IPV4 VERSUS IPV6 INTERWORKING WITH QOS GUARANTEES

Mario Marchese[♣], Annamaria Raviola[♦], Maurizio Mongelli[♣], Alessandro Garibbo[♦], Vincenzo Gesmundo[♦]

[♣]*DIST - Department of Communication, Computer and System Sciences*
University of Genoa, Via Opera Pia 13 - 16145 Genoa, Italy
{ *Mario.Marchese, Maurizio.Mongelli* }*@unige.it*

[♦]*Selex Communications S.p.A., a Finmeccanica Company*
Via Pieragostini 80 - 16151 Genoa, Italy
{ *Annamaria.Raviola, Alessandro.Garibbo, Vincenzo.Gesmundo* }*@selex-comms.com*

ABSTRACT

The paper analyzes two solutions (IPv4 and IPv6) for interworking of network portions implementing different technologies belonging to diverse Autonomous Systems (ASes). While the implementation of QoS is a AS's concern, three topical problems should be solved at the interworking points (called Relay Points, RPs): ***1)*** *the definition of the RP convergence technology,* ***2)*** *the signalling between the RPs,* ***3)*** *the bandwidth pipes dimensioning for flows traversing the ASes. The paper investigates these points and proposes a description of the Service Level Agreements available in the heterogeneous network as function of the RP protocol architecture.*

INTRODUCTION

The support of *end-to-end* (e2e) QoS over a heterogeneous network, composed of different portions (also called *Autonomous Systems*, ASes), is a hot topic of research. The problem involves a common language for QoS definition, interworking solutions, signalling, and control mechanism implementations. Having in mind hazardous and challenging environments as in military and civil protection world, it is often recommendable to have QoS for each user. It means to identify each single e2e connection having a specific *Service Level Agreement* (SLA) each or, at least, to identify a large number of SLAs. Last but not least, there can be the need of dropping some connections already in progress because other calls with higher priority require the access to the network and there is no sufficient bandwidth for all of them. It is called *Multi Level Priority Pre-emption* (MLPP) and is often part of the SLA, especially in military environments.

The connection point interconnecting two ASes is defined as *Relay Point* (RP). The role of RP is **1)** to establish a proper interface between two ASes; **2)** to transfer the QoS needs for each e2e connection across them. **3)** Once transferred the QoS requests among the ASes, it is topical to map the performance requests over the peculiar technology implemented within each AS.

It is worth noting that IPv4-centric approaches not always solve the main objectives listed above, even if they represent a reasonable solution and an important reference. So, retaining many important details of IPv4 solutions recently proposed in the literature, it is important to highlight alternative solutions to match advanced inter-domain QoS delivery.

In this view, the paper recalls the advantages of the MPLS interworking solution of [1] and proposes an alternative approach, based on IPv6, by focusing both on inter-domain signalling and on other IPv4-centric alternatives. It also generalizes the results presented in [1] by considering real VoIP and video traces with a large range of QoS metrics.

The rest of the paper is organized as follows. The following section summarizes the IPv4 solution for RP. Section III deals with the proposed IPv6 architecture. Performance evaluation is the subject of section IV. Conclusions and future work are outlined in section V.

IPV4 RELAY POINT ARCHITECTURE

The first solution for QoS interworking that can be suggested is based on regular IP protocol version 4 [2, 3]. It means that the common e2e language is IPv4 both concerning QoS definition and interworking. The architecture of IPv4 RP protocol stack is detailed in Fig. 1.

The work is part of a scientific project between Selex Communications S.p.A, Italy, and the Department of Communication, Computer and System Sciences of the University of Genoa.
Some material of the work was partially used by Selex Communications within the framework of the TACOMS Post 2000 project [2].

A. A common set of Service Level Agreements

It means that RP acts as an IPv4 router concerning all the aspects (routing, encapsulation, processing). The DiffServ paradigm for QoS management is chosen for scalability purposes with respect to IntServ solution. A proper definition of the *DiffServ Code Point* (DSCP) of the IPv4 header is thus necessary to cover the entire network with a common set of *Service Level Agreements* (SLAs) (the *extended QoS class* concept, in [4] terminology).

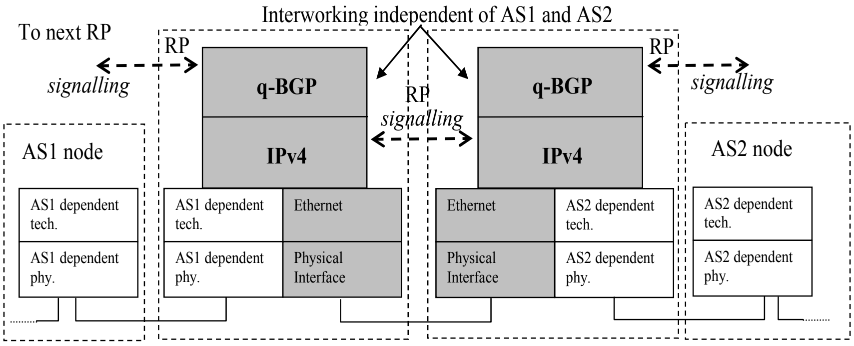


Fig. 1. IPv4 Relay Point.

To define a common set of SLAs among the ASes, there are 14 traffic classes characterized by a common assignation of the DSCP field. Each single data packet arriving at the IP layer of each RP needs to be treated in conformance with the DSCP assignation performed for all the traffic. A first possibility of DSCP assignation within the RPs is reported in Table 1, together with possible examples of traffic types taken from [5]. An alternative DSCP assignation considering some mission critical applications is proposed for specific tactical environments by the USA *Department of Defence* (DoD) within the framework of the *Global Information Grid* [6] (Table 2). The topical point is that each of the mentioned services deserves its specific SLA, expressed in terms of: **1)** traffic description, **2)** conformance testing parameters and **3)** required performance guarantees (e.g., loss rate, delay and delay jitter of the packets) and, when needed, MLPP and *connection protection* [7] levels.

Service	Traffic class	DSCP assignation	Example of applications
Telephony	EF	101110	IP Telephony bearer
Multimedia conference	AF41	100010	Video-conference
	AF42	100100	
	AF43	100110	
Multimedia streaming	AF31	011010	Streaming video and audio
	AF32	011100	
	AF33	011110	
Data of low latency transactions	AF21	010010	Client/server web-based transactions
	AF22	010100	
	AF23	010110	
High Throughput Data	AF11	001010	Client/server web-based transactions
	AF12	001100	
	AF13	001110	
Standard Data	Default	000000	Not specified
Low Priority Data	CS1	001000	Best Effort
Broadcast Video Events	CS3	011000	Broadcast TV
Real-time interaction	CS4	100000	Interactive applications and gaming
Operation and Management (OAM)	CS2	010000	OAM
Signalling	CS5	101000	IP telephony signalling
Network Control	CS6	110000	Routing and control information
Administrative	CS7	111000	Routing and control information

Table 1. Possible DSCP assignation within RP [5].

Service	Traffic class	DSCP assignation	IP-D	IP-DV	IPLR
			Delay	Delay Variation (Jitter)	Loss Rate
Continuous Bit Rate CBR	EF	101111, 101110, 101101, 101011, 101001,10100	100-400 ms	30-50 ms	10^{-2}-10^{-3}
Variable Bit Rate VBR	AF41	100010	100-400 ms	30-50 ms	10^{-2}-10^{-3}
	AF42	100100			
	AF43	100110 100000			
Multimedia	AF31	011010	5-10 s	Not applicable	10^{-2}-10^{-3}
	AF32	011100			
	AF33	011110			
Mission Critical	AF21	010010	20ms-100ms	1ms-50 ms	0
	AF22	010100			
	AF23	010110			
Mission Critical	AF11	001010	1ms – 50 ms	Not applicable	0-10^{-3}
	AF12	001100			
	AF13	001110			
Best Effort	Default	000000, 001000, 101000, 011000	Unspecified	Unspecified	Unspecified
Control and Management	CS7	111000	50 ms – 1 s	Not applicable	0-10^{-3}
Control and Management	CS6	110000	1s – 10 s	Not applicable	10^{-2}-10^{-3}

Table 2. DoD SLAs DSCP assignment [6].

B. *IPv4 end-to-end signalling architecture*

QoS mechanisms imply the presence of a signalling protocol to transfer the QoS needs and possible feedback about the congestion of the network.

The IPv4 e2e architecture presented here summarizes the approaches of the literature (see, e.g., [4, 8] and references therein). Figs. 2-4 show a possible abstraction of the architecture at management plane. The way to transport QoS requirements between RPs (i.e., the signalling protocol) relies on *QoS-Border Gateway Protocol* (q-BGP) and its architectural improvements [4]. It allows inter-domain QoS-guaranteed delivery of the packets belonging to the common SLAs.

Each single network portion implements a *Bandwidth Broker* (BB) that negotiates SLA with neighbour ASes, implements *Call Admission Control* (CAC) and QoS management (see, e.g., [9]). Management and data planes are completely decoupled: there is one centralized BB for each domain, which communicates with the RPs separating the different network domains (Fig. 3). RPs perform data encapsulation, while the resource management functions (bandwidth allocations, SLA transfer and mapping), hidded in RPs, are implemented by BBs, which communicate each other. q-BGP-based RPs communicate the reachability of specific destinations with a fixed degree of service (i.e., the SLA), associated to a DSCP value. An agent-based architecture is employed with the structure shown in Fig. 4. The *SLA agent* is responsible for the contract between neighbour domains. On the basis of the contract, the SLA agent controls the configuration agent to set the forwarding path in the RP and the related controls (such as classifier, marker, and scheduler).

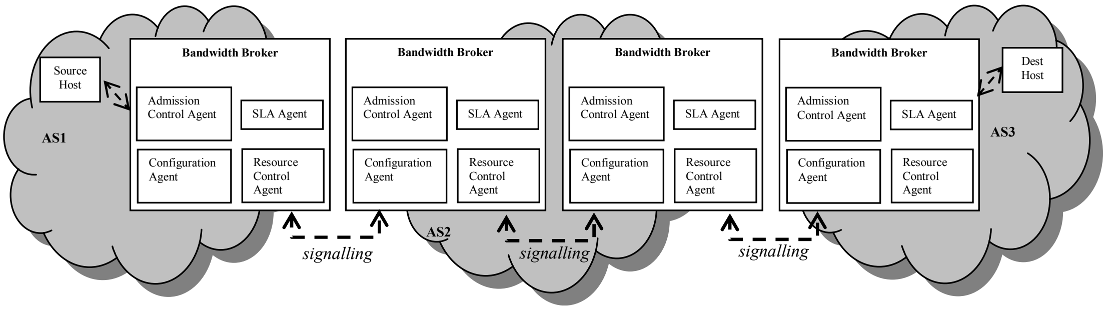


Fig. 2. IPv4 RP: management plane.

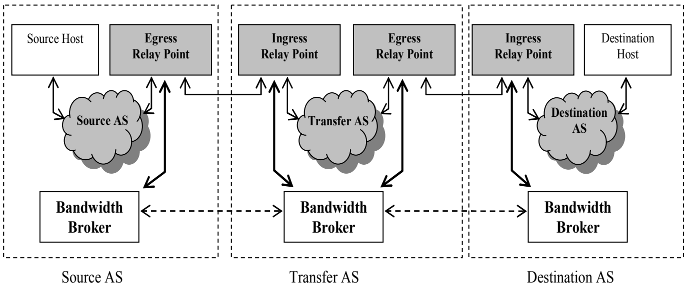


Fig. 3. IPv4 RP: Bandwidth Broker.

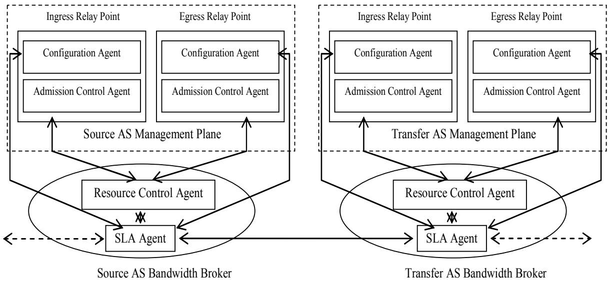


Fig. 4. IPv4 RP: Agents interaction.

IPV6 RELAY POINT ARCHITECTURE

A. *Towards hard guarantees QoS*

Actually, the solution presented in previous section offers *loose guarantees QoS* [4], which may not support both tactical applications (requiring additional requirements as summarized in the following) and *traffic engineering* (TE). Anyway, also generally speaking and considering a *hard guarantees QoS* [4] supported by signalling (RSVP-like) over the IPv4 architecture, the key point, in the authors' viewpoint, is that the exclusive application of the DiffServ paradigm may not be completely satisfying. **i)** It looses the reference to the single connection and **ii)** does not guarantee sufficient SLA flexibility. As should be clear also from the results of this paper, no bandwidth optimization can be reached. More specifically, concerning point **i)**, mission critical scenarios are supported with some difficulty: no guarantee may be provided to the single user and MLPP and recovery management are applicable through very complex solutions (some good examples are reported in [10]). Concerning point **ii)**, if the number of traffic classes increases (for example if enlarging the granularity of QoS constraints is necessary due to novel applications), or MLPP and connection protection classification is required, the 8-bits of the DSCP may be unsufficient for SLA categorization, especially if some parts of the DSCP itself are used for control purposes (as either in tables 1 and 2 or in [10]). As a result, the adoption of an alternative technology matching the previous points reveals to be much more effective, especially from the TE viewpoint.

In this view, the adoption of MPLS within RPs is proposed in [1] to match the envisaged problems. The key idea is to establish MPLS connectivity among the RPs through regular label binding and signalling. In this way, the SLAs definition is based on the MPLS label and QoS management exploits full TE [4]. The MPLS shim header is tunneled across the ASes not MPLS capable. A sligthly similar approach is adopted in [2], even if assuring QoS with less flexibility. Actually, no MPLS signalling is used in [2] for inter-ASes communication. The potentialities of the MPLS solution are limited to the features available through the DiffServ paradigm outlined in section II [3]. A statical provisioning of the tunnels having inter-ASes scope is supposed to be always in effect, too.

Here, the advantages for QoS management offered by the MPLS-centric approach of [1] are combined with the simplicity of the IPv4 solution through the introduction of IPv6 within RP.

B. QoS: IPv4 versus IPv6

There are two versions of the Internet Protocol: IPv4 and IPv6, whose main difference concerning QoS stands in the features to identify a flow. Actually, if DiffServ approach is used, there is no difference between the two versions concerning QoS [11] but, with a longer vision over the future, it is possible to exploit the IPv6 QoS features. In other words, if the 8-bit *Traffic Class* field of the IPv6 header is used to identify a flow, IPv6 QoS is strictly equivalent to IPv4 one (where the DSCP field is used) and DiffServ paradigm may be applied exactly in the same way, but, if the 20-bit *Flow Label* (FL) is exploited, there is a strict equivalence with MPLS (and also with ATM) concerning flow identification, thus opening the door to new QoS management possibilities. In the IPv6 standard, the FL field was originally proposed to support IntServ-oriented functionalities. However, the IntServ solution is widely known to suffer scalability problems. To face this drawback, the IPv6 FL can be managed through switching techniques as in MPLS (ATM).

C. IPv6 switching

The first works outlining the essential elements of an IPv6 switching core architecture (the so called *IPv6 Label Switching Architecture*, 6LSA) are [12] and [13]. The label switching (instead of regular IP routing) is introduced as function of the FL of the IPv6 header. In brief, the 6LSA follows the guidelines of the MPLS protocol. An importante difference relies on the deficiency of a *Label Distribution Protocol* (LDP) performing label binding. 6LSA looses the label coordination along specific routes. Label binding scope is defined only among adiacent routers, thus limiting e2e control of the resulting *Label Swith Path* (LSP). To some extents, it recalls the adoption of the first MPLS LDP before the definition of *Contrained Routing* (CR) LDP and RSVP-TE. Moreover, the switching mechanism of [12] and [13] requires to be triggered by the 128-bits address field of IPv6 header in specific conditions, thus limiting the advantage of switching on the basis of the label.

D. IPv6 Relay Point

In this work, the IPv6 label switching principle is applied at RPs in function of the FL, with emphasis on the adoption of a proper signalling to control the RPs e2e path (as also suggested in [13]: "*one of the existing label distribution protocols could be used between two 6LSRs with a minimum of modification to the protocol*").

The IPv6-based RP protocol architecture is reported in Fig. 5. Label swithing of [12, 13] is applied, supported by e2e signalling as detailed in the following. In [1], MPLS is similarly used acting both as a layer 2 and a layer 3, excepts for addressing the RPs at signalling level (actually, MPLS has no addressing capabilities without IP). Using IPv6 avoids decoupling between data and signalling and there is no need of any 2.5 (MPLS) shim header to support switching within routers. The traffic flows of the ASes come from the hosts plus the IPv6 header added at the first RP. The key idea is to exploit labelled packets to be tunnelled along the ASes (not necessarily IPv6 capable) and forwarded. The inference at RPs of routing and QoS is a function of the 20-bits IPv6 label. The label is used at RPs to classify packets of each traffic class, thus inferring the guaranteed bandwidth, the class-related scheduling, the packet discarding treatment, and, in general, the SLA of the packet.

The identification of the switching devices follows the [12, 13] notation. The first RP met along the e2e path acts as a regular *IPv6 Label Edge Router* (6LER), by identifying the flow and applying the label. The opposite operation is implemented at the last RP before the destination. Intermediate RPs act as conventional *IPv6 Label Switch Routers* (6LSR). At the RP, host packets are encapsulated within the MPLS information and transported over the AS backbone.

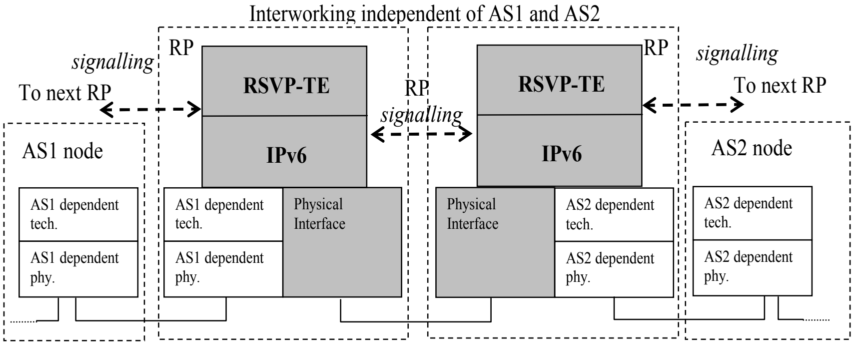


Fig. 5. IPv6 Relay Point.

E. IPv6 end-to-end signalling architecture

Differing from [12, 13], regular RSVP-TE (Fig. 5) is used to set the FLs over the e2e path and to signal QoS requirements among the RPs. It is assumed that an IPv6 address plane is available in each RP for signalling. Differing from q-BGP solution of previous section, triggering the establishment of specific QoS routes at RPs allows implementing inter-doman TE [4].

RSVP-TE guarantees a common format for service requests flowing through RPs and carrying information about the flows entering the network. The management of the bandwidth within each single AS is left to the AS itself. RSVP-TE transports QoS requests from one RP up to the next RP along the path. The BBs architecture described in section II may be similarly used to map the SLA over a single AS (if IP-based AS is taken as an example), so getting a properly dimensioned “bandwidth pipe” to guarantee SLA up to the next RP. The “bandwidth pipe” could be not available. The check is performed locally, within each single AS querying a database constantly updated about the AS resource status (actually, through a BB: a *Quality Network Server*, as in [8] or a *Path Computation Element* as in [4]). If no resource is available, the connection is rejected by the BB.

To summarize, the choice of IPv6 as interworking technology allows obtaining:

1. QoS with single connection granularity if needed (e.g., for specific mission critical applications is a mandatory requirement, even if it might affect scalability);
2. the definition of a large set of SLAs: tables 1 and 2 may be extended with respect to larger granularity of QoS contraints, MLPP and connection protection classification;
3. MLPP (the RSVP-TE “Session_Attribute” field is dedicated to it);
4. re-routing to guarantee connection protection [7]: the “loose” option, make before break, route pinning and crankback techniques may be applied through RSVP-TE;
5. inter-ASes TE [4].

Special attention is devoted in this paper to point 2 above (the adoption of a large set of SLAs). The flexibility of service differentiation may allow significant bandwidth saving during the traffic aggregation process. This constitutes an ongoing topic of research and it is the subject of the following performance evaluation section.

PERFORMANCE EVALUATION

If a specific technology does not offer the possibility of separating the required number of SLAs, there is the need to aggregate together traffic flows that not only can be characterized by different source models, but also by performance requirements. The effect of it over bandwidth allocation and network performance is evaluated in this section. If traffic requiring different performance is joined in one flow, it is necessary to investigate the addition (or reduction) of bandwidth required to keep the performance levels required by each flow. For example, it is interesting to check the bandwidth shift (if any) required by DiffServ architectures that use a limited number of classes with respect to IPv6 approach, in which a large number of SLAs can be defined using the FL. Many studies confirm the efficiency of aggregating homogeneous traffic, but the performance of non-homogeneous trunks (from the statistical behaviour and QoS requirement viewpoints) is still an open issue.

Even if, due to computational reasons, the results cannot include a full comparison between the 14 QoS classes of DiffServ and the virtually infinite classes of 6LSA, the authors do hope that the presented results can help understand the problem and also suggest possible operative indications.

The RP is modelled through buffers. The allocated bandwidth is the service rate assigned to buffers. Two types of SLAs are considered for performance evaluation: VoIP and video. VoIP SLA considers sources modeled as an exponentially modulated on-off process, with mean on and off times (as in the ITU P.59 recommendation) equal to 1.008 s and 1.587 s, respectively. When in the active state, they are 16.0 kbps flows over RTP/UDP/IP. The VoIP packet size is 80 bytes. As far as the video service is concerned, real traces (taken from [14]) have been used. Data are H.263 encoded and have an average bit rate of 260 kbps and a peak bit rate ranging from 1.3 to 1.5 Mbps, depending on the specific trace. Each video trace lasts about 1 hour. QoS constraint of both SLAs is *Packet Loss Probability* (Ploss).

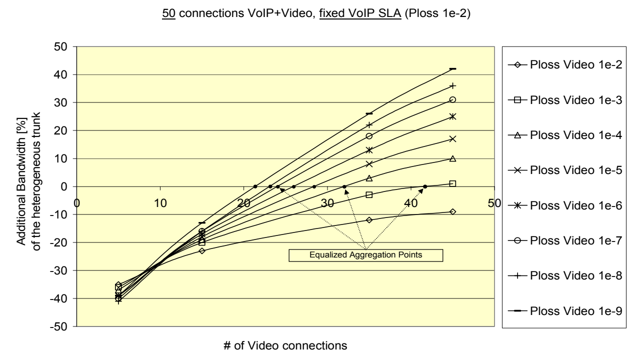
The tests are performed with the mentioned SLAs and supposing that the two SLAs need to be aggregated because there are not enough classes to be assigned within the specific technology. An ad-hoc simulator in C++ has been used to get the results. The width of the confidence interval over the performance measures is less than 1% for the 95% of the cases.

To achieve low Ploss values (e.g., below 10^{-5}, referring to most literature), not obtainable by ordinary simulation analysis for computational reasons, the well-known *equivalent bandwidth* (EqB) formula:

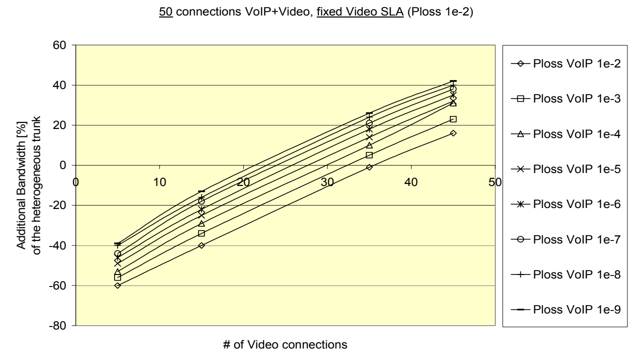
$$C = m + a \cdot \sigma \tag{1}$$

is used to compute the bandwidth provision *C* of a given trunk for all results. The quantities and denote the *mean* and the *standard deviation*, respectively, of the input process of the buffer; and $a = \sqrt{-2\ln(\text{Ploss}^{*}) - \ln(2\pi)}$ being Ploss^{*} the upper bound on the allowed PLP (the most stringent Ploss in the heterogeneous case). The mentioned statistics (m and σ) are estimated by simulation inspection for each traffic composition.

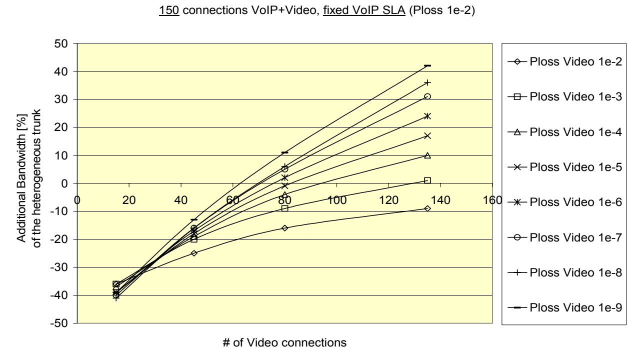
Fig. 6 shows the additional bandwidth (in percentage) of the aggregated trunk necessary to satisfy both the SLAs, with respect to the resource allocation corresponding to the traffic separation case. Fig. 6.(a) and 6.(b) is obtained by aggregating 50 connections globally. Fig. 6.(c) and 6.(d) by aggregating 150 connections. VoIP SLA is fixed and video SLA is changed within the range [10^{-2}, 10^{-9}] in Fig. 6.(a) and 6.(c), viceversa in Fig. 6.(b) and 6.(d).



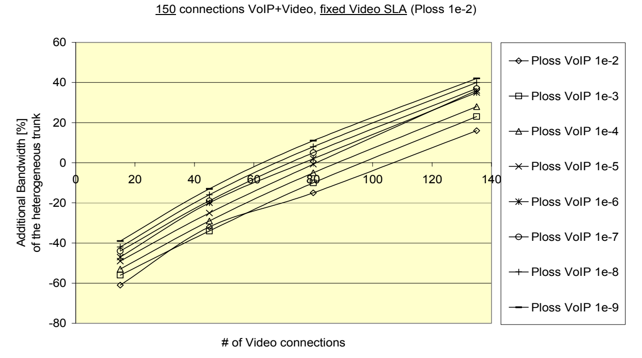
(a). 50 connections, fixing the VoIP SLA.



(b). 50 connections, fixing the Video SLA.



(c). 150 connections, fixing the VoIP SLA.



(d). 150 connections, fixing the Video SLA.

Fig. 6. Traffic aggregation performance.

The results highlight that provisioning in heterogeneous conditions is not a straigthforward matter. Due to the multiplexing gain in presence of bursty sources, below a given threshold (the intersection point of each curve with the x-axis), aggregating is always convenient (the gain is negative), despite QoS heterogeneity. Above the threshold, on the other hand, a portion of bandwidth is wasted if the traffic classes are not kept separated. Such a threshold is defined as *Equalized Aggregation Point* (EAP) in this paper, because it represents the equilibrium point where aggregating and separating is indifferent for bandwidth allocation.

It is worth noting that Fig. 6.(a) and 6.(b) has the same trend of Fig. 6.(c) and 6.(d). The position of EAPs is almost invariant if the number of total connections is scaled up. For instance, the curve of 'Ploss video 1e-3' meets the x-axis of 42 video connections point in Fig. 6.(a) and of 130 video connections point in Fig. 6.(c). Both cases correspond to the 85% of video connections in the aggregated trunk. Knowing that the EAPs are traffic invariant constitues a powerful and simple tool for planning the aggregation of VoIP and video. For each Ploss curve, the quantity of additional bandwidth is a function of the percentage of video connections in the trunk.

CONCLUSIONS AND FUTURE WORK

The paper has presented and compared IPv4 and IPv6 solutions for the protocol stack interconnecting network portions implementing different QoS technologies. The proposals are investigated in detail specifying the data flows along the end-to-end paths both for data and signalling. The advantages of the IPv6 architecture are highlighted, with emphasis on the effect of traffic aggregation. The results reported concern this topic and try providing operative indications applicable in the field.

Future extensions concern testing the implementation of IPv6 switching within Selex Communications devices and exploiting the other IPv6 functionalities (such as: mobility, explitic routing, anycast) to extend RP features.

REFERENCES

[1] Garibbo, M. Marchese, M. Mongelli, "MPLS-based QoS Interworking Among Wide Area Subsystems," Proc. of Military Communication Conference 2005 (*Milcom 2005*), Atlantic City, NJ, Oct. 17-20, 2005, pp. 1-7.

[2] Tacoms Post 2000 Project (TACOMS), TACOMS STANAG 4637, "TACOMS HEAD STANAG" (draft ed. 1), NATO Steering Committee, http://www.tacomspost2000.org, NSA, 2005.

[3] Sorteberg, O. Kure, "The Use of Service Level Agreements in Tactical Military Coalition Force Networks," *IEEE Comm. Mag.*, vol. 43, no. 11, Nov. 2005, pp. 107-114.

[4] M. Howarth, M. Boucadair, P. Flegkas, N. ASg, G. Pavlou, P. Morand, T. Coadic, D. Griffin, H. Asgari, P. Georgatsos, "End-to-end Quality of Service Provisioning Through Inter-provider Traffic Engineering," *Comp. Commun.*, vol. 29, no. 6, March 2006, pp. 683-702.

[5] J. Babiarz, K. Chan, F. Baker, "Configuration Guidelines for DiffServ Service Classes," <draft-ietf-tsvwg-diffserv-service-classes-01>, IETF Internet Draft, work in progress, July 2005.

[6] DoD. Proposed Draft Strawman DSCP Mapping for GIG Enterprise IP Networks Version 11p, DoD GIG QoS/CoS Working Group, March 2004.

[7] P. Pongpaibool, H. S. Kim, "Providing end-to-end Service Level Agreements Across Multiple ISP Networks," *Computer Networks*, vol. 46, no. 1, Sept. 16, 2004, pp. 3-18.

[8] V. Fineberg, "A practical architecture for implementing end-to-end QoS in an IP network," *IEEE Comm. Mag.*, vol. 40, no. 1, Jan. 2002, pp. 122-130.

[9] Y. Jia, M. Chen, "A new architecture of providing end-to-end quality-of-service for differentiated services network," Proc. of Military Communication Conference 2001 (*Milcom 2001*), Washington, D.C, Oct. 28-31, 2001, no. 1, pp. 1451-1456.

[10] Briscoe, P. Eardley, D. Songhurt, F. Le Facheur, A. Charny, J. Barbiaz, K. Chan, "A Framework for Admission Control over DiffServ using Pre-Congestion Notification," <draft-briscoe-tsvwg-cl-architecture-01.txt>, IETF Internet Draft, work in progress, Oct. 2005.

[11] T. Suthar, "IPv6 - A Service Provider View in Advancing MPLS Networks", *The Internet Protocol Journal*, vol. 8, n. 2, June 2005, pp. 2-12.

[12] S. Chakravorty, "IPv6 Label Switching Architecture (6LSA)," <draft-chakravorty-6lsa-01.txt>, IETF Internet Draft, work in progress, Feb. 2005.

[13] J. Bound, S. Chakravorty, D. Chirieleison, "Binding Packets to FECs in 6LSA," <draft-chakravorty-bcc-fec-00>, IETF Internet Draft, work in progress, Feb. 2005.

[14] http://www-tkn.ee.tu-berlin.de/research/trace/trace.html.