allow the user to request that the serving domain provide appropriate QoS for the user's service.

Rationale: This requirement is in contrast with R7 which allows the home domain to request QoS on the user's behalf, for the visiting user's session. This requirement does not specify how the user requests QoS, but could include mechanisms such as the user interacting with a serving domain application, which signals to a serving-domain PDF on the user's behalf.

(R18) For QoS provided by a serving domain to a nomadic or roaming user, policy infrastructure shall enable the serving domain to support accounting needed for charging the home domain for the services provided to the user.

Rationale: Note that billing mediation is itself beyond the scope of policy control; however, policy infrastructure may provide usage metering that provides input for billing mediation.

(R19) When an enterprise subscribes to multiple service providers for network access, common QoS should be applied to enterprise users' traffic related to the same application, regardless of the access network used.

Rationale: A given enterprise site may be served by two access providers (e.g., fixed and wireless broadband), or different sites of the enterprise may be served by different services providers. Although this

requirement implies similar provisioning by all access network providers, the PM-FG has agreed that policy schema should not be standardized.

6.3 Policy Coordination within Network Domains

This section deals with policy coordination within a standardized policy framework. It is worth noting that some functions, such as packet processing, can be used to apply policy either within or outside the standardized policy framework. If these functions are deployed independently of a standardized policy infrastructure (i.e., without a mechanism for coordinating policy applied by the independent packet processing functions, with policy applied by the standardized policy infrastructure -- conflicting policy actions are possible). This could lead to unpredictable behaviors, which is undesirable but out of scope for this standards analysis.

(R20) Packet processing can optionally identify applications to the PDF, either via PEP event notification or as a proxy "application function."

Rationale: Derived from R4. The behavior in this requirement is discussed in 3GPP2 X.S0053-0 v1.0.

6.4 Policy-Controlled Functions

(R21) Policy shall support fine-grained control over charging.

Rationale: Specified in second requirement in Section 5.1 of ATIS EGC Report & Recommendations, and confirmed by service providers in PM-FG. This fine-grained charging control includes but is not limited to volume, QoS, location, access-type, duration, time (time of day and day of week), event, and/or service-based accounting.

(R22) Policy infrastructure shall enable collection of charging data that applies to users, to application service providers, or to both.

Rationale: Service providers want the flexibility to offer capabilities to both the user and the application provider, when the application request effectively overrules the user's request or self-provisioned policies.

(R23) Policy control shall enable limiting the invocations or usage of a given service.

Rationale: From fourth requirement in Section 5.1 of ATIS EGC Report & Recommendations*, affirmed by service providers in PM-FG.*

(R24) When requested by applications, policy shall control transport-plane aspects of near-end, IP address mediation (i.e., dynamic NAPT & NAPT-PT).

Rationale: Derived from R2. Note that both ETSI ES 282 003 and ITU-T Y.2111 specify this capability.

(R25) Border policy shall enable the control of hosted firewall service.

Rationale: Support for firewalls is needed.

(R26) Policy control shall enable the control of content filters.

Rationale: It is recognized that either application-related policy or network-resource policy could control content filters. This requirement is for network-resource policy to be able to control content filters.

(R27) Policy shall enable the control of nomadic and roaming access.

Rationale: From use cases. Note that this does not include policy control over cellular handover for active sessions, given concerns raised over minimizing handover break time.

(R28) Policy shall enable control of the QoS afforded to packet flows associated with users' service.

Rationale: User selected QoS is required.

(R29) Policy shall enable gate control and rate limiting to ensure that only authorized packet flows obtain QoS.

Rationale: Derived from R28.

(R30) Policy control shall enable rate limiting via traffic policing.

Rationale: Derived from R29.

(R31) Policy shall enable Layer-7 validation that QoS-enabled bandwidth is being used by authorized application(s).

Rationale: From use cases. Goal is to minimize bandwidth theft. This capability could be afforded by Packet Processing, as discussed in 3GPP2 X.S0053-0 v1.0, Section 6.6.

(R32) Policy shall provide resource admission control for both unicast and IP multicast traffic flows.

Rationale: All traffic types require policy control.

6.5 Policy Administration

(R33) Management infrastructure shall allow secure provisioning of per-subscription, per-user, per-user-role, per-application, and per-network policies.

Rationale: From Section 5.1 of the ATIS EGC Report and Recommendations.

(R34) Management infrastructure shall allow provisioning of per-application policies per subscriber, including policies for 3rd party applications.

Rationale: Fine-grained policy control is required.

(R35) Authorized users shall be allowed to securely provision certain subscription-related and user-related policies, including policies associated with application-specific QoS, firewall control, and content filtering.

Rationale: From Section 5.1 of the ATIS EGC Report and Recommendations.

6.6 Policy Interaction with Regulatory Services

(R36) Policy infrastructure shall provide mechanisms to prioritize traffic during emergencies, based on priorities established by the carrier, in accordance with applicable regulatory obligations and restrictions. Examples of potential priorities include, but are not limited to:

- Give priority to emergency service (E911) usage of network resources with a specified, guaranteed QoS, independent of user-specific policies related to the user who initiates the communication. E911 service must also be supported in the absence of a subscription.
- Grant, to authorized emergency (NS/EP) responders within a disaster zone, priority access to both access-network and interconnect-network resources, with a guaranteed QoS.
- For non-emergency (non-NS/EP) traffic to and from a disaster zone, prioritize outbound communications over inbound communications.
- Give priority to specific applications (e.g. relatively low-bandwidth voice over streaming entertainment video.)

6.7 Policy Interaction with Network Management

(R37) Policy infrastructure shall prioritize authorized network-operations' requests for network resources with a specified QoS, using a different priority and QoS level for daily operation of the network versus that needed during times of elevated operations traffic (e.g., public emergency or outage scenario).

Rationale: Network management traffic may need a different priority.

6.8 Policy Controls for Aggregate Traffic

(R38) Policy control of the UNI, for both small business customers and consumers, shall enforce aggregate limits on the transport both of sessions (or traffic flows) of a certain type and of all sessions, where such limits may be derived from the end customer's subscription or from any wholesale-traffic SLA that is applicable to nomadic or roaming users.

Rationale: Policy control at the UNI will be based on aggregate traffic.

(R39) Policy control of the NNI, for both enterprise and wholesale customers, shall enforce aggregate limits on the transport of both sessions (or traffic flows) of a certain type and all sessions, where such limits may be derived from the end customer's aggregate subscription or from any applicable wholesale-traffic SLA.

Rationale: "Wholesale customers" may include those with SLAs for nomadic and roaming services.

(R40) QoS-related policies for peer-interconnect traffic's use of NNI network resources shall enforce aggregate bandwidth limits.

Rationale: Derived from scalability concerns expressed by multiple service providers and vendors. The view is that the NNI will be governed by more static QoS policies that apply interconnect SLAs to traffic

in the aggregate. FMC, roaming, and nomadic traffic that transits the NNI of an access network provider would be subject to both interconnect policies for traffic in the aggregate, as well as dynamic policy decisions applied to individual users' sessions at the UNI.

(R41) VOID - Although this requirement was derived from a use case, subsequent analysis suggested that this type of pre-emption was not allowed within public networks, even if all the traffic was for a single enterprise. Therefore this requirement has been deleted.

(R42) VOID - Although this requirement was derived from a use case, subsequent analysis suggested that this type of pre-emption was not allowed within public networks, even if all the traffic was for a single enterprise. Therefore this requirement has been deleted.

(R43) Policy infrastructure shall enable authorized users, or service provider trusted 3rd party providers, to securely request exceptions to subscription limits.

Rationale: While the use case was specific to business customers, we here generalize to allow incremental revenue from consumers as well.

(R44) The override requests of R43 shall enable a charge notification and acceptance transaction.

Rationale: It is important there be positive acceptance of additional charges.

6.9 Derivation of Policy Decisions

(R45) A PDF shall be able to account for the user's location in its derivation of policy and charging decisions.

Rationale: Necessary to support location based services.

(R46) A PDF shall be able to account for the time of day and/or day of week in its derivation of policy and charging decisions.

Rationale: Necessary to support time of day sensitive billing.

(R47) Where an application's policy request is in conflict with a user's self-provisioned policy preferences or with a user-initiated policy request related to the application, whether the request is approved by the policy infrastructure depends on business agreements.

Rationale: If filters are enabled (such as parental controls), the request should be denied.

(R48) In the event that the PDF grants an application's policy request that is effectively not authorized by the user and an incremental charge is incurred, the policy infrastructure shall provide the usage information necessary to enable charging to the application service provider.

Rationale: Necessary if applications have the ability to authorize additional bandwidth.

6.10 HNET-Related Requirements

(R49) It must be possible for SP-A (home network) to advise SP-B (visited network) about QoS and charging for femtocell usage by the SP-A subscriber. In addition, settlement between SP-B and the broadband provider (SP-C) is independent of this relationship.

Rationale: If the service provider offers policy management within the user's home (HNET) then it must be possible to provide proper billing if a user moves into a different user's HNET.

7 LOGICAL FRAMEWORK

7.1 General Network Policy Architectural Framework – Non Roaming

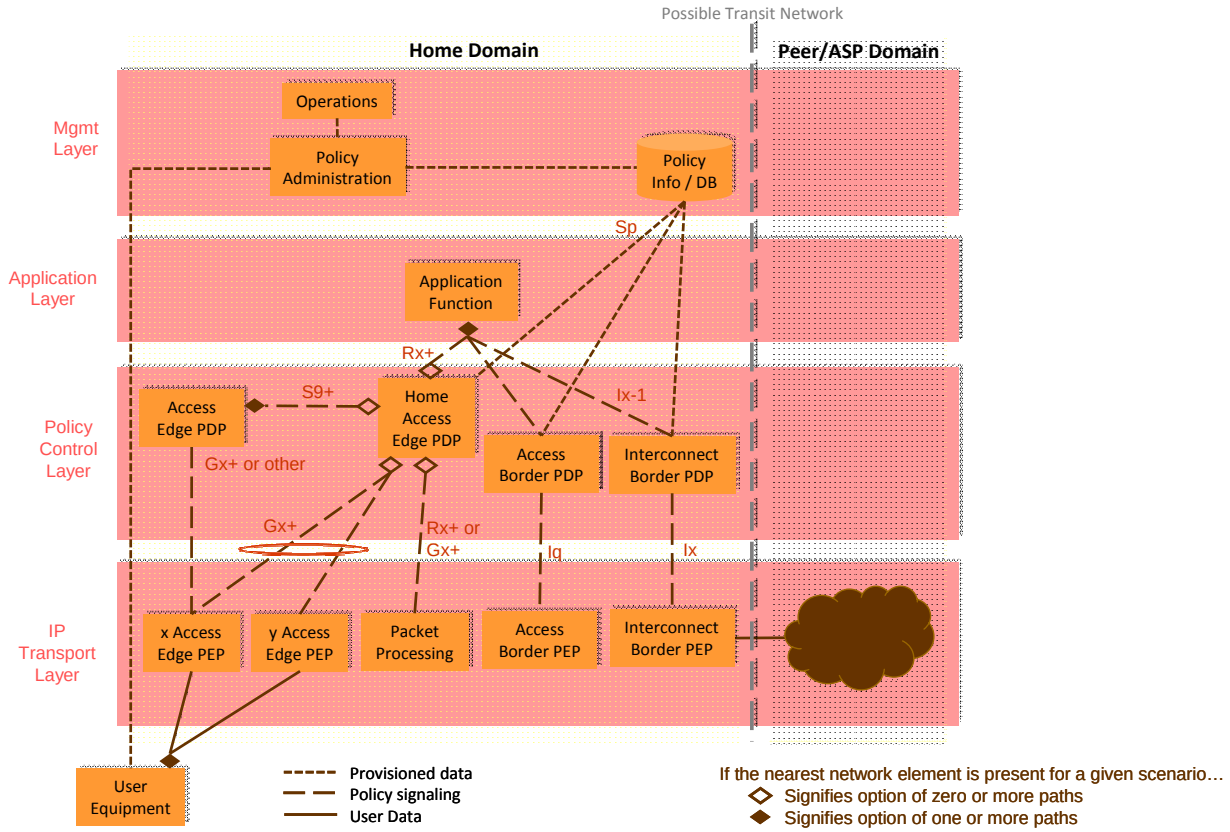
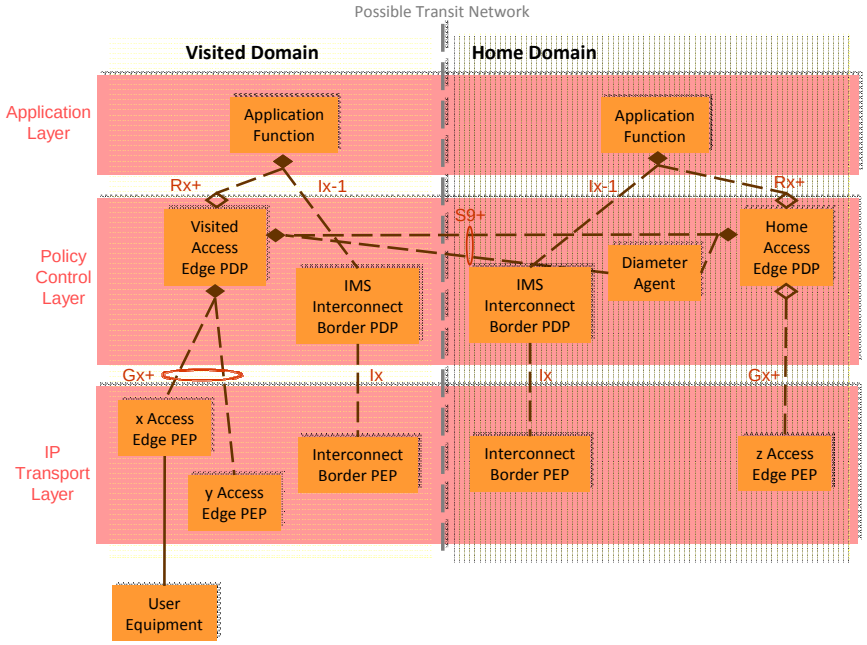


Figure 7.1 – General Network-Policy Architectural Framework -NRoaming

7.2 General Network-Policy Architectural Framework – Roaming



- Relative to the non-roaming framework diagram, this diagram shows incremental architectural aspects related to roaming requirements
- There are 3 roaming scenarios of interest:
  - Roaming with home-routed access (with access edge PDP in home domain & possibly in visited domain)
  - Local Breakout (with one or two access edge PDPs in visited domain only)
  - Local Breakout with IMS border policy (like preceding, with addition of interconnect border elements in one or both domains) – e.g., IMS P-CSCF resides in visited domain & IBCF in one or both domains.

Figure 7.2 – General Network-Policy Architectural Framework - Roaming

NOTE: See Appendix E for mapping of requirements to framework network elements & interfaces.

7.3 HNET Policy Architectural Framework

The following diagram provides an architectural framework for service provider management of HNET. Note that user policy preferences for outbound traffic on the residential access gateway that are provided by the HNET are subordinate to service provider policies set for the service provider network.

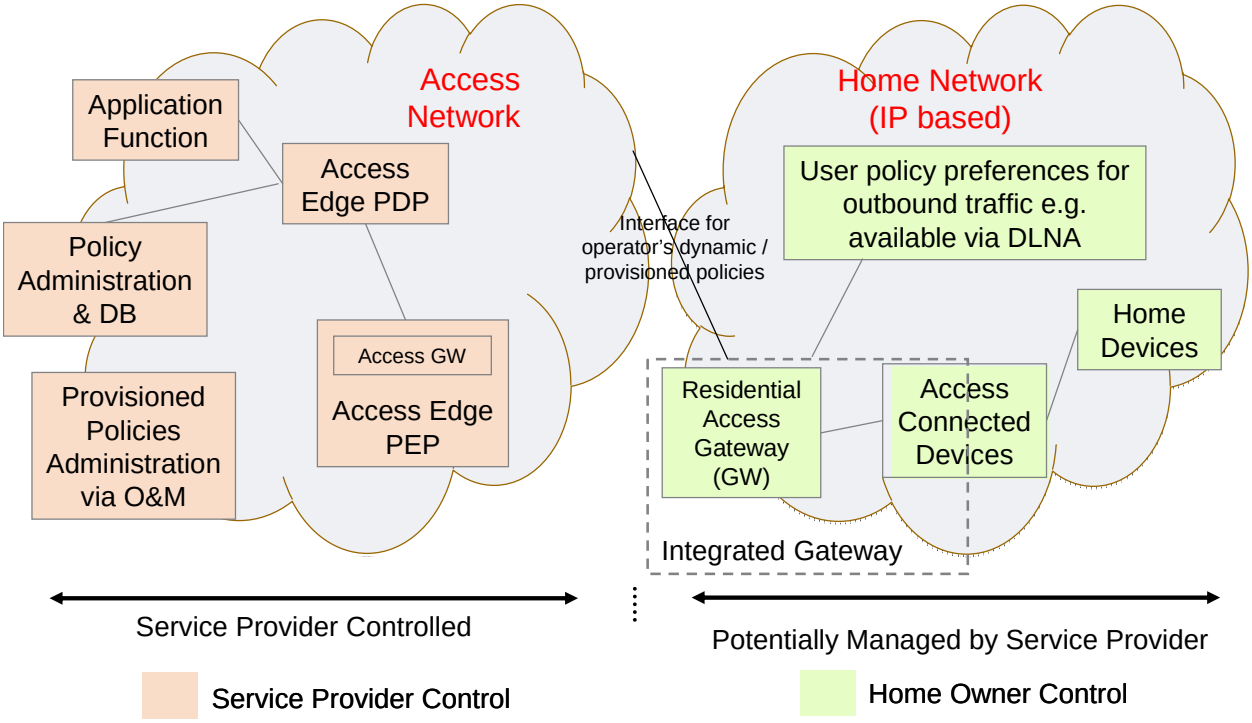


Figure 7.3 – HNET Policy Architectural Framework

8 GAP ANALYSIS

8.1 General Recommendations for Policy Inter-working and Convergence

Most current wireline and wireless networks use static policy mechanisms that are applied by provisioning users upon attachment to networks. In general, today's networks do not use automated policies (with if-then type rules). Some service providers (wireline and wireless) have dynamic policy solutions deployed in very specific scenarios (e.g. by some cable operators for traffic monitoring and differential charging). Some of these solutions are pre-standards-based, but there are some deployments that are based on the current state of standards, such as those in 3GPP and ETSI TISPAN. However, even products that are based on standards typically include additional vendor proprietary functionality. The proposals of this focus group do not conflict with the use of these existing mechanisms and are not intended to preclude continued use of those mechanisms.

The 3GPP has developed a PCC Framework for performing dynamic policy control at initial network attachment and afterwards based on subscriptions and applications launched by the end-user. While this framework was initially designed for mobile access networks, it can also provide support for wireline access networks. This report recognizes this, and proposes the following directions:

1) Existing static policy control frameworks must be able to co-exist with future dynamic policy control.

2) Where desired, wireline networks should aim to develop a single dynamic policy control framework. The implementation and deployment of this consistent framework will depend on the service provider's business and service requirements, but the standards should allow this approach where desired.

3) Policy infrastructure standards should take a phased approach:

   Phase 1: In the near term, wireline access networks should work towards specifying interworking with the 3GPP PCC Framework,

   Phase 2: In the long term, relevant SDOs should work toward converging fixed and mobile network dynamic policy control frameworks.

4) The 3GPP PCC Architecture can be considered as a basis for a possible solution for wireline but perhaps not an exclusive solution. A preliminary view is that 3GPP PCC presently falls short in meeting wireline requirements only insofar as multicast, fixed, video service is concerned. It is also possible that in other areas 3GPP PCC is unnecessarily complex for wireline broadband access. This will need to be considered by the relevant SDOs in their long term work plan.

Note that the interconnection solution is needed in any case, even if convergence work is done, to support roaming between wireline and wireless operators.

At the February 18-19, 2010 Workshop with the BBF and 3GPP, a number of proposals for future directions were presented and considered. Ultimately, 3GPP asked the BBF to consider how best to interwork with the PCC Framework defined in 3GPP. 3GPP also encouraged BBF to consider 3GPP PCC in its fixed broadband network policy work.

In addition, ATIS PTSC-SAC has initiated Issue S0083, 3GPP PCC Based Converged Policy Management Architecture. This activity will develop a technical report that identifies the impacts on protocols, procedures, subscriber profiles and charging in order for the 3GPP PCC to support wireline access, Non-IMS services and QoS for 3rd party applications. Based on these activities, this report recommends that the ATIS Committees (primarily the PTSC Committee) should continue their policy related work, and ensure these activities also examine the various policy architectures from a long term convergence perspective. PTSC-SAC Issue S0083 already recognizes that related work is being conducted by the PM-FG. This report should be sent to PTSC-SAC to provide initial input for their technical report. This will allow PTSC to progress this important work item while engaging appropriately with other SDOs and without duplicating efforts.

The proposed phased approach adopted in various standards bodies seems like the most feasible way forward. Towards this end, the near term priority should be to define standards to support the interworking of wireline networks with the 3GPP PCC architecture. There are many issues, as identified in this report that need to be addressed to support this interworking. Once the work on inter working is completed, using the gap analysis conducted in this report, enhancements to PCC can be recommended for wireline access and transport. For any wireline related enhancements to PCC, convergence on the interface between applications and the policy server should be prioritized above convergence on other policy interfaces.

8.2 Service Awareness and Privacy Policies

8.2.1 Description

The network may have policies related to specific services but currently it is not always aware of usage of these services. The service unawareness can occur when there is no explicit service level signaling and hence no interaction between the AF and PCRF or when filters related to a service have not been installed in the PCEF. The user experience can be enhanced if the network becomes service aware and the network is able to apply service specific policies. Service traffic detection mechanisms can help achieve service awareness. Traffic detection functionality can be implemented as a standalone entity or it can be collocated with the PCEF. Use of service traffic detection mechanisms however may require user consent and for this purpose PCC architecture would have to be extended to include user privacy policies.

Examples of actions that may be a result of service detection include:

- Bearer modification
- Charging rules modification
- Gating of the detected service traffic

8.2.2 Alternative solutions

8.2.2.1 Alternative 1

At the time of IP-CAN session establishment, the PCEF contacts the PCRF as per existing procedures. User privacy policy settings are received from the SPR together with the other subscriber related information (the management of the user privacy policy settings is out of scope) The PCRF checks the user privacy policy settings to see if usage of service traffic detection mechanism is allowed

and for what services. If it is allowed the PCRF in its response to PCEF, can instruct the TDF on what services it should detect. After detecting a service, the TDF informs the PCRF about the detected service. The PCRF can then take the appropriate policy and charging control actions.

A mechanism is needed to instruct the TDF on what service traffic to detect. New mechanisms (e.g., a new type of PCC rule) may be a possibility. The actual mechanism for the service traffic detection should not be standardized, but a standard mechanism is required to flag the start and end of a specific service.

8.2.2.2 Alternative 1a - Rx based service detection reporting

After detecting a service, the TDF informs the PCRF via an Rx based interface. The TDF provides an AF application identifier corresponding to the detected service (which could be the PCC rule name) and the detected filter information. The PCRF may then create/modify the PCC rule by adding the received filter information as well as the service provider configured policy and charging control information which is to be used for this service. When the TDF detects the end of the service, the Rx session to the PCRF is terminated. This triggers the PCRF to remove/modify the PCC rule back to the initial settings.

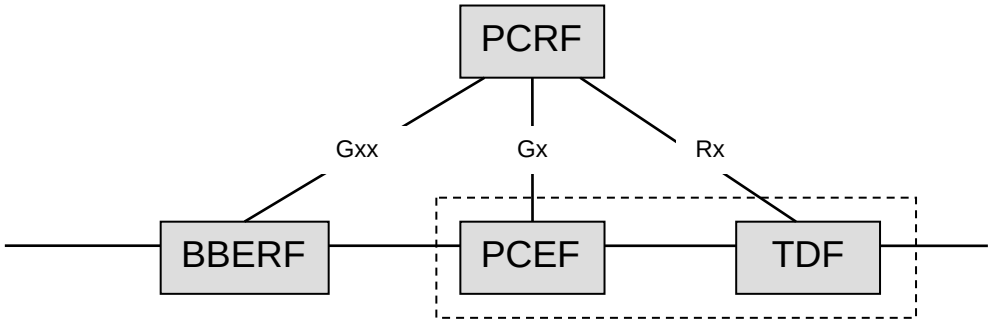


Figure 8.2.2.2 - Architecture for Rx-based solution

NOTE: This architecture option can be applied for a stand-alone TDF or for a TDF that is collocated with the PCEF in the same gateway.

8.2.2.3 Alternative 1b - Gx -Based Service Detection Reporting

To trigger the interaction with the PCRF, the start and the end of a detected service are added as new event triggers. After detecting a service, the PCEF/TDF informs the PCRF via the Gx by sending the PCC rule name of the detected service and the event trigger. Detected filter information could also be provided to the PCRF to simplify the IP packet handling after the service detection. Existing Gx parameters can be used together with the new event trigger to minimize the Gx protocol impacts. The PCRF can then modify the PCC rule in the desired way with regard to the policy and charging control information (e.g. the charging key or the QoS can be modified). When the PCEF/TDF detects the end of the service, the PCRF is informed again and the PCRF modifies the PCC rule back to the initial setting.

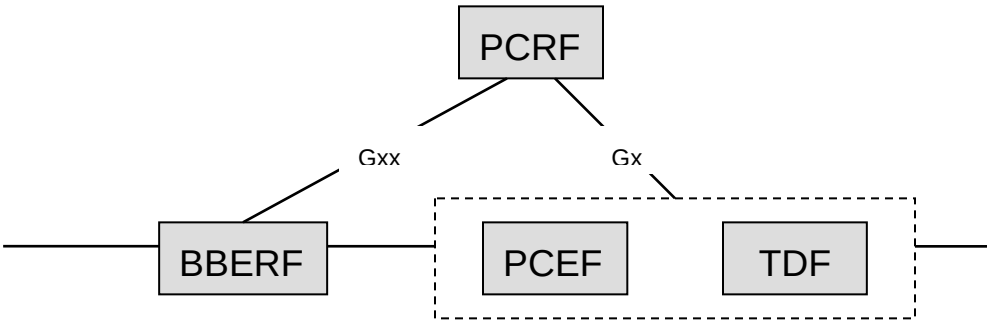


Figure 8.2.2.3 - Architecture for Gx-based solution

NOTE: This architecture option can be applied for a stand-alone TDF or for a TDF that is collocated with the PCEF in the same gateway.

8.2.3 Parental Controls

The FG collectively reaffirmed that the ability to provide parental controls is required. Such controls are deemed in scope for 3GPP R10 TR 23.813, although to date no related contributions have been received beyond introducing the TDF for packet processing detection of applications that are not policy enabled. The TDF is tentatively viewed as providing scalable, Layer 7 filtering as a PEP (e.g., for the traffic that passes through existing Layer 3 and 4 gate controls at the AG's PCEF).

8.3 Policy Control of Charging for Selected IP Traffic Offload

8.3.1 Description

Requirement R18 stipulates that:

> *For QoS provided by a serving domain to a nomadic or roaming user, policy infrastructure shall enable the serving domain to charge the home domain for the services provided to the user.*

Dynamic charging control for 3GPP's Selected IP Traffic Offload (SIPTO) was singled out as the only potential gap.

8.3.2 Further Analysis of Related 3GPP Initiatives

8.3.2.1 Local IP Access (LIPA) and Selected IP Traffic Offload (SIPTO) Work Item

Progressing LIPA and SIPTO have been approved as a 3GPP Release 10 work item, as described in SP-090618. Thus far, the related TR 23.829 v1.0.1 (2010-03) has only concluded that support of SIPTO at or above the RAN will be provided by two solutions:

1. *Solution 4 – SIPTO at Iu-PS*. In this 3G-only solution, a standalone, Radio Network Controller (RNC)-integrated, or Home Node Base station (HNB)

GW-integrated Traffic Offload Function (TOF) inspects Non-Access Stratum (NAS) signaling, Radio Access Network Application Part (RANAP) signaling, and General Radio Packet Service (GPRS) Tunneling Protocol for User Plane (GTP-U) traffic exchanged over the IuPS interface between the Radio Access Network (RAN) and the Serving GPRS Support Node (SGSN). The TOF employs NAT for detunneled, uplink, offloaded traffic, and reverse Network Address Translation (NAT) and GTP-U tunneling for downlink, offloaded traffic. To enable charging for offloaded traffic, statically configured charging parameters will be conveyed by the SGSN over Iu-PS to the TOF.

2. *Solution 5 – SIPTO based on a local Public Data Network (PDN) GW GPRS Support Node (GGSN) selection*. This solution – or more precisely, collection of solution alternatives for both 3G and 4G traffic – enables SIPTO on a per-APN basis, and identifies means by which a Local PDN GW (L-PGW) or GGSN (L-GGSN) for offloaded traffic may be selected that is geographically or topologically near the RAN. For 3G, direct tunneling is used between the RNC and L-GGSN; for 4G, the L-PGW may be integrated with the Serving GW (S-GW). One alternative allows use of the same APN for both Internet and service provider services. The solution description does not explicitly account for charging, but this is implicitly provided via already standardized, (evolved) packet core interaction with the Home Subscriber Service (HSS) and PCRF.

Both of these solutions support static charging for offloaded traffic, and the latter solution implicitly supports dynamic policy control of charging for such traffic. Minutes published from February's 3GPP SA2 meeting indicate that the former solution (i.e., Option 4) is viewed as a temporary, stopgap measure. Service providers participating in the PM-FG likewise view the former solution as a "dead end" for which static charging is deemed adequate.

8.3.2.2 Support for BBF Accesses Inter-working Work Item

This Release 10 work item, introduced in SA2 contribution S2-101822 in February, is intended to address agreements from 3GPP's February 18-19, 2010 workshop with the BBF. The work will be progressed as three, independent Building Blocks, capturing conclusions in a technical report. When each Building Block is completed, it will be decided which parts of the documented Building Block will transfer to normative specifications. The three Building Blocks include the following aspects related to SIPTO or charging:

- **Building Block 1 –** policy and QoS inter-working between 3GPP and BBF architectures when Home (Evolved) Node B (H(e)NB) or WLAN is being used and traffic is routed back to the Evolved Packet Core (EPC); SIPTO for H(e)NB with *static* QoS policies.
- **Building Block 2 –** to the functionality of the first Building Block, this block adds policy and QoS inter-working between 3GPP and BBF

architectures when H(e)NB or WLAN is being used and traffic offload occurs in the local wireline network.

- **Building Block 3 –** this block augments the functionality of the Building Block 1 with policy and QoS inter-working between 3GPP and BBF networks when services and policies are provided by the wireline network.

8.3.3 SIPTO Conclusion

The only potential specification gap related to dynamic policy control of charging for SIPTO is for FMC scenarios wherein femtocells or WLAN provide access and traffic is offloaded in the wireline network. While Building Block 2, described above, would address this gap, the expected start and completion of this work in 3GPP and BBF is to be determined.

8.4 Policy Management and HNET

The analysis of policy management requirements for HNET determined that the TR-69 related family of specifications in conjunction with PCC specifications and capabilities would enable a service provider to offer HNET policy management, including the ability to support dynamic QoS. However, the extent of interactions (manual or automatic) required between these two systems, or any necessary enhancements to these systems has not been studied and represents a potential gap, which can be addressed within the scope of the ongoing joint 3GPP and BBF activities." The convergence of TR-69 and PCC architectural models is also within scope for the convergence study in PTSC Issue S0083.

9 POLICY MANAGEMENT IN THE HOME NETWORK

As part of the Policy Management focus group, a sub-team was formed to consider the application of policy to a user's network (HNET). The sub-team proposed use cases specific to a service provider managing a user's HNET. If management of a user's HNET is offered by the service provider, it must be provided as an optional service that would require the user to opt-in, or subscribe to this additional service. If the service provider is not managing the HNET, all other aspects of policy management must continue to function normally.

In the home network, there may be traffic from sources other than the Service Provider's network and devices in the home – e.g., satellite broadcast-- that could potentially cause cross-traffic QoS disruption if not managed properly. Addressing such traffic from other than the Service Provider's network is deemed out of scope for our effort.

The PM-FG only considered interworking between the service provider network and the HNET in the context where management of both networks was from the same service provider. Interworking of carrier-provided policy enablement of QoS with any independent policy framework in the enterprise or home network (e.g., Institute of Electrical and Electronics Engineers (IEEE) WiFi QoS framework) is out of scope for our effort.

The use cases, requirements, and analysis for HNET have been incorporated into the relevant sections in this report.

10 CONCLUSIONS & RECOMMENDATIONS

10.1 Policy Interworking

The analysis in this focus group, based on realistic end-user use cases contributed by service provider members of the group, identified policy interworking between domains as the number one policy related standards priority. Policy interworking will be based on PCC S9 interface, with the specification of the required interworking to broadband networks. This activity will also consider extensions to the PCC S9 interface to incorporate specific policy functions that are required for broadband networks. Policy interworking between domains is a necessary capability for service providers to offer consistent service capabilities to users independent of the access technology, or the service provider.

Both 3GPP and BBF have identified policy interworking between domains as the top policy-related priority, and are jointly working a solution to this gap:

- Direct input to this process by FG members.
- Agreement from all that trying to solve the broader problem of policy convergence should be deferred, so as to avoid introducing unnecessary complexity and detracting from progress on simple inter-working.
- Providing input directly into 3GPP and BBF by the FG members was necessary to avoid a slow, linear process. An example of how this FG tried to work faster and smarter, and satisfy the service provider's business drivers.
- Recommended that members continue to provide direct input into this work item in 3GPP and BBF to complete the policy interworking capabilities. Trying to accelerate this work by introducing it into any other forum would be counter-productive, and more likely to simply slow things down.

10.2 Policy Convergence

The FG concluded that there is a business driver for developing a converged policy architecture, driven largely by operational expense reduction. There was general agreement that policy convergence should take 3GPP PCC as the starting point for convergence, and enhance this solution where necessary. However, there was no consensus on timing, or how far the convergence should be taken. In part this was because the value of converged policy depends on each service provider's business model. The policy convergence work will start with the existing Gx interface between the PDF and the PEP, enhance the protocol (resulting in Gx+) in a way that is suitable to wireline technologies and is important for convergence. A preliminary view is that Gx should only need to be enhanced to accommodate fixed, multicast video, although further analysis is needed and may identify additional informational elements.

Interworking can accommodate differences between architectures in a relatively straightforward manner with the interworking function. However, going beyond interworking to consider full convergence, can introduce additional complexity. It is important that this be fully understood before committing to convergence.

Recommendations: BBF has decided to focus on developing an information model applicable to the wireline policy management architecture. Progress in this work is expected to help accomplish components, which will contribute to the convergence goals that ATIS PM-FG has identified. ATIS PTSC-SAC has an active issue (Issue S0083 – 3GPP PCC based Converged

Policy Management Architecture) that is developing a technical report to study converged policy framework. The report from this FG should be provided to PTSC as a contribution to help progress work on this topic as required. PTSC may share this report (or portions of this report) to other SDO as relevant.

10.3 Specific Long Term Gaps

In addition to issues associated with policy interworking, and policy convergence, the FG identified a number of other issues. In general, these were not viewed as immediate, or even near term gaps. These were viewed as longer-term requirements that should be progressed in the context of ongoing standards work. There was a strong consensus that these items should not be allowed to distract attention from higher priority work on policy interworking or policy convergence. Nevertheless these are important requirements that should not be forgotten.

All these current gaps were potentially in scope for existing study items within 3GPP or other SDOs. To ensure that these gaps are addressed, leading to solutions in the appropriate time frame, the PM-FG identified a primary point of contact (POC) for each activity. The POC identified below will be responsible for progressing the work in 3GPP or other SDOs on the identified gaps.

10.3.1 User Privacy Policies

Several of the requirements identified by this focus group depend on the ability of packet processing to identify applications, and initiate action as appropriate. This may require an ability to define user privacy policies so that applications are only detected when it is allowed.

3GPP study item SP-090361 is a study on policy solutions and enhancements that includes consideration of user privacy policies for packet processing. Input will be provided into 3GPP to continue progressing this work.

POC: GENBAND

10.3.2 Application Aware Content Filtering

Support for application aware content filtering, including capabilities such as parental controls, is deemed to be in scope for 3GPP R10 TR 23.813, although only moderate progress has been made on this issue to date. Three architectural alternatives have been identified that could provide this functionality. All of these alternatives require additional work in 3GPP to complete the specification. The focus group did not have consensus on which of these alternatives was preferred, however there was agreement that this work should continue to be worked in 3GPP. The focus group members will provide contributions to 3GPP to progress this work.

POC: Huawei

10.3.3 Group Subscriptions

A requirement to support group subscriptions was identified from the use case analysis, and the group agreed to provide input to 3GPP to add this to the scope for TR 23.813. Contributions are being submitted to 3GPP to achieve this.

POC: Alcatel-Lucent

10.3.4 Support for Fixed Video Delivery

The specific capabilities necessary to support the delivery of fixed, multicast video has not yet been fully defined, although work is ongoing in ATIS IIF. This analysis in IIF must be completed before assessing whether or not PCC has the necessary functionality to support it. Therefore this item will be input to ATIS PTSC-SAC Issue S0083 for more detailed analysis. The results of that analysis will determine if the appropriate next step is to input it to BBF, 3GPP, or both.

POC: Cisco

10.3.5 Charging control for SIPTO

Only for certain FMC scenarios - when femtocells or WLAN provide access and traffic is offloaded in the wireline network - is there a potential specification gap for dynamic policy control of charging for Selective IP Traffic Offload. Building Block 2 in the Release 10 work item for "Support for BBF Accesses Inter-working" would address this gap, but this building block will not receive airtime before the Stage 2 freeze date. The building block's completion date is to be determined. Moreover, the completion of this work is dependent upon BBF making sufficient progress in developing a charging framework that can interact with other service providers to support various charging models such as online charging and offline charging. Therefore, the PM-FG recommends that participating, interested companies support this work in 3GPP and BBF.

POC: AT&T

10.3.6 TR-69 Support for dynamic QoS

The PM-FG Home Networking sub team analysis concluded that TR-69 had the necessary functionality to support dynamic QoS across the access network, and into the home network. The only additional analysis required it to ensure that TR-69 QoS can interwork with PCC QoS, and ultimately be integrated into a converged policy model. This will be contributed into ATIS PTSC-SAC Issue S0083 and it will be addressed as part of that analysis. When the S0083-related report is completed, it is recommended that it be shared with appropriate SDOs to facilitate their specification effort: preferably BBF but, if necessary, 3GPP under the auspices of Building Block 3 of the work item for "Support for BBF Accesses Inter-working."

POC: Cisco

11 ISSUES FOR FURTHER CONSIDERATION

The following potential issues have been tentatively identified, but are beyond the scope of the PM-FG charter. These issues are noted for further consideration by the ATIS technical committees as they see relevant.

- For a node that functions as a PEP, how should conflicts be best addressed between policies conveyed from the PDF and (legacy) provisioned policies already residing within the node? The consensus is that this issue is out of scope for standards work, but it may be worth noting in the ongoing work in PTSC Issue S0083.
- 3GPP PCC only consults with the RAN to confirm that radio resources are available, but PCC's PCRF does not have visibility to real-time availability of all transport resources with in a network or domain, and thus cannot factor all transport network-resource availability into its decisions (e.g., when the backhaul or core network is overloaded, and experiencing congestion). For FMC and roaming scenarios, coordinated admission control for both wireline and wireless should be considered. This work is complicated by the lack of a strong consensus among service providers on the need for dynamic resource admission control in the core and backhaul portions of the network. There is also ongoing debate on the need for dynamic resource admission control in fixed broadband networks, some of which tend to have high available bandwidth and "all you can eat" data plans. The ongoing work in BBF and collaboration with 3GPP may address some of these issues.
- 3GPP addresses border policy that's IMS and Circuit Switched (CS) specific. Some service providers have an interest in more general border policy; however, their specific requirements are to be determined.

APPENDIX A: ACRONYMS

Acronym	Definition
3GPP	3rd Generation Partnership Project
AF	Application Function
AGW	Access Gateway
AMF	Access Management Funcion
ANCP	Access Node Control Protocol
ANI	Applications Network Interface
APN	Access Point Name
ARF	Application Resource Funciont
ASN-GW	Access Service Network - Gateway
BBERF	Bearer Binding and Event Reporting Function
BBF	Broadband Forum
BGF	Border Gateway Function
BMF	Bearer Management Function
CAPEX	Capital Expenditures
CLF	Contactless Front-end Interface
CNG	Customer Network Gateway
CNGCF	Customer Network Gateway Configuration Function
COPS	Common Open Policy Service
CPE	Customer Premise Equipment
CRF	Charging Rules Function
CS	Circuit Switched
DB	Database
DHCP	Dynamic Host Configuration Protocol
DLNA	Digital Living Network Alliance
DNS	Domain Name System
DSL	Digital Subscriber Line
DVR	Digital Video Recorder
eHRPD	Evolved High Rate Packet Data

Acronym	Definition
EPC	Evolved Packet Core
ETSI	European Telecommunications Standards Institute
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
FMC	Fixed Mobile Convergence
GETS	Government Emergency Telecommunications Service
GGSN	Gateway General Packet Radio Service Support Node
GPRS	General Packet Radio Service
GTP-U	GPRS Tunneling Protocol for User Plane
GW	Gateway
H(e)NB	Home (Evolved) Node B
HNB	Home Node Base station
HNET	Home Network
HRPD-SW	High Rate Packet Data – Serving Gateway
HSS	Home Subscriber Service
I-BGF	Interconnect Border Gateway Function
IBPCF	Interconnection Border Policy Control Function
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IIF	IPTV Interoperability Forum
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IP-CAN	Internet Protocol-Connectivity Access Network
IPTV	Internet Protocol Television
ITU-T	International Telecommunications Union- Telecommunication
LAN	Local Area Network
LIPA	Local IP Access
LTE	Long Term Evolution
L-PGW	Local PDN GW
MGW	Media Gateway
NACF	Network Attachment Control Function

Acronym	Definition
NAPT	Network Address Port Translation
NAPT-PT	Network Address Port Translation – Protocol Translation
NAS	Non-Access Stratum
NASS	Network Attachment Subsystem
NAT	Network Address Translation
NGN	Next Generation Networks
NNI	Network-to-Network Interface
NPR	Network Policy Resource
NS/EP	National Security / Emergency Preparedness
OPEX	Operational Expenditures
PBDF	Profile Data Base Function
PCC	Policy and Charging Control
PCC S9	Policy and Charging Control - S9 reference point
PCEF	Policy Charging Enforcement Point
PCRF	Policy Charging Rules Function
P-CSCF	Proxy Call Session Control Function
PDF	Policy Decision Function
PD-FE	Policy Decision Functional Entity
PDN	Public Data Network
PE-FE	Policy Enforcement Functional Entity
PEP	Policy Enforcement Point
PFO	Packet Flow Optimization
PDN	Packet Data Networks
PDN-GW	Packet Data Network - Gateway
PDSN	Packet Data Serving Node
PMIP	Proxy Mobile IP
PM-FG	Policy Management Focus Group
POC	Point of Contact
PTSC	Packet Technologies and Systems Committee
RACF	Resource and Admission Control Functions

Acronym	Definition
RACS	Resource and Admission Control Subsystem
RAN	Radio Access Network
RAN AP	Radio Access Network Application Part
RCEF	Resource Control Enforcement Function
RCIP	Resource Connection Initiation Protocol
RNC	Radio Network Controller
SBBC	Service Based Bearer Control
SDO	Standards Development Organization
SGSN	Serving GPRS Support Node
SIP	Session Initiation Protocol
SIPTO	Selected IP Traffic Offload
S-GW	Serving Gateway
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SON	Service Oriented Networks
SPDF	Service-based Policy Decision Function
TDF	Traffic Detection Function
TE	Terminal Equipment
TISPAN	Telecommunications and Internet converged Services and Protocols for Advanced Networking
TMF	Tele Management Forum
TMOC	Telecom Management and Operations Committee
TOF	Traffic Offload Function
TOPS	Technical and Operations Council
TPF	Traffic Plane Function
TRC-FE	Transport Resource Control Functional Entity
TRE-FE	Transport Resource Enforcement Functional Entity
TrGW	Transition Gateway
UAAF	User Access Authorization Function
UE	User Equipment

Acronym	Definition
UNI	User Network Interface
VoIP	Voice over Internet Protocol
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WPS	Wireless Priority Service

APPENDIX B: GENERAL TERMS

Term	Definition
Admission Control	Admission Control, employed when sessions are being setup, is a mechanism that prevents oversubscription of network resources that would negatively impact the performance of in-progress sessions.
Nomadic	Nomadic, in the context of PM-FG discussions, is a term qualifying fixed broadband connectivity as being supplied by access facilities other than those associated with the user's subscription - e.g., by a network service provider other than that with which the user has a subscription. The analogous term, for a cellular subscriber, would be "roaming."

APPENDIX C: ATIS ACRONYMS & DEFINITIONS

Term	Definition	Description
ATIS	Alliance for Telecommunication Industry Solutions	ATIS is committed to providing leadership for, and the rapid development and promotion of, worldwide technical and operations standards for information, entertainment and communications technologies using a pragmatic, flexible, and open approach.
IIF	IPTV Interoperability Forum	The IIF enables the interoperability, interconnection, and implementation of IPTV systems/services by developing ATIS standards and facilitating related technical activities. This forum will place an emphasis on North American and ATIS Member Company needs in coordination with other regional and international standards development organizations.
OBF	Ordering and Billing Forum	The OBF provides a forum for representatives from the telecommunications industry to identify, discuss, and resolve national issues that affect ordering, billing, provisioning, and exchange of information about access service, other connectivity, and related matters.
PTSC	Packet Technologies and Systems Committee	PTSC develops and recommends standards and technical reports related to services, architectures, and signaling, in addition to related subjects under consideration in other North American and international standards bodies.
TMOC	Telecom Management and Operations Committee	The Telecom Management and Operations Committee (TMOC) develops operations, administration, maintenance and provisioning standards, and other documentation related to Operations Support System (OSS) and Network Element (NE) functions and interfaces for communications networks - with an emphasis on standards development related to U.S. communication networks in coordination with the development of international standards.
TOPS	Technology and Operations Council	A standing committee of the ATIS Board of Directors, the Technology and Operations Council identifies the industry's most pressing technical and operational priorities, and coordinates standardization efforts across the industry to produce interoperable, implementable, end-to-end solutions.

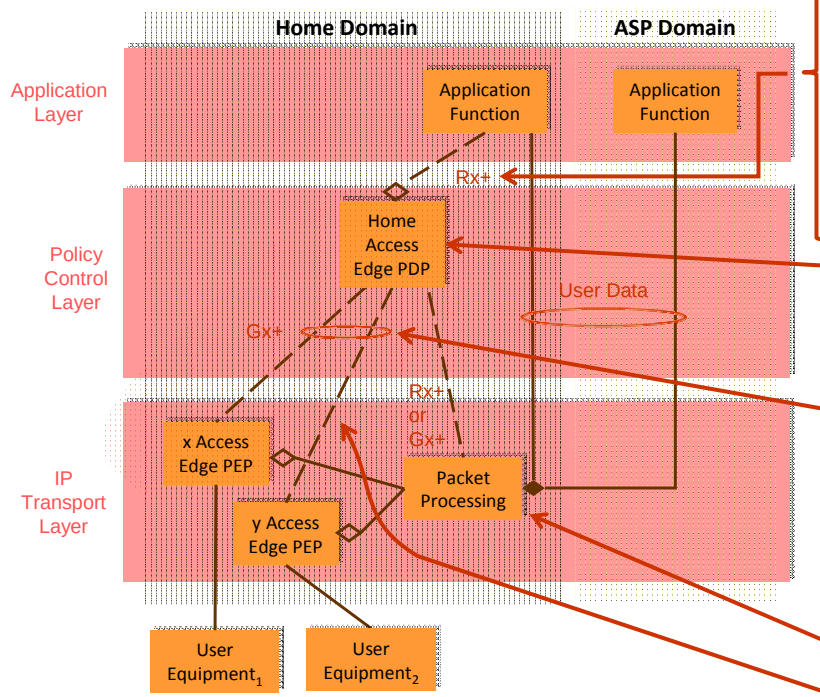
APPENDIX D: ACTIVE 3GPP WORK AND STUDY ITEMS RELATED TO POLICY

The following table shows the key 3GPP R10 / R11 work items that will be targeted by contributions from the PM-FG members.

Work or Study Item		Related TS / TR	Policy-Related Aspects of Scope Include
Document #	**Title**		
SP-090361	Study on Policy Solutions & Enhancements	TR 23.813	Packet Processing with user privacy policies; service- & PDN-based traffic steering; redirection of IP flows; firewall control
SP-080559	Study on Enhancements to IMS Border Functions for IMS Interconnection of Services	TR 23.848	SLA Enforcement, QoS mgmt, harmonizing fixed & mobile architectures
SP-100222	Support BBF Accesses Inter-working	TS 23.203, TS 23.401, TS 23.402 TR 23.xxx	•Building Block 1 – S9+ inter-working between 3GPP and BBF architectures when H(e)NB or WLAN is being used and traffic is routed back to the EPC. Focus of R10. •Building Block 2 – will add dynamic policy and QoS inter-working between 3GPP and BBR architecturs when H(e)NB or WLAN is being used and traffic offload occurs in the local wireline network. Work may start in R11. •Building Block 3 – "architecture optimizations," while subject to interpretation, could include a converged policy framework. Work may start in R11.

APPENDIX E: MAPPING OF REQUIREMENTS TO FRAMEWORK NETWORK ELEMENTS & INTERFACES

Vertical Coordination



Notes:
•x & y Access Edge PEPs are related to different access types
•All data passing between the UE and AF passes through Packet Processing in a manner that is generally transparent to both endpoints.

- (R1) A given application requesting or authorizing use of network resources shall signal to at most one PDP using a uniform, access- and transport-network-independent protocol.

  Note for standards gap analysis: we've agreed this should be 3GPP Rx-based.

- (R2) The protocol of R1 shall account for the requirements of all network access types (e.g., fixed broadband, cellular, WLAN, and cable network service providers).
- (R3) The protocol of R1 shall allow the application to be advised of the underlying access type or its capabilities.
- (R5) For network service providers supporting both wireless and fixed broadband access networks, it shall be possible for a single PDP to control network resources related to multiple access types, while accounting for access-specific differences in such resources.
- (R6) The PDP of R5 shall control, via a single protocol, subtending PEPs associated with different access types.

  Note for standards gap analysis: we've agreed that this should be 3GPP Gx+ based.

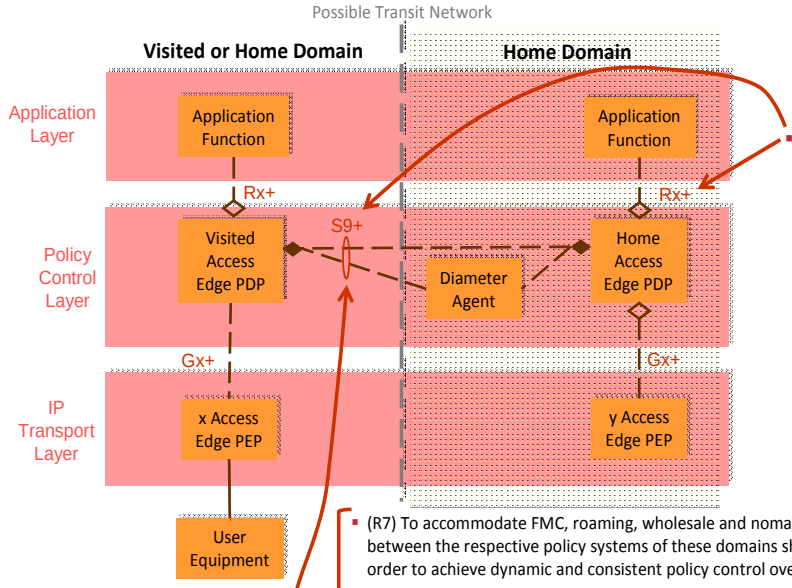
- (R4) Network infrastructure shall be able to apply policy control to applications without policy signaling from the corresponding application function.

  Options (for standards gap analysis) include

  •Packet Processing identifying application & signaling either as application's proxy over Rx+ or with event notification over Gx+

  •R8 supports provisioned L3 filters (e.g., IP address of over-the-top app server) which, when pushed to the PEP, allows event notification by & consequent QoS policy decision being pushed to PEP.

Horizontal Coordination – Roaming & Non-Roaming Scenarios (1 of 3)



The requirements of this page apply to both roaming scenarios (with Home & Visited Domains) & non-roaming scenarios (with a single Home Domain)

- (R11) The inter-domain protocol of R9 shall allow semantic expression that is at least equivalent to the application-PDP protocol of R1.

Notes (to facilitate standards gap analysis):

- S9 supports distinct Rx & Gx protocols, the former for some non-LBO roaming scenarios & the latter for LBO roaming
- TISPAN Ri is roughly equivalent to Rx
- In 3GPP2, equivalent of S9 is based on Ty (based on R7 Gx)
- It is FFS whether the inter-domain protocol may include policies specific to access network in the serving domain.

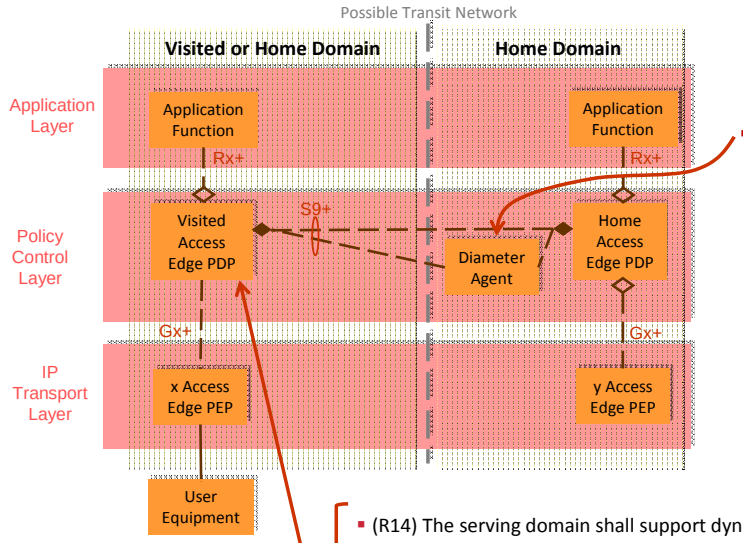
- (R7) To accommodate FMC, roaming, wholesale and nomadic scenarios involving two network domains, an interface between the respective policy systems of these domains shall enable the two domains to exchange policy information in order to achieve dynamic and consistent policy control over the access network provider's support of the user's sessions.

Note for standards gap analysis: we've agreed this should be based on 3GPP's S9.

- (R8) The inter-domain interface of R7 shall enable the home domain to request provisioning of policies in the serving domain, so that the serving domain may provide appropriate QoS for the user's session.
- (R9) Regardless of the home and serving domains' policy systems being interworked, the inter-domain interface of R7 shall employ a uniform control protocol and set of information elements.
- (R10) The inter-domain protocol of R9 shall allow the PDP of the home domain to be advised of the underlying access type in the serving domain or of the serving domain's capabilities.

  Note to facilitate standards gap analysis: there is presently no exchange of capabilities between peers.
- (R12)The inter-domain protocol of R9 shall allow access- and transport-network-independent semantic expressions.

Horizontal Coordination – Roaming & Non-Roaming Scenarios (2 of 3)



The requirements of this page apply to both roaming scenarios (with Home & Visited Domains) & non-roaming scenarios (with a single Home Domain)

- (R15) It shall be possible for the home domain to direct policy requests from serving domains to an appropriate PDP.

  Notes (for standards gap analysis):

  - GSMA plans to augment IPX/GRX capabilities to include Diameter routing.
  - 3GPP TS 23.203, Section 7.6 provides principles governing the use of a Diameter Routing Agent (DRA) for PCRF discovery & selection.
  - RFC 3588 specifies Diameter routing based on UE-NAI domain part, where the Diameter Agent may be a redirect, relay or proxy agent.

- (R14) The serving domain shall support dynamic discovery or provisioning of the home-domain PDP, in order to enable cross-domain policy signaling.

  Notes (for standards gap analysis)

  - Possibilities include DNS or Diameter proxy routing.
  - Requirement already realized in R9 PCC
  - GSMA plans to augment IPX/GRX to include inter-domain PCRF discovery.

- (R16) Using its own policies, including relevant SLAs, the serving domain shall be able to evaluate policy requests from the home domain, to determine how the request should be handled.

Horizontal Coordination – Roaming & Non-Roaming Scenarios (3 of 3)

The requirements of this diagram are roaming specific

- (R13) It shall be possible for one or more transit domains to support transport of policy signaling between the home and serving domains with QoS that is appropriate for that signaling.

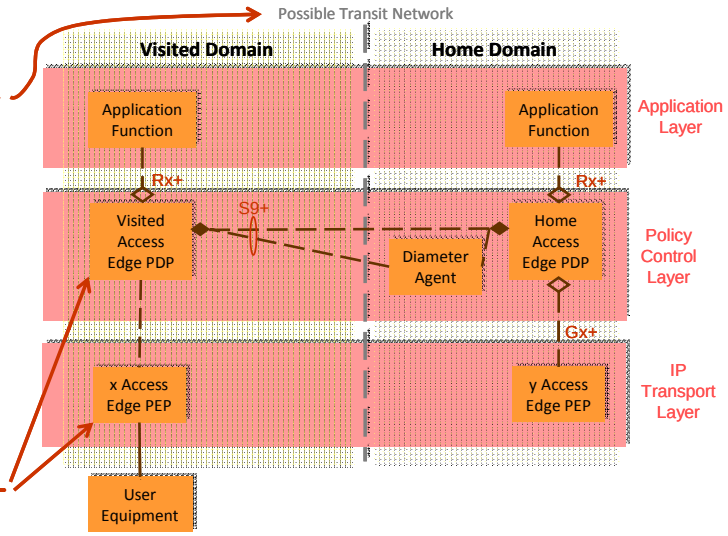
  Note (for standards gap analysis): policy control of transit network segments is currently not addressed, & GSMA's IPX/GRX assumes that such is unnecessary due to provisioning of sufficient bandwidth and, with IPX, enforcing the DiffServ markings of Service Provider (wholesale) customers, where these should all uniformly mark analogous traffic. IPX customers may include mobile operators, fixed NGN operators, ISPs, and application service providers (ASPs).

- (R17) For nomadic or roaming users, policy infrastructure shall allow the user to request that the serving domain provide appropriate QoS for the user's service.

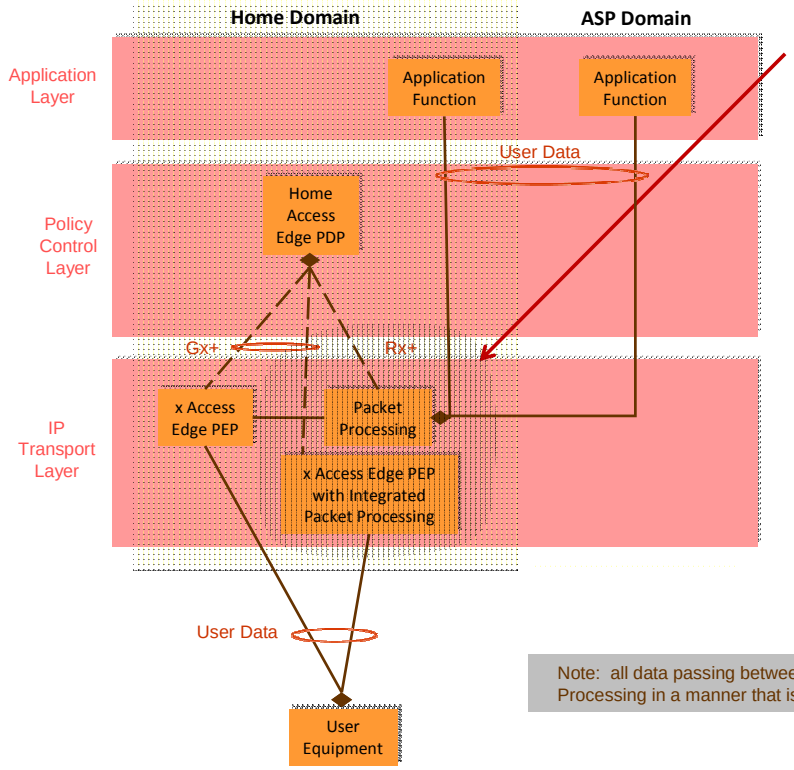
  Notes (for standards gap analysis): User may possibly interact with visited domain application, which signals to visited domain PDP on user's behalf. Direct signaling of the PDP is not currently supported.

- (R18) For QoS provided by a serving domain to a nomadic or roaming user, policy infrastructure shall enable the serving domain to charge the home domain for the services provided to the user.

Note (for standards gap analysis): billing mediation is beyond policy control's scope; however, policy infrastructure may provide usage metering & charging that provides input for billing.



Policy Coordination within Network Domains



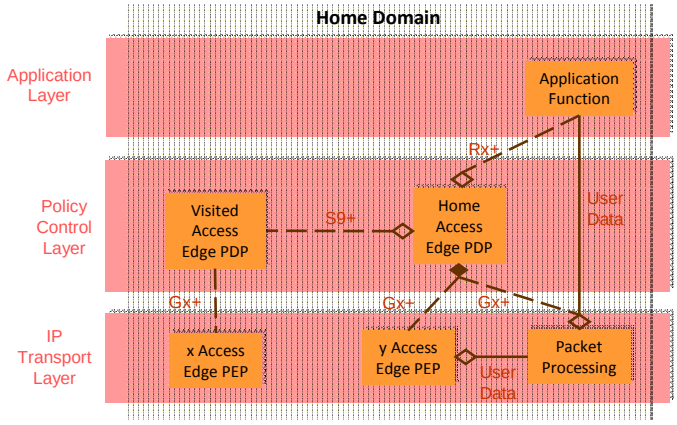
- (R20) Packet processing can optionally identify applications to the PDP, either via PEP event notification or as a proxy "application function."

Notes (for standards gap analysis):

- Packet Processing identification of applications is expounded in 3GPP2 X.S0053-0 v1.0, where standalone Packet Processing may function as a proxy application function, and Packet Processing integrated with the Access Gateway may serve as part of the PEP.
- In this latter case, application filters may be installed when the user equipment attaches to the network, in order to improve scalability.

Note: all data passing between the UE and AF passes through Packet Processing in a manner that is generally transparent to both endpoints.

Policy Controlled Functions (1 of 3)



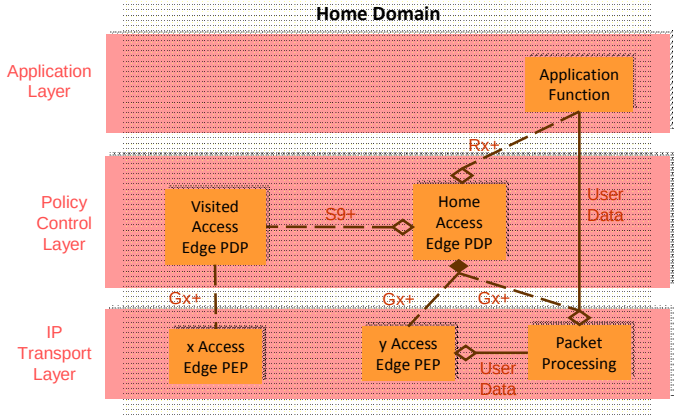
Rqmt	Possibly Implicated Network Element or Interface						
	Rx	Gx	S9	H-PDF	V-PDF	PEP	Packet Processing
R21		X	X	X	X	X	
R22				X	X	X	
R25	X	X	X	X	X	X	X
R26		X	X	X	X	X	
R27	X	X	X	X	X	X	
R28	X	X	X	X	X	X	

- (R21) Policy shall support fine-grained control over charging.

  Note (for standards gap analysis): ITU-T RACF doesn't support usage-based metering or charging, & one participating service provider has deployed IIF's IPTV architecture, which includes RACF.
- (R22) Policy infrastructure shall enable collection of charging data that applies to users, to application service providers, or to both.
- (R23) Policy control shall enable limiting the invocations or usage of a given service.
- (R26) Policy control shall enable the control of content filters.
- (R27) Policy shall enable the control of nomadic and roaming access.

  Note (for standards gap analysis): doesn't include policy control over cellular handover for active sessions, given concerns over minimizing handover break time.
- (R28) Policy shall enable control of the QoS afforded to packet flows associated with users' service.

Policy Controlled Functions (2 of 3)



Rqmt	Possibly Implicated Network Element or Interface						
	Rx	Gx	S9	H-PDF	V-PDF	PEP	Packet Processing
R29		X	X	X	X	X	
R30		X	X	X	X	X	X
R31		X	X	X	X	X	

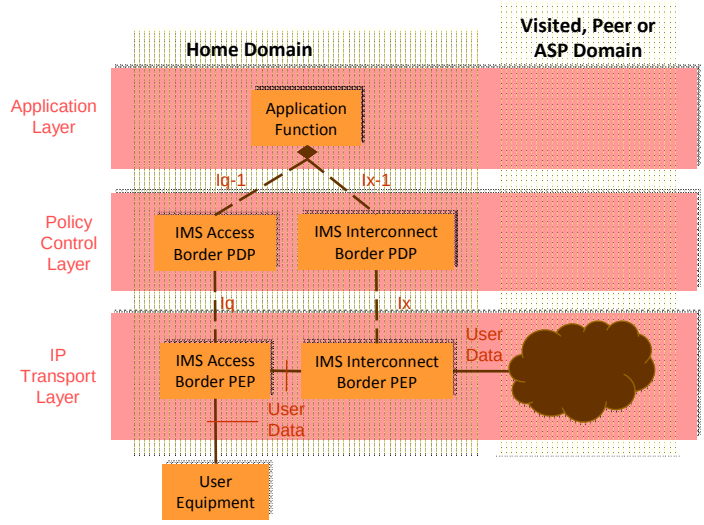
- (R29) Policy shall enable gate control and rate limiting to only provide QoS for authorized packet flows.
- (R30) Policy control shall enable rate limiting traffic policing.

  Note (for standards gap analysis): ITU-T allows traffic shaping too, & some ATIS specs use ITU-T policy control; 3GPP provides traffic policing.
- (R31) Policy shall enable Layer-7 validation that QoS-enabled bandwidth is being used by authorized application(s).

  Note (for standards gap analysis): could be done with packet processing, as per 3GPP X.S0053-0 v1.0, Section 6.6.
- (R32) Policy shall provide resource admission control for both unicast and IP multicast traffic flows.

  Note (for standards gap analysis): ITU-T & TISPAN policy controls both unicast & multicast traffic flows, & some ATIS specs use ITU-T policy. Wireless-specific multicast rqmts aren't needed, since participating cellular network providers use MediaFLO, & 3GPP R9 hasn't seen fit to include MBMS traffic in PCC's scope.

Policy Controlled Functions (3 of 3)



Framework Network Element	3GPP Network Element	Notes
IMS Access Border PDP	Integrated with P-CSCF	TS 23.228, Annex G; TR 23.848 could introduce IBPCF distinct from P-CSCF
IMS Access Border PEP	IMS Access Gateway	TS 23.228, Annex G
IMS Interconnect Border PDP	IBPCF or integrated with IBCF	TR 23.848; TS 23.228, Annex I
IMS Interconnect Border PEP	Transition Gateway (TrGW)	TR 23.848; TS 23.228, Annex I
Note: PM-FG consensus was to use generic network element names; however, the above mapping is provided to facilitate standards gap analysis.		

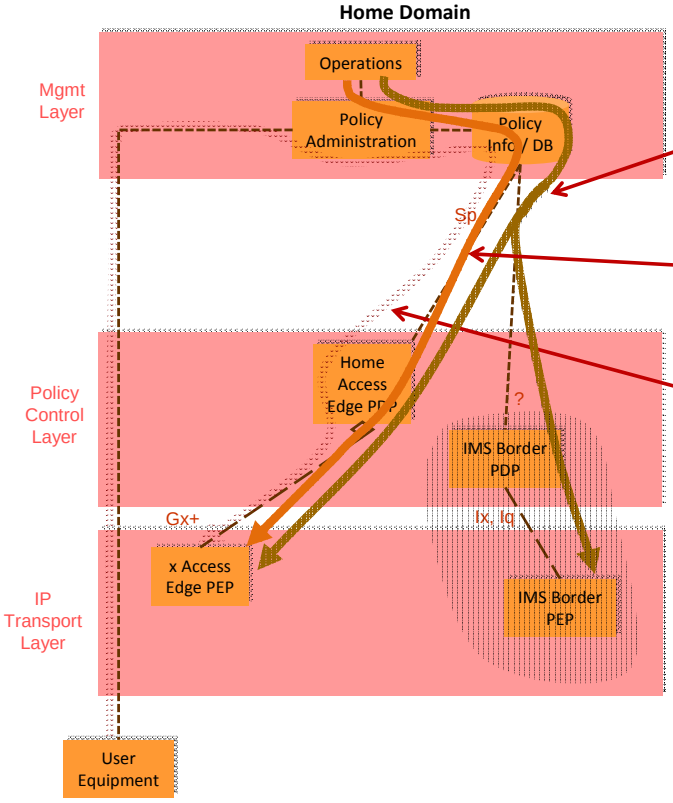
The following requirements apply to both the access & interconnect border PDPs & PEPs:

- (R24) When requested by applications, policy shall control transport-plane aspects of near-end, IP address mediation (i.e., dynamic NAPT & NAPT-PT).
  - Notes (for standards gap analysis):
    - ITU-T RACF and TISPAN RACS account for NAPT/NAPT-PT, as does 3GPP2 SBBC.
    - 3GPP has provided for NAPT/NAPT-T via the Ix interface between the IBCF & TrGW, & recently specified a protocol for establishing NAT bindings over Iq, the interface between the P-CSCF and Access Gateway (AGW). TR 23.848 delineates Border PDP from AF , & the TR scope was expanded in 11/2009 SA plenary to include access border.
- (R25) Border policy shall enable the control of hosted firewall service.
- (R28) Policy shall enable control of the QoS afforded to packet flows associated with users' service.
- (R29) Policy shall enable gate control and rate limiting to only provide QoS for authorized packet flows.
- (R30) Policy control shall enable rate limiting via either traffic shaping or traffic policing.

  Note (for standards gap analysis): ITU-T allows both, & some ATIS specs use ITU-T policy control; 3GPP provides at least traffic policing.

Note for standards gap analysis: ATIS PTSC has specified access border PDPs

Policy Administration



- (R33) Management infrastructure shall allow secure provisioning of per-subscription, per-user, per-user-role, per-application, and per-network policies.

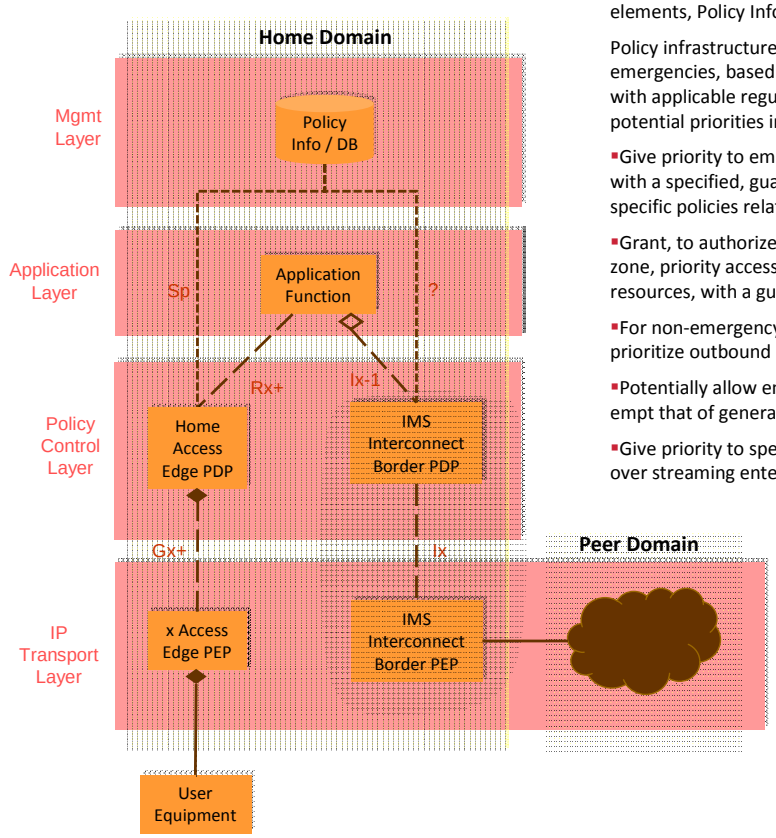
  Note (for standards gap analysis): how the current role – e.g., personal versus business – is determined and identified to the PDP is deemed to be beyond scope.

- (R34) Management infrastructure shall allow provisioning of per-application policies per subscriber, including policies for third-party applications.

- (R35) Authorized users shall be allowed to securely provision certain subscription- and user-related policies, including policies associated with application-specific QoS, firewall control, and content filtering.

- Flows from UE or Operations to Policy Info / Db are for provisioning
- Flows from Policy Info / Db to PDPs & PEPs are for resulting updates of any already installed but modified policy rules & policies

Policy Interaction with Regulatory Services (1 of 2)



R36 has implications for the Application Function, PDP & PEP network elements, Policy Info / Db, & related interfaces:

Policy infrastructure shall provide mechanisms to prioritize traffic during emergencies, based on priorities established by the carrier, in accordance with applicable regulatory obligations and restrictions. Examples of potential priorities include, but are not limited to:

- Give priority to emergency service (E911) usage of network resources with a specified, guaranteed QoS, apart from any subscription- or user-specific policies related to the user who initiates the communication.
- Grant, to authorized emergency (NS/EP) responders within a disaster zone, priority access to both access-network and interconnect-network resources, with a guaranteed QoS.
- For non-emergency (non-NS/EP) traffic to and from a disaster zone, prioritize outbound communications over inbound communications.
- Potentially allow emergency traffic of state and local responders to pre-empt that of general users.
- Give priority to specific applications (e.g. relatively low-bandwidth voice over streaming entertainment video.)

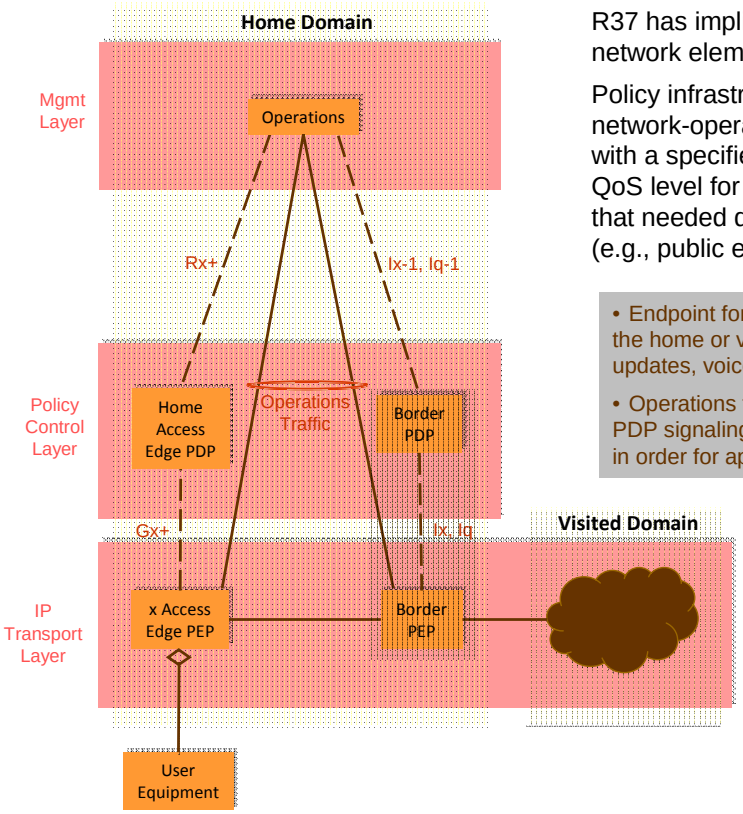
Note: regional requirements may in general take precedence over 3GPP requirements. E.g., for the participating operators, U.S. Gap analysis will additionally be needed against NCS NS/EP (GETS/WPS) specifications.

Policy Interaction with Regulatory Services (2 of 2)

Notes (for standards gap analysis):

- 3GPP PCC already supports bypassing SPR policies when an emergency APN is specified (e.g., E911 service in the U.S.). Although 3GPP PCC supports prioritization of emergency services sessions, this is not required in the U.S.
- ALU advises that NS/EP specs already support the capabilities described in the second example above, and should have been completed by YE 2009.
- ALU advises that NS/EP specs, while ensuring GETS users receive priority, don't differentiate between outbound and inbound traffic for non-GETS users. For this requirement to be realized, there are seemingly two gaps: (a) presumably the policy infrastructure should take some responsibility here – e.g., maintaining state info to the effect that certain resources are in a disaster zone – and not rely strictly on non-GETS policy requests being marked with differentiating priorities; (b) there doesn't appear to be a means to indicate whether the endpoint on behalf of which the request is signaled is the originating or terminating party, & it's debatable whether such context should be signaled by the AF to the PDP.
- 3GPP PCC already supports prioritization & preemption. Rx has a Reservation-Priority AVP from ETSI TS 183 017, an enumerated type with Priority-One through Priority-Fifteen. Gx has a grouped Allocation-Retention-Priority (ARP) AVP with Priority-Level ranging from 1-15 (one is highest). Levels 1-8 should be assigned only to resources for services authorized to receive prioritized treatment within an operator domain (i.e., that are authorized by the serving network). Levels 9-15 may be assigned to resources authorized by home network (e.g., applicable during roaming). Levels 1-8 are intended to prioritize, for example, emergency requests, and could be used cross-domain only if operator's collaborated on values. ALU advises that with LTE/EPC, 7 priority levels have been reserved for GETS-like services, and 1 level for emergency services. Note that, in the U.S., E911 service does not receive priority access. Also within Allocation-Retention-Priority, Pre-emption-Capability and Pre-emption-Vulnerability may be set to 'yes' or 'no.'
- Participating operators have taken an action to determine whether they have interest in a requirement to restrict certain forms of traffic by general users within a disaster zone – e.g., entertainment video.

Policy Interaction with Network Management

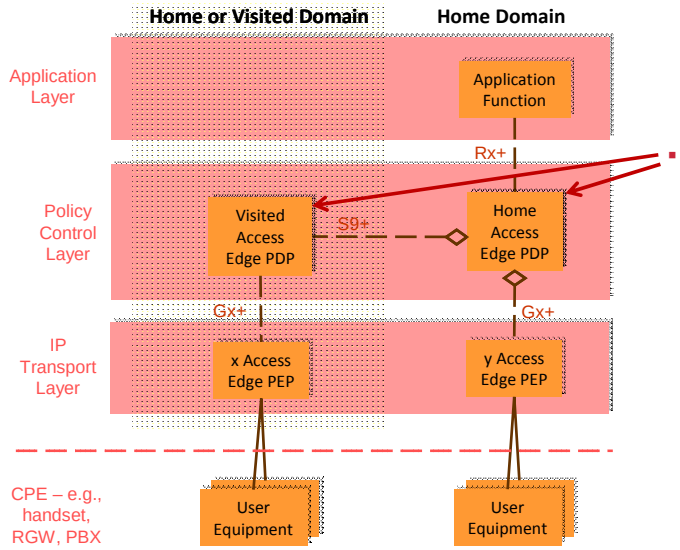


R37 has implications for Operations, PDP & PEP network elements, & related interfaces:

Policy infrastructure shall prioritize authorized network-operations' requests for network resources with a specified QoS, using a different priority and QoS level for daily operation of the network versus that needed during times of elevated operations traffic (e.g., public emergency or outage scenario).

- Endpoint for operations traffic may be user equipment in the home or visited network (e.g., software or parameter updates, voice-quality tests) or network elements
- Operations traffic may or may not be accompanied by PDP signaling. If not, PEP may notify PDP of such traffic in order for appropriate QoS to be provided.

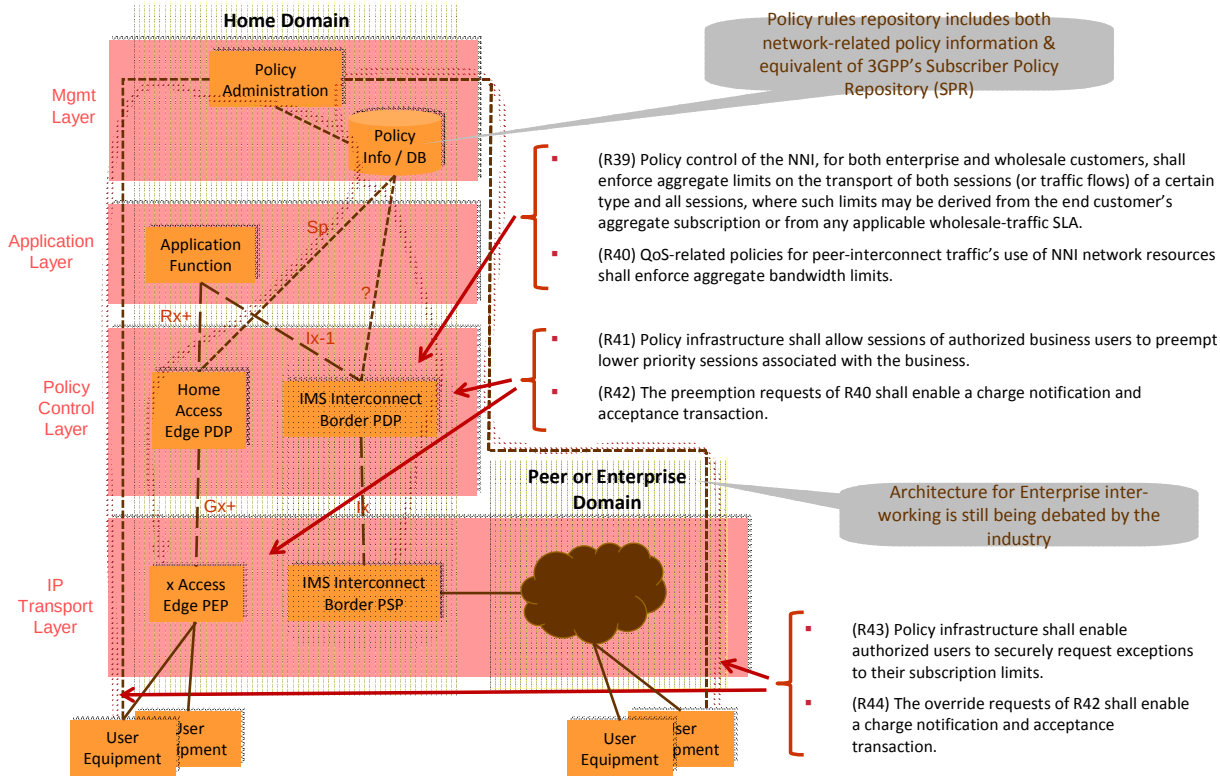
Policy Controls for Aggregate Traffic (1 of 2)



This requirement applies to both roaming scenarios (with Home & Visited Domains) & non-roaming scenarios (with a single Home Domain)

- (R38) Policy control of the UNI, for both small business customers and consumers, shall enforce aggregate limits on the transport both of sessions (or traffic flows) of a certain type and of all sessions, where such limits may be derived from the end customer's subscription or from any wholesale-traffic SLA that is applicable to nomadic or roaming users.

Policy Controls for Aggregate Traffic (2 of 2)



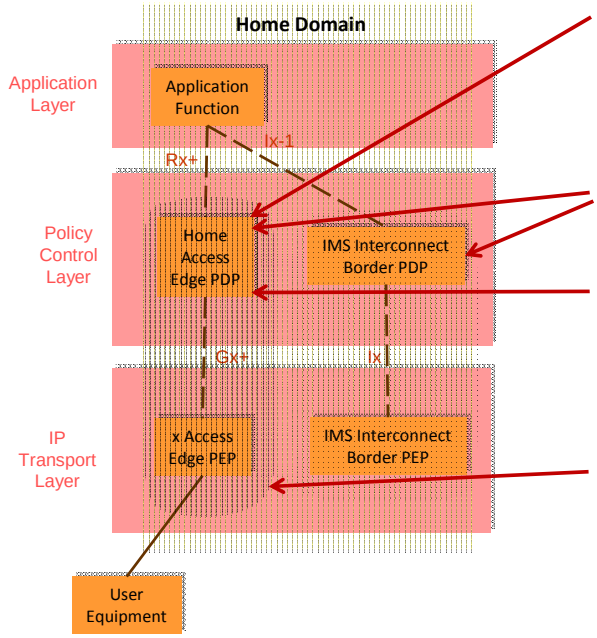
Policy rules repository includes both network-related policy information & equivalent of 3GPP's Subscriber Policy Repository (SPR)

- (R39) Policy control of the NNI, for both enterprise and wholesale customers, shall enforce aggregate limits on the transport of both sessions (or traffic flows) of a certain type and all sessions, where such limits may be derived from the end customer's aggregate subscription or from any applicable wholesale-traffic SLA.
- (R40) QoS-related policies for peer-interconnect traffic's use of NNI network resources shall enforce aggregate bandwidth limits.
- (R41) Policy infrastructure shall allow sessions of authorized business users to preempt lower priority sessions associated with the business.
- (R42) The preemption requests of R40 shall enable a charge notification and acceptance transaction.

Architecture for Enterprise inter-working is still being debated by the industry

- (R43) Policy infrastructure shall enable authorized users to securely request exceptions to their subscription limits.
- (R44) The override requests of R42 shall enable a charge notification and acceptance transaction.

Derivation of Policy Decisions



- (R45) A PDP shall be able to account for the user's location in its derivation of policy and charging decisions.
- (R46) A PDP shall be able to account for the time of day and/or day of week in its derivation of policy and charging decisions.
- (R47) Where an application's policy request is in conflict with a user's self-provisioned policy preferences or with a user-initiated policy request related to the application, whether the request is approved by the policy infrastructure depends on business agreements.
- (R48) In the event that the PDP grants an application's policy request that is effectively not authorized by the user and an incremental charge is incurred, the policy infrastructure shall enable charging to the application service provider.

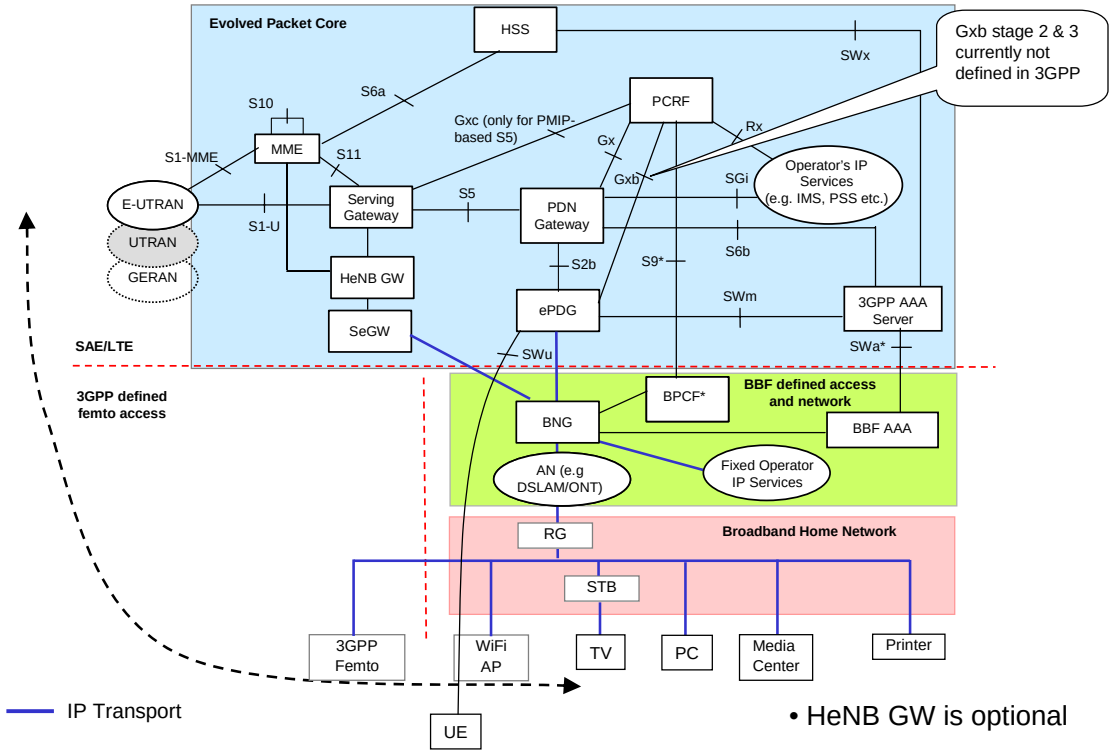
APPENDIX F: SUMMARY OF KEY FINDINGS FROM THE 3GPP/BBF WORKSHOP – FEBRUARY 2010

The following is an over view of the key findings from the 3GPP/BBF/ATIS/TISPAN FMC workshop that was held in San Francisco - Feb 18-19,2010. Co-chairs: Dave Allan, Stephen Hayes.

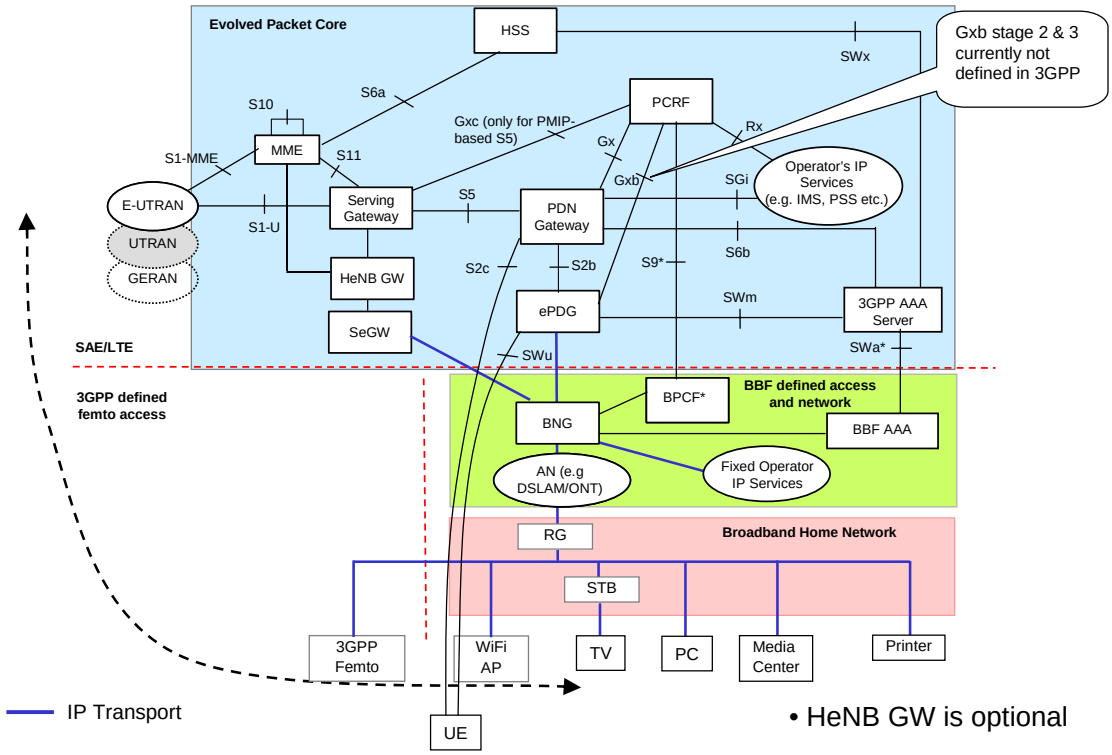
Use Cases & Requirements

- Use cases associated with:
  - It was agreed that offloading cellular access onto wifi access should be considered (e.g., similar to 3GPP IFOM)
  - It was agreed that support of multiple PDN gateways should be considered (e.g., MAPCON)
  - It was agreed that WiFi use cases can cover:
    - Residential WiFi
    - Hot spots
    - Enterprise WiFi
- This functionality should be included in the requirements of BBF WT-203 and in 3GPP 22.278
  - Proposed CR in FMC100044 drafted to upcoming SA1 meeting
  - WT203 editors will bring proposed edit of document incorporating additional use cases to BBF Q1 meeting for ratification

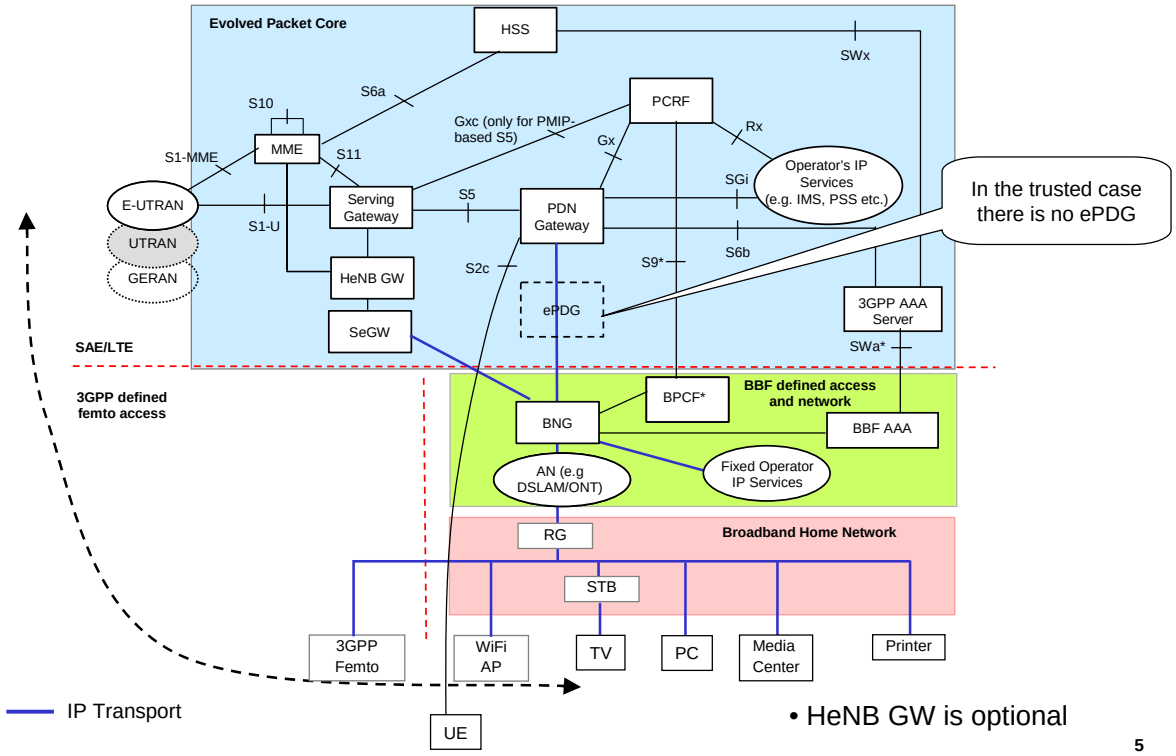
Reference Architecture (Applicable to WiFi over S2b over untrusted fixed access)



Reference Architecture (Applicable to WiFi over S2c over untrusted fixed access)

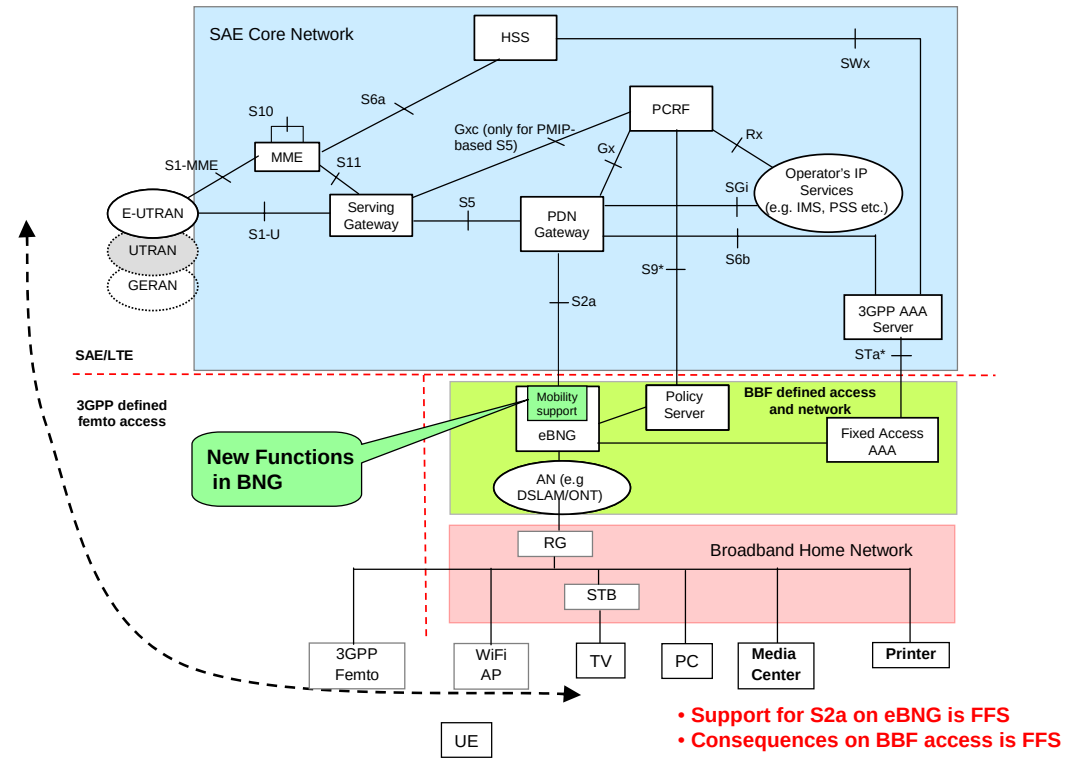


Reference Architecture (Applicable to WiFi over S2c over trusted fixed access)



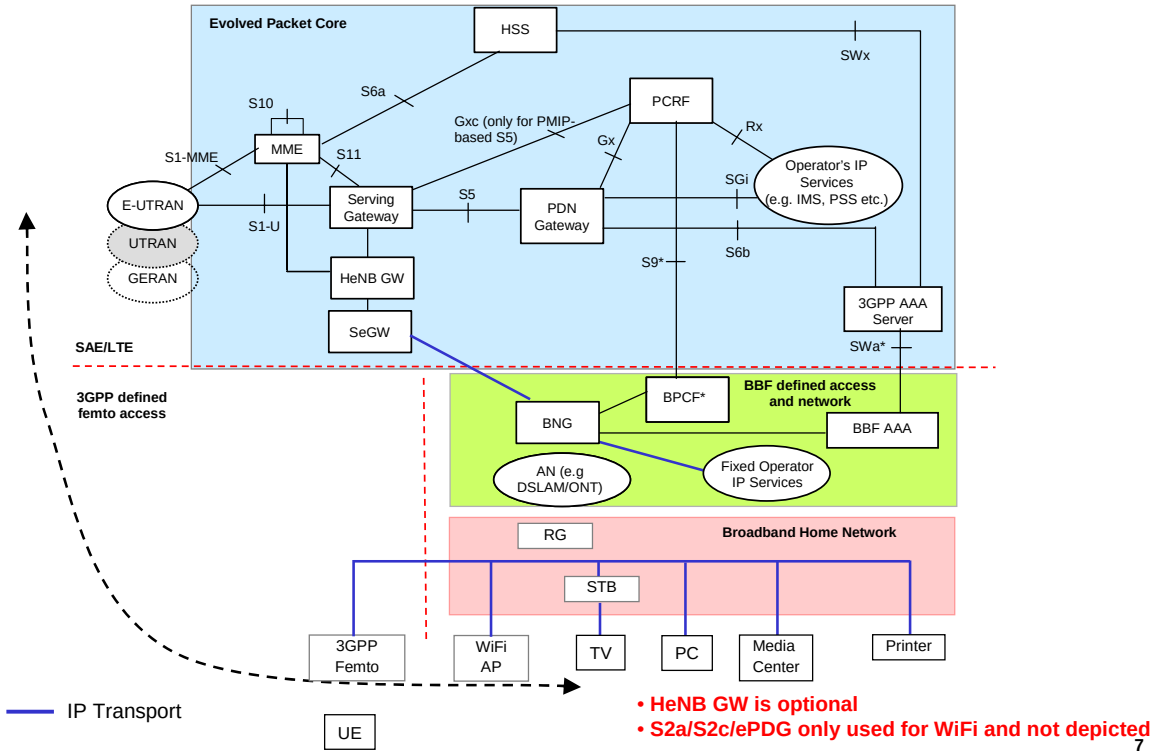
5

Potential Reference Architecture for Trusted Fixed Access (WiFi using S2a)



6

Reference Architecture (Applicable to Femtocells)



Architectural Agreements/1

- Initial interworking work should assume the case of a mobile owned subscriber
  - Rationale: the corresponding interfaces for wireline owned subscriber are not yet fully specified
- The feasibility of interworking will depend on business agreements between the wireless and fixed providers. Without business agreements to cover areas such as reconciliation, authentication, providing Qos, then it may be difficult to have more than basic connectivity.
- It is a 3GPP matter on whether to add integrity protection to s2c.
- There is interest in s2a, s2b, and s2c interconnection scenarios. Further study is needed on the options and feasibility associated with s2a.
- Additional protocol alternatives to PMIP may be considered for network based trusted mobility

Architectural Agreements/2

- S9* is based on S9 and is created by determining the required deltas to S9.
  - SA2 will initially investigate S9* alternatives and communicate this to BBF
- Desire to minimize impacts on wireline RGs

  - Hence S2a option (trusted) with MAG in RG requires further study
- Rx in s9* as is used for AF in the BBF is out of scope

Open Issues Identified (1)

- From 0038 (Mobility/Roaming/Nomadism):
  - Identities
  - IP Address Allocation
  - Network Discovery and Selection
  - How 3GPP MBMS interworks with Fixed Access Multicast functionality?
- From 0012 (AAA)
  - Will charging be offline/online (cross-domain)?
    - How will settlements occur?
  - What tunneling protocols will be supported?
    - In which contexts, and what scenarios?
    - Taking into account the different interworking models.
  - RADIUS/Diameter interworking?
    - 3GPP STa and SWa interfaces are Diameter based whereas BBF AAA interfaces may be still on RADIUS. Therefore, where should be performed the interworking/translation?
  - Is there a need for new functional entities to interwork existing systems?
    - If so, where?

Open Issues Identified (2)

- From 0013 (Policy and Charging):
  - How does the BBF recognize a device in the BBF access?
  - How to correlate the 3GPP service data flows with the BBF IP flows? In the home routed scenarios both for Femto and untrusted IWLAN, the IP flows are tunneled to the home network (using IPSEC). In these scenarios, the BNG cannot look at the inner headers of a tunnel and do service flow detection.
  - What extensions are needed to S9/R to support interworking (S9*/R*)?
  - Can R* be proxied S9* or is something else needed?
  - What is the high-level functional split between the PCRF and the BPCF?
  - What is Minimum set of information exchanged between the PCRF and the BPCF?

  - How charging is done for offloaded traffic (that does not traverse 3GPP network) from a 3GPP subscriber? (both Femto and non-Femto cases need to be considered).
  - How is reconciliation done between 3GPP/BBF network?

Open Issues Identified (3)

- From 0033 (Authentication):
  - UE requires distinct treatment and has to authenticate itself to the wireline network in order to justify much of what FMC wants to achieve. This likely requires changes to the wireline network….
    - Are there business drivers to justify this change?
    - If so, a solution to giving the UE unique treatment is required

Converged Policy

- A converged policy controller is beyond WT-203
- 3GPP encourages BBF to consider 3GPP PCC in its fixed policy work
- If it is deemed desirable to progress policy convergence (in addition to interworking) a different initiative is needed.

Next Steps

Near term

- SA2 will perform preliminary gap analysis of S9 interface capability and report to BBF meeting
- WT-203 editors will bring proposed edit of document incorporating additional use cases to BBF Q1 meeting for ratification

Longer term

- BBF should address the following issues
  - Identification of UEs behind the RG
- The window for the closure of new use cases and requirements for WT203 should close after Q1.
- Further work in 3GPP should proceed as per the agreed work item in document FMC100053

APPENDIX G: RELEVANT POLICY MANAGEMENT STANDARDS

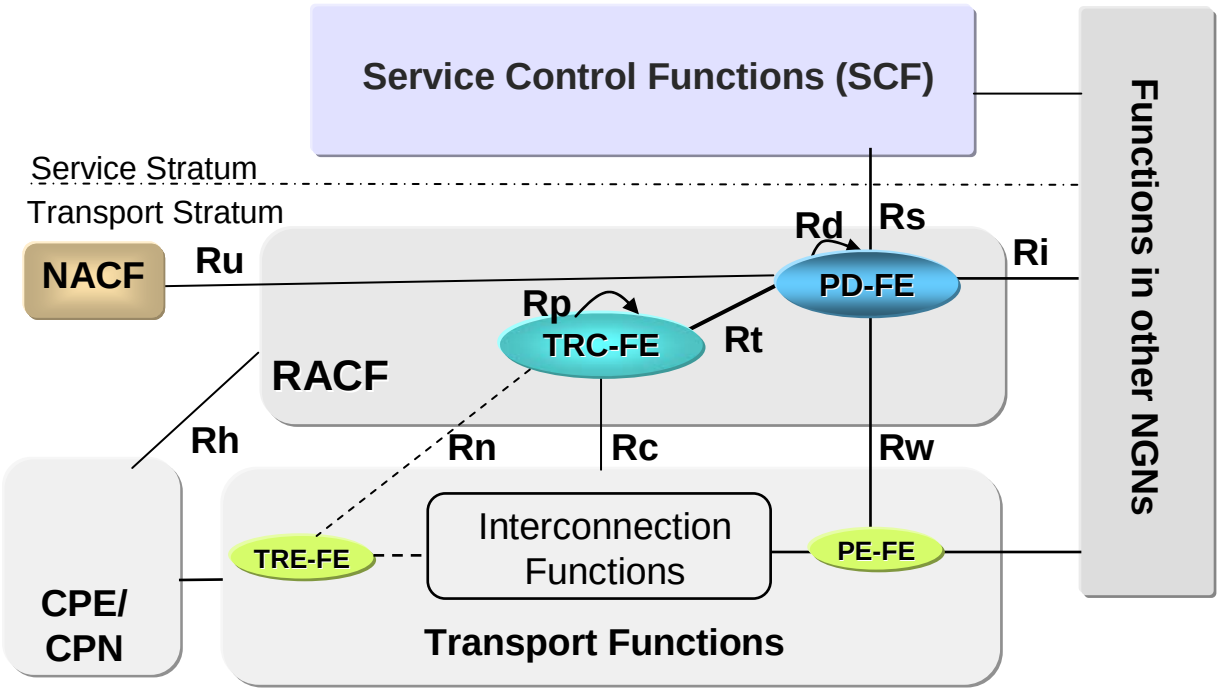
The following section provides an inventory of policy management standards activities ongoing in the industry, identifying relevant organizations that are performing policy management standards development.

ITU-T

ITU-T RACF: Resource and Admission Control Functions (RACF) for NGN (Y.2111)

Key Features of the ITU-T RACF for NGN include dynamic, service-independent management of a variety of resources (e.g., bandwidth or IP addresses) across varied transport networks—different technologies, administrative domains, and ownerships. This also includes:

- Managing network congestion via admission control
- Ensuring end-to-end QoS
- Enabling new services such as Turbo Boost
- Hosted NAT traversal, NAPT
- Wholesale versus Retail business models



- PD-FE - Policy Decision Functional Entity – service-based, transport technology independent
- TRC-FE - Transport Resource Control Functional Entity - service-unaware, transport-technology dependent, network-segment specific
- PE-FE - Policy Enforcement Functional Entity

- TRE-FE - Transport Resource Enforcement Functional Entity
- NACF - Network Attachment Control Functions

RACF Highlights

RACF provides Transport Policy and Resource Management Capabilities such as:

- Application-driven (network-independent) "real-time" control
- Management of transport resources within networks (access or core) and at network boundaries
- Resource admission control for unicast and multicast (e.g. VoD and IPTV)
- Policy-based authorization and allocation of the resources supporting
  - End-user equipment of varying QoS control capabilities
  - Push and pull models for policy control
  - Multiple transaction models for resource authorization, reservation and commitment
  - A combination of resource management methods based on accounting, measurement and reservation
- RACF interfaces to Service Control Function (e.g. SIP Proxy Server or IMS) to allow an Application to request resources including:
  - QoS (BW Guarantees, per flow traffic shaping/policing, priority, …)
  - NAPT control and NAT Transversal capabilities
  - Gate control and other border control functions
- RACF can interface across network boundaries to support a variety of business models
  - Addresses Session Border Control Issues
  - Can integrate transport charging capabilities as needed (future)

RACF Key Elements

- PD-FE – Policy Decision Functional Entity
  - Apply network policies to resource management requests from Service Control Functions
  - Check subscription profile
  - Given an IP address pair and required BW, determine if the given flow can be supported in the network
  - Policy enforcement control for PE-FE along the flow path
- TRC-FE – Transport Resource Control Functional Entity
  - "Connection Admission Control"

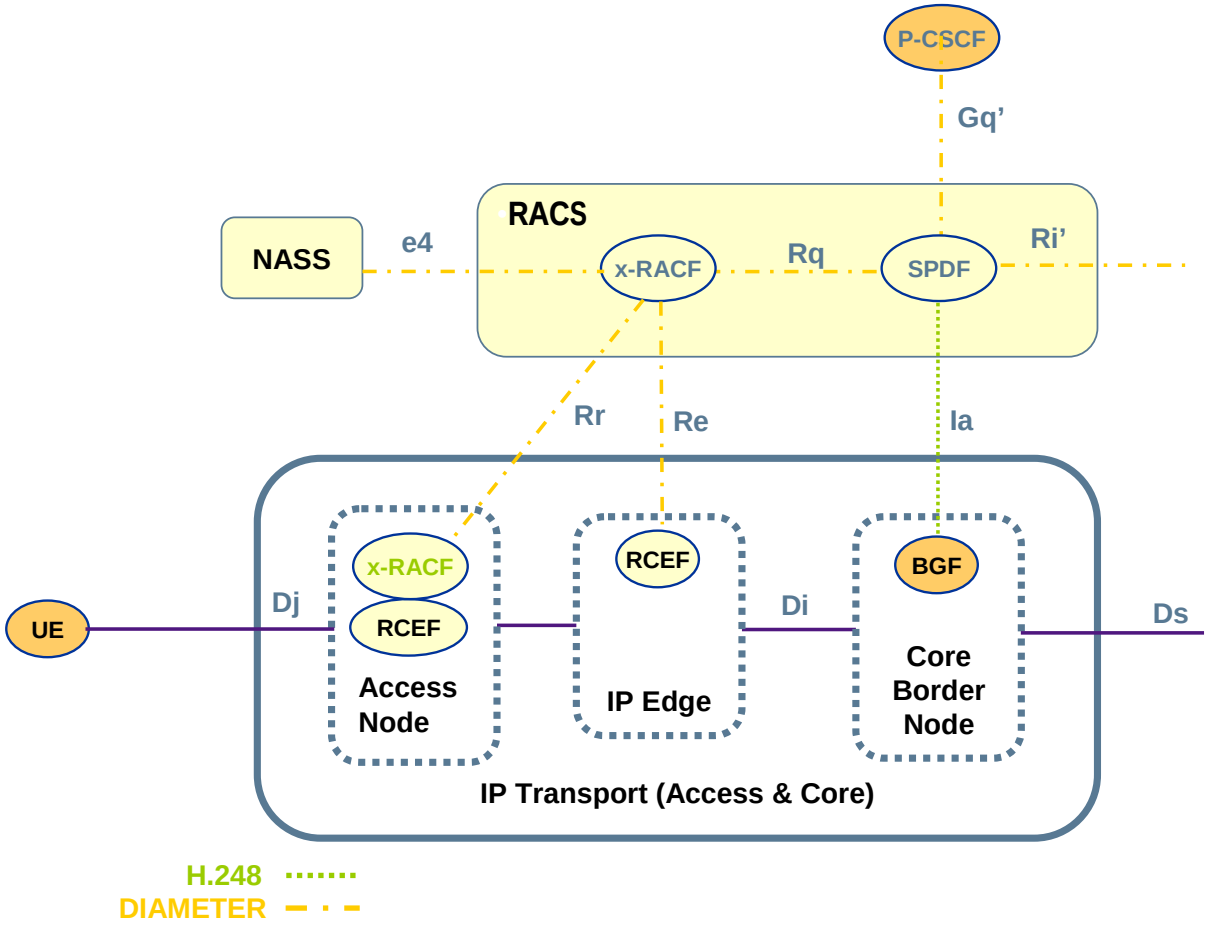
  - Monitor network resource utilization and network topology to manage path bandwidth availability (reservation and/or monitor)
- PE-FE – Policy Enforcement Functional Entity
  - Provides media path functions such as gate control / Firewall
  - NAPT translation and NAT Transversal
  - Per flow policing and QoS-marking
  - Can provide congestion/capacity information to Service Control

Key Reference Points

- 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.

ETSI TISPAN

TISPAN RACS (ETSI ES 282 003)



- SPDF = Service Policy Decision Function
- A-RACF = Access-Resource & Admission Control Function
- BGF = Border Gateway Function
- RCEF = Resource Control Enforcement Function
- NASS = Network Attachment Subsystem

RACS Key Elements

- SPDF – Service Policy Decision Function
  - Apply network policies to resource management requests from Application Functions
  - Given an IP address pair and required BW, determine if the given flow can be supported in the network
  - Manage resources only in BGF including NAPT Transversal, NAPT and Gate Control
- x-RACF – Resource Admission Control Function

  - Check subscription profile
  - "Connection Admission Control"
  - Policy enforcement control for RCEF e.g. AN and BNG
- BGF – Border Gateway Function
  - Gate control and traffic policing/marking
  - NAPT translation and NAT Transversal
- RCEF – Policy Enforcement Functional Entity
  - Provides media path functions such as gate control
  - Per flow policing and QoS-marking

RACS Key Reference Points

- Gq': AF - SPDF
  - For AF to request transport resource authorization and control
  - Information exchanged: session ID, media descriptor, application QoS requirements, priority, gate or NAPT control policy, etc.
- Ia: SPDF - BGF
  - For SPDF to apply controls to BGF concerning NAPT, hosted NAT traversal, gating, bandwidth, packet marking, etc.
  - Information exchanged: media descriptor, DSCP value, bandwidth committed, bandwidth authorized, gate control command, NAPT control command, usage information, etc.
- Rq: SPDF - x-RACF
  - For SPDF to request resource availability check by x-RACF
  - Information exchanged: media descriptor, bandwidth, other network QoS requirements, network path, etc.

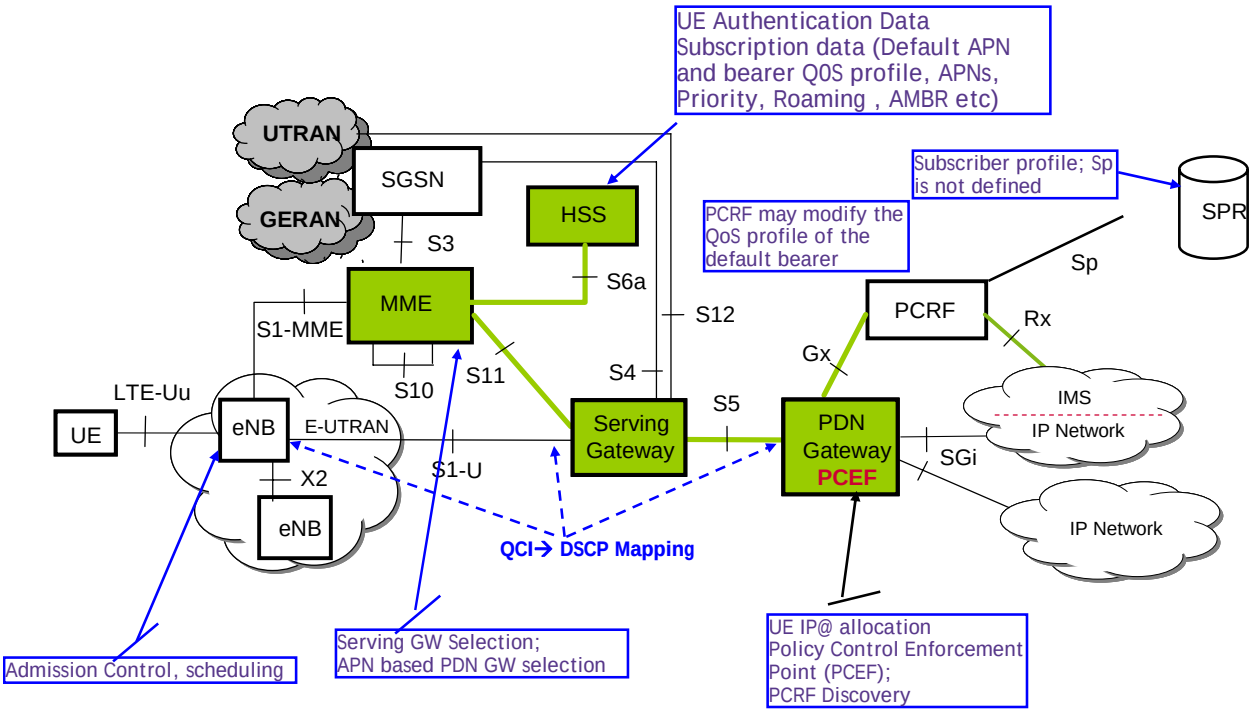
3GPP

UE Initial Attach

The following aspects are covered in the UE Initial Attach:

- UE Authentication & Authorization
- Location Update
- Default Bearer set up with QoS & priority for ALWAYS ON connectivity
- Dedicated bearer for SIP signaling may be established at the same time

UE Attach Procedure



3GPP Border Control Policy

3GPP TS 23.228 is the current state of the art Border Control Policy and is outlined below. In addition, R10 study item SP-080559 related to TR 23.848 proposes insertion of a PDF between the control- and user-plane network elements.

IMS-ALG and IMS Access Gateway Model

Figure 4.4.4.1 presents the general reference model for IMS access when both the signalling and media traverses NAT devices. Figure G.2 presents the general reference model when IP address translation is needed between the IP-CAN and the IMS domain. The IMS network architecture is the same for both cases. The NAT integrated with the IMS Access Gateway is under service provider control in this reference model.

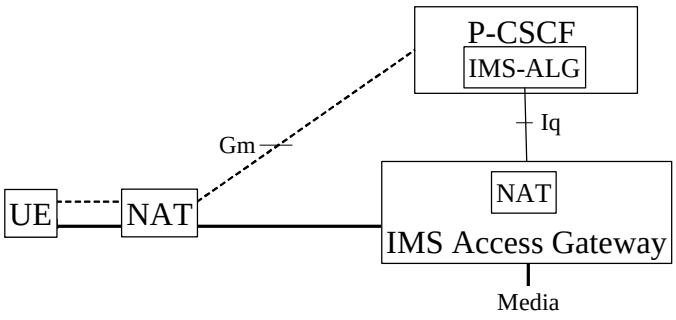


Figure 4.4.4.1 Reference model for IMS access when both the signalling and media traverses NAT

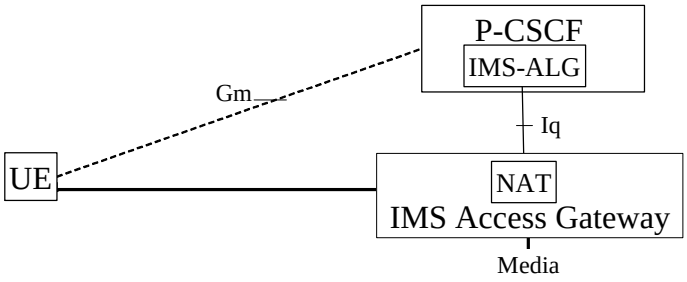


Figure 4.4.4.1 Reference model for IMS access when NAT is needed between the IP-CAN and the IMS domain

ICE and Outbound reference model

Figure 4.4.4.2 presents the general reference model for IMS access when both the signalling and media traverses NAT devices. Functional elements with dashed lines represent optional functionality. The transport of the Gm signalling is also subject to the policy enforcement.

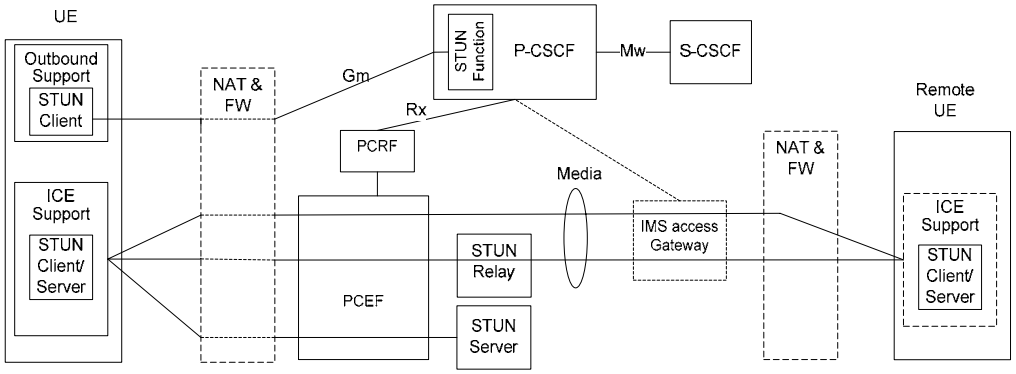


Figure 4.4.4.2: Reference model for ICE and Outbound Methodology

The STUN Function shown within the P-CSCF is a limited STUN Server for supporting STUN keep-alive messages.

For deployments where the IMS Access gateway (or other media manipulating functional entities, such as a MRFP, are used, such functional entities shall be placed on the network side of the STUN server and STUN relay server (i.e. not between the UE and the STUN server or STUN relay server) as shown in figure 4.4.4.2. Otherwise they will prevent STUN messages from reaching the STUN Relay/Server outside of a session.

Border Control Functions

Figure 4.4.4.3 presents a high-level architecture diagram showing how Border Control Functions fit into the IMS architecture.

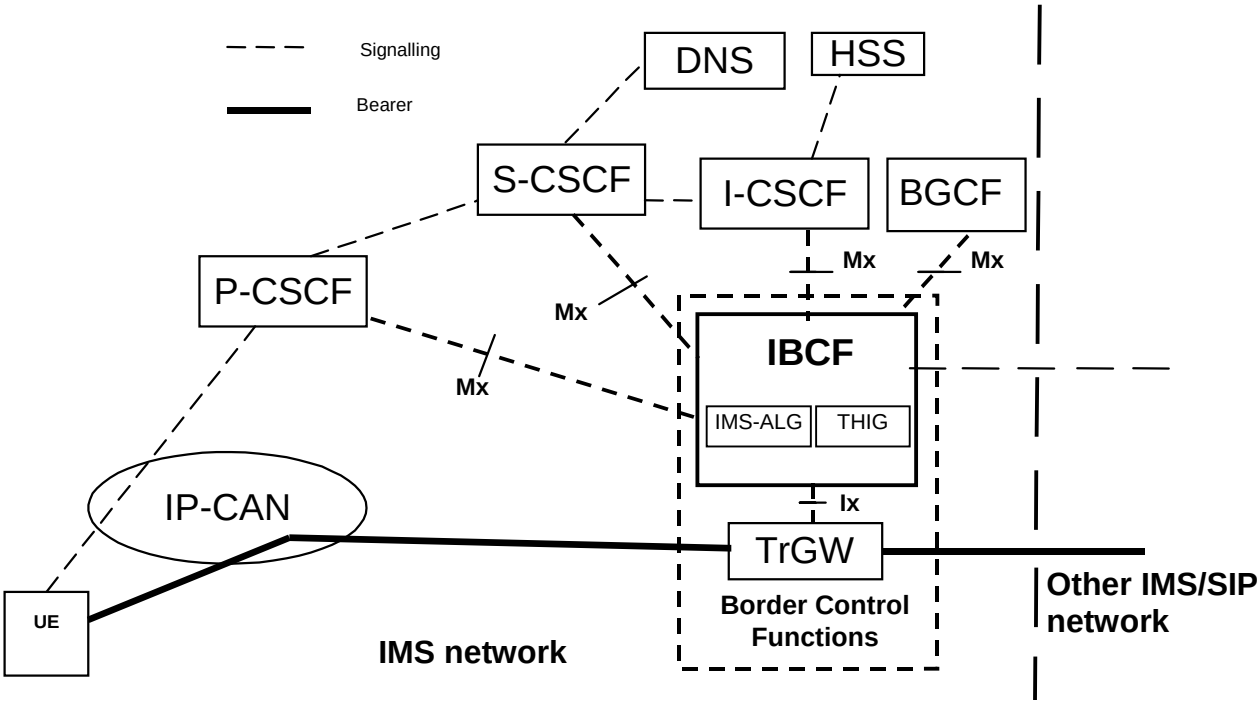


Figure 4.4.4.3: Border Control Functions

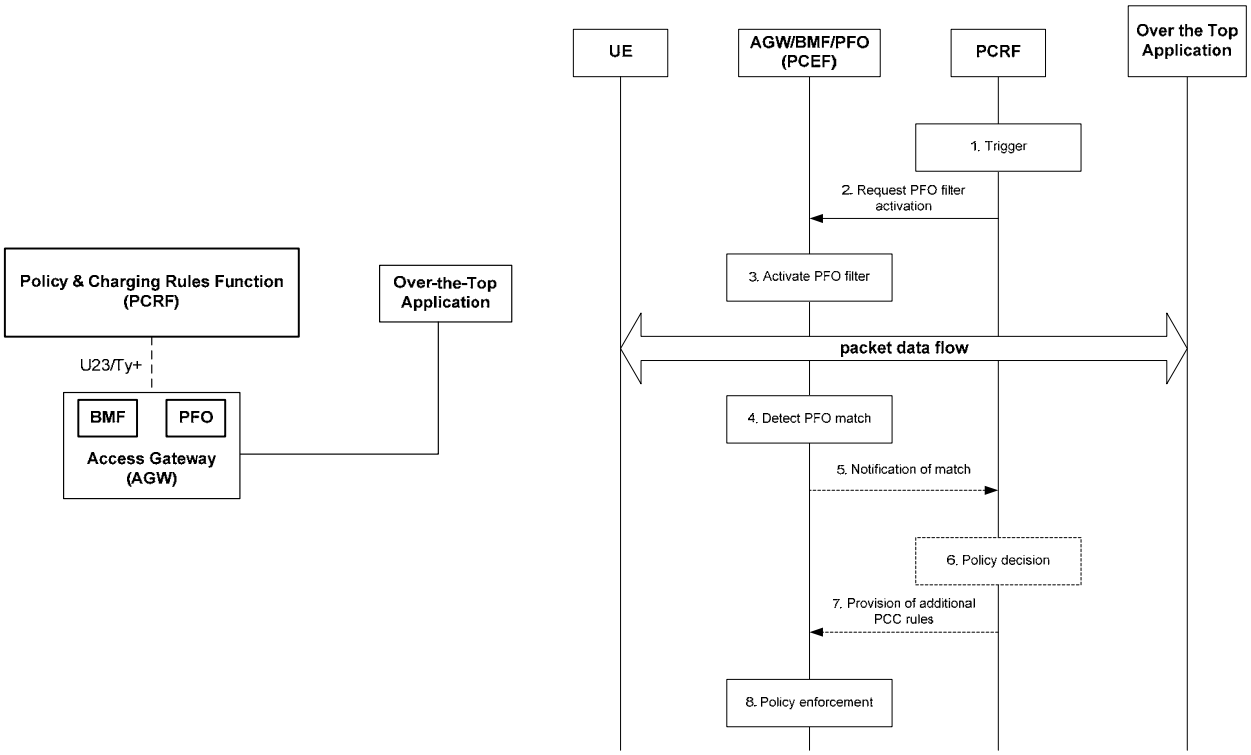
NOTE: The standardisation and functional requirements of Ix reference point are FFS.

The Mx reference point allows S-CSCF/I-CSCF/P-CSCF to communicate with an IBCF in order to provide border control functions. The Mx & Ix reference points are not specified within this release of the specification.

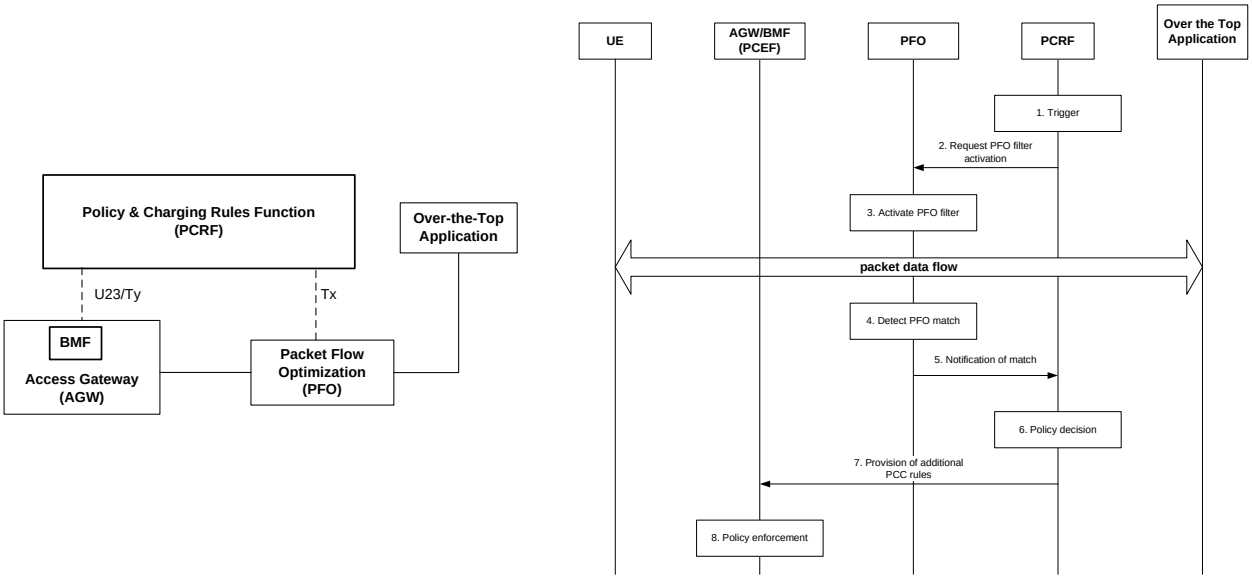
3GPP2

The following depicts 3GPP2's Packet Flow Optimization (PFO) Management. Please note that reference should be made to TR 23.813 (related to R10 Study Item SP-090361) which borrows from this aspect of 3GPP2 policy architecture.

Packet Flow Optimization (PFO) Management – Integrated in AGW



Packet Flow Optimization (PFO) Management – Separate PFO Entity



Broadband Forum

A BBF policy framework specification is still forthcoming; however, WT-203 proposes S9+ based inter-working between 3GPP PCC and (proprietary) fixed broadband policy frameworks as depicted in WT-203 diagram (or choose a representative diagram from FMC workshop agreements presentation), and 3GPP approved in February a new work item for support of BBF accesses inter-working.

APPENDIX H: POLICY MANAGEMENT FOCUS GROUP MEMBERS

Chair	
Charlie Vogt	GENBAND
Members	
Ken Biholar	Alcatel-Lucent
Konstantin Livanos	Alcatel-Lucent
Farooq Bari	AT&T
Mike Hammer	Cisco
Vojislav Vucetic	Cisco
Fred Kemmerer	GENBAND
Woody Denman	GENBAND
Marc Brandt	HP
Mark Montz	HP
Tony Saboorian	Huawei
Robert Jaksa	Huawei
Marco Spini	Huawei
Gregory Dalle	Juniper
Reinhard Nappert	Juniper
Bill Welch	Juniper
Victor Coello	Nokia Siemens Networks
James McEachern	Nortel
Chris Hogg	Nortel
Mike Fargano	Qwest
Joe Scivicque	Qwest
Kong Cheng	Telcordia
Naseem Khan	Verizon

ATIS Staff	
Tim Jeffries	
Tom Payne	