QoS in Access Networks

QoS is key in multi-service access
End-to-End QoS solutions (e.g. IntServ)
- commercially failed because of complexity
Priority based QoS (e.g. Diffserv)
- works in over-provisioned networks
- insufficient for Access & Aggregation
=> Simplified QoS control in Access & Aggregation needed
Ethernet Network Model

- CPN
- CPG
- Ethernet switch (802.1ad)
- Ethernet switch (S-VLAN aware or 802.1Q)
- Ethernet (MPLS) aggregation network
- BRAS or Edge Router
- NSP/ISP
- AEN
- NAP
- ASP
Potential BottleNecks in Access Networks

Because of the nature of sharing the connectivity resources, there can be potential bottlenecks Upstream & Downstream traffic at Access Nodes, Aggregation Nodes & Edge Nodes depending on the quantity & the required quality of service.
**Muse QoS Drivers**

- The need for a pragmatic, simple and cost-effective approach for delivering mass market services with an acceptable QoS from the point of view of both the customer experience, and the willingness of the service provider to pay for the additional network functionality.
- Not all traffic but only a subset of traffic requires hard, parameterized QoS guarantees.
- A global QoS solution across access, regional and core networks is not needed.
- The need to support a retail/wholesale split in the QoS business model.
- The need to provide upstream QoS, especially across the access link, to support services like quality VoIP, video telephony, etc.
- The need for multiple service edges. There are several different types of service edges in addition to BRAS, for example video servers (already covered to a degree in TR-101), soft switches, and PE routers. Typically the services associated with these edge nodes do not go via the BRAS (for scaling and reliability reasons), and so there is no longer a single point of QoS control.
QoS Based on Resource Admission Control

AF - Application Function
NAP - Network Access Provider
PDF - Policy Decision Function
RAC - Resource Admission Control

ASP - Application Service Provider
NSP - Network Service Provider
QoS - Quality of Service
RNP - Regional Network Provider
On-demand and Pre-provisioned CAC

- On-demand CAC means that the CAC decision is based on calculating the current usage and availability of network resources for the requested QoS in real time. On-demand CAC can support requests that are heterogeneous in the sense that the calls need not have the same QoS parameters.

- Pre-provisioned CAC refers to the CAC process where decision is simply made on the basis of the number of accepted requests, which must not exceed a previously specified number. Pre-provisioned CAC supports only homogeneous calls, i.e. those having the same network requirements, since only the number of accepted calls is counted.

*Issue: Synchronization of active calls as per CAC & in reality!*
Selective CAC

• One set of resources that can be used by services without an on-demand or Signaled CAC process. For best-effort traffic, which has no QoS guarantees, there is no CAC needed with respect to usage of network resources. *(Some operators have indicated that Voice calls may fall into this category, since it is expected that residential voice service may need to be offered almost free)*

• Another set of resources for which Signaled CAC is needed on a call/session basis. Note that, a given pipe can either be completely dedicated to traffic subject to CAC, or to improve network utilization may be share between CAC and non CAC traffic. In the case of sharing, then prioritization mechanisms will be required in addition to CAC. Depending on the network architecture and dimensioning. CAC may only be needed for certain links within an end to end path.
Central CAC system

There are several proposals in the industry for providing QoS using CAC, which implicitly involve using a central CAC system in the sense that there is one CAC system for the network and all call admission requests have to be signaled to this central system. The central CAC system has a complete view of the resources of the appropriate parts of the Network. For each and every call (signaled) request or (non-signaled) detection, the central CAC system is consulted, which depending on the availability of the resources decides either to allow or block the requested call. This decision is sent to the boundary node (the Access Node or the Edge Node) where enforcement may be done.
Local CAC

A local CAC system (meaning local to a given node) is where the CAC decision is made at the Access or Edge Node. For a CAC decision to be made locally, it is necessary that there is a local view of the availability of network resources that are exclusively available to that border node.

To do that, it is necessary that network resources are previously partitioned and allocated to the different border nodes.

This naturally leads to a reduction of the potential multiplexing gains that could be obtained, as unused resources allocated to a given border node can not be used by another border node. In order to avoid this, partitions should be updated on a regular basis by a central authority that has an historic and global view of network resource usage.

Further refinements of the local CAC are possible, with the introduction of usage thresholds in the allocations of a resource to different border nodes.
Policy Enforcement Points

After a CAC decision is made, enforcement of the allowed QoS policy (bandwidth, QoS class, maximum size of packet, etc.) may be required so that misbehaving flows do not impact the QoS of the other flows. Total protection can only be provided if enforcement is done on a per flow basis. However it is recommended that policy enforcement be done on aggregate of IP flows where possible to lower the processing power required at the nodes.
Models of Access Networks

‘Carrier’ model
- The network just provides transport/connectivity services.
- The network is not application/session aware.
- Current best-effort Internet access model.
- Can be implemented by enhancing with multiple QoS connectivity services, tailored and classified for the most prevalent group of services.

‘Application’ model
- The provisioning of an end service is controlled & guaranteed by the operator. The user requests (dynamically) for a service, and the network sets-up the most appropriate transport/connectivity service (service-based policy push).
- The network is application/session aware.
Flow based QoS Control in ‘Application’ Model

Flow based

FB monitoring
FB gating
FB policing

FB monitoring
FB gating
FB policing

CPN A

CPN B
Aggregate based QoS in ‘Application’ Model

Traffic Class “per Service Provider” Based control: All the traffic flows belonging to the same traffic class and served by the same SP are aggregated together and treated as a whole in the ENs.
QoS in ‘Carrier’ Model

Traffic Class “per User” & “per SP” Based control
- TCB monitoring
- TCB gating
- TCB policing

Traffic Class “per SP” Based control
- TCB monitoring
- TCB gating
- TCB policing

Traffic Class “per User” & “per SP” Based control
- FB monitoring
- FB gating
- FB policing

Intelligent RGW: It must solve the applications contest for bandwidth according to the end user preferences and the available transport services
Converged QoS Model

Border nodes (AN & EN) must be able to perform these tasks both at IP flow and traffic class level.

Network operator’s choice of policy:

- Appropriate application of ‘flow’ or ‘aggregate’ QoS model based on specific requirements for individual access networks
- Mix and match of ‘carrier’ or ‘application’ models
Inter-domain Transfer of Policies

Inter-domain transfer of policies may be accomplished by the use of SLA for Static and / or for Dynamic Policy Handling. These terms correspond to two different ways of performing policy control in roaming/nomadic situations and are associated with how policies from the home network are transferred to the visited network.
Inter-domain Static Transfer of Policies

Static transfer means that the required policies to support services for nomadic / roaming users are provisioned and distributed during SLA process or default policies are used as per SLA. This implies that a nomadic / roaming user may experience a completely different service offering in a visited network, than at the home network. Additionally, it is possible that there are restricted per user service differentiation possibilities in the visited network, since it would be gargantuan to have all nomadic / roaming user details provisioned in all possible visited networks.
Inter-domain Dynamic Transfer of Policies

By dynamic transfer it is meant that the policies have not been transferred before a visiting user associates to the visiting network, i.e. the policies have not been transferred during the SLA process. There are 2 ways of dynamically transferring policies:

- **Local Control**: The checking of policies or policy execution is performed in the visited network, which means that once the subscriber is detected, relevant policies are transferred over the management plane.

- **Remote Control**: The check of policies or policy execution is performed in the home network, which means that there is no initial or pre-transfer of policies. This could lead to undesirable delays that may affect service delivery.
Policy Execution

Central Policy Server
User, service, network & business rules
Local Policy Server
User, service, network & business rules

Packager
CPs

Nomadism Provider
FMC Provider
RN PDF
SP1
SP2
SP3

User, service, network & business rules
Access Policy Manager

The Access Policy Manager is a functional entity which is used to provision policies in the Access Network at the appropriate nodes & can be divided into the following additional (sub) functional entities: the External Policy Management (EPM), the Service Policy Management (SPM), the Network Policy Management (NPM), and the User Policy Management (UPM). The individual functional entities - EPM, SPM, NPM & UPM maybe implemented as separate independent modules or they can be sub-modules of a combined Access Policy Manager.
External Policy Manager (EPM)

The External Policy Manager (EPM) is responsible for generating business related policies, (such as roaming agreements and SLAs) and pushing them down to the correct policy decision points. The EPM plays a key role when it comes to nomadism support. In nomadic cases where policies need to be transferred or re-generated based on location, the EPM is always the starting point. The EPM stores information about the roaming agreements that have been reached with other providers / operators / packagers. This information will generally be retrieved for the first time, when a user moves to a new visited network.
Service Policy Manager (SPM)

The Service Policy Manager creates and pushes service related policies to proper policy enforcement points. Service policies describe the overall business logic that is applied to requests from application servers and from peer SPMs. The interface between peering SPMs is also an important step towards nomadism support. In 3GPP, a similar interface, s9 between PCRFs, is being standardized. SPMs are hosted by individual application service providers.

The most significant service policies include service resource requirement policies, QoS policies, nomadic policies, etc. To support nomadism, it is recommended to have at least two sets of policies for the same service, one set used in home network case and the other used in visited network case. Service policies generated by SPMs are based on the SLA policies held by the EPM, and depending on how the roaming policies are defined in the EPM, the SPM could decide whether multiple policy sets are needed for the same service.
Network Policy Manager (NPM)

The Network Policy Manager (NPM) receives service policies from service policy managers and maps them to network dependent policies if defined business policies allow it. Additionally it can create network related policies based on the existing network status, in an active manner. Some of the functions of the NPM are:

- Definition and maintenance of a default set of static policies for the stability of the access network.
- A conflict solving mechanism to detect and remove potential policy conflicts from different SPMs.
- A priority setting mechanism to prioritize policies, e.g. home policies to have higher priority than external ones.
- A rollback mechanism. When the access network enters into an unstable status due to undetected policy conflicts, the NPM should provide a policy set which helps the network to roll back to the latest previous stable status.
- A conflict reporting mechanism. When there are unsolvable policy conflicts, the NPM should be able to report the situation to all related SPMs and to the overall management systems.
User Policy Manager (UPM)

The User Policy Manager (UPM) controls all end-user related policies, such as user identification, AAA, billing records, etc. It corresponds to functionalities in NASS in the TISPAN specification. User Policy Manager should also hold information about service subscriptions of a specific user. When a user is in a nomadic status, AAA will be performed against this information before services can be used.
Service Controller (SC)

The Service Controller handles service requests by performing a check of its contents against service policies, and sends requests for resources to the Resource Controller.
Resource Controller (RC)

The Resource Controller handles resource requests from the Service Controller by performing a check of its contents against the subscriber profile based on network policies and user policies, as well as by performing a check on the availability of resources necessary to deliver the requested service with the requested network parameters such as QoS. If resources are available, the Resource Controller (RC) may derive traffic policies to be enforced in the underlying transport network elements.
Policy Control: Nomadic User Moving Between Roaming Networks

Fixed Access Network
- Home domain
  - User's home
  - Service Provider (ASP)
  - Packager

Mobile network
- Visited domain
  - Mobility Anchor Point (M-Anchor)
  - Service Provider (ASP)
  - Packager

= Policy Repository

3GPP RAN
- Subscription Policy Rules
  - PCRF (Policy and Charging Rules Function)
  - Online Charging System

3GPP CN
- Offline Charging System
- SGSN
- GGSN

3GPP CN
- NPM
- UPM
- SPM
- EPM

NPM
- Fixed Access Network
- Mobile network
Example: Policy Interactions in FMC

Nomadic Use Case Action:

Jose brings his own laptop to his parents and attaches it to a dedicated nomadism port on the RGW. The terminal authenticates to the network and gets an IP address.
Example: Policy Interactions in FMC

Use Case Action: He uses the Internet to access his media centre (can be in his CPN or at another location), where he has stored all the pictures from his daughter’s last birthday, and shows it on the TV screen at his parents home.

<table>
<thead>
<tr>
<th>Visited Network</th>
<th>Home Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Control</td>
<td></td>
</tr>
<tr>
<td>• vNAP enforces network policies for internet access.</td>
<td>• hSP controls user policies (application level authentication).</td>
</tr>
<tr>
<td>• User policies are checked either by vNAP or vISP as per implementation</td>
<td>• Optionally, hNAP enforces network policies as per SLA with hSP.</td>
</tr>
<tr>
<td></td>
<td>Note: NAT transversal mechanisms to be enforced where needed, e.g. at Residential Gateway.</td>
</tr>
</tbody>
</table>

Note:
Example: Policy Interactions in FMC

Use Case Action: Due to the nomadic feature, he has access to the list of available services in visited network according to his service profile.

Assumptions: A video call SP exists in visited network, so that video call can use high priority traffic (i.e. not internet based) in the visited network.

<table>
<thead>
<tr>
<th>SLA Policy Management (Static)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Visited Network</td>
</tr>
<tr>
<td><strong>vSP/Packager:</strong> Transferred service policies &amp; general network policies related to services offered to nomadic users of home SP, as per SLA.</td>
</tr>
</tbody>
</table>

Due to the nomadic feature, he has access to the list of available services in visited network according to his service profile. A video call SP exists in visited network, so that video call can use high priority traffic (i.e. not internet based) in the visited network.
Example: Policy Interactions in FMC

**Use Case Action:** Due to the nomadic feature, he has access to the list of available services in visited network according to his service profile.

**Assumptions:** A video call SP exists in visited network, so that video call can use high priority traffic (i.e. not internet based) in the visited network.

<table>
<thead>
<tr>
<th>Visited Network</th>
<th>Home Network</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Policy Management (Dynamic)</strong></td>
<td></td>
</tr>
<tr>
<td>• vUPM may receive specific user policies. (vNAP vCP vSP hSP).</td>
<td>• hUPM optionally transfers specific user policies to visited network based on user-subscribed nomadic services.</td>
</tr>
<tr>
<td>• vNAP may receive specific network policies, incl. QoS. (vNAP vCP vSP hSP).</td>
<td>• hSP optionally transfers specific network policies to visited network based on user-subscribed nomadic services.</td>
</tr>
<tr>
<td><strong>Policy Control</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• hSP controls user policies, related to available &amp; subscribed services at visited network.</td>
</tr>
</tbody>
</table>