Broker Architecture for Quality of Service

Dinesh Kumar Saini, Sanad Al Maskari, R G Dabhade, Sandhya V Khandage and Lingaraj A. Hadimani

***Abstract*— Attempt is made to study the Quality of service framework in this paper. The hierarchical bandwidth broker architecture is proposed in the paper for managing the Quality of Service, with suggestions and improvement in the existing architectures like Common Open Policy Services and DiffServ technologies which are used the context. In the solution proposed it focuses on resource allocation and resource admission control involving Admission control servers located at different levels of hierarchy.**

Index Terms- software architecture, broker, quality of service, internet

I. Introduction

Internet is growing exponentially; end-to- end Quality of Service (QoS) guarantees demand has gained significant importance and priority in the current time. Internet is characterized by applications like voice, video to normal data. These applications are seamlessly integrated into the Internet, it require right kind of Quality of service support in the environment. Currently and traditionally best effort service is provided by the internet. Traffic is analyzed and processed very fast, still timeliness and actual delivery is the concern in the current setup. Quality and quantity of the traffic must be assured under the QoS which provide the assurance for the same. When packet transmission happens end-to end QoS is required and assured while when packet transmission happens in non QoS network liability of QoS guarantee is not there [2], [10].

This paper aims at bringing architecture by proposing improvisation over existing Common Open Policy Service Services model (COPS) [15]. The COPS supports policy control and it is considered as policy control in IP Quality of service environment. In the he model it is aimed to preserve end to end signaling without losing scalability. The proposed architectural model proposes that policy servers must administrate the network stuff which is used in communicating the decisions to policy clients (eg. network elements) and enforces the policy decisions. Network resources and their access is monitored and it concerns the quality of service. Users are allowed to access deferent transport services and the access of this transport services are monitored and administered regularly. The new model is proposed to complement the resource-related admission control defined in the IntServ model with a policy-related admission control which is the need of time.

Edge nodes or the network nodes which provides the policy enforcement points (PENs) is taken into consideration in the present scenario, and policy server (PSNs) acts as logically centralized element. Request is made by the PEN to PSN for policy-related admission control and the PSN make availability of the needed policy decisions in the current status. DiffServ (Differentiated Services), which is an extension to COPS, is hierarchical structure of PEN/PSN supports the resource provisions inside the network elements. Scalability and improved management of resources and admission control is enforced through the hierarchy in the proposed model.

Dinesh Kumar Saini is with Sohar University, Sohar, Sultanate of Oman (dinesh@soharuni.edu.om)

Sanad Al Maskari is Sohar University, Sohar, Sultanate of Oman (sanad@soharuni.edu.om)

Ravindra G. Dabhade is with SND College of Engineering and Research Center, Nasik Maharashtra, India (rgdabhade@gmail.com)

Sandhya V Khandage is with Brahma Valley College of Engineering and Research Inst., Nasik, Maharashtra, India (sandhyav.khandage@gmail.com)

Lingaraj A. Hadimani is with Caledonian College of Engineering, Muscat, Sultanate of Oman (lingaraj@caledonian.edu.om)

II. Problem Analaysis and Specification

Best effort services are covered in the current internet. The current use of internet in the rapid developing commercial activities and actions Quality of Service is a must condition in the current internetworks. Almost all applications are mission critical these days and demand of high quality of service is rising. Voice and video services over the World Wide Web is growing like anything over the non real time applications like ftp and email services. Online real time application with multimedia stuff is growing heavily with high demand of quality of service. All these putting together put additional pressure in the network with real time support in the applications. [10]

Multi-media applications are growing and distributed multimedia applications are becoming ubiquitous in the professional commercial business environment. Performance improvement is also required in the communication platforms with admission control in the networks. Applications such as videoconferencing, online medical diagnostics, distributed games, and video on demand all of them require high performance and better quality of service throughout the sessions established in the communication in these sessions [16].

Bandwidth, delay, jitters and loss rate are some of the parameters considered in the critical applications and most of these parameters are must required in these critical applications. Admission control, traffic policing, resource reservation, packet scheduling, and signaling, all are needed in order to enforce the traffic constraints of a session in the network and network components participate in all of them .

ISBN: 978-988-18210-6-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

Quality of Service

- Service reliability and availability - User connection with internet service must be reliable.
- Jitter – It is delay variation, which is variation in time duration between all packets in a stream taking the same route in the network.
- Delay and latency- Time interval between transmitting and receiving packets between two reference points in the network
- Packet loss rate - Packet discarding rate during transfer in a network; packet loss typically results from congestion in the network.
- Throughput – which can also expressed as peak or average rate is the rate at which packets is transmitted in a network.

Requirement for QoS

- Advanced applications support
- Scalability
- Administrable and controllable
- Measurable service support
- Supports end host operating systems and middleware systems.

III. EXISTING QoS TECHNOLOGIES: OVERVIEW

Integrated Services (Intserv)

The IntServ framework [RFC 1633] supports multiple level controlled delivery services and the respective data packets. The following four components are implemented by integrated services are the signaling protocol like RSVP, [9], the packet scheduler, the admission control routine, and the classifier. Best-effort service is divided into three main categories: interactive burst like Web, interactive bulk, like FTP and asynchronous service like e-mail.

The quantitative service requirements is the main point which is required for guaranteed service and controlled load classes. The guaranteed service and controlled class requires admission control and signaling in the network nodes. Per flow aggregate or per flow is the measure used for these services considering the flow concentration in the networks at that point of time, this in turn asks for flow-specific state in the routers". RSVP [RFC 2205] which is a signaling protocol for applications to reserve resources in the networks. [9].

Other Related concerns with Intserv architecture:

There are still some problems associated with the integrated services architecture which are as follow:

- Huge growth, number of flows increases with the amount of states. Storage and processing of this huge growth put pressure and it is overhead on the routers. The internet core does not approve this architecture and it does not approve this kind of article. There is scalability problem in this architecture.
- The routers requires RSVP, admission control and MF classification and packet scheduling which is very high demand and it is on higher side of requirements
- Guaranteed service requires ubiquitous computing. Controlled –load services support incremental deployment for RSVP even at bottle neck domain and tunneling. Controlled load service and RSVP function supports incremental deployment of controlled-load service. Tunneling is also supported in the domain.
- One more type is the sub classing of best-effort service, which is considered rough in the professional commercial networks and currently flat best –effort service is being offered in the Internet. To have finer-grained sub classing of the best-effort service class in the present scenario can be made profitable.

Differentiated Services (DiffServ)

DiffServ supports and provide range of services with scalability. Scalable framework offers numerous services with quality of service even without supporting per flow state in every router. The whole exercise is done by aggregating flows with similar treatment to the flows [5]. Simple and scalable service differentiation is supported by DiffServ and this is carried out by discriminating and treating the data flows according to their traffic class and flow, this provides a logical separation in the traffic of the different classes. The traffic profiles and negotiated contract are marked by DiffServ flows and used for egress routers. In this DiffServ the core routers only deals the aggregated traffic. [6]

Hierarchical model for network resources support scalability and flexibility in DiffServ:

- Interdomain resource management which is nothing but unidirectional service levels, service in one direction. Traffic contracts which are boundary point between customer and provider traffic are agreed in this unidirectional service.
- Configuration and provisioning of resources within the domain and outside the domain is the main responsibility of Intradomain resource management service provider, service policies are decided at the discretion of the provider.

Traffic classes which provide controlled unfairness and traffic characteristics which are responsible for traffic contract respect are building at the boundaries of the service provider. DiffServ is one way good, it don't put traffic classes or even their characteristics on the service provider. Controlling the balance service demand is also carried out at DiffServ. Service providers control the meters, traffic conditioning and shapes and markets in the networks.

DiffServ code point is a six bit code point which is present in TOS filed of the IP packet. Per-hop behavior (PHB) is examined by DiffServ code point.

PHB is very crucial which defines forwarding behavior in the router for the flow [7].

Egress router is responsible for dropping or marking the out of profile packets by another PHB.

The ingress router also classifies traffic into aggregation based on DHCP. Aggregate profiles are used for policing for profiles. A core router may introduce some burstiness into in-profile traffic because of queuing or increased aggregation [8]. So, the egress may have to shape the traffic so that the downstream clouds do not police this traffic unfairly. It is possible to provide end-to-end services by having a concatenation of multiple DiffServ clouds. The clouds negotiate contracts with the neighboring clouds for the aggregates. These contracts are also characterized by

ISBN: 978-988-18210-6-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

traffic profiles. Bandwidth brokers [13] make admission control decisions. The bandwidth brokers are also involved in configuring the DiffServ modules in the routers. To initiate a connection, the sender first signals its local bandwidth broker [13], [14].

Remaining Issues

DiffServ lays a valuable foundation for IP QoS, but it cannot provide an end-to-end QoS architecture by itself. Effectively, DiffServ markings behave as a lightweight signaling mechanism between domain borders and network nodes, carrying information about each packet's service quality requirements. Another set of below mentioned requirements must be addressed before a workable implementation can be built.

- A set of DS field code points in lieu of standards
- Quantitative descriptions of class performance attributes
- A mechanism for efficiently aggregating the many sources of premium class traffic
- that can converge at transit routers
- A solution to the single-ended SLA problem
- An interworking solution for mapping IP CoS to ATM QoS
- Management tools to facilitate deployment and operation
- See table I for the brief comparison of IntServ and Diffserv in appendix I.

IV. PROPOSED FRAMEWORK: COMMON OPEN POLICY SERVICES –AN EXTENSION

The policy control in an IP quality of service (QoS) environment is basically supported by the COPS protocol [15].The architectural model proposed is decisive in determining that the policy servers effectively administrate the network communicating decision to the policy clients which effects the decisions. The users get an access if the IP QoS is implemented however it is highly important to regulate and administer this access. The COPS model [15] is deployed here complements and has a policy related admission control over the resource-related admission control defined in the IntServ model [12].The IntServ RSVP protocol was primarily considered while defining the admission control architecture and of COPS protocol

In the given architecture, the edge nodes which are the network nodes (edge nodes) express the policy enforcement points (PENs). The policy server (PSN) which is a centralized element in the architecture enforces policies. The PSN receives a request by PEN for admission control policy and then the PSN makes the decision regarding the policy.

COPS are extended by for DiffServ and provisions are provided for resources which are available in PEN/PSN hierarchy. PSN which is logically centralized management center is installed proper configuration which makes decisions for the elements of the networks.

Hierarchical structure of PSN/PENs with nested topology extended from COPS model which provides topology for this architecture with some of the important issues liked to be resolved are

- Scalability maintenance
- Maintenance of End-End Signals
- DiffServ routers interaction with PSN/BB
- Inter Domain Communication.
- Optimum Utilization of Network Resources.
- Better Admission Control mechanism.

A. Architecture Design Specification

Volume and resource in the internet traffic and the router limitation in access link the specified architecture must be scalable and must be deployed in the incremental fashion. The following design principles are adopted in the following architecture:

• Control is hierarchical in nature. All the basic routing domains are part of the networks which get aggregated in the logical domain. Then the larger logical domain gets formulated from these small domains aggregated together and this continues like that. A hierarchical tree with PSN of logical domains gets established in this structure. Messages are treated as client and server with each control unit which is one level height in the tree. Individual PSNs are acting as agents that are responsible for managing total aggregate reservations in the domain for links in the hierarchy at that level. The main parent PSN node is responsible for reserving the neighborly domains. Virtual Overlay Networks (VON) is formed by the nodes hierarchical tree in the WAN topology.

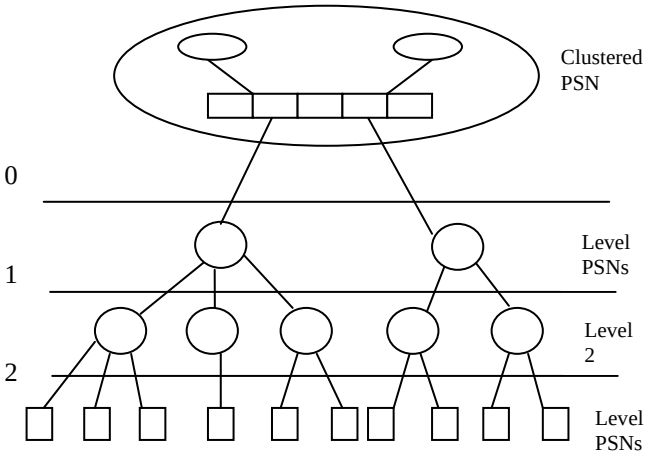

Fig. 1 Hierarchal PSNs

• Aggregation of traffic is considered in this approach which is not directed for individual flows. Per Flow state maintenance is not required in this structure. Total aggregated incoming flow for group ingress ER and it provides a method for assigning a unique flow identifier smartly which helps in tracing a particular flow whenever needed.

Assumptions for the proposed framework:

- Scheduling, packet marking and queue management mechanism services are provided by the networks. The network is very capable in this regards. Packet loss, queuing delay variance are determined by the edge routers.
- Statistics regarding outgoing and incoming traffic is collected and monitored in the routing domains.
- Application which is latency sensitive like multimedia applications like voice and video is divided into special category as "high-priority".

ISBN: 978-988-18210-6-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

B. Hierarchical and Logical Structure of PSNs/PENs

In the proposed architecture network management tasks are divided between various nodes forms a local hierarchy in the ISP domain. Because of this structure efforts and amount of information needed at each node is reduced drastically and it reduces chances of getting failure at any single point at nodes. System characteristics like fault tolerance and redundancy is achieved due to the hierarchical and distributed nature of this proposed architecture. The proposed architecture also supports crash recovery and this can be done by clustering of PSNs nodes at the top most level. With clustering the availability feature of the architecture is supported in the proposed architecture because the top most level of the tree is using clustering.

PSNs are loosely coupled and works as one server to the clients.

In the proposed model, logical domains shown in figure one is obtained by aggregations of administrative and geographic domains (Appendix I). Further aggregation is carried out for these logical domains and it will continue to grow. For the aggregate traffic exchange between multiple domains, the top level PSN node for the ISP works in P2P relationship to regulate the resource allocation properly.

PSN (child) and PSN (parent) are local at one higher level:

Assumption is that non overlapping basic domains are available to the user and unique node to contact for resource reservation.

The PSN responsibility for a basic domain is for the following set of operations:

- The reservations and bandwidth availability with the links is determined by the child PSN in the basic domain. This is one of the operations performed by the PSN. Child PSN keeps track of the amount of existing reservations and the available bandwidth on all the links between edge routers within its own basic domain. Based on the statistics of the intra domain traffic, a local PSN performs resource reservations on the intra-domain links. It also makes local admission control decisions when a new intra-domain request arrives.
- Estimation of the bandwidth required for future is carried out by the local PSN. Aggregation of outgoing and incoming traffic is monitored for this purpose and statistics is collected for the same purpose.
- The top PSN manages resources available in the network on the end to end path adjust the inter-domain reservations accordingly and sends updates to Local PSN on release request send by local PSN. Upon receiving acknowledgements from parent PSN, the local PSN will adapt resource allocation on its edge routers.
- If the existing inter-domain load is less than the allocated bandwidth, new requests will be admitted. Otherwise, the local PSN aggregates inter-domain reservation requests as a single request and forwards it to the parent PSN.
- A particular PSN node aggregate reservation for its children because the children makes the request. PSN also performs advance reservation for inter domain links which resides in the basic domain. There is forwarding of request is also performed for the neighbor logical domain in the connected level; the request is made to the upper level PSN node.
- Parent PSN at the highest level sits on the top of the tree for a particular ISP and adapts trunk reservations between different domains. In addition to general tasks for any PSN described above, the Parent PSN accounts the cost of bandwidth reservation on the internal link. Parent PSN can then choose the optimal route that satisfied the performance constraints while minimizing the total costs.

Admission Control Protocol

This protocol supports client server architecture resources are reserved by clients and resources are released also at the same time from the server control. Transportation of messages in the ACP is done over the TCP and it is done comfortably in this layer of the protocol. Message is handled by request response in the admission control.

Some of the important factors PSN must consider admission request message is as follow:

- Hierarchical and aggregate request Identification
- Egress domain identifier and Ingress domain identifier
- Route information and Requested bandwidth

The PSN to PSN admission response message considers the parameters which are Aggregate request Identification and Response (ACK_NAK) acknowledgement.

The parameters which are carried in release request and release response is the exactly same as admission release and response request. The Request Identification is used to correlate a request with the response in this case.

All the information is aggregated like per edge device and per link in the admission control server and the proposed PSN-RA support all these. Edge router also maintains some information like per flow information. The edge router maintains per flow soft sate receiving from RESV message which is generated by RSVP-RESV messages.

The hard state is maintained which is resource allocation with ACP admission request message and it get de-allocated

.

.

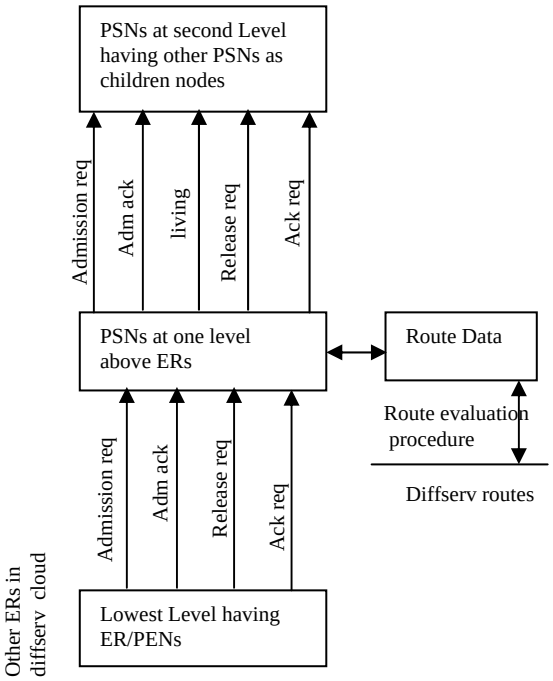

Fig. 2 Admission control procedure

ISBN: 978-988-18210-6-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

In the Fig. 2 which explains the conceptual architecture of When release request is made. With this it support scalability and helps in reduction in the interactions of edge router with PSN. In the paper edge routers and PSNs procedures are described and all the data required for the same the PSN and the control functions in the PSN and procedure to handle RSVP messages and control procedure for the admission control. It also describes two modules that are PSN Functions which are Processor for PSN and resource allocation data so PSN_processor and RA_data are the two main module.

PSN processor has to do comparison between the resource requested and the bandwidth availability for all links for computing request which is made by admission request message.

Edge router gets the message when the results computed from the admission request message. It can accept or even can reject the request and this information must be send to the edge router. Links usage array send updating message if the PSN_processor accepts the request. The resource is being allocated and it will continue with it unless it is de-allocated with release request message. Edge router maintains the list of resources allocated because Edge router is responsible for failure handling in the edge devices. If any crash happens in the edge device it leads to inconsistency in the link usage array on real time basis. To avoid the failures ER on continuous intervals send a message to PSN so that failures can be avoided. PSN has to release the resources when ER stops working or not behaving properly. In the given scenario RA_data module plays very important role which represent the database of the resources which are allocated. Link usage array is maintained in the DiffServ and the DiffServ acts as cloud as a global like between the total bandwidth and available bandwidth. Each ER has specific usage information, the information about the resource used with edge router over the particular link. Cache memory is maintained for the paths of the ERs and Rout _Data can also be asked and this information is not easy to store so it require cache memory. This cache is refreshed, using the route discovery procedure in the ERs over the continuous intervals. This information is compared with actual path taken by the routs on continuous basis. Session information, Flow _spec and filter _Spec information are stored in SLA _Data module in the soft state and all the information about its routing path into the Diffserv cloud. ER receives a RSVP RESV message related to a new flow, ACS will get a message about the admission request. The ED forwards this RSVP RESV message towards the sender or a RSVP RESV_ERR message towards the receiver, it can be both ways. When a “refresh” RSVP RESV message is received, only the state in the SLA_data is refreshed in the continuous intervals. When a timer gets expired or When a RSVP RESV_TEAR message is received, a release request message is sent to the PSN. When rout path is changed the old path resources must be released and a new request is made for the admission control for the new resources.

Algorithm for admission control

At any point of time a particular node can act as PSN as well as PEN. i.e. at every level except lowest level each controlling node will have two routines running. One is

Server routine and another is Client routine. Job of Server routine is to coordinate the s control procedure depending upon resource availability, it decides to acknowledge or reject any particular request.

Whereas Client routine forwards the request messages that it receives either from application or from its child nodes and wait for decision from its parent node to act further (fig. 3)

It will check available bandwidth by looking reserved bandwidth in the link usage array vector and subtracting it from total bandwidth in a particular link available in the

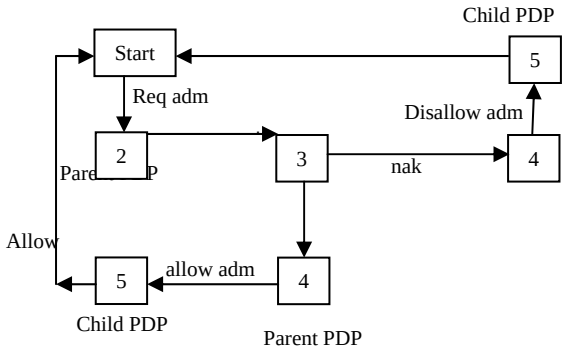

Fig. 3 State Transition diagram showing various states of Admission Control Procedure

two dimensional array. Then PSN compares the available bandwidth with requested bandwidth. If requested bandwidth is lesser then available bandwidth then it will send acknowledgement to flow and update the link usage array vector.

But if the destination is outside the scope of its own domain then local PSN will send aggregated request to its parent PSN. The parent PSN upon receiving the aggregated requests forwards the request to its next child node which uses the attached list for finer-grained admission control in its own domain.

Then if the destination local PSN accepts aggregate request, then parent PSN checks if there is enough resources between inter sub-domain links to satisfy the request. If parent PSN founds enough resources to satisfy the aggregate request then it will send acknowledgement to its local PSN(i.e. from where the request came).

See fig. 3 for State Transition diagram showing various states of Admission Control

V. CONCLUSION

As discussed in the paper it is found that QoS is one of most important aspect in the current IP networks as a whole. In the paper Admission control layer is studied in detail and it is proposed to have policy based admission control. Broker architecture is implemented in multi layer admission control which handles all types of request like reservation request, policy based admission control and configuration in the network resources. Top down design approach is implemented with broker in managing network resources and elements of the networks. One of the aspects like distribution and redistribution of resources and network

ISBN: 978-988-18210-6-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

elements are implemented using policy control according to broker architecture. COPS architecture is extended with broker architecture in hierarchical manner for better and effective management of network resources. Broker is like an agent who acts as control agent PSNs which are distributed all over the networks.

REFERENCES

[1] Laurent Mathew et al., "The Internet: A Global Telecommunications Solution", IEEE Networks, July/August 2000.
[2] Xipeng Xiao and Lionel M. Ni, "Internet QoS: A Big Picture", IEEE Network, March/April 1999.
[3] G. Huston, "Next steps for the IP QoS Architecture", RFC 2990.
[4] R. Yavatkar et al., "A Framework for Policy-based Admission Control", RFC 2753, Jan. 2000.
[5] D. Black et al., "An Architecture for Differentiated Services," RFC 2475.
[6] K. Nichols et al., "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers," RFC 2474, Dec. 1998.
[7] V. Jacobson et al., "An Expedited Forwarding PHB", RFC 2598, June 1999.
[8] J. Heinanen et al, "Assured Forwarding PHB Group," RFC 2597, June 1999.
[9] R. Braden et al., "Resource ReSerVation Protocol (RSVP) — Version 1 Functional Specification," RFC 2205, Sept. 1997.
[10] E. Crawley et al., "A Framework for QoS-based Routing in the Internet," RFC 2386, Aug.1998.
[11] Bhatti, S.N.; Crowcroft, J., "QoS-sensitive flows: issues in IP packet handling," IEEE Internet Computing, July-Aug. 2000.
[12] Bernet, Y.; Yavatkar, R.; Ford, P.; Baker, F.; Zhang, L.: A Framework for End-to-End QoS Combining RSVP/Intserv and Differentiated Services. Internet Draft, IETF, 1998.
[13] Internet2 QBone Bandwidth Broker Advisory Council, www.internet2.edu/qos/qbone/QBBAC.shtml
[14] R. Neilson, J. Wheeler, F. Reichmeyer, and S. Hares, editors. A Discussion of Bandwidth Broker Requirements for Internet2 Qbone Deployment. Internet2 Qbone Bandwidth Broker Advisory Council, http://www.merit.edu/working.groups/ i2-qbone-bb, August 1999.
[15] Boyle, J.; Cohen, R.; Durham, D.; Herzog, S.; Rajan R.; Sastry, A.: The COPS (Common Open Policy Service) Protocol. Internet Draft, IETF, 2000.
[16] Rahul Banerjee: Quality of Service and IPv6: Design and Implementation Issues, IPv6 global Summit, Bangalore, January 2008.

TABLE I
COMPARISON BETWWEN TWO ARCHITECTURES

	IntServ	**DiffServ**
Differentiation for service Coordination	End -to- End	Peer hop which is local
Scalability	Flows are limited	Independent of no. of flows
Network Accounting	Flow characteristics is considered	Class usage is considered
Granularity of service differentiation	Individual flow	Aggregated flows
State in routers (eg. scheduling buffer management)	Per flow	Per aggregate
Traffic classification basis	Several header fields	DS field
Signaling protocol	Required (RSVP)	Not required for relative schemes
Type of service differentiation	Deterministic or statistical guarantees	Absolute or relative assurance
Interdomain Deployment	Multilateral agreements	Bilateral agreements
Admission control	Required	Required for absolute differentiation
Network management	Similar to circuit switching networks	Similar to existing IP networks
Inter domain deployment	Multilateral agreements	Bilateral agreements

ISBN: 978-988-18210-6-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)