



MSF Whitepaper on Quality of Service (QoS) over the Network-to-Network Interface (NNI)

MSF-TR-SERVICES-006.FINAL

Editor(s): Wayne Cutler (Ericsson)
Contributor(s): Rajesh Bhalla, Arye Epharth, David Hutton, Bhumip
Khasnabish, Larry Ma , George Yum, Shedman Tam, Chris
Gallon
Author: Wayne Cutler
Document Source: MSF Services & Architectures Working Group
Version Number: Msf2010.079.02
Day and Date: June 14, 2010

Abstract and Executive Summary

Network-to-Network Interface (NNI) defines how two networks interconnect and exchange information. QoS over NNI interconnect is important for optimal network utilizations and for delivering high quality services economically. Traditionally, carriers have addressed the issue of QoS by over-provisioning of their networks. That could possibly be managed for networks carrying VoIP traffic only. However, with the increasing volume of TDM traffic being migrated to IP based networks, and with the increasing uptake of IP based multimedia services; it will not be possible to dimension networks to meet all peak bursty traffic requirements effectively. Hence, QoS over NNI is an important topic of study in major Standards Development Organizations (SDOs) and an issue that must be addressed prior to widescale NGN deployment.

Issues related to QoS over NNI are being debated actively in various industry SDOs/fora. This paper provides an overview of the current ongoing work in the industry regarding QoS over the NNI and discusses the similarities and differences between the different organisations.

The paper concludes that there does seem to be a desire in the industry to avoid divergence between the different SDOs and that there is a trend for the GSMA to be the lead SDO in this definition via its IPX work.

Finally, given the MSF's role as a facilitator of IOT events to prove inter-operability of adopted/profiled standards, some potential IOT activities are also discussed which could help prove the realization of a converged NNI QoS solution in a multi-vendor environment.

Table of Contents

Introduction4

Problem Statement4

A Survey of Current Industry Solutions5

QoS Over NNI Analysis15

IOT Opportunities18

Summary and Conclusions19

References19

Abbreviations20

Introduction

Network-to-Network Interface (NNI) defines how two networks interconnect and exchange information. While the interconnected network domains are external to each other and typically operated by different carriers, such interconnected networks consist of separate internal domains as well. *Quality of Service* (QoS) for such NNI connected IP networks relates to the upper limit on end-to-end (E2E) packet delay, upper limit on packet loss and packet transfer delay variation (jitter), and attributes such as bandwidth profiles, traffic classification and availability requirements defined in Service Level Agreements (SLAs). QoS over NNI relates to the capability of differentiating classes of services (CoS) and the ability to assign corresponding QoS guarantees in terms of bandwidth allocations and traffic characteristics across interconnected carrier domains.

This paper discusses mechanisms for guaranteeing QoS over Network-to-Network Interfaces (NNI) based on ongoing work in various other fora. Other NNI issues, such as security, charging, accounting, and transcoding etc. are out of scope of this paper.

Problem Statement

Early generation of IP networks often achieved QoS guarantees by relying on over provisioning bandwidth thus resulting in low network capacity utilizations. Over provisioning could possibly be managed for networks carrying typical VoIP traffic only. However, with the increasing volume of TDM traffic being migrated to IP based networks and with the increasing uptake of IP based multimedia services; it will not be possible to dimension networks to meet all peak bursty traffic requirements effectively. Better leveraging of network resources for enhanced user experience is quite enticing to carriers even with adequate bandwidth resources. With more and more networks moving towards all IP architecture and IP multimedia services, service providers are looking for solutions for optimal network utilizations and cost reductions for network interconnections. Quality of Services for IP-based services, therefore, plays a vital role for Network-to-Network Interconnections.

Network-to-Network Interconnections have been recognized by the industry as an important topic of study. There are ongoing discussions related to NNI in standards organizations (SDOs) and fora such as 3GPP, ATIS, ETSI TISPAN, GSMA, i3Forum etc., mostly from the system architecture perspective. Until fairly recently, there have, however, been very few discussions on QoS mechanisms and services over NNI. There is not yet an agreed upon definition on

the roles of carriers for guaranteeing QoS over NNI due to the required technical details of how to realize QoS over NNI still being under discussion.

A Survey of Current Industry Solutions

Major SDOs/fora have defined NNI interface and related network elements. Some SDOs/fora have defined QoS functions as well. The following is a high level synopsis of the major SDO's/fora's current efforts regarding QoS over NNI:

GSMA:

Built upon the world-wide success of GRX (GPRS Roaming eXchange), GSMA has defined an architectural framework for IP Packet eXchange (IPX) as documented in "Inter-Service Provider IP Backbone Guidelines" (see [1]). IPX allows all types of Service Providers – Mobile Network Operators (MNOs), Fixed Network Operators (FNOs), Internet Service Providers (ISPs) and Application Service Providers (ASPs) – to obtain connections to Inter-Service Provider IP Backbone (IPX) using a local tail. The local tail may be implemented via Layer 1 physical connections, logical connections at Layer 2 or Layer 3 IP VPN connections over the public IP network; though Layer 3 connectivity is not the recommended option. Service Providers may connect to more than one IPX Provider. IPX is formed from separate and competing IPX Providers. Figure 1. depicts a high level IPX Architecture model.

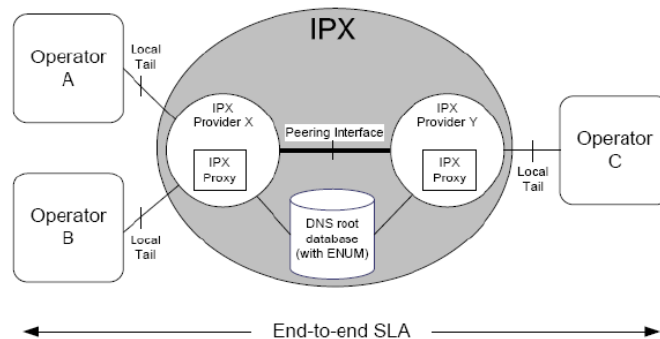


Figure 1. IPX Architecture Model

IPX Interconnect supports three types of connectivity options:

- Transport-Only Connectivity - , a bilateral agreement between Service providers using the IPX transport layer with guaranteed QOS end-end.
- Bilateral Service Transit Connectivity - , a bilateral agreement between Service providers using the IPX Proxy Functions and IPX transport layer with guaranteed QOS end-end. This model provides the opportunity to include service based interconnect charging to the transport charging of the previous model.

- Multilateral Service Hub Connectivity – this model provides multi-lateral interconnect with guaranteed end-end QOS and service based charging. Traffic may be routed from one Service Provider to many destinations via a single agreement with the IPX provider. The hub functionality is provided by IPX Proxies.

Note that the cited IPX end-to-end (E2E) Quality of Service encompasses the leg between the originating Service Provider Border Gateway the terminating Service Provider Border Gateway. IPX Proxy functions in the later two types of connectivity options facilitate IPX Providers to ensure E2E QoS for all traffic classes as per Service Level Agreements. Note that whilst [1] only cites SIP as a control protocol between IPX Service providers, the architecture does not preclude other protocols (e.g. SIP_I) being used – see [14] and [15].

In IPX, E2E QoS is built on Class of Services (CoS) and QoS Profiles defined in the SLAs. SLAs define service specifications between a Service Provider and an IPX Provider, and also between two IPX Providers. Service availability, jitter, packet loss and delay are the metrics included in the QoS Profiles and related target requirements to be met for each metric are documented in /1/. Such QoS metrics need to be supported over an individual connection between a Service Provider and an IPX Provider. This SLA extends to the whole IPX network as well, comprising of multiple IPX Providers. The Border Gateways at the Source and Destination Service Providers are the demarcation points for the measurement/enforcement of the agreed upon QoS Profiles. The IPX Proxy is also responsible for applying admission control checks to the IPX on a per SP basis, including being able to apply the SP’s black/white lists.

In order to ensure E2E QoS; GSMA IR.34 recommends Traffic Classification and DiffServ markings of Service Provider traffic as shown in Table 1. The 6-bit DSCP marking indicates the Per Hop Behavior (PHB) that belongs to each traffic class as recommended in IETF RFC3246 and RFC2597.¹

QoS Information		DiffServ PHB	DSCP Marking	Typical Applications
Traffic Class	THP			

¹ IETF is working on providing DiffServ code point for another class conforming to Expedited Forwarding PHB but subject to capacity admission dynamically. Such class of services might be applicable for emergency and priority services, or for other users with preferential service contracts, or individual users gaining access with special credentials. The recommendation is for another code point ‘101100’, paralleling EF code point of ‘101110’. This new code point may be referred to as ‘EF-ADMIT’. This will allow service providers to distinguish between special-policy traffic and other classes; such as existing VoIP services that may perform no or only very coarse capacity admission and can exceed their allocated resources.

Conversational	N/A	EF	101110	VoIP, Video Share
Streaming	N/A	AF41	100010	Push to Talk, Video Streaming
	1	AF31	011010	Online Gaming, Signaling Traffic
Interactive	2	AF21	010010	WEB browsing
	3	AF11	001010	Instant Messaging
Background	N/A	BE	000000	Email, MMS

Table 1 Traffic Classification and DSCP Markings

- Conversational traffic class imposes strict requirements on delay and jitter values. For streaming traffic class, the requirements are not as tight as the user equipment normally buffers data before play out. Interactive class of traffic requires bandwidth reservation to meet service requirements. For background traffic class, the packet size is usually large, though not delay and jitter sensitive. Packet drop has to be minimized to avoid retransmissions and extra load on the network.

Service Providers mark the packets according to traffic classification rules before forwarding the traffic to IPX Provider. Queuing, packet treatment algorithms and other techniques that might be used with the DiffServ are decisions for the IPX Providers. It may be noted that such traffic classification is on the basis of an aggregate of user traffic flows that belong to the same class. Traffic belonging to different classes is DSCP marked and sent to the IPX Provider, possibly encapsulated in GRE tunnels. The IPX Provider may remark DSCP values for routing within their own domains, as long as they return the original DSCP markings at the egress point of their respective domains.

Though the GSMA IPX model defines E2E QoS criterion, requirements for traffic classification and DiffServ support – how to build an E2E QoS solution based on such framework - is a topic of ongoing study. 3GPP has taken up the study of requirements for IPX connectivity that are being addressed in 3GPP TR 22.893.

There has also been a good deal of IPX testing/trialing activity under the GSMA banner – see [16] and http://gsmworld.com/our-work/programmes-and-initiatives/ip-networking/ipx_pci_trials.htm.

i3Forum:

The i3Forum is a consortium of Tier 1 operators who are interested in the inter-connection between different carrier networks to enable international voice services. The i3Forum have defined a general reference architecture (see [2]) as shown in figure 2.

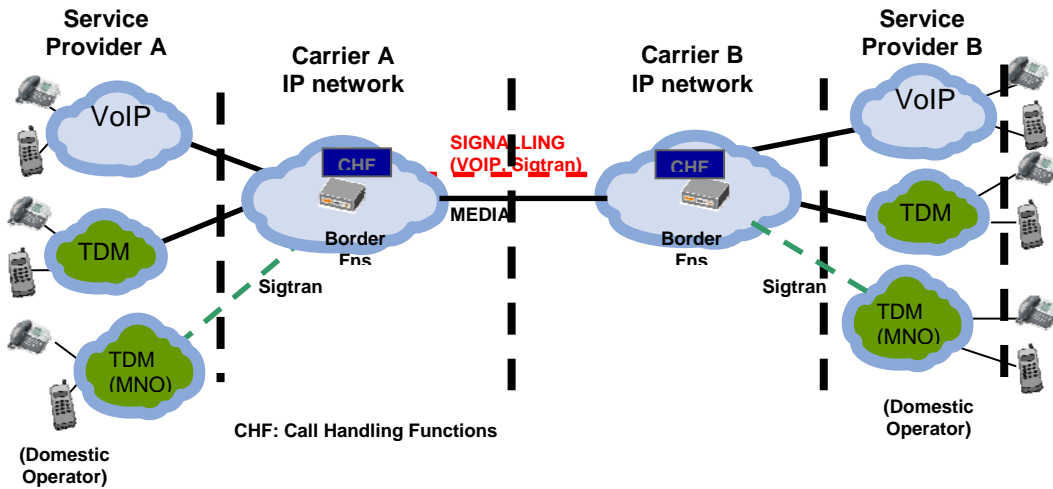


Figure 2. i3Forum Reference Architecture

The i3F focuses on the inter-carrier NNI (between Carrier A and Carrier B in figure 2). The i3F have defined 3 options for carrier inter-connect, namely Layer 1 inter-connection, Layer 2 inter-connection or Layer 3 inter-connection. The Layer 3 option assumes a 3rd party IP network provider between the 2 carrier networks and is compatible with the GSMA IPX architecture (see figure 2).

Like GSMA, the i3Forum recommends the use of DSCP marking to distinguish between traffic classes, with the specific packet marking for a given class being pre-agreed between the two carriers. Table 2 provides the recommended DSCP marking for the different traffic classes.

Traffic Type	DSCP Marking	Diffserv PHB	IP Precedence	802.1Q VLAN
Voice Media	101110	EF	5	5
Voice Signalling	011010	AF31	3	3
	101110	EF	5	5
SIGTRAN for Mobile Signalling	011010	AF31	3	3
	101110	EF	5	5
Other Traffic	000000	BE	0	0

Table 2 i3Forum DSCP Classifications

Note that [2] explicitly cites support of, and profiles both SIP and SIP-I between Carrier Networks. The SIP is based on RFC 3261 ([13]) whilst the SIP-I is based on [8] – i.e. “Profile C”. In addition, the i3Forum (due to its pressing need to realize IP based voice services over the NNI) has also done a good deal of

additional detailed work covering such aspects as ISDN supplementary service support, ISDN bearer services, SIGTRAN support, Fax/Modem handling, Codec support, Transcoding and handling of the P-Early-Media header – i.e. functionality required to support all legacy services over the IP based NNI.

The i3Forum also defines a set of QOS parameters to be used as the basis for KPIs at an inter-connection point. The QOS parameters include transport layer, service layer and call attributes, as follows :-

- Transport layer
 - Round trip delay
 - Jitter
 - Packet loss
- Service layer
 - MOSCQE / R-factor
 - ALOC (Average Length of Call)
 - ASR (Answer to Seize Ratio)
 - NER (Network Efficiency Ratio)
 - PGRD (Post Gateway Ringing Delay)
- Call Attributes
 - CLI Transparency
 - One-way speech

The i3Forum recommends that each end of the inter-connect point perform its own measurements of the required parameters and requires RTCP to be transited end-end (else the MOSCQE values apply to a limited or partial scope of the end-end path).

ETSI TISPAN:

The TISPAN NGN Functional Architecture ([3]) defines a number of functions and interface reference points to support NGN inter-connection. TISPAN defines a service related and bearer related interface at the NNI (namely Ic and Iz reference points) as shown in figure 3. Note that the Iw reference point is optional and applicable where there is a need to map/inter-work at the service control layer (e.g. SIP-H323 mapping).

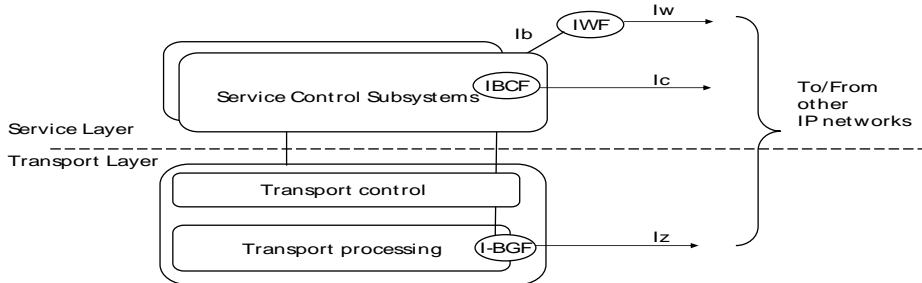


Figure 3. TISPAN IP Interconnection

TISPAN also permits the absence of Ic at the NNI (i.e. only bearer related Iz at the NNI). This is termed CoIx (Connection Oriented Interconnect) as opposed to SoIx (Service Oriented Interconnect) where both Ic/Iz are present. TISPAN defines a H.248 profile to enable the IBCF to control the I-BGF (see [12]).

TISPAN permits two modes of Interconnection between NGNs (either in CoIx or SoIx modes), namely direct or indirect. Direct interconnection refers to the interconnection between two network domains without any intermediate network domain. Indirect interconnection refers to the interconnection between two network domains with one or more intermediate network domain(s) acting as transit networks. The intermediate network domain(s) provide(s) transit functionality to the other network domain. Figure 4 illustrates indirect interconnection for SoIx.

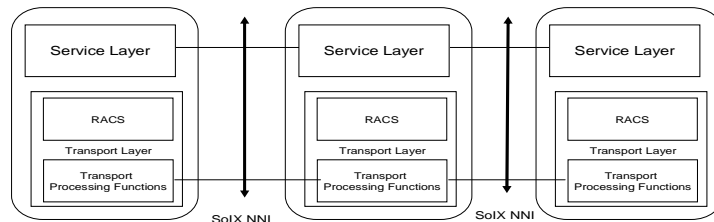


Figure 4. TISPAN Indirect SoIx Interconnection

Note that TISPAN permits both SIP and SIP-I inter-connect. The SIP-I is specified in [11], which is an endorsement of [8].

In summary, TISPAN covers the three GSMA IPX types of interconnections viz. Transport-Only Connectivity, Bilateral Service Transit Connectivity, Multilateral

Service Hub Connectivity. NNI QoS is achieved by each peer performing its own bandwidth checks (e.g. at a BGF) independently based on the signalling exchanged across the NNI.

Finally, it is noted that the term “TISPAN IPX” is not used in [3], but does appear in [6] where it is defined as an “inter-operator IP backbone network that is compliant with TISPAN standards and is transparent to subscribers”.

3GPP:

3GPP SA1 has published a study into the technical requirements for inter-operator IP Interconnections to support IMS Multimedia services and for legacy voice and video PSTN/PLMN services transported over IP infrastructure (e.g., VoIP) (TR 22.893, [4]).

3GPP TR 22.893 has identified three interconnect scenarios: Inter-Operator Direct Connection, Inter-Operator Indirect Connection and Operator to 3rd Party Connection. *Inter-Operator Indirect Connection* envisages IP connection between Service Providers via. IP-Interconnection Intermediate Carrier such as IPX. Operator to 3rd Party Connection is a special case of indirect-connection scenario and supports Service Provider interconnection to Application Provider(s) using interconnects such as IPX.

3GPP TR 22.893 IPX model expands the focus from just transport and connectivity approach of GRX to service-aware interconnection by the use of proxy functions in interconnected networks. Interconnection points are uniquely identified by means of SLAs. The interconnections support E2E QoS by differentiating and marking classes of traffic. Signaling and media traffic is treated according to their markings in order to guarantee adequate E2E QoS. This is very much in line with the approach being taken by GSMA IPX Guidelines in IR.34.

Note that in terms of the session control protocol, 3GPP IMS permits the use of only SIP, but SIP-I is supported in the pre-IMS CS (Circuit Switched) specifications (see [9] and [10]).

There is also an active Work Item in 3GPP SA1 to update the TR as part of 3GPP Release 10. In general, the contents of the TR do closely align with GSMA IR.34 – although there is also some deviation and a good deal of overlap/repetition. It is envisaged that the work in 3GPP will result in better compatibility and reduced overlap/repetition as the SDOs converge to a common solution.

In addition, 3GPP CT4 have published a SIP Profile in Release 9 for the inter-IMS NNI (see [5]). The profile covers the Ici and Izi (session and bearer)

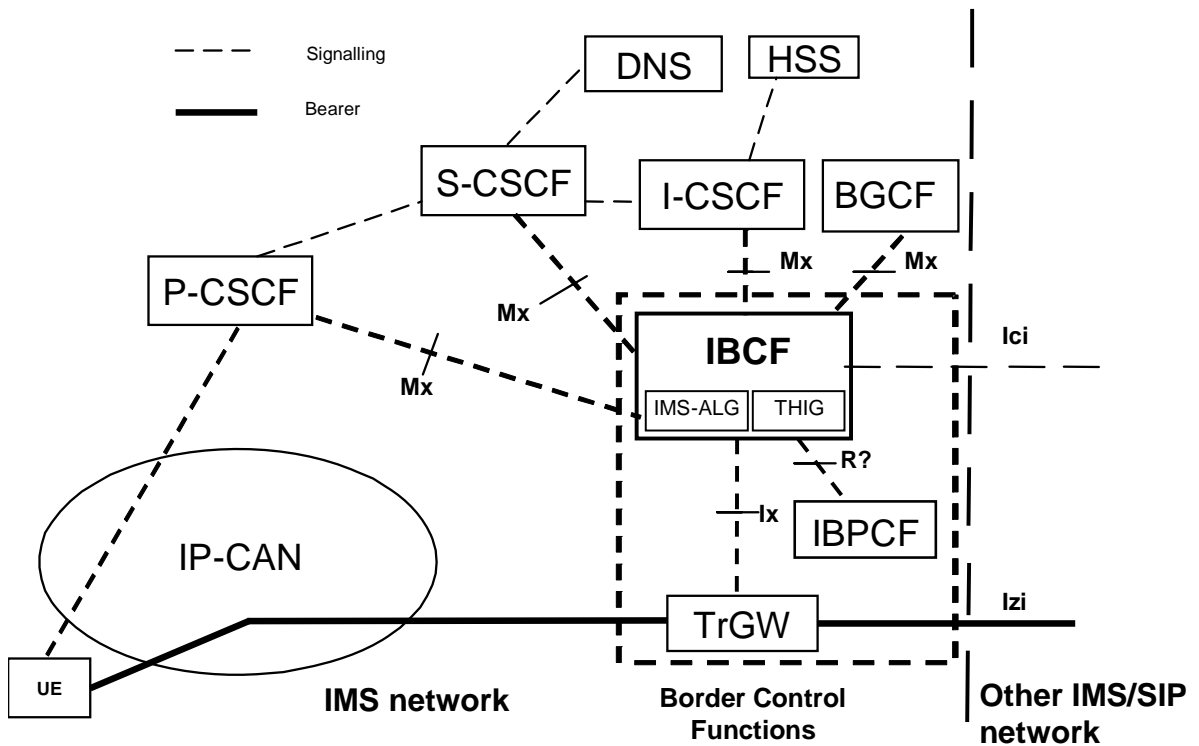


Figure 7. Separate IBPCF and new interface to IBCF

ATIS:

The Next-Gen Carrier Interconnection (NG-CI) working group in ATIS has defined a number of use cases and the QoS requirements over NNI for interconnection scenarios, including mechanisms for QoS for VoIP, Video Conferencing, Data, and IPTV. Although ATIS has proposed a few application scenarios based on the concept of an IP Proxy network which acts as 3rd party network to provide interconnection for two service providers serving as the originating and terminating parties, it has not yet defined the architecture for achieving such objectives. The IPX architecture defined by GSMA is under serious consideration though.

IETF:

IETF has defined solutions for guaranteeing QoS over NNI for MPLS networks by combining DiffServ and RSVP-TE. DiffServ distinguishes CoS per packet, allocates priority and ensures precedence in forwarding packets for higher priority services. However, DiffServ cannot schedule bandwidth for different class of

services. In the event of traffic exceeding the available bandwidth, DiffServ can guarantee precedence for higher priority services at the expense of lower priority services. In the extreme circumstances, even high priority services are not immune to latency and packet loss. Therefore DiffServ technology alone, as defined for IPX networks, does not guarantee E2E QoS and Service Level Agreements.

IETF defined RSVP-TE protocol addresses this problem by ensuring routing paths against congestion and thus guaranteeing bandwidth resources for defined service classes. RSVP-TE does not have service identification capability and because of this QoS sensitive services will be affected once the traffic in the MPLS tunnel exceeds reserved traffic rate. Therefore, RSVP-TE alone cannot solve the E2E QoS guarantee problem either.

Combining DiffServ and RSVP-TE technologies enables MPLS IP core networks to distinguish CoS, ensures resource reservation based on CoS and forwarding precedence for higher priority services. Therefore, by combining DiffServ and RSVP-TE technologies can guarantee E2E QoS and Service Level Agreements across NNI for MPLS based core networks.

MEF:

Metro Ethernet Forum has been defining procedures for managed Ethernet services for multi-site deployments via external networks operated by different service providers. The E-NNI interface is the demarcation point across which MEF has defined procedures for inter-carrier handoff of Ethernet services by including considerations for Quality of Service (QoS), OAM, SLAs etc. As an example, looking at QoS tagging – at the E-NNI reference point where two service provider networks meet, the E-NNI measures an Ethernet service stream via two sets of QoS parameters: bandwidth profiles of either Committed or Excess Information Rate (CIR or EIR) and performance measured by delay, loss and availability. The E-NNI preserves this priority information across the boundary of the networks by encapsulating each Ethernet frame with an appropriate VLAN header. In this way, if a stream of packets contains both; high-priority traffic such as VoIP and low-priority traffic such as web-browsing, the preservation of QoS tagging across the E-NNI ensures that critical VoIP calls get through. Such MEF approach to E-NNI is essentially a Layer-2 QoS solution, different from the DiffServ based Layer-3 approach being pursued by other organizations.

The MEF model of QoS is particularly relevant however when considering services that are ultimately delivered to the customer over broadband access networks. For reasons of cost and scalability these networks typically utilize a relatively few traffic classes when compared to solutions architected around the DiffServ QoS model. In reality this means that multiple traffic classes in the core of the network may be mapped in the access network to the same traffic class.

QoS Over NNI Analysis

As seen in clause 3, QoS over NNI is under discussion in various industry fora. For the most part, there is a good deal of commonality between the different fora. In addition, industry momentum is building around GSMA IPX and there does seem to be a growing desire amongst the SDOs to avoid divergence and work toward a common solution with GSMA as the lead SDO. Such a trend is facilitated by the commonality of membership in the GSMA and other fora and growing co-operation between the GSMA and other fora. Thus, as time goes on, it is expected that the GSMA will define the baseline text for QoS over NNI and other SDOs will refer to or endorse that work. It is expected that, in the longer term, the Multilateral Service Hub Connectivity option would be preferred option as this enables IPX to be service aware (with implications of being able to use this knowledge when routing, charging etc.) as well as simplifying the interface to the connecting Service Providers (i.e. they have a single agreement with the IPX Provider). However, in the shorter term, it is also likely that the Bi-lateral Service Transit Connectivity option would be used – probably as a stepping stone toward the eventual Service Hub option. A general reference architecture is shown in figure 8.

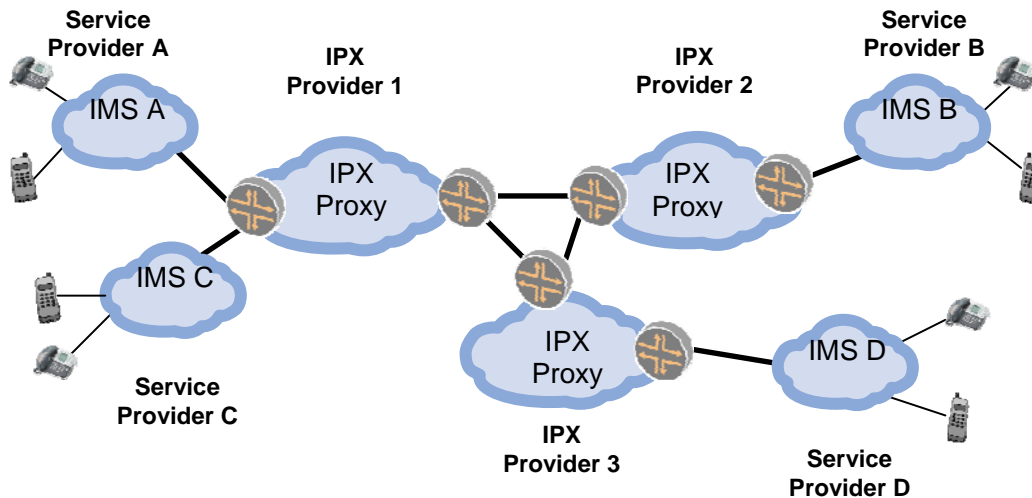


Figure 8. Generic Reference Architecture

In reality, the interconnection between networks would traverse BGW functions. More specifically, Service Provider IMS-based networks would connect to the IPX Provider via an IBCF and TrGW. In addition, the IPX Proxy would be composed of an IBCF function, a TrGW and (optionally for hub mode) routing functionality such as a BGCF / ENUM Server. This is shown in figure 9. The TrGW is controlled via the Ix reference point (see [7]) which enables a range of

BGW capabilities to be controlled (e.g. pin-hole control, NAT, bandwidth policing, DSCP marking etc.).

NOTE - The “H.248 Ix profile version 1” (see [7]) does **not** (yet) support any H.248 statistics, which would be required for call-dependent performance and QoS measurements. Subsequent profile versions in future 3GPP releases may provide that additional capabilities. It has to be noted that the companion profile for Border Gateways in ETSI TISPAN (see [12]) does provide support of H.248 statistics.

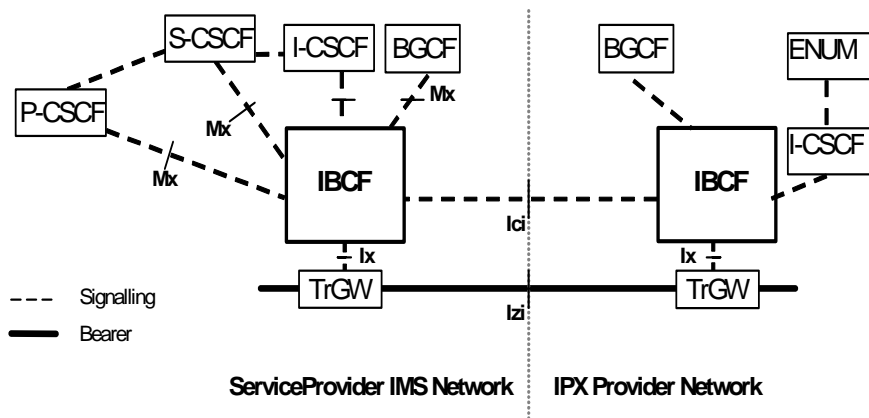


Figure 9. IMS – IPX Interconnection

At all inter-connect points (both from Service Provider-IPX Provider as well as IPX Provider-IPX Provider), there must be a SLA governing the number of sessions and amount of bandwidth to be carried across a point of inter-connect. The SLA would typically define a classification of the traffic into a number of groups or classes and diffserv would be used to tag the traffic appropriately dependent on its *traffic class*. The aggregated flows within a traffic class may be regarded as a logical *trunk* at the point of inter-connect. All egress traffic from the Service Provider BGW is allocated to such a logical class based trunk and tagged appropriately as per the SLA. Traffic which breaks the SLA would be handled appropriately (e.g. discarded). Such handling would part of the SLA. In order to be able to enforce the SLA fairly, there is a need to be able to perform admission control (i.e. to allocate resources to a given flow) and to police that flow to ensure that it does not exceed its bandwidth reservation. Figure 10 shows the concept of *logical trunks*.

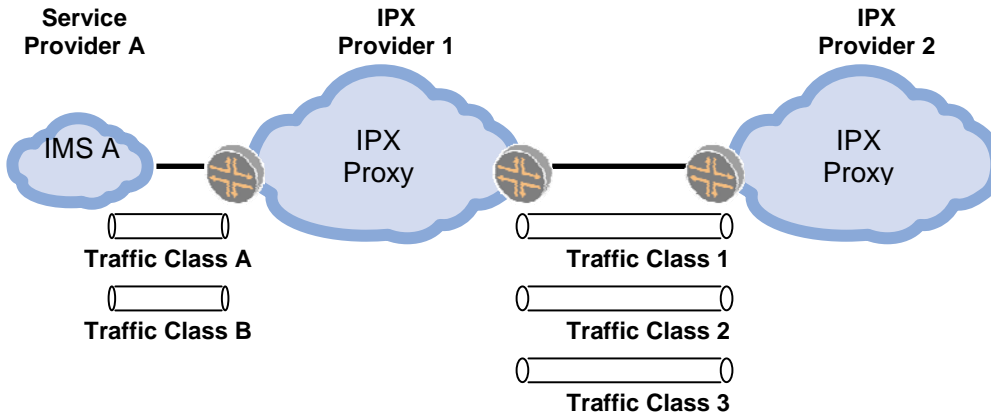


Figure 10. Logical Trunks at Inter-connect Points

Within a domain, be it a Service Provider or IPX Provider, the provision of QoS is the responsibility of that domain. At the current time, this is done by use of an engineered core network with a level of over-provision built in together with admission control. In the longer term, such over-provision may not matter as the transport layer will support multi-services and the volumes of best effort traffic will outweigh the volumes of call session related data (voice & video). The only standardization for resource admission has been done at the access side via 3GPP PCRF and TISPN RACS.

In summary the current industry position for QoS over NNI in IPX consists of the following elements:

1. Service Level Agreements (SLAs) at all the inter-connection points between different domains.
2. DiffServ markings on traffic trunks based on agreed upon classification criterion.
3. All domains interconnected via BGWs, enforcing admission control, bandwidth policing and diffserv packet marking. The diffserv packet marking may be set up by default BGW settings or else via Ix interface on a per flow basis.
4. Inter-domain SIP session signaling at the control layer and RTP/RTCP at the transport layer. The RTCP may or may not be end-end. The latter is preferred but is dependent on all domains transiting RTCP packets across their domain boundary.
5. All domains perform session/call related measurements.

6. All domains perform transport layer estimates based on RTCP (and impacted by whether the RTCP is end-end or not).
7. Intra-domain QOS achieved via over-provisioning or some proprietary method.

The MSF notes that one potential area of concern is in the area of RTCP performance statistics. There are a great number of RTCP reports and packages of varying quality and utility, primarily defined by the IETF. Furthermore if RTCP is end to end then a network operator may be dependent on the accuracy and behavior of a residential or access gateway in another network. The network operator may never have tested or encountered such a device but may ultimately rely on its accuracy to inform them as to the customer experience. The MSF believes that this is an area which would benefit from further analysis, especially with regards to the complexities caused by the need to measure both end to end and network performance. The MSF is also concerned that any defined solution be developed in conjunction with the silicon vendors who produce the DSPs that ultimately have the job of performing the measurements. These components are often in cost sensitive devices which limits the processing power and memory available.

Although many SDOs are working on the NNI, the technology is still maturing in respect to end to end deployments. Whilst there has been some trialing activity on this area, it is believed that there is potential scope for further IOT activities to prove NNI QOS concepts and test key interfaces. This is further discussed in clause 5.

IOT Opportunities

There are a number of potential areas for IOT activities for proving NNI QOS concepts based on the current industry position and likely partitioning of equipment in terms of multi-vendor interoperability :-

- IMS Service provider to IPX Proxy via Ici and Izi reference points,
- Inter IPX Proxy via the i3Forum interface.
 - This can be SIP or SIP-I based.
- Testing of the Ix interface between IBCF/IPX Proxy and TrGW to establish signaling & media pin-holes, perform NAT, police flows etc.
- Measuring of call related stats at IPX Proxies / IBCFs to check consistency between reports at different interconnect points,
- Measurement of transport layer stats at all TrGWs and checking of consistency between reports at different interconnect points.
- Transiting of RTCP end-end and comparing end RTCP reports with measurements at intermediate TrGWs at interconnect points.
- Testing of SLAs based on a standardized and/or agreed set of metrics.

Summary and Conclusions

There is a good deal of commonality between the different for a and a desire to avoid divergent solutions. Industry momentum is building around GSMA IPX and is expected that the GSMA will define the baseline text for QoS over NNI and other SDOs will refer to or endorse that work. In addition, other bodies (notably the i3Forum) have also done a lot of detailed work due to their pressing need to realize legacy services over an IP based NNI. Initially, it is likely that the Bi-lateral Service Transit Connectivity option will be used – probably as a stepping stone toward the eventual Service Hub option. The Multilateral Service Hub Connectivity option would be expected to be the preferred long term option as this enables IPX to be service aware (and being able to use this knowledge when routing, charging etc.) as well as simplifying the interface to the connecting Service Providers. At the current time, there is an opportunity for IOT activities to prove key interfaces in a multi-vendor environment.

The MSF's primary role is to test real world implementations of (other) SDO defined architectures and protocols with a view to accelerating the deployments of those technologies that are identified as being critical by the forum's members. Given the importance of a QoS assured IP based NNI, the MSF would be keen to work with other fora working in this space to identify parts of the solution that would benefit from an IOT event and to realize such events.

References

- [1] GSMA IR.34 “Inter-Service Provider IP Backbone Guidelines (Version 4.9, March 2010).
- [2] i3Forum Technical Interconnection Model for International Voice Services (Release 3.0, May 2010)
- [3] ETSI TISPAN ES 282 001 “TISPAN NGN Functional Architecture” (Version 3.4.1, September 2009)
- [4] 3GPP TR 22.893 “Study into Identification of Advanced Requirements for IP Interconnection of Services” (Version 1.0.0, September 2009)
- [5] 3GPP TS 29.165 “Inter-IMS Network to Network Interface” (Release 9, December 2009)
- [6] ETSI TISPAN TR 184 008 “Infrastructure ENUM Options for TISPAN IPX” (Version 2,1,1, February 2002)

- [7] 3GPP TS 29.238 “Interconenction Border Control Functions (IBCF) – Transition gateway (TrGW) Interface, Ix Interface; Stage3” (Version 9.0.0, December 2009)
- [8] ITU-T Rec. Q.1912.5 “Inter-working between Session Initiation Protocol and Bearer Independent Call Control or ISDN User Part”, March 2004.
- [9] 3GPP TS 29.231 “Application of SIP-I Protocols to Cicuit Switched (CS) Core Network Architecture; Stage 3” (Version 9.1.0, March 2010)
- [10] 3GPP TS 29.235 “Interworking between SIP-I based circuit-switched core network and other networks” (Version 9.4.0, March 2010)
- [11] ETSI EN 383 001 “TISPAN; Inter-working between Session Initiation Protocol (SIP) and Bearer Independent Call Control (BICC) or ISDN User Part [ITU-T Recommendation Q.1912.5, modified]” (Version 1.1.1 June 2006).
- [12] ETSI TS 183 018 “TISPAN; Resource Admission Control: H.248 Profile Version3 for controlling Border Gateway Functions (BGF) in the Resource Admission Control Subsystem (RACS); Protocol Specification” (Version 3.5.1, July 2009)
- [13] IETF RFC 3261 “SIP – Session Initiation Protocol”, June 2002
- [14] GSMA IR.83 “SIP-I Interworking Description” (Version 1.2, May 2009)
- [15] GSMA IR.87 “SIP-I Interworking Test Cases” (Version 1.0, June 2009)
- [16] IPX and Practical Trial Activity Review, April 2009.

Abbreviations

3GPP – 3rd Generation Partnership Project (see www.3gpp.org)

AF - Assured Forwarding

ALG - Application Level Gateway

ALOC – Average Length of Call

ASP - Application Service Provider

ASR - Answer to Seize Ratio

ATIS - Alliance for Telecommunications Industry Solutions (see www.atis.org)

BE - Best Effort

BGCF – Breakout Gateway Control Function

BGF - Border Gateway Function

BGW - Border Gateway

CIR - Committed Information Rate

CLI - Calling Line Identity

CoIx - Connection Oriented Interconnect

COS - Class of Service

CS - Circuit Switched

CSCF – Call Server Control Function

DNS - Domain Name Server

DSCP – Differentiated Services Code Point
DSP - Digital Signal Processor
E2E – End to End
EF - Expedited Forwarding
EIR - Excess Information Rate
E-NNI – Ethernet NNI
ENUM – E.164 Number Mapping
ETSI - European Telecommunications Standards Institute (see www.etsi.org)
FNO - Fixed Network Operators
GRE - Generic Routing Encapsulation
GRX - GPRS Roaming eXchange
GSMA – GSM Association (see www.gsmworld.com)
HSS - Home Subscriber Server
i3Forum – International IP Interconnection Forum (see www.i3forum.org)
IBCF - Interconnection Border Control Function
IBPCF - Interconnection Border Policy Control Function
I-BGF – Interconnect BGF
I-CSCF – Interrogating CSCF
IETF - Internet Engineering Task Force (see www.ietf.org)
IMS - IP Multimedia Subsystem
IOT- Interoperability Testing
IP - Internet Protocol
IPTV – IP Television
IPX – IP Packet eXchange
ISDN -Integrated Services Digital Network
ISP – Internet Service Provider
IWF - Interworking Function
KPI - Key Performance Indicator
MEF - Metro Ethernet Forum (see www.metroethernetforum.org)
MNO -Mobile Network Operators
MOSCQE – Mean Opinion Score, Communication Quality Estimated
MPLS – Multi Protocol Label Switching
MSF – Multi-Service Forum (see www.msforum.org)
NAT – Network Address Translation
NER - Network Efficiency Ratio
NG-CI – Next Generation Carrier Interconnection
NGN - Next Generation Network
NNI - Network to Network Interface
OAM – Operations, Administration & Maintenance
PCRF – Policy Control and Charging Rules Function
P-CSCF – Proxy CSCF
PGRD – Post Gateway Ringing Delay
PHB - Per Hop Behaviour
QOS - Quality of Service

RACS – Resource Admission Control Subsystem
RFC - Request For Comments
RSVP-TE – Resource Reservation Protocol-Traffic Engineering
RTP - Real Time Protocol
RTCP – RTP Control Protocol
S-CSCF – Serving CSCF
SDO – Standards Development Organisation
SIP - Session Initiation Protocol
SIP-I - SIP with encapsulated ISDN User Part
SLA - Service Level Agreement
SoIx - Service Oriented Interconnect
TDM - Time Division Multiplexing
THIG – Topology Hiding Interconnecting Gateway
THP - Traffic Handling Priority
TISPAN – Telecoms & Internet converged Services & Protocols for Advanced
Networking
TrGW – Transition Gateway
UE - User Entity
VLAN – Virtual Local Area Network
VoIP - Voice over IP
VPN - Virtual Private Network