FROM STATIC TO DYNAMIC QOS

mag. eng. Nikolay Milovanov

Резюме *– Докладът разглежда методите за прилагане на динамични политики за качество на обслужване в IP мрежи. За целта са разгледани три такива:*

Налагане на динамично качество на обслужване чрез системата за създаване, управление и оценка на услуги.

Управление на политиките за качество на обслужване чрез COPS протокол.

Налагане на динамично качество на обслужване чрез Diameter.

Ключови Думи *– IP мрежи , Качество на обслужване, динамично управление на политиките за качество на обслужване, създаване и оценка на услуги, COPS, Diamater.*

Abstract *– The article considers the methods for dynamic Quality of Service application in IP based networks. Three methods are proposed:*

The first one is through the Service fulfillment and assurance platform.

Then is proposed a protocol specially created for the purpose – COPS.

Afterwards is considered the newly born Diameter Protocol.

In the last section are presented the main advantages and disadvantages of the different methods.

Keywords *– IP networks, QoS, Dynamic QoS policy enforcement, Service Creation and Assuarance, COPS, Diameter.*

1. Introduction

Two of the fundamental NGN principles are the following: different services shall be able to work on any access network technology and using any access technology the network provider shall be able to provide many different services without quality degradation for the end users. The fulfillment of these two has moved the networks from one level to another – starting with circuit switching and vertical architectures and migrating to converged networks, Web 2.0 technologies over 40GIG DWDM core nowadays.

These principles sound “sweet” but were relatively difficult to be achieved. In fact when the access technology offers enough bandwidth it is not a problem to deliver many services on the same media. But when there is not enough bandwidth that might be a nightmare. The problem is that each service requires different traffic profile and requirements. For example voice services have different requirements than video and completely different from email and HTTP. The technology that allows network operators to apply the principles throughout their networks is Quality of Service – QoS. Through the years were developed two approaches for applying QoS – Integrated and Differentiated Services.

Integrated services (IntServ) work on per flow/service level and are based on RSVP signaling protocol. Basically the source sends RSVP path message and requests from each network node up to the receiver to reserve certain capacity. The nodes reply with an RSVP RESV message that contains a confirmation of the reserved bandwidth. Due to the huge signaling overhead the Intserv approach is not widely used today. The only place where it is still popular is MPLS traffic engineering clouds. Therefore the extension of RSVR - RSVP TE is used for reserving huge capacities in providers' core networks [11].

The second approach - Differentiated services (DiffServ) are much widely used. DiffServ is based on bits marking in the IP packet/Ethernet Frame headers. The traffic shall be marked as close to the source as possible, then it could be policed, shaped and queued throughout the networks till the recipient of the packet. Differentiated services are usually statically configured on the network nodes, have no signaling overhead and could be met in all kinds of networks: ISP, Telecoms, Mobile, Cable and even Enterprise still use them today [11].

Nowadays with the deeper market penetration of the mobile data services a new problem arises. How to apply the QoS not just per customer level but also per service level? With other words how to change the customer QoS policies dynamically depending on the services, billing and current traffic situation?

There are several approaches for implementing Dynamic QoS in Service provider networks. The first one is solely based on OSS architecture and service fulfillment platform. The second approach is standardized by IETF and is based on Common Open Policy Service (Cops) protocol. The newest and most promising one is based on Diameter protocol. It is also developed by IETF (still not standardized) but already gained popularity through it's widely adaptation in IMS architecture by 3rd Generation Partnership Project (3GPP).

2. Architecture

2.1. Dynamic QoS through automated service fulfillment

Dynamic Policy enforcement could be accomplished using provider's service fulfillment platform. Service fulfillment is defined in the FAB (fulfillment, assurance and billing) model as part of TM forum ETOM architecture.

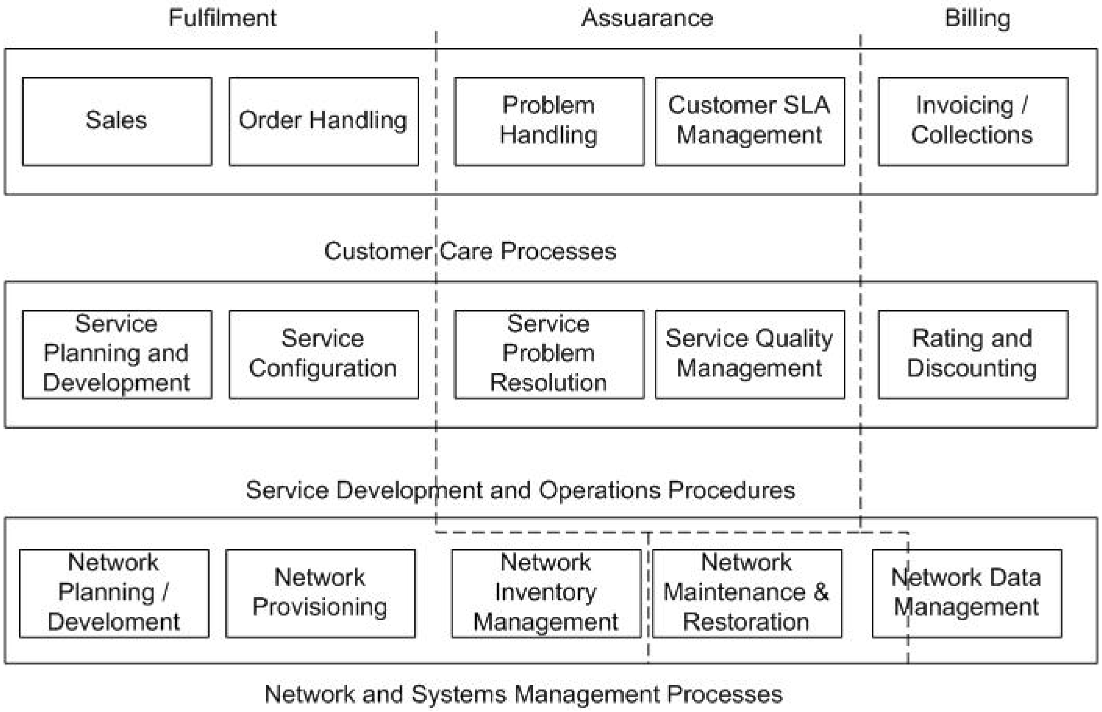
Fulfilment
Assuarance
Billing
Sales
Order Handling
Problem Handling
Customer SLA Management
Invoicing / Collections
Customer Care Processes
Service Planning and Development
Service Configuration
Service Problem Resolution
Service Quality Management
Rating and Discounting
Service Development and Operations Procedures
Network Planning / Develoment
Network Provisioning
Network Inventory Management
Network Maintenance & Restoration
Network Data Management
Network and Systems Management Processes

Figure 1 FAB model

As per that model the fulfillment is part of the OSS of the operator and consists of several API's, Inventory (the module that contains a logical model of the Service Provider Network), Order to Service (the layer that executes the business logic of the operator) and Service Activation (the layer that activates the customer services, apply QoS policies and talks to the network) [12] [13].

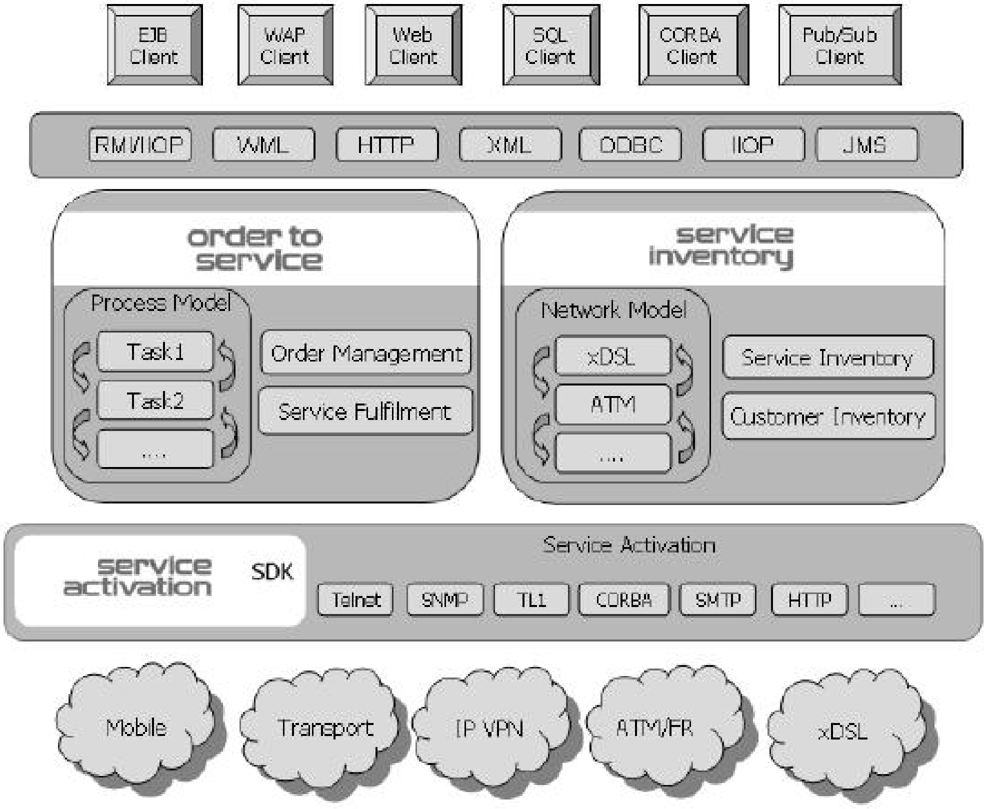

Figure 2 Service fulfillment Architecture

The end result of the Service fulfillment architecture considering dynamics is presented on Figure 3. QoS change request enters the SP OSS through the CRM then it is passed to the Order to Service workflow, QoS policy changes are determined, after that service activation applies the change to the requested resources and the needed info is provided to the billing system.

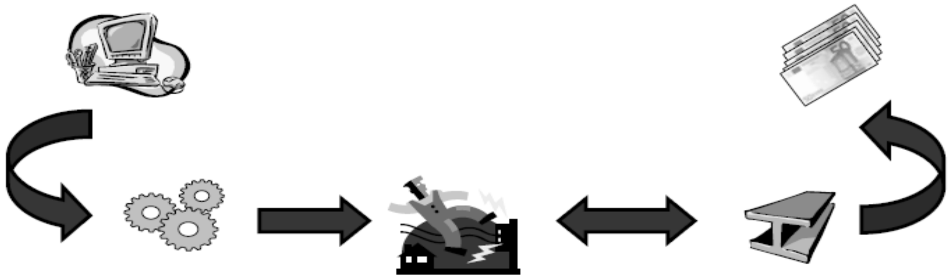

Figure 3 Automated QoS policy change

This type of a solution allows network operators to apply automated changes to the QoS profiles and settings of their customer. The solution is flexible enough but won't be suitable for situations in that the QoS has to be really dynamic and the QoS profile changes every second. It is suitable for Service providers offering MPLS L2/L3 vpn services, DSL and FTTX operators but won't be proper for an HSDPA mobile operator.

2.2. COPS

Deployment of value added IP services was a big challenge for the network and cable operators 10 years ago. Dynamic resource provisioning was impossible for them at that time. Therefore a protocol able to support QoS service automation and dynamic policy enforcement was created. COPS has a simple but extensible by design [1]. The main characteristics of the COPS protocol include:

- The protocol employs a client/server model where the router (Policy Enforcement Point – PEP) sends requests, updates, and deletes to the remote policy server (Policy Decision Point – PDP) and the PDP returns decisions back to the PEP.
- The protocol uses TCP as its transport protocol for reliable exchange of messages between policy clients and a server. Therefore, no additional mechanisms are necessary for reliable communication between a server and its clients.
- The protocol is extensible in that it is designed to leverage of self-identifying objects and can support diverse client specific information without requiring modifications to the COPS protocol itself. The protocol was created for the general administration, configuration, and enforcement of policies.
- Additionally, the protocol is statefull. It allows the client to pull a policy from the server and the server to push configuration information to the client, and then allows the client/server to remove such state from the other side when it is no longer applicable.

COPS supports two main modes – outsourcing and provisioning. The outsourcing mode is also known as COPS-RSVP. Under it external events such as an admission control request or a QoS traffic flow request has to be handled with a policy decision. The PEP delegates that decision to the PDP with an explicit request message. In the provisioning mode that is also known as COPS-PP, the network elements are preconfigured prior to processing events, based on policies sent by the PDP [11].

Nowadays the routers that are COPS enabled may have COPS-PR clients or COPS-RSVP clients and supports the following capabilities:

- A PEP capability for the IP TE client-type. The support of the RSVP client type is notified by the PEP to the PDP, and is unique for the area covered by the IP routing/ traffic engineering policy, so that the PEP can treat all the COPS client-types it supports as non-overlapping and independent namespaces.

- A local policy decision point (LPDP), which can be assimilated to the routing processes that have been activated on the router. The LPDP will therefore contribute to the computation and the selection of the IP routes.
- Several instances of routing information bases (RIBs), according to the different (unicast and multicast) routing processes that have been activated–one can easily assume the activation of at least one interior gateway protocol ((IGP), like OSPF, ISIS) and BGP-4.
- Conceptually, one forwarding information base (FIB), which will store the routes that have been selected by the routing processes, but within that section we do not make any assumption about the number of FIBs that can be supported by a router [e.g. within the context of an IP virtual private network(VPN) service offering].

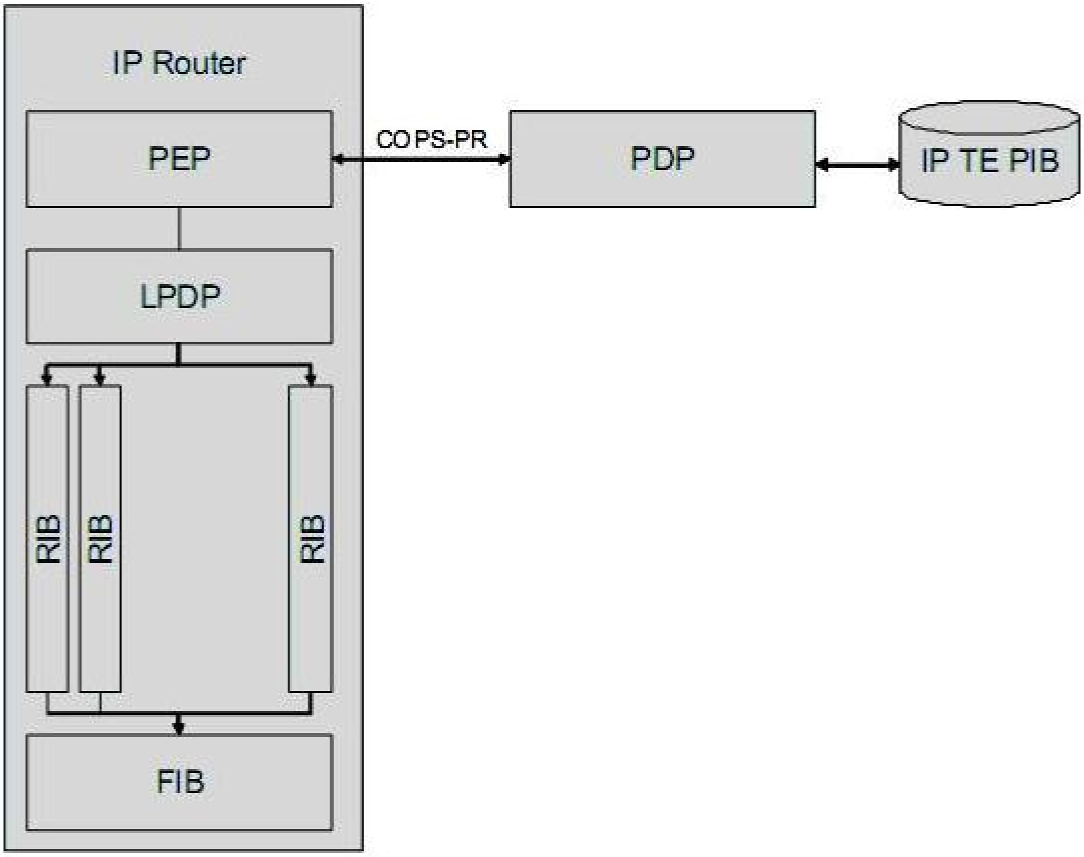

Figure 4 COPS model for IP routing/Traffic engineering policy enforcement

As previously mentioned COPS has been developed 10 years ago. At that time the IntServ model was still popular and therefore COPS was oriented for dynamic provisioning and monitoring/accounting of RSVP tunnels. For one reason or another IntServ proved as not scalable enough and now COPS is used only for dynamic provisioning of MPLS-TE tunnels with RSVP-TE. The protocol is still widely supported and is quite popular among the network equipment vendors as Juniper and Cisco and among the Tier 1 connectivity providers. Despite that COPS-PR was developed and is suitable for DiffServ networks the standard gained limited popularity among the operators and vendors. There are many reasons for that but the main one is the fact that COPS clients does not provide AAA capabilities. Internet Society used Radius for the purpose and Radius is much more common then COPS.

2.3. DIAMETER

As the IP protocol became the reference technology to build new networks, the need for a reliable protocol that can handle network client capabilities as AAA, Mobile IP, QoS, security and online charging was crucial Simple requirement for providing access on a remote access server in a secured manner, a connection to the Internet or to the company's VPN have strongly shifted to support a more sensitive and demanding exploitation of networks. Initially IETF decided to extend RADIUS standard to be able to handle the new demands. The limited field size and the restricted numbering space proved that such task was quite difficult although it might be possible through private extensions [3]. As a final result IETF created three working groups to specify the requirements that the new protocol shall handle.

- NASREQ: specific requirements related to the network access server, in order to provide at least the same level of service as provided by RADIUS;
- ROAMOPS: specific requirements related to roaming operations, as the new AAA protocol is supposed to service roaming users;
- MOBILEIP: specific requirements related to the mobile IP technology, in order to provide appropriate messages and features that could be usable for users connected to mobile IP.

As a final result IETF published [2] and DIAMETER was born. Then the protocol has been adopted by 3GPP in the newly created IP Multimedia Subsystem (IMS) architecture. Next, ETSI/TISPAN decided to adopt the IMS architecture design for fixed networks built upon IP, meaning that Diameter is now a central piece of technology to be used in the core of new voice architectures, for both mobile and fixed networks, thus leading to a real Next-Generation Network (NGN).

The Diameter base protocol [2] has been conceived as a peer-to-peer protocol that provides support for reliable exchange of information between Diameter nodes, whereas RADIUS was built as a transactional protocol following a client–server model. The Diameter base protocol provides the minimum set of functionalities required for any AAA protocol, including support for accounting, while specific service information is handled at the application level. Diameter is based upon TCP or SCTP running over IPv4 or IPv6 (whereas RADIUS runs over UDP), using destination port 3868, thus ensuring a reliable delivery of the message at the transport layer, even though acceptance of specific messages requires an explicit applicative acknowledgment, especially for accounting messages. A Diameter client is not required to support both transport protocols, but intermediate nodes or servers are mandated to allow a connection with both protocols.

Using a reliable transport protocol also eases failover mechanisms, as a network failure can be detected without having to wait for an applicative acknowledgment. Explicit applicative acknowledgment is needed, however, since a network reliable delivery does not mean that the Diameter process was able to treat the message. This is particularly crucial for accounting messages that are directly linked to the billing system, and can lead to a loss of revenue.

The use of TLS or IPSec is also required, in order to ensure security between nodes. Even though TLS or IPSec is sufficient for hop-by-hop security, it is not a satisfactory method for protecting the payload all over the AAA signaling path: a proxy-broker, connected to the Diameter client of network A and to the Diameter server of provider B, will be able to read sensible payload and correlate identity with resource usage. The Diameter specification encourages the usage of an end-to-end security mechanism.

The Diameter protocol model describes three different categories of nodes:

- Diameter client. Designates the Diameter node in charge of providing access to a resource for which Diameter messages have to be generated. The access device is likely to be a Diameter client, but it can also be a service platform commanding a policy enforcer that can control the transport plan.
- Diameter agent. Designates a large category of nodes implied in routing and treating Diameter messages.
- Diameter server. Designates the terminal node in charge of final AAA operations.

One of the most important features of the initial Diameter standard is the ability to support different applications. Diameter application can be described as a set of messages, attributes and message treatment rules that are defined to fulfill the requirements for a specific usage. So far, five different applications have been defined to extend Diameter: mobile IP (RFC 4004 [4]), NASREQ (RFC 4005 [5]), credit control (RFC 4006 [6]), EAP (RFC 4072 [7]) and SIP (RFC 4740 [8]).

Diameter QoS application is still not defined as an RFC and currently is in its 13th draft version [10]. Despite that it was already adopted by 3GPP in the IMS architecture. It enables the Network Element to interact with Diameter Server when allocating network resources in the network.

The Diameter QoS application runs between a NE (acting as a Diameter client) and the resource AE (acting as a Diameter server). A high-level picture of the resulting architecture is shown in Figure 5.

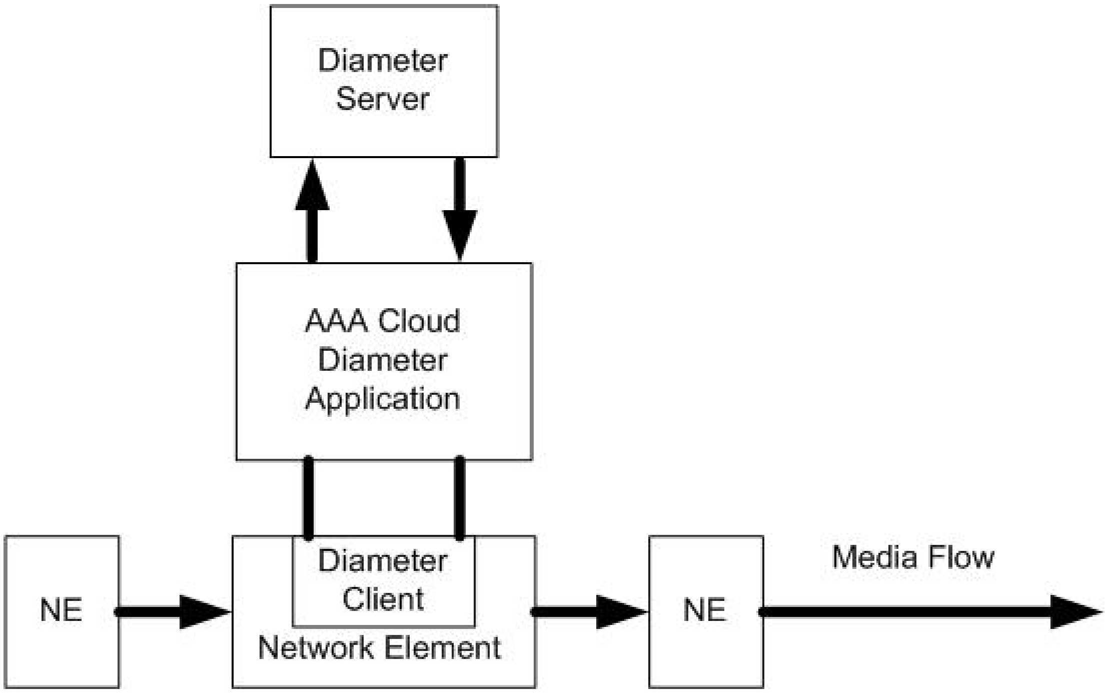

Figure 5 An Architecture Supporting QoS-AAA

It specifies three different sets of endpoints capabilities:

- Category 1 Application Endpoint has no QoS capability at either the application or the network level. This type of AppE may set up a connection through application signaling, but it is unable to specify resource/QoS requirements through either application or network-level signaling.
- Category 2 Application Endpoint only has QoS capability at the application level. This type of AppE is able to set up a connection through application signaling with certain resource/QoS requirements (e.g., application attributes), but it is unable to signal any resource/QoS requirements at the network level.
- Category 3 Application Endpoint has QoS capability at the network level. This type of AppE may set up a connection through application signaling, translate service characteristics into network resource/QoS requirements (e.g., network QoS class) locally, and request the resources through network signaling, e.g., Resource ReSerVation Protocol (RSVP) [RFC2205] or NSIS [I-D.ietf-nsis-qos-nslp].

Currently are defined two modes of operation - Pull and Push. In "Pull" mode, the network element requests QoS authorization from the Diameter server based on some kind of trigger (such as a QoS signaling protocol) that arrives along the data path. In "Push" mode, the Diameter server pro-actively sends a command to the network element(s) to install QoS authorization state. The trigger could be off-path signaling such as Session Initiation Protocol (SIP) [RFC3261] call control.

Push mode is applicable to certain networks, for example, Cable network, DSL, Ethernet, and Diffserv-enabled IP/MPLS. The Pull mode is more appropriate to IntServ enabled IP networks or certain wireless networks such as the GPRS networks defined by 3GPP. Some networks (for example, WiMAX) may require both Push and Pull modes.

For Category 1 and 2 Application Endpoints, Push mode is REQUIRED. For a Category 3, either Push mode or Pull mode MAY be used.

Despite of the rich feature set and the good design and specification Diameter is relatively new protocol that does not have a wide network presence. Most of the routers do not support it at all and only a limited number of specific network devices have diameter clients. The server side is also definitively not so popular among the clients and vendors compared to Radius. Only a few HSS developments exist mostly provided by the large Telecom equipment vendors like Ericsson, Nokia and Siemens.

3. Conclusion

The rapid deployment of broadband services for end users and corporate clients requires precise policy and resource control. The static QoS policy enforcement works quite well in most of the situations but in certain cases is not the best approach. Dynamic QoS is the better solution in every case when the frequent policy changes have to be done. That allows operators to keep their customers happy with less resource and preserves the overall revenue of those companies. Dynamic QoS policies could be combined with the operator OSS solution or could be applied by a separate QoS server or even integrated with the online charging application of the mobile operators. Currently for each of these cases there is a separate solution.

Definitely the Dynamic QoS application could be deployed through a platform for service assurance and fulfillment. This will be a common approach for the cases in that certain customer is willing to pay for a certain higher resource reservation only during a certain period.

It looks like that COPS - will stay as the common solution for dynamic MPLS traffic engineering resource reservation. Regarding the COPS-PR functionality it most likely will be mitigated by the Diameter protocol.

Regarding the Diameter itself it looks like as the most promising and feature rich approach for dynamic QoS provisioning. Sooner or later the industry will need diameter clients that support AAA, Dynamic QoS, Online Charging and mobile IP.

4. References

[1] IETF RFC 2748: "The COPS (Common Open Policy Service) Protocol".

[2] IETF RFC 3588: "Diameter Base Protocol".

[3] IETF RFC 3127: "Authentication, Authorization, and Accounting: Protocol Evaluation".

[4] IETF RFC 4004: "Diameter Mobile IPv4 Application"

[5] IETF RFC 4005: "Diameter Network Access Server Application"

[6] IETF RFC 4006: "Diameter Credit Control Application"

[7] IETF RFC 4072: "Diameter Extensible Authentication Protocol (EAP) Application".

[8] IETF RFC 4740: "Diameter Session Initiation Protocol (SIP) Application".

[9] 3GPP TS 29.209: "Policy Control over Gq Interface".

[10] IETF Internet Draft v.13: "Diameter Quality of Service Application".

[11] Jacquenet Chr., Bourdon G., Boucadair M., "Automation and Dynamic Provisioning Techniques in IP/MPLS Environments", Wiley, 2008.

[12] TMFORUM, GB921 Business Process Framework Release 8.0, 2009

[13] Clemm, Al., Network Management Fundamentals, Cisco Press, 2006