QUALITY OF SERVICE ARCHITECTURES APPLICABILITY IN AN INTRANET NETWORK

Codruţ Mitroi[1]

Abstract

The quality of service (QoS) concept, which appeared initially as a necessity to improve Internet users perception, deals actually with new valences along with information society maturation. At the organisation's level, the Intranet network shall assure in a similar manner as the Internet all kinds of services, which are useful to the organisation's users. Starting from the traditional QoS architectural models, network administrators shall plan and design a QoS architecture, which will map on the organisation's requirements, having at disposal not only own network elements but also communication services provided by other operators.

The aim of this paper is to present, starting from the general QoS models, a comparative study of main advantages and drawbacks in implementing a specific Intranet QoS architecture taking into consideration all kind of aspects (material, financial, human resources), which impact on a good Intranet QoS management.

Keywords: QoS, IntServ, DiffServ, IntServ over DiffServ, VPN-MPLS, Intranet network

1. Introduction

Taking into consideration the large spread of IP protocol in actual Intranet networks, the Intranet QoS architectural models follow closely the main QoS models, which are associated with Internet. The difficulties in Intranet QoS implementation started to appear in the matter of big organisations, which have a great geographically spread and use a WAN Intranet networks based on communication resources or services, which are purchased from communication providers.

According to organisation's specificity and to available financial resources, QoS level in Intranet WAN networks could be improved through a guaranteed bandwidth assurance, which can be done either at phisycal or data link level, like e.g. purchasing guaranteed TDM (E1, E3, SDH) or ATM connections, or at IP level through strictly SLAs with operators, which assure virtually leased connections between organisation's sites.

Main QoS architecture presented in a comparative manner in next sections are *Integrated Service* (IntServ), *Differentiated Service* (DiffServ), *Integrated Service* over *Differentiated Service*, which represent a mix of the two previous models and *Virtual Private Network* with support of MPLS technology (VPN MPLS), because these architectures answer very well to Intranet QoS requirements.

[1] PhD Candidate, Control and Computers Faculty, University POLITEHNICA of Bucharest, engineer, Advanced Technologies Institute, e-mail: cmitroius@yahoo.com

2. IntServ architecture

IntServ model was presented for the first time in IETF RFC 1633 [1], in order to developp a differentiated treatment between network traffic, which assumes a guaranteed QoS assurance and the rest of traffic, which continues to be „best effort“ assured. It’s a complex architecture, which assures however a great granularity QoS level and also an end-to-end QoS, if all network elements, which are involved in service assurance are IntServ compatible.

IntServ defines two service classes, named *Guaranteed Service* and *Controlled Load Service*, which could be associated according to QoS requirements of provided services:

i) *Guaranteed Service* (GS) assures a service delivery with the maximum well defined delay, according to the flow’s specification. This kind of guarantee assures practically the delivery of services, which are constrainedly to respect maximal source to destination delay, like e.g. audio-video services. GS doesn’t assure also a minimisation of delay variation, but controlling the maximum switch delay in network elements it assures that this parameter doesn’t influence the quality of service;

ii) *Controlled Load Service* assures a „best effort“ delivery approximation when the network isn’t congested, taking into consideration some services, which accept a certain level of packet loss or delay tolerance. To prevent congestion, each flow, which requires resources, transmits also certain QoS attributes to network elements, in order to be accepted. According to the available resources within network elements (bandwidth, processing capacity) the flow’s delivery requirement could be validated or not.

In order to process the flows according to the 2 classes, network elements shall get information regarding flows QoS requirements, which are grouped in *flow descriptor*, which contains 2 attributes: *filterspec*, needed for flow’s identification (e.g. according to source and destination address) and *flowspec*, in charge with the flow’s properly specifications. The last attribute is also divided in 2 specifications: *traffic specification* (Tspec) and *Service Request Specification* (Rspec).

Within IntServ a great importance is done by management and control plan, in charge of reserving resources and guarantee flow’s requesting parameters (*Figure 1*).

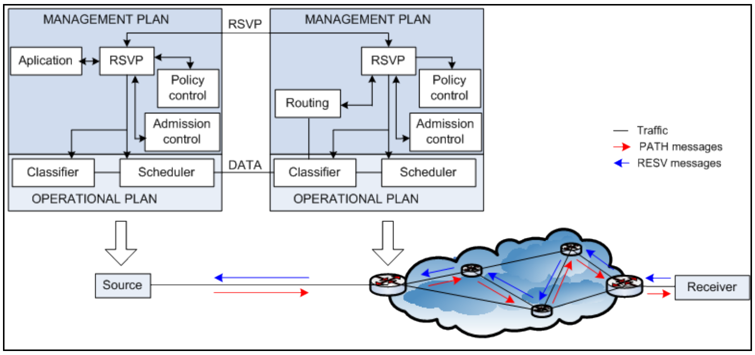

Figure 1: IntServ architecture

Essentially, IntServ architecture is based on an IETF developed protocol – *Resource Reservation Protocol* (RSVP) [2], which builds a link between source and receiver with a guaranteed flow's quality parameters along network path. When receiver requires a service, source initiates a PATH message, which establish a data flow path through communication network together with flow's *Tspec*. The neighbour network element will receive PATH message, will store source address and *Tspec* characteristics and also will insert his own address into the message before passing it to next network element. The process repeats until the message arrives to the receiver, at the end of the process, a path between the source and the destination is being built. All intermediate network elements are informed of the source probability to transmit a data flow with *Tspec* and a potentially flow reservation made by receiver.

After PATH message receiving, the receiver initiates to the source a reservation message RESV, which contains the receiver's required QoS parameters, grouped in *filterspec* and *flowspec*. RESV message will transmit the network's backward PATH message asking to each element to reserve proper resources for data flow processing. This requirement translates into an interrogation of modules in charge of admission control and QoS policy control. If any of these interrogations doesn't confirm, the reservation is rejected and the receiver gets an error message *ResvErr*. If both interrogations are valid, the two attributes are transmitted to operational plan, *filterspec* being processed by classifier and *flowspec* by scheduler. RESV message is forwarded to next network element, where the reservation process will be repeated. When the message arrives to the source, this could begin flow transmission. The guarantee that the flow will be treated according QoS requirements is done by classifiers and schedulers within each network element. RESV message is used only for GS, in case of CLS is enough that source transmits only *Tspec*.

When receiver requested service assumes a multi-source transmission, like e.g. audio- or videoconferences, or collaborative applications, RSVP protocol behaviour seems like a multicast transmission, PATH and RESV messages are mixed on common sections between sources and receivers. From this point of view, RSVP offers a greater flexibility regarding to resources reservation for different sources originated flows, whereas it could be established a distinct reservation for each source or an unique reservation for all flows provided by all sources, which belong to the same session. Another option refers to source selection mode, which could be done through an explicit source list or through an generically indication of all sources involved in a session. From the two previous reservation types result 3 reservation styles [3]:

i) *Fixed filter* (FF) assumes an unique reservation for a source. In case of many receivers, which demand reservations from that source, the network element will transmit to the source a reservation with maximum *flowspec* value for all receivers reservations (*Figure 2.a.*);

ii) W*ildcard filter* (WF) assumes a reservation for all sources involved in a session, network element will transmit to the sources the maximum *flowspec* value for all receivers requested reservations (*Figure 2.b.*);

iii) S*hared explicit* (SE) assumes a reservation for an explicit set of sources, which result from a concatenation between all receivers requested reservations, network element will transmit to the sources the maximum *flowspec* value for all receivers requested reservations (*Figure 2.c.*)

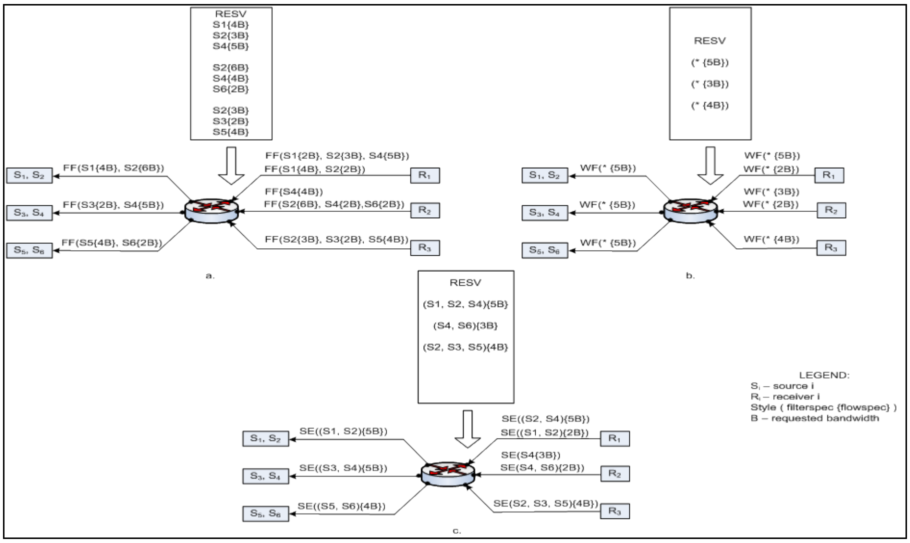

Figure 2. IntServ reservation styles

Main IntServ advantage is the assurance of end-to-end QoS control through a delivery of QoS parameters which have established maximum value and through their monitoring for each flow. This advantage has also a drawback related to a higher complexity of the architecture, the periodically RSVP message transmission requires supplementary processing capabilities from network elements. As the number of flows rise, it's obviously that the architecture scalability suffers.

Difficulties for IntServ architecture applicability in an Intranet network

As results from the previous description, IntServ main benefit is guaranteed class of services, which could assure an end-to-end QoS approach within Intranet network. For the corporate services, which demand very strictly delay, IntServ architecture offers this guarantee, but in some circumstances it could get into situation when this kind of services take control over the links bandwidth and the rest of services will concurrently share a small portion of bandwidth, some of this services requiring a better treatment than „best effort“.

Such an example could be the case of a corporation, which use IP telephony, portal access and an ERP application. IP telephony gets a GS class and the other two services get a CLS class. Corporation owns a headquarter (HQ) and 2 branches (B1, B2), interconnected as follows: HQ and B1 through a 100 Mbps connection and HQ and B2 through a 10 Mbps connection, B1 and B2 are not directly connected. Within HQ are 300 IP terminals, within B1 200 IP terminals and within B2 100 terminals. In order to have a good speech quality a G.711 codec will be used, so layer 2 (Ethernet) throughput is about 87 kbps/call. Between HQ and B1 are estimated a number of 100 simultaneous calls, between HQ and B2 a number of 40 simultaneous calls and between B1 and B2 a number of 10 simultaneous calls. A simple calculation shows that estimated calls required bandwidth is about 9,5 Mbps between HQ and B1 (under 10% of the total link bandwidth) and about 4,4, Mbps between HQ and B2 (over 40% of the total link bandwidth), each of this values being accompanied of about 3% bandwidth needs for associated signalling. It results a necessary of 9,87 Mbps for the first case and 4,48 Mbps for the second. The other services mean needs are 50 Mbps for B1 and 5 Mbps for B2. As we can see, in case of the HQ-B2 link, total bandwidth value for useful services is 9,48 Mbps, with supplementary load produced by portal and ERP signalling. It’s obviously that in certain moments the allocated bandwidth for CLS services will be insufficient, conducting to congestion, which will be treated only in a classical „best effort“ manner.

Previous example shows that before implementing IntServ architecture in an Intranet network a severe analysis must be done regarding GS service weight within all corporate services. A special attention demands the load level of the reservation processing resources, because a high load or a rapid increase of waiting queues storage capacity represent an alarm signal, meaning that network elements doesn’t have specific capacity to support IntServ associated mechanisms behaviour. In this case intranet administrator has to choose between an increase of network elements processing capacity and another QoS architecture identification.

As a conclusion, it can be stated that IntServ architecture applicability in an Intranet environment is strong dependent on guaranteed bandwidth links between all sites which build the organisation.

3. DiffServ architecture

In order to eliminate IntServ scalability drawback, IETF proposed DiffServ model [4], which is based on a differentiated classification of flows, according to QoS requirements, followed by flows treatment through each class specific mechanisms. DiffServ architecture deals with a specific field within IP datagram, named *Differentiated Services Code Point* (DSCP) [5], which resulted through a new definition of previous defined TOS field. From 8 bits are used the first 6, the last 2 bits being further defined as indicators within congestion avoidance mechanisms (*Figure 3*).

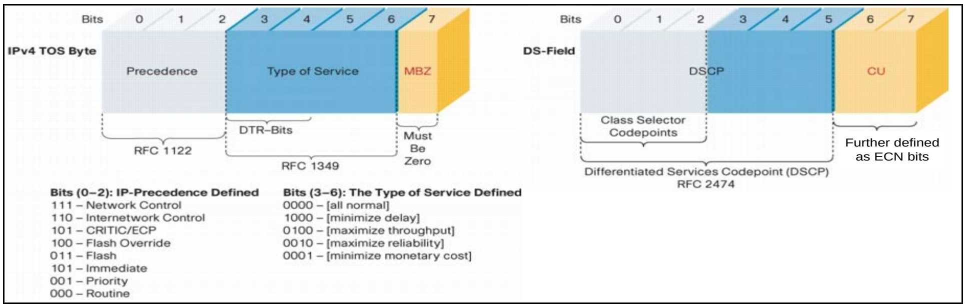

Figure 3. TOS and DSCP field structure comparison

As we can see in the figure, the three most significant bits within DSCP field grouped in *Class Selector* (CS) subfield assure a backward compatibility with *IP Precedence* from TOS field, so that DiffServ-capable network elements could treat also packets, which arrive from non-DSCP network elements. Once DSCP field defined, flows treatment mechanism simplifies through the collection of all packets which have the same DSCP value and their routing according to an identical algorithm, reducing so the required processing capacity in network elements.

A number of 4 packet forwarding mechanisms, named *Per Hop Behaviour* (PHB) are now defined:

i) *Default PHB* is designated to forward packets, which belong to „best effort“ services and assumed a DSCP value equally to 000000. The mechanism offers also an alternative treatment for packets who has a DSCP value which doesn't retrieve in network element's list. This kind of packets will be accepted into the network but treated as „best effort“;

ii) *Class-Selector PHB* is designated to compatibility assurance with IP Precedence and assumes a xxx000 DSCP value in order to permit coexistence between DiffServ and non-DiffServ capable network elements;

iii) *Expedited Forwarding PHB* assures the most rapidly treatment for packets marked with DSCP value 101110. This treatment applies specially to packets belonging to flows which are associated to voice services (IP telephony);

iv) *Assured Forwarding PHB* assures a differentiated treatment of packets according to certain values establishment. There are defined 4 classes AF: AF_1, AF_2, AF_3, AF_4, each of these being divided in 3 subclasses according to packet drop probability (1 – low, 2 – medium, 3 – high)

DiffServ architecture is characterised by a DS domain concept, which corresponds generally speaking to a communication network owned by a single operator and is characterized by uniform traffic forwarding mechanisms. Figure 4 illustrates the main modules within edge, respectively core element, which assure specific treatment for flows, according DSCP field value.

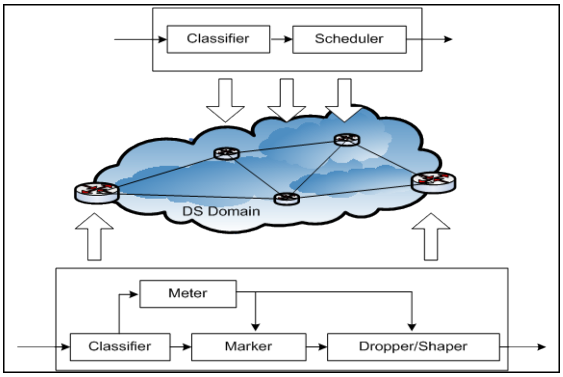

Figure 4. Traffic conditioning mechanism within network elements

Traffic conditioning mechanism contains generally 4 modules:

i) classifier – select the traffic according to DSCP field. It could be some variants with selection based on other parameters like e.g. source and destination address, in this case it's a matter of *multifield* classifier;

ii) meter – measure certain flow's parameters and compare their values with reference values in order to transmit information to the other modules, like e.g. non-conform traffic, which requires remarking or dropping;

iii) marker – in charge of well-defined values packet marking so that further network elements will treat rapidly packet flows;

iv) shaper/dropper – in charge with certain traffic profile building according to a previous well-defined profile. This action could be done in 2 ways, through traffic shaping, which means delay of certain non-conform packets or traffic dropping, which means drop of non-conform packets.

Taking into consideration that core network elements treat an already structured traffic, normally these elements contain only classifier, which selects traffic type and scheduler, which forward selected traffic to egress interface.

Main DiffServ architecture advantages are linked to the reduced complexity of flows processing resources. Even if DS domain edges deal with traffic classification and shaping, these processes a low number of flows comparing with flows number that crosses DS domain, so that edge elements doesn't need a complex processing capacity. Regarding core network elements, these deals only with traffic class identification and traffic forwarding to egress interface, so that forwarding speed is higher compared with IntServ specific mechanisms. Another advantage over IntServ is that DiffServ offers a greater flexibility regarding traffic classification, through a sufficient number of service classes compared with only 2, in case of IntServ.

Main drawback of DiffServ is the inexistence of resource reservations, which could conduct in case of an individual flow to a potentially alteration of end-to-end QoS level. It could exist also some congestion situation when lower priority marked packets could be dropped, conducting so to resources taking over from higher priority flows.

Difficulties for DiffServ architecture applicability in an Intranet network

Together with DiffServ scalability advantage relieves also a certain limitation that could conduct to difficulties in architecture implementation within Intranet network, the most significant are the following:

- DiffServ assumes a relative high investment regarding administration, especially in the field of human resource specialisation;
- in case of a higher number of services with different QoS level it comes to some limitation of flows differentiation possibility, because limited values of x and y indexes in case of AF_{xy} classification;
- when the number of service increases it's more difficult to assure individual QoS guarantee;
- in case of an Intranet network which uses also a DiffServ transport network purchased from an operator it's necessary a very close correlation between Intranet applied classification and classification defined by the operator, so that certain operator's mapping and remarking doesn't produce service alteration;
- insufficient resources within network elements which process level 2 traffic in order to deal with detailed flows classification;

4. Combining the two architectures – Intserv over DiffServ

Starting from previous described architectures advantages and drawbacks it was elaborated an architectural model, which achieves a combination of these, through an IntServ implementation in edge networks and DiffServ architecture maintaining in core network [6]. Essentially it's the question of an assurance through aggregation network of certain traffic processing capacity, which permit the transparently transport of data flows between 2 edge IntServ networks with guarantee assurance regarding these specific quality requirements.

The architecture is based on elements, which are placed at the border between the 2 networks – *Customer Edge* and *Provider Edge*, in charge of formulate, deal and reserve specific IntServ treating requests within DS domain, as follows:

i) in IntServ domain source request is processed normally based on RSVP protocol, according to PATH message attributes;

ii) PATH message is transparently transmitted through DS domain towards IntServ destination domain, where is also normally processed;

iii) receiver send RESV message, which is transmitted through Intserv domain towards CE element;

iv) CE transmit towards PE an admission request, which according to RSVP capable or not DS domain it will allocate the resources in a static or dynamic way;

v) in case of a static reservation, request is translated into a corresponding Diffserv class, according to flow’s specification, which are multifield based;

vi) dynamic resource allocation may be achieve in 3 ways:

- through RSVP requests aggregation case when PE elements interact with elements placed within the network in order to reserve resources within DS domain. This variant offers a dynamic and network topology non-dependent admission control and a high level of scalability;
- through an association of RSVP reservation to each flow, case when the advantage consist in usage of the specific IntServ concept, but also with drawback related to requirements processing resources;
- through a specific admission control mechanism (*Figure 5*), within PE elements translate CE elements requirements towards *bandwidth broker*, which are in charge with management of resources that assure a specified QoS within a DS domain.

vii) finally RESV message arrives to the source through IntServ network, which she belongs;

viii) source begins transmit data flow.

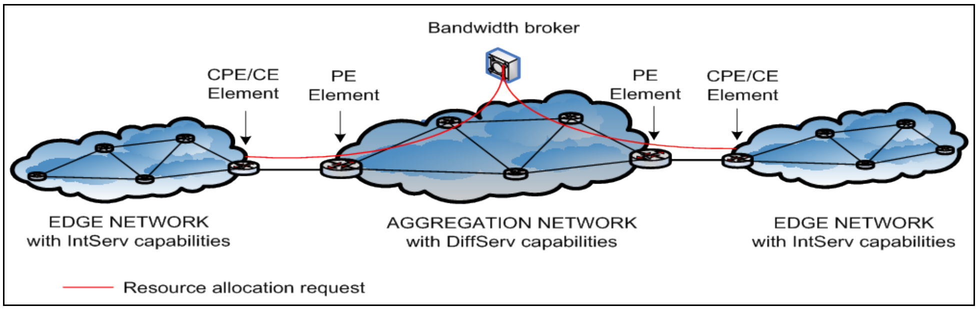
Bandwidth broker
CPE/CE Element
PE Element
PE Element
CPE/CE Element
EDGE NETWORK with IntServ capabilities
AGGREGATION NETWORK with DiffServ capabilities
EDGE NETWORK with IntServ capabilities
Resource allocation request

Figure 5. IntServ over DiffServ architecture in case of dynamic resource allocation by bandwidth broker

Regardless of the way in which the reservation is done at DS domain level, it’s essential that translation of IntServ specific service classes into equivalent DiffServ classes must be done very rigorously, a certain mapping being proposed in [7] and synthesized în *Table 1*.

Table 1. IntServ classes into DiffServ classes mapping

IntServ classification	**Priority**	**PHB DiffServ**

Guaranteed service	–	EF
Controlled load	High	AF_{1X}
	Medium	AF_{2X}, AF_{3X}
	Low	AF_{4X}

Difficulties for IntServ over DiffServ architecture applicability in an Intranet network

IntServ over DiffServ architectural model address especially to Intranet networks which profit by a communication provider infrastructure. Within different organisation's sites Intranet network appears like an access network towards transport infrastructure, which seems like a DS domain or a chain of DS domains. Besides of the advantages regarding traffic predictability relatively to used communication links, this combination could deliver also a range of implementation drawbacks, like:

- a high complexity of design and administration of networks, which combines the two architectural models, with the effect of highest human resource specialisation. When Intranet network is based also on communication provider infrastructure, supplementary it's necessary a closest correlation between the two network's designs and administration;
- model conserve the complexity of *Traffic Engineering* methods, which are applied in case of IntServ architecture, an example being linked to waiting queues explicit configuration (IntServ associated protocols create communication links at control level and not at operational plan);
- it maintains the difficulties occurred at IntServ model regarding the linking elements (applications), which support associated protocols, like e.g. RSVP.

5. Virtual private networks architecture based on MPLS technology – VPN-MPLS

Together with convergent networks development appears also the necessity of traffic separation. Main benefit of traffic separation is linked to different corporate needs, when a common infrastructure is used and their requirements that own traffic shall not interferes with other organisation's traffic. Virtual Private Network concept was developed in order to separate the traffic in a variety of situation, beginning with a communication provider, which offer services to users and following with service delivery in Intranet and Extranet networks conducting to many VPN types: layer 1 VPN (L1VPN), like e.g. *Virtual Private Wire Service* or *Virtual Private Line Service*, layer 2 VPN (L2VPN), like e.g. *Virtual Private LAN Service*, layer 3 VPN (L3VPN) in point-to-point or point-to-multipoint IP configuration.

Actually, more VPN implementations are *Multi Protocol Label Switching* (MPLS) based, which contribute substantially to quality and security of delivered services. MPLS is an architectural model defined by IETF [8], which introduce a new term, *Forwarding Equivalence Class* (FEC), who's in charge of packet forwarding within network. FEC has a 4 octets length, which is divided in 4 fields: label, EXP, S and TTL. (*Figure 5.a.*).

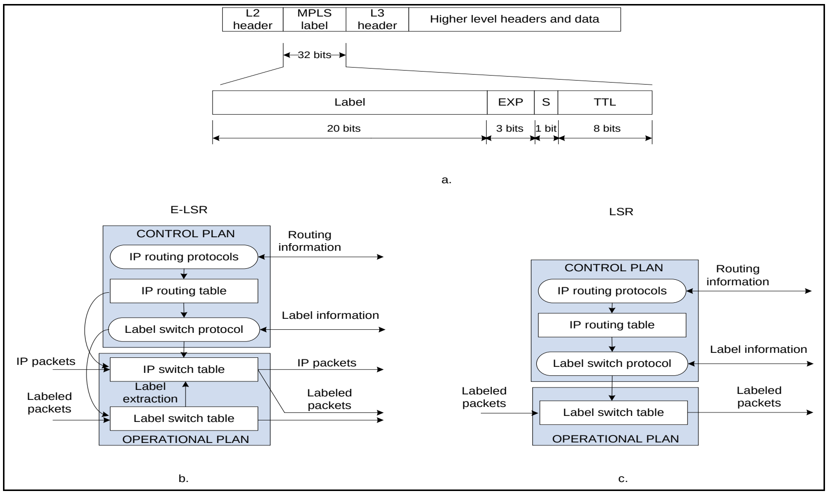

Figure 6. MPLS architectural model

MPLS architecture (*Figure 5.b.* and *5.c.*) is based on 2 important terms: *Label Switched Path* (LSP), which represent the packet path within a network and *Label Switched Router* (LSR), which represent the network element within is implemented a label distribution procedure. LSR has 2 architectural planes, illustrated in Figure 5.b. and 5.c., control plan, in charge of information exchange with other network elements and operational plan, who's responsibility is to switch packets. The two planes interact as follows [9]:

i) label creation and distribution is the process which associate FEC to labels through a specific protocol – Label Distribution Protocol (LDP). LDP mission is to announce and maintain presence of LSRs and to establish and maintain LSR sessions within a LSP. Label distribution is initiated by downstream LSR;
ii) table creation is the process which associate within each LSR a correspondence between labels, FECs and LSR's interfaces;
iii) LSP path creation, which is done in a backward sense as label distribution;
iv) label insertion – E-LSR (edge LSR) interrogate his own label table to identify packet next hop and ask a new label for established FEC. The other LSRs use labels to identify next LSR belonging to specific LSP. When the packet arrives at network egress, E-LSR pop up label and forwards packet to destination;
v) packet forwarding is done according to previous created LSP.

In *Figure 7* is illustrated an Intranet network, which use VPN-MPLS approach. As it can see in order to do better corporate service isolation, each of service use physically or logically separated resources within different organisation's sites. To maintain higher security level when services transit the provider's network, at Intranet A and B edges are 2 MPLS capable aggregation elements. VPN-MPLS construction is based on *VPN Routing and Forwarding* (VRF) [10], which suppose VPN-associated information tables within aggregation elements. This information are exchanged between aggregation elements and service distribution elements. Traffic is forwarded according a combination between IP header information and VPN assignation information contained in VRF tables. The traffic between the two distribution elements is a MPLS traffic, which could be transported on proprietary layer 1 or 2 links, or on leased links, purchased from a provider, when we talk about an Intranet with *MPLS carrier over carrier* capability.

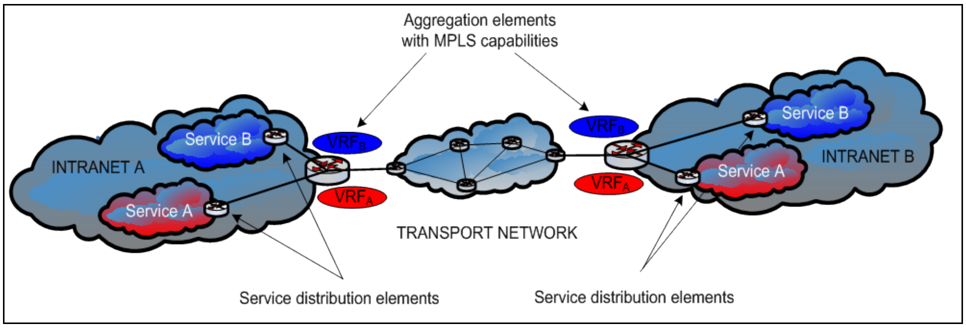

Figure 7. VPN-MPLS Intranet architectural model

Main advantages of MPLS adding technology in VPN construction are scalability, (layer 3 architecture is not-connection oriented, permitting traffic isolation without tunnelling), security through label distribution (users deal only with IP traffic) and QoS capabilities through EXP field, who can deal natively with higher levels QoS marking.

Difficulties for VPN-MPLS architecture applicability in an Intranet network

Intranet VPN-MPLS limitations are linked especially to usage of a communication provider network, main difficulties being:

- the necessity to assure a proper QoS level for different service classes defined within Intranet through a corresponding mapping and traffic measuring, without changing Intranet traffic transparency;
- some limitation in level 2 service class assurance, because insufficient available resources within elements, which process this kind of traffic.

6. Conclusions

This paper’s aim was to present that in an Intranet network, the administrator could deal with a certain QoS architectural models, which bring alongside explicit advantages, but also some drawbacks. Table 2 illustrates a synthesis of the way in which the main characteristics of previous described QoS architectures respond to an Intranet network requirements.

The result of the study confirms the fact that a QoS architecture option shall base on a previous rigorous Intranet design, which act on corporate service types and their QoS characteristics, security requirements in terms of traffic separation, technical and financial resources, which are able to assure services delivery and last but not least human resource, which refers to the IT&C specialists that organisation afford.

Table 2. QoS architectures charactristics versus Intranet network requirements

Characteristic	**QoS architecture type**		
	IntServ	DiffServ	VPN-MPLS
QoS granularity	Per flow	Per class	Per class defined by service provider
Service classes	GS (quantitative)	EF (quantitative)	EF (quantitative)

	CLS (qualitative)	AF (qualitative)	AF (qualitative)
Resource allocation	Dynamically	Statically Dynamically	Statically Dynamically
Signalling	RSVP (host and network element)	RSVP (host) RSVP/COPS/LDAP (bandwidth broker) Isn't necessary for network core element	RSVP associated to IntServ elements (Traffic Engineering, FRR) Doesn't interact with RSVP associated to customers networks
Classification	Multifield (host and network element)	Multifield at edge DS field in the core	Multifield at edge MPLS field in the core
Control	At host/network element level	Edge marking, congestion control in the core	Edge marking, congestion control in the core
Complexity	High	Low	Low

Finally it could be mentioned also that any QoS architecture is based on the operational plan, in charge with effective data flows treating. In order to do this, a well adjusted congestion management mechanisms must be designed [11], which could deal with overloaded network situation.

References

[1] *R. Braden, D. Clark, S. Shenker,* Integrated Services in the Internet architecture: an overview, RFC 1633;

[2] *R. Braden, L. Zhang, S. Berson, S.Herzog, S. Jamin,* Resource ReSerVation Protocol (RSVP), RFC 2205, 1997;

[3] *Paul P. White, Jon Crowcroft,* The Integrated Services in the Internet: State of the Art, Department of Computer Science, University College London;

[4] *S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, W. Weiss,* An Architecture for Differentiated Services, RFC 2475;

[5] *K. Nichols, S. Blake, F. Baker, D. Black,* Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers, RFC 2474;

[6] *Y. Bernet, P. Ford, R. Yavatkar et. al.,* A Framework for Integrated Services Operation over Diffserv Networks, RFC 2998;

[7] *Werner Almesberger et. al.,* A Prototype Implementation for the IntServ Operation over DiffServ Networks, Globecom 2000;

[8] *E. Rosen, A. Viswanathan, R. Callon,* Multiprotocol Label Switching Architecture, RFC 3031;

[9] *International Engineering Consortium,* Multiprotocol Label Switching, web proforum tutorial (trillium), 2005;

[10] *J. Guichard, I. Pepelnjak, J. Apcar,* MPLS and VPN Architectures, Cisco Press, 2003;

[11] *Codruţ Mitroi,* A comparative study of the quality of service (QoS) queue management mechanisms in modern optical networks, Romanian Journal of Optoelectronics, vol. 15, 2011;