IPV6: Quality of Service: Support for real-time traffic, priority and flows

Achala Varshney[1],Ajay Rastogi[2]

[1]MCA Lateral, College of Computing Science Information Technology, Teerthanker Mahaveer University MORADABAD

[1]achalarythem@gmail.com

Abstract— **The deployment of IPV6 will progressively be made in an orderly coexistence with IPV4 which will be displaced. With the strong pressure of communications in our lives, devices used for work or for convenience, are more likely to be designed to connection each other in order to achieve a quick and capable way through the network, or better said, the internet. Communications between the different elements of the network uses a protocol called IP. To face with collapse of ipv4 addresses, the new version of this protocol, IPV6, occur as a feedback to the problem.**

In this article issues are addressed such as transitional preparations and implementations proposals for its design to make certain backward compatibility and coexistence between systems. The work presents statistics and organization worldwide which promote a beneficial and optimal transition to IPV6.

Current IP networks provide better traffic delivery effort providing partial guarantees in terms of "Quality of Service". In this paper we describe the mechanisms and architectures that are used to provided QoS on a network.

Keywords— **Include at least 4 keywords or phrases**

I. Introduction

The IPv6 header has a priority field which enables the starting place to classify the data transmits and delivery priority of each packet comparative to other, packets from the same starting place. There are two separate priority-related individuality for each packet. A packet is first classified as being part of traffic for which the starting place provides congestion control or not, and is then assigned one to eight absolute priority levels within the classification.

II. Congestion Controlled Traffic

This refers to traffic which the starting place reduces in response to congestion, for example TCP. If there is congestion in the network, TCP segment will take longer to reach your destination at their destination, and acknowledgments from the destination.

Take longer, too. As a result, the starting place reduces the number of segments it generate. As congestion increases packets may have to be unnecessary by routers. For a unnecessary packet, the acknowledgment does not arrive at all and it has to be retransmitted.

IPv6 defines the following categories of congestion-controlled traffic in decrease priority:

A. ***Internet control traffic:***

Such as router updates etc. This is the most significant traffic to deliver in times of congestion as it contains information about traffic condition which is used to update routes and is used by network management to remove congestion.

B. ***Interactive traffic:***

Client online to congregation (host) connection. Here client efficiency depends on reaction time.

C. ***Attended bulk transmit*:**

move of large volumes of data where the client is usually waiting for transmit to complete transmit of large volumes of data where the client is usually waiting for transmit to complete.

D. ***Unattended data transmit:***

Transmit initiated by a client but not expected to be delivered instantly.

E. ***Filler traffic:***

Estimated to be handle in the backdrop in the nonexistence of higher-priority traffic.

F. ***Uncharacterized traffic:***

If no supervision about priority is given, then lowest priority is assigned.

III. Non-congestion controlled traffic

This is traffic for which a constant data rate and a constant delivery delay are attractive. For example, real time audio and video, for which it makes no sense to retransmit a unnecessary packet and the delivery flow, should be smooth. For this type of traffic, priority is assigned on the basis of

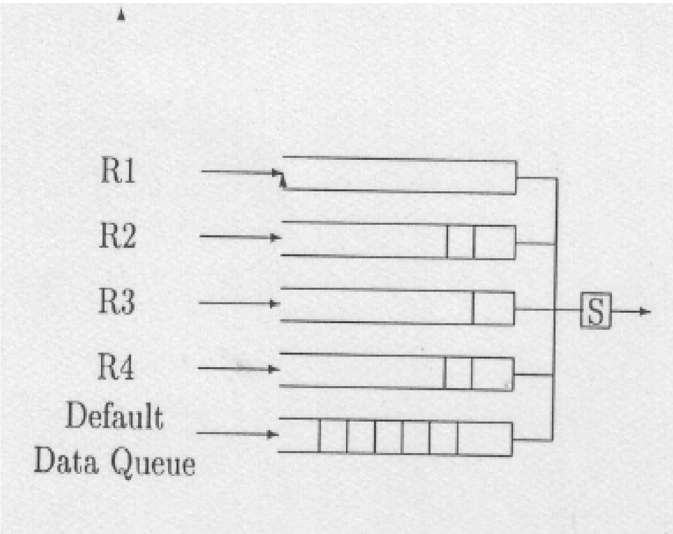
How much the quality will improve in the face of some dropped packets?

There is no priority relationship between congestion controlled and non-congestion controlled traffic. Priorities are absolute only within each grouping.

IV FLOW LABEL

The IPV6 standard defines a flow as a sequence of packets sent from a particular starting place to a particular destination for which the starting place desires special handling by the intervening routers. A flow is uniquely identified by a combination of a starting place.

Address and a non zero flow label. All packets that are part of the same flow are assigned the same flow label by the starting place. From the starting place's point of view, a flow typically will be a sequence of packets generated from a single application instance at the starting place and having the same transmit service requirements. From the router's point of view, a flow is a sequence of packets that share attributes which affect how they are handled by the router, like path, restarting place allocation, discard requirements and so on. Routers may treat packets from different flows in different ways, such as by requesting different qualities of service from sub network.



Flows basically provide for a better quality of service that the client pays for. In traditional packet switches, when a packet is received. it is passed to the routing module, which then decides on which outgoing line the packet should be forwarded. If the line is available, the packet is forwarded immediately and if not, it must wait in the queue. In order to make sure higher quality of service for real-time communication, we must make sure that the service rate for real-time data is higher than the arrival rate (queuing theory terminology). To achieve this, we can have one queue for each real-time communication and one default queue for all packets.

In the Figure we see four real-time flows. The flow label together with the starting place address is used to assert which packets belong to what flows. Packets not recognized as part of one real-time flow are part of the default data queue. It

will never suffer from unpredictable queuing delays or experience congestion. The data queue will be served on a best effort basis and receive only whatever capacity is left after servicing real time flows.

IV. QUALITY OF SERVICE

A flow is described using a token bucket and given the description of a flow, a service element (a router, a subnet etc.) computes various parameters, describing how the flow's data will be handled. By combining the parameters from the various service elements, the maximum delay a piece of data will experience, when transmitted via that path, can be established To achieve a bounded delay requires that every service element in the path supports guaranteed service in its backbone and provide guaranteed service

Between customers because a delay bound is produced, it has two parts: a fixed delay (transmission delays) and a queuing delay. The fixed

Delay is a property of the chosen path, which is determined not by guaranteed service but by the set up mechanism. Only queuing delay is determined by guaranteed service. And the queuing delay is mainly a function of two parameters: the token bucket and the data rate (R) the application requests. These two values are completely under the applications control. An application can usually accurately approximation, a priori, what queuing delay guaranteed service will likely promise. Additionally if the delay is larger than expected, the application can modify its token bucket and data rate in predictable ways to achieve a lower delay.

VI. RESTARTING PLACE RESERVATION PROTOCOL (RSVP) AND (FLOWS)

The key assumption of RSVP ([12], pp 129- 130) is that restarting place reservation will mostly be needed for multicast applications like high speed video transmission. Such applications usually have a large number of receivers that may be experiencing very different transmission conditions. RSVP is therefore a receiver driven protocol. Receivers decide from which starting place they want to receive and how much bandwidth they want to reserve and pay for. The protocol

o Starting places enable reservation by regularly sending PATH messages alongside regular data packets.

o Routers learn about ongoing communications through these messages.

o Receivers specify the starting place from which they want to receive, bandwidth etc. by sending RSVP messages on the network.

o These messages are sent on the reverse path marked by PATH messages so that restarting places are reserved on the same link that is used to propagate data.

. VII. CONCLUSIONS

In this article issues are addressed such as transitional preparations and implementations proposals for its design to make certain backward compatibility and coexistence between systems. The work presents statistics and organization worldwide which promote a beneficial and optimal transition to IPV6.

Current IP networks provide better traffic delivery effort providing partial guarantees in terms of “Quality of Service”. In this paper we describe the mechanisms and architectures that are used to provided Quality of service on a network.

REFERENCES

[1] Stallings W. [1996], IPv6: The New Internet Protocol, http//www.comsoc.org/pubs/surveys/stallings/stallings-orig.htmlfgfen

[2] C. Perkins and P. Bhagwat, [1993], "A Mobile Networking System Based on Internet Protocol [IP]", Proceedings Usenix Symposium Mobile and Location Independent Computing, August, Usenix Association, pp 69-82

[3] Huitema C. [1996], IPv6: The New Internet Protocol, 1st Bdition, Upper Saddle River, NJ:Prentice Hall.

[4] Dowden D. C. , Gitlin R. D. , Martin R. L. [1998], Next-Generation Networks, Lucent Technologies Journal, Lucent Technologies, December. Steve King, Ruth Fa*, Dimitry Haskin, Wenken Ling, Tom Meehan; Bay Networks;

[5] P. Bhagwat, C. Perkins and S. K. Tbipathi,[1996], "Network Layer Mobility : An Architecture and Survey", IEEE Personal Communications, Vol 3, No 3, June, pp 54-64.

[6] • J. Postel [1981], Internet Control Message Protocol (for IPv4), Darpa Internet Program Protocol Specification, RFC 792, September http: //www.isi.edu/in-notes/rfc792.txt.

[7] Douglas E. Comer [1999], Computer Networks and Internets, Prentice-Hall, Inc., pp 295-296

[8] Perkins C., [1998j "Mobile IP : Design Principles and Practice", Addison-Wesley Longman, Reading, Mass

[9] A. Karnik, “Performance of TCP congestion control with rate feedback: TCP/ABR and rate adaptive TCP/IP,” M. Eng. thesis, Indian Institute of Science, Bangalore, India, Jan. 1999.

[10] J. Padhye, V. Firoiu, and D. Towsley, “A stochastic model of TCP Reno congestion avoidance and control,” Univ. of Massachusetts, Amherst, MA, CMPSCI Tech. Rep. 99-02, 1999