PCN
Internet-Draft
Intended status: Informational
Expires: April 17, 2007

J. Babiarz
K. Chan
Nortel
G. Karagiannis
University of Twente
P. Eardley
BT Research

October 14, 2006

SIP Controlled Admission and Preemption
draft-babiarz-pcn-sip-cap-00

Status of this Memo

Copyright Notice

Abstract

This framework defines a method of providing Explicit Congestion Control to real-time inelastic traffic like voice and video through the use of session admission control and preemption mechanisms. This approach uses the Pre-Congestion Notification Marking (PCN) [1]

mechanism. PCN marking is deployed in routers to measure and convey two levels of onset of congestion with the SIP controlled endpoints responding to the marking. This approach is different from what is defined in An edge-to-edge Deployment Model for Pre-Congestion Notification [3], as here the admission and preemption control function resides in the application (either in the endpoint or the application server that controls the endpoint. This framework is focused on using Session Initiated Protocol (SIP) as the application signaling protocol but other application signaling protocols could be extended for this purpose.

Table of Contents

1. Introduction

Converged networks that are configured for multiple-services are normally engineered to provide the required quality of service using Diffserv [5], [6] technologies. Real-time inelastic traffic (e.g. voice) is normally configured to use the Expedited Forwarding (EF) PHB [8] to provide very low delay, loss and jitter transport. To stay within that engineered quality of service, and to ensure a quality of service level for that traffic, some type of admission control mechanism is necessary. Due to the sensitive nature of voice and other telephony applications (video conferencing), freely allowing these types of sessions onto a network where resources are limited can quickly lead to degradation of service that users may not tolerate. And in a packet based network, the degradation is not limited only to the offending flows, but all real-time flows within the same service class [12] are impacted.

This document proposes an admission control solution based on Pre-Congestion Notification (PCN) Marking [1] process for real-time traffic and probing during session setup. The gist of the solution is that routers at selected points in the network, where congestion is most likely to occur, measure traffic per service class and perform PCN Marking [1] based on observed traffic against two levels, "admissible rate" and "supportable rate". For admission control during session setup, a probing mechanism is used between endpoints to verify bearer path connectivity and the traffic level along the path. SIP endpoints process information that is obtained during probing and make session admission decisions based on application service policy.

PCN marking offers two levels of pre-congestion indication, an "admissible rate" and a "supportable rate". This adds flexibility to admission control decisions. The admissible rate indication essentially warns that network resources have reached the pre-configured traffic limit for admission of new flows but that there is still some available bandwidth. Using this information, applications can decide to filter out certain types of sessions for admission in favor of other types. For example, normal voice flows might be denied, while higher precedence calls such as E911 emergency voice flows are admitted. Whatever the admission control policy, PCN marking enables some discernment in the decision making rather than wholesale denial of sessions.

Normally flows are only admitted as long as the admissible rate is not exceeded, but the admitted traffic on a link can exceed the supportable rate, e.g., due to changing flow behavior or due to redirected traffic after link or router failures. In such a case, corrective actions may be taken to reduce the traffic on the link,

e.g., by preempting already admitted flows in order to restore the QoS to the service class. The preemption procedure is as follows, SIP endpoints monitor PCN markings of media packets from already admitted flows and when they see PCN marking indicating that traffic is above the supportable rate, they invoke their session preemption policy. This session preemption policy is local to the application. The preemption policy can even be "take no action" at jurisdictions where preemption is not allowed.

This proposed framework for session admission control and preemption does not introduce a significant amount of overhead to the network. The PCN marking can be implemented using simple packet metering techniques without the need for flow state information.

2. Requirements Notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [4].

3. Terminology used in this Document

Here we provide a brief definition of the terminology used in this document as it applies to the PCN work. A more complete definition and explanation of terminology for this framework is provided in Section 7.

- PCN - Pre-Congestion Notification is a method for detecting the onset of congestion (before any packets are significantly queued or lost) and signalling to the endpoints via packet marking of the IP header. This method is applicable to real-time inelastic traffic. The marking of the IP header will be defined in Pre-Congestion Notification Marking [1].

- ECN - Refers to the use of the standardized two bit field in the IP header that is used for signalling Explicit Congestion Notification [7]. In this framework the ECN field maybe reused to signal two levels of Pre-Congestion Notification Marking [1].

- Admissible Rate - A bandwidth or resource threshold configured in network elements that when crossed marking of packets occurs to indicate that additional flow/session should not be admitted. In Pre-Congestion Notification Marking [1] this is called the "configured-admission-rate".

- Supportable Rate - A bandwidth or resource threshold configured in network elements that when crossed marking of packets occurs to indicate that on-path traffic has exceeded the configured service level. Normally, this would be before any significant queuing or packet loss occurs for traffic being forwarded by this service class. In Pre-Congestion Notification Marking [1] this is called the "configured-pre-emption-rate".

- Service class - By service class we mean a grouping of packets belonging to one or more applications or services that generated traffic with similar characteristics and requiring similar QoS treatment. See RFC 4594 [12] for details.

- Endpoint - SIP controlled media device such as a phone, a media gateway or a multi media terminal.

- Admission Control - It is the action of blocking the adding of new flows or sessions in to the network in the attempt to prevent overload condition.

- Preemption - During an overload condition, it is the action of removing excess traffic by randomly terminating flows or sessions. Some solution may have additional policies where termination of flows or sessions is performed in some controlled hierarchical fashion.

4. Operational Overview with SIP

In the following sections, we address "how this framework is put together" by providing an operational overview using SIP. We provide an overview of the pre-congestion measurement and packet marking mechanism, and leave the details and PCN marking syntax and metering marking behavior definition to Pre-Congestion Notification Marking [1] draft. The SIP protocol provides a mechanism for two or more endpoints to join a session where they exchange media packets between each other. SIP messages control the setup and tear down of the session. The following subsections provide an operational overview for the SIP application environment, with description of session admission control and session preemption respectively.

4.1. PCN Metering and Marking Overview

Routers in the network are configured to meter traffic per service class (DSCP or group of DSCPs) and when the aggregate metering rate exceeds the configured rate, perform PCN marking of packets being forwarded. The metering and marking policy may be per DSCP or group of DSCPs. The routers meter traffic against two configured rates,

"admissible rate" and "supportable rate" whereby the supportable rate is larger than the admissible rate. The "supportable rate" normally is less than the maximum service rate (but may be equal) for this service class, which itself is less than the physical links maximum line rate. The metering and marking algorithms are configured such that they provide optimal response to changing traffic levels without reacting too fast or too slow. Details of metering and marking can be found in Pre-Congestion Notification Marking [1]. Note, in Pre-Congestion Notification Marking [1], "admissible rate" is referred to as "configured-admission-rate" and the "supportable rate" is referred to as "configured-pre-emption-rate".

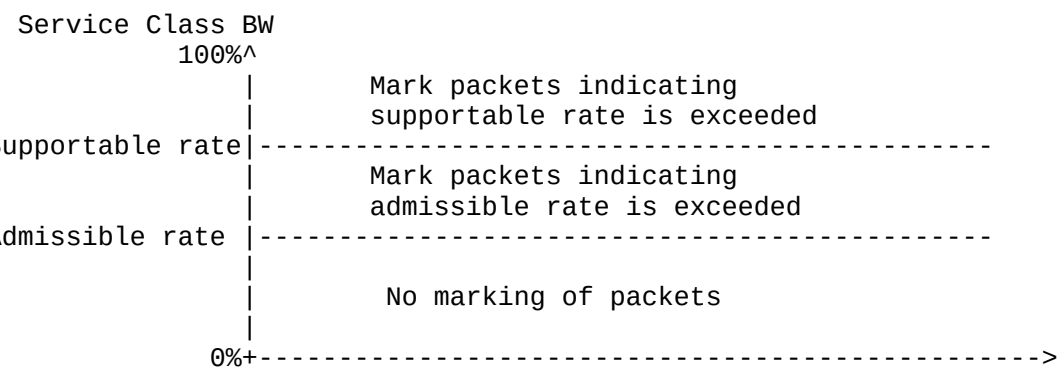

Figure 1: Packet Marking by Routers

We believe that the above described measurement concept and marking behavior can be extended and applied to other transmission technologies such as radio transmission. For example, a wireless access node may measure radio resources that are currently used for traffic transmission using "rise over thermal" measurement method and mark packets as per the defined thresholds and marking behaviors. It is believed that the measurement method or algorithm that is used for measuring forwarding resource and bandwidth utilization may be different and do not need to be standardization as long as they conform to the marking behavior.

4.2. Probing Mechanism

The probing mechanism is an application level function residing in the application control endpoint (this can be implemented in an end user device, a phone, a media gateway, a multi media terminal or a proxy for the end user device). The probing mechanism is designed to verify:

- Media packets can be sent between the application endpoints.

- The current on-path traffic level, with inclusion of the probe traffic, does not violate the required QoS of the service class.

The probing mechanism is used during the session setup process prior to when real media flow packets are allowed to be sent. During the session setup process, the probing mechanism provides these additional benefits:

- Should some method of route control such as ECMP (Equal Cost Multi-Path) be used, probing verifies the path that real media packets will take.

- During the session admission phase, probing can also be used to detect packet loss which also can be used as additional information input to the admission decision.

- Probing effectively can control over admission during "flash calling events".

The probing mechanism being proposed is unidirectional UDP based packet flow with IP source and destination addresses and port numbers matching media packets. For bidirectional flows (VoIP) probing needs to be performed in both directions.

With the probing mechanism being an application function, much of its configuration and detail functional goals are application dependent. The following are some considerations when the application is VoIP using SIP:

- How closely does the probe traffic need to be to real media traffic? Our current simulation and analyses indicate the admission control results can be achieved when the probing flow only consumes a percentage of what the real media traffic would have used if it was admitted.

- When should the probing be stopped during the admission control process? Our current simulation and analyses indicate the probing should be continued during the admission control process until the application level connection is completed, that is until the phone is answered. Our simulation results show that this use of the probing mechanism can control the probability of over admission of flows during "flash calling events" (large number of users placing calls at the same time). Hence, it effectively eases the requirement for having a large bandwidth separation between admissible and supportable rate levels.

The simulation work indicated above is part of another document to be published. More detail will be provided in that future document.

The complete definition of a probing method that can be used for admission control needs to be agreed upon. And, as being part of the application function, the probing mechanism depends on and needs to be coordinated with its application usage.

4.3. Session Admission Control

In this approach admission control uses a probing mechanism to determine whether there is available bandwidth for a new session. The endpoints of a session perform this probing which occurs during session setup. Depending upon results of the probing mechanism, the session will be either admitted or denied. This decision can be made within an endpoint, or by a session control server.

Using SIP, the session setup procedure begins with the calling endpoint sending an "INVITE" to the called endpoint. The called endpoint must send a response. If it is busy, it will send a response indicating it is busy. Assuming that it is not busy and doesn't answer automatically, it will typically alert the user and send a response indicating that it is alerting the user (e.g. 180 Ringing). When the user responds, it will send a final (non-failure) response to the calling endpoint. The calling endpoint will acknowledge that response and media packets will begin to flow between the two endpoints. Notice this is a highly simplified overview of SIP for the purpose of this example.

Admission control decisions must be made prior to the point where the called endpoint alerts the user or sends a final non-failure response. This implies that the SIP protocol itself must accommodate this decision. The mechanism for doing so is called a precondition and its operation is described in "Integration of Resource Management and Session Initiation Protocol" RFC 3312 [10]. Basically, a response from the network about network resource usability and path connectivity status is a precondition to allowing the session setup process to continue. The called party interrupts its normal call processing before alerting the user and initiates a procedure to determine the network resource usability status.

The procedure in this example uses a pre-media probe flow for determining the status of the network. A probe flow consists of small UDP packets that have no real-media information, possibly transmitted at the codec packet time interval, with the endpoints monitoring for PCN marking in IP header of the received packets. Routers along the path perform PCN marking of the packets to provide path utilization levels. Because probe packets have the same source/ destination IP address and port information as the media packets, they will be forwarded along the same path as the media packets. Because the path through the network for media packets going in each

direction may be different, and loading of each link may be different in each direction, probing must take place in both directions for bidirectional flows.

Details of the interaction between probes sent through the network and SIP will not be given here. However, a high level walk through is provided to illustrate the process. The walk through assumes that probing is unidirectional. That is, each device independently initiates probing as soon as it knows the destination address of the other endpoint. The number, frequency and size of probe packets to be sent falls outside the scope of this document. Suffice it to say that probe packets are sent in each direction to determine network status before call processing at the called party proceeds to the point of alerting the user. Probe packets may be sent in both directions until user answers the phone or the originator terminates the call attempt.

When a new session is being setup, SIP signalling is used to exchange endpoint capabilities, including whether the endpoints are PCN capable. The following is an overview of a method that can be used for admission control of new session using the PCN method of providing network's ability to support or not to support additional traffic. Figure 2 shows the sequence of events that would take place:

1. Alice, the session originator, sends INVITE sip:bob@abc.com message to Bob, indicating that the precondition [10] for PCN needs to be met before alerting begins.

2. Upon reception of the INVITE message, Bob starts sending probe packets to Alice. As well, Bob generates and sends a 183 Session Progress SDP2 (Answer) to Alice providing Alice sufficient information so that Alice can sending probe packets to Bob.

3. Alice, upon reception of 183 Session Progress SDP2 (Answer) message, starts sending probe packets to Bob.

4. Alice monitors the PCN markings of probe packets sent by Bob and sends the received PCN marking information to Bob in UPDATE SDP3 message.

5. Bob monitors the PCN markings of probe packets sent by Alice as well as the status information received in the UPDATE SDP3 message. If all the probe measurement conditions are met, then the precondition is met and the session setup proceeds as normal. However, should one or more of the conditions not be met, then session setup is terminated with an appropriate failure message sent to Alice.

The above simplified approach is just one way of how SIP signalling can be used with PCN marking to provide admission control.

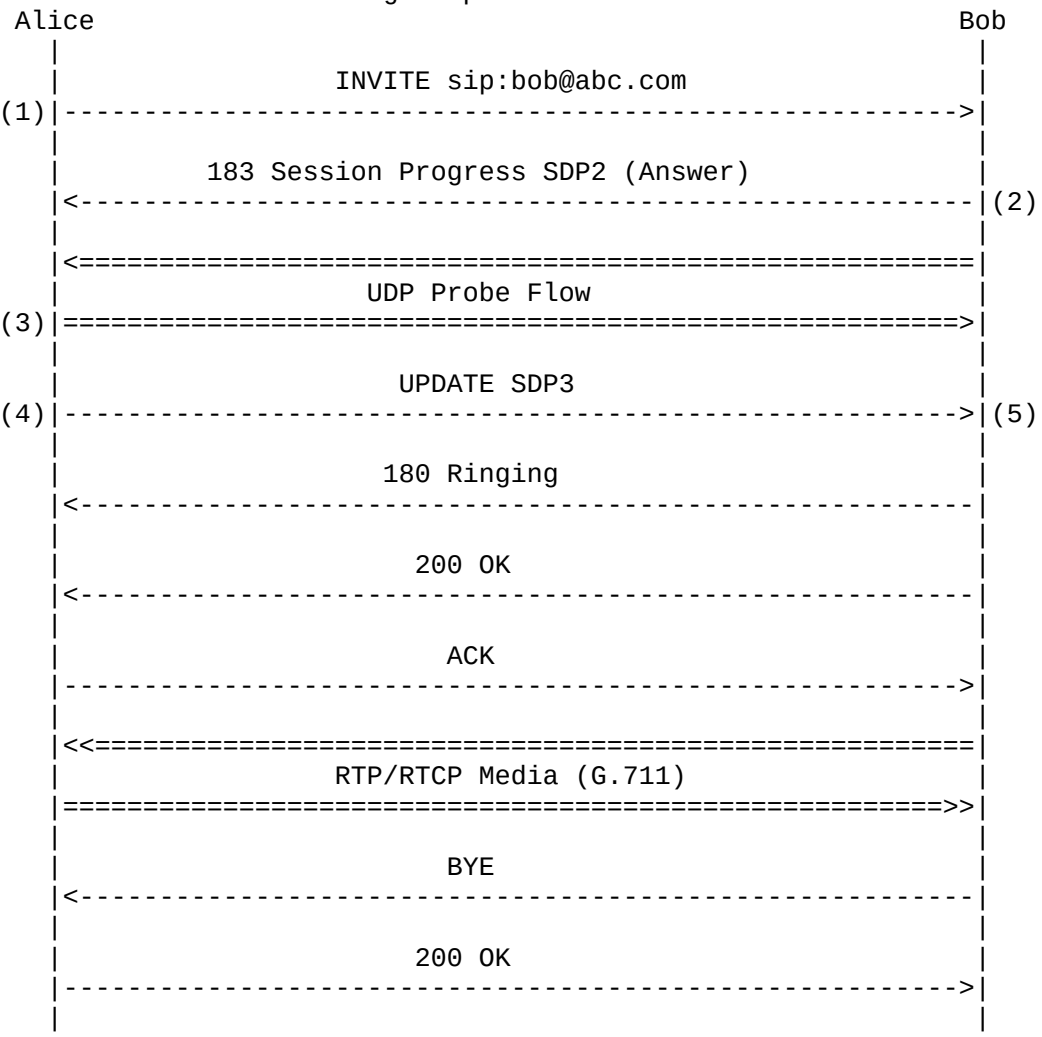

Figure 2: SIP Session Setup

The procedures used by the endpoint to determine whether to proceed with session setup depend on which endpoint is receiving the result and on local policy with respect to the precedence of the session. If there is a need to handle emergency (or within a self contained network other traffic designated as higher precedence) session differently than normal session, and since the network device is unaware of the precedence of the session, this decision must be made at the endpoints. In the context of admission control, application

level session admission policy may dictate that higher priority sessions may get admitted when probe packets indicate traffic level that prevent normal sessions from being admitted, e.g., PCN marking indicates traffic is above "admissible rate" but below "supportable rate".

Endpoints should be authenticated as complying with the end-to-end call admission control requirements before they are allowed to initiate sessions on the network using this mechanism. With SIP this implies that the SIP Proxy or Call Server that services them directly should perform this authentication. In the absence of complying endpoints, edge device which can proxy the PCN monitoring and probing functions on behalf of the endpoint may be used.

Also note that this implies that a trust relationship must exist between the endpoints, the SIP server that controls the service and routers performing the metering and marking in the network. If such trust relationship is not possible, the enforcement of the action as signalled by the PCN marking in the IP packet headers needs to be enforced at trusted network edge nodes. The methods to achieve this is for further study but some form of packet filtering may be used.

4.4. Session Preemption

There are situations where the network must shed any extra traffic that it can not forward. This is normally done through packet dropping. This approach works reasonably well for elastic traffic that use flow control protocols such as TCP. However, inelastic traffic such as voice or video normally does not have the ability to adapt to available bandwidth in the network, therefore excess traffic is dropped, causing quality of service degradation to all users until the offered load is reduced. Session preemption is a method whereby some inelastic flows equaling the excess traffic are removed so that the remaining traffic can experience good quality of service. Normally, the session preemption procedure would be applied only to inelastic flows.

To better understand how preemption can work, we provide an overview of one of the approaches that is currently being studied. Note, this approach is different to what is currently described in Pre-Congestion Notification Marking [1] and An edge-to-edge Deployment Model for Pre-Congestion Notification [3]. With this approach, routers using a token bucket measure the rate that is in excess of the configured supportable rate and mark a packet every "n" bytes. This marking approach marks a packet every "n" bytes of traffic that is above the "supportable rate". The marking frequency is dependent on the value of "n", the size of measured packets at the time that traffic has exceeded the supportable rate and the amount by which the

traffic has exceeded. This marking behavior is proportional to the rate that is in excess of the supportable service rate. When traffic is above the supportable rate by small amount, marking is infrequent, and when traffic exceeds by large amount, packet marking becomes more frequent. The other property of this approach is that routers mark packets belonging to random flows when traffic is in excess of supportable rate at the measuring point.

Routers in the network meter packets per service class (per DSCP or group of DSCPs) and when the measured rate exceeds the configured "supportable rate" of the service class, mark packets. In this document we will call this marking as Preemption Marking (PM). PM is conveyed to the SIP controlled endpoints using the agreed upon PCN marking method in the IP header. The SIP endpoints monitor the received media packets and on detecting a packet that is PM marking, invoke the defined preemption procedure for the session. A PM marked packet is as an indication that the "supportable rate" on the packet forwarding path was exceeded. Should the service policy allow for network initiated termination of a session to proceed, the endpoint signals using SIP to the traffic origination endpoint to stop sending packets belonging to that session. For applications that need bidirectional flows, e.g., VoIP, the application using SIP signalling would terminate both sessions. In summary, the routers at the congestion points in the network mark a packet and the endpoints react to the marking by terminating the session or flow that had the marked packet.

Simulation results of this preemption mechanism will be provided in another document to be published. More details will be provided in that future document.

Also note that this implies that a trust relationship must exist between the endpoints, the SIP server that controls the service and routers performing the metering and marking in the network. If such trust relationship is not possible, the enforcement of the action as signalled by the PCN marking in the IP packet headers needs to be enforced at trusted network edge nodes. The methods to achieve this is for further study but some form of packet filtering may be used. One approach could be where edge nodes drop packets belonging to the marked flow.

5. Summary

The high level walk through of session admission control and session preemption in previous sections provided an operational overview of this framework:

1. In the Diffserv enabled network, routers meter real-time inelastic traffic per service class and mark packets indicating that admissible rate or supportable rate at the measuring point was exceeded.

2. SIP controlled endpoints look at the markings of received packets to determine bandwidth utilization along the path from sender to receiver, and based on the marking, session state and service policy take action, admit, block or preempt.

3. During session setup, probing is performed to verify that media packets can be sent end-to-end and that the end-to-end path will have sufficient network resources (bandwidth, etc.) once real media packets are sent to meet its QoS needs.

The solution provided by this framework indicates couple of dependencies:

1. There needs to be a standardized way for indicate the current resource (bandwidth, etc.) utilization condition in the network, to convey the exceeding "admissible rate" and "supportable rate" conditions. We think this dependency will be fulfilled by PCN Marking [1] draft.

2. There needs to be a way for SIP to allow the consideration of network resources prior to admitting new sessions. We think this dependency can be fulfilled by SIP precondition RFC 3312[10].

3. There needs to be a way for the probe packets to be sent prior to making the session admission decision. There needs to be further work on this.

4. A method needs to be agreed upon for SIP endpoints to signal results of probing and reaction to PCN marking. It is believe that this will need to be done in the appropriate SIP working group.

5. Some form of trust relationship may need to be established between different control functions of the solution. This need will depend on the environment that utilize this solution. Further work on this will be needed with the attempt of using existing trust relationship method as much as possible.

6. There may be a need for the trusted network edges to enforce the reaction to PCN marking should the endpoints not behave properly. Further work on this will be needed with the attempt of using existing edge traffic filtering methods.

The resolution of these dependencies may be provided by work in PCN or by other working groups or areas.

6. Open Issues

In this section we list the currently known open issues, some with possible resolutions and discussions.

1. Initially the focus of this workgroup is to define how admission control and where need preemption would be invoked in trusted networks. By trusted we mean that routers will mark packets correctly and that SIP endpoints and the application that is controlling them will respond to the marking per defined polices. This assumption maybe valid for solutions that are controlled by a single administrator or where the trust relationship is established and enforced by other means between two administrators. However, in situation where this trust relationship is not possible, a method needs to be defined so that the network edge devices can enforce the behavior that is signalled from internal network routers using PCN marking, mainly to block the addition of new flows or removal of existing marked flows. This is to address scenarios where the transport network can not trust SIP controlled endpoints or the application controlling the service.

    1. Need to investigate other trust relationships, like can endpoints trust the marking as well can one network segment trust the marking of the previous network?

    2. Is the ECN nonce as defined in RFC 3168 [7] and RFC 3540 [11] useful for this application? Or can one of the codepoints be reused for other purpose, possibly to indicate one of the pre-congestion traffic level?

    3. What method will be used to validate the markings and is it needed with PCN where signalling is used to close the congestion control loop?

2. Currently only non rate-adaptive media codecs are addressed in this draft. A method needs to be defined so that PCN can take advantage of rate-adaptive media codecs. To start the discussion, here is one possible approach:

    * During session setup primary and secondary (being a lower rate) codecs are negotiated and agreed upon.

* Once a flow has been admitted and the traffic exceeds the admissible rate, routers in the network PCN marking media packet.

* Upon detection by the endpoint that the admissible rate was exceeded, endpoints that have the ability to dynamically react to PCN marking do so and reduce their sending rate as agreed to during session setup. Endpoints switch to lower rate codec.

* The signalling of codec change is performed using RTCP (Real Time Control Protocol) message sent from the receiver to the transmitter.

7. Explanation of Terminology

In this section we provide additional explanations to terminology unique to this framework:

- Admissible Rate: The configured parameter for determining if the current measured IP packet rate is within the limit for allowing flow/session admission. Notice this rate measurement is done for each service class, hence this is a "bulk" rate, not a per flow/session rate. Please note this parameter:

  * Is local to each measurement point (router) of the end-to-end flow/session path.

  * Can be expressed in terms of percentage of total bandwidth allocated to the Diffserv Service Class [12] for handling this type of flow/session, or in absolute terms like bit per second.

- Supportable Rate: The parameter for determining if the current measured IP packet rate is within the limit for providing the required QoS, the QoS support required by the application/service. Notice this rate measurement is done for each service class, hence this is a "bulk" rate, not a per flow/session rate. Please note this parameter:

  * Is local to each measurement point of the end-to-end flow/session path.

  * Can be expressed in terms of percentage of total bandwidth allocated to the Diffserv Service Class [12] for handling this type of flow/session, or in absolute terms like bit per second.

- Admission Control: The action process taken by the application entity, based on the network condition indication provided by the packet marking, for determining if a new flow/session is to be admitted. Please note this action process:
  - Resides in an application functional module.
  - Normally occurs in the application control point of an end-to-end flow/session or intermediary node that is in the path.
- Preemption: The action process taken by the application entity, based on the network condition indication provided by the packet marking, for determining if a previously admitted flow/session is to be terminated. Please note this action process:
  - Resides in an application functional module.
  - Normally occurs in the application control point of an end-to-end flow/session or intermediary node that is in the path.
- Flow/Session Precedence: An application level flow/session parameter. This parameter:
  - Is used to indicate the relative importance of its associated flow/session.
  - Can be used by the application control point for admission control or preemption purpose.
  - Is an application level parameter. The network does not have any knowledge of this parameter.
- Probing: An application level function for generation of traffic for the purpose of obtaining current network condition indication provided by packet marking and loss measurement. This is needed when there is no normal flow/session packet traffic, for example before a flow/session is admitted. The probing traffic generated needs to:
  - Be treated by the network the same as the normal flow/session packet traffic. Needs to be forward along the same end-to-end path that normal flow/session packet traffic.
  - Be understood by the application control point as different from the normal media packet traffic.

8. Security Considerations

This section needs to be completed.

The network needs to protect its self from overload through filtering (dropping packets) at the edges and rate limiting traffic to agreed levels. Further, in the interior network nodes, should traffic in a service class exceed the forwarding capacity, the excess traffic needs to be dropped. Methods to establish, maintain, and enforce trusts need to be defined and used. As well in networks were trust relations are not possible, enforcement of the action as indicated by PCN marking is required at network edges, blocking of new flows and removing of PM marked flows.

9. Acknowledgement

The authors acknowledge a great many inputs into this framework, including the following: Corey Alexander, Marvin Krym, Stephen Dudley, John Rutledge, and Lars Westberg.

10. Informative References

[1] Briscoe, B., "Pre-Congestion Notification marking", draft-briscoe-tsvwg-cl-phb-02 (work in progress), June 2006.

[2] Chan, K., "Pre-Congestion Notification Problem Statement", draft-chan-pcn-problem-statement-00 (work in progress), September 2006.

[3] Briscoe, B., "An edge-to-edge Deployment Model for Pre-Congestion Notification: Admission Control over a DiffServ Region", draft-briscoe-tsvwg-cl-architecture-03 (work in progress), June 2006.

[4] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[5] Nichols, K., Blake, S., Baker, F., and D. Black, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers", RFC 2474, December 1998.

[6] Blake, S., Black, D., Carlson, M., Davies, E., Wang, Z., and W. Weiss, "An Architecture for Differentiated Services", RFC 2475, December 1998.

[7] Ramakrishnan, K., Floyd, S., and D. Black, "The Addition of

Explicit Congestion Notification (ECN) to IP", RFC 3168, September 2001.

[8] Davie, B., Charny, A., Bennet, J., Benson, K., Le Boudec, J., Courtney, W., Davari, S., Firoiu, V., and D. Stiliadis, "An Expedited Forwarding PHB (Per-Hop Behavior)", RFC 3246, March 2002.

[9] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.

[10] Camarillo, G., Marshall, W., and J. Rosenberg, "Integration of Resource Management and Session Initiation Protocol (SIP)", RFC 3312, October 2002.

[11] Spring, N., Wetherall, D., and D. Ely, "Robust Explicit Congestion Notification (ECN) Signaling with Nonces", RFC 3540, June 2003.

[12] Babiarz, J., Chan, K., and F. Baker, "Configuration Guidelines for DiffServ Service Classes", RFC 4594, August 2006.

Authors' Addresses

Jozef Z. Babiarz
Nortel
3500 Carling Avenue
Ottawa, Ont. K2H 8E9
Canada

Phone: +1-613-763-6098
Email: babiarz@nortel.com

Kwok Ho Chan
Nortel
600 Technology Park Drive
Billerica, MA 01821
USA

Phone: +1-978-288-8175
Email: khchan@nortel.com

Georgios Karagiannis
University of Twente
P.O. BOX 217, 7500 AE Enschede
The Netherlands

Email: g.karagiannis@ewi.utwente.nl

Philip Eardley
BT Research
B54/77, Sirius House Adastral Park Martlesham Heath
Ipswich, Suffolk IP5 3RE
United Kingdom

Email: philip.eardley@bt.com

Full Copyright Statement

Intellectual Property

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).