Transport Working Group	F. Baker	
Internet-Draft	J. Polk	
Updates: 4542, 4594	Cisco Systems	
(if approved)	M. Dolly	
Intended status: Standards Track	AT&T Labs	
Expires: August 27, 2008	February 24, 2008	

TOC

DSCPs for Capacity-Admitted Traffic
draft-ietf-tsvwg-admitted-realtime-dscp-04

Status of this Memo

Abstract

This document requests one Differentiated Services Code Point (DSCP) from the Internet Assigned Numbers Authority (IANA) for real-time traffic classes similar to voice conforming to the Expedited Forwarding Per Hop Behavior, and admitted using a call admission procedure involving authentication, authorization, and capacity admission.
It also recommends that certain classes of video traffic described in RFC 4594 and which have similar requirements be changed to require admission using a Call Admission Control (CAC) procedure involving authentication, authorization, and capacity admission.

Requirements Language

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 (Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," March 1997.) [RFC2119].

Table of Contents

---

1. Introduction

TOC

This document requests one Differentiated Services Code Point (DSCP) from the Internet Assigned Numbers Authority (IANA) for a class of real-time traffic. This class conforms to the Expedited Forwarding (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)," March 2002.) [RFC3246] [RFC3247] (Charny, A., Bennet, J., Benson, K., Boudec, J., Chiu, A., Courtney,

W., Davari, S., Firoiu, V., Kalmanek, C., and K. Ramakrishnan, “Supplemental Information for the New Definition of the EF PHB (Expedited Forwarding Per-Hop Behavior),” March 2002.) Per Hop Behavior. It is also admitted using a CAC procedure involving authentication, authorization, and capacity admission. This differs from a real-time traffic class conforming to the Expedited Forwarding Per Hop Behavior but not subject to capacity admission or subject to very coarse capacity admission.

It also recommends that certain classes of video described in [RFC4594] (Babiarz, J., Chan, K., and F. Baker, “Configuration Guidelines for DiffServ Service Classes,” August 2006.) be treated as requiring capacity admission as well.

These applications have one or more potential congestion points between the video distribution/conferencing bridge or gaming server and the user(s), and reserving capacity for them is important to application performance. All of these applications have low tolerance to jitter (aka delay variation) and loss, as summarized in Section 2 (Implementation of the Admitted Service Classes), and most (except for multimedia conferencing) have inelastic flow behavior from Figure 1 of [RFC4594] (Babiarz, J., Chan, K., and F. Baker, “Configuration Guidelines for DiffServ Service Classes,” August 2006.). Inelastic flow behavior and low jitter/loss tolerance are the service characteristics that define the need for admission control behavior.

One of the reasons behind this is the need for classes of traffic that are handled under special policies, such as the non-preemptive Emergency Telecommunication Service, the US Department of Defense's Assured Service (which is similar to Multi-Level Precedence and Preemption (International Telecommunications Union, “Multilevel Precedence and Preemption Service,” 1990.) [ITU.MLPP.1990] procedure), or e-911, in addition to normal routine calls that use call admission. It is possible to use control plane protocols to generally restrict session admission such that admitted traffic should receive the desired service, and the policy (e.g. Routine, National Security or Emergency Preparedness [NS/EP] communications, e-911, etc) need not be signaled in a DSCP. However, service providers need to distinguish between special-policy traffic and other classes, particularly the existing VoIP services that perform no capacity admission or only very coarse capacity admission and can exceed their allocated resources.

The requested DSCP applies to the Telephony Service Class described in [RFC4594] (Babiarz, J., Chan, K., and F. Baker, “Configuration Guidelines for DiffServ Service Classes,” August 2006.). The video classes addressed include the

*interactive real-time traffic (CS4, used for Video conferencing and Interactive gaming),

*broadcast TV (CS3) for use in a video on demand context, and

*AF4 Multimedia conferencing (video conferencing).

Since the admitted video classes have not had the history of mixing admitted and non-admitted traffic in the same Per-Hop Behavior (PHB) as has occurred for EF, an additional DSCP code point is not recommended. Instead, the recommended "best practice" is to perform admission control for the above video classes.
Other video classes are not believed to be required by the targeted services and to not have the current problem of confusion with unadmitted traffic. Within an ISP and on inter-ISP links (i.e. within networks whose internal paths are uniform at hundreds of megabits or faster), one would expect all of this traffic to be carried in the Real Time Traffic Class described in [RFC5127] (Chan, K., Babiarz, J., and F. Baker, “Aggregation of DiffServ Service Classes,” February 2008.).

1.1. Definitions

TOC

The following terms and acronyms are used in this document.

PHB: A Per-Hop-Behavior (PHB) is the externally observable forwarding behavior applied at a Differentiated Services compliant node to a DS behavior aggregate [RFC2475] (Blake, S., Black, D., Carlson, M., Davies, E., Wang, Z., and W. Weiss, “An Architecture for Differentiated Services,” December 1998.). It may be thought of as a program configured on the interface of an Internet host or router, specified drop probabilities, queuing priorities or rates, and other handling characteristics for the traffic class.

DSCP: The Differentiated Services Code Point (DSCP), as defined in [RFC2474] (Nichols, K., Blake, S., Baker, F., and D. Black, “Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers,” December 1998.), is a value which is encoded in the DS field, and which each DS Node MUST use to select the PHB which is to be experienced by each packet it forwards [RFC3260] (Grossman, D., “New Terminology and Clarifications for Diffserv,” April 2002.). It is a 6-bit number embedded into the 8-bit TOS field of an IPv4 datagram or the Traffic Class field of an IPv6 datagram.

CAC: Call Admission Control includes concepts of authorization and capacity admission. "Authorization" includes and procedure identifies a user, verifies the authenticity of the identification, and determines whether the user is authorized to use the service. "Capacity Admission" refers to any procedure that determines whether capacity exists supporting a session's requirements under some policy.
In the Internet, these are separate functions, while in the PSTN they and call routing are carried out together.

UNI:

A User/Network Interface (UNI) is the interface (often a physical link or its virtual equivalent) that connects two entities that do not trust each other, and in which one (the user) purchases connectivity services from the other (the network). Figure 1 (UNI and NNI interfaces) shows two user networks connected by what appears to each of them to be a single network ("The Internet", access to which is provided by their service provider) that provides connectivity services to other users.

UNIs tend to be the bottlenecks in the Internet, where users purchase relatively low amounts of bandwidth for cost or service reasons, and as a result are most subject to congestion issues and therefore issues requiring traffic conditioning and service prioritization.

NNI: A Network/Network Interface (NNI) is the interface (often a physical link or its virtual equivalent) that connects two entities that trust each other within limits, and in which the two are seen as trading services for value. Figure 1 (UNI and NNI interfaces) shows three service networks that together provide the connectivity services that we call "the Internet". They are different administrations and are very probably in competition, but exchange contracts for connectivity and capacity that enable them to offer specific services to their customers.

NNIs may not be bottlenecks in the Internet if service providers contractually agree to provision excess capacity at them, as they commonly do. However, NNI performance may differ by ISP, and the performance guarantee interval may range from a month to a much shorter period. Furthermore, a peering point NNI may not have contractual performance guarantees or may become overloaded under certain conditions. They are also policy-controlled interfaces, especially in BGP. As a result, they may require traffic prioritization policy.

Queue: There are multiple ways to build a multi-queue scheduler. Weighted Round Robin (WRR) literally builds multiple lists and visits them in a specified order, while a calendar queue (often used to implement Weighted Fair Queuing, or WFQ) builds a list for each time interval and enqueues at most a stated amount of data in each such list for transmission during that time interval. While these differ dramatically in implementation, the external difference in behavior is generally negligible when they are properly configured. Consistent with the definitions used in the Differentiated Services Architecture (Blake, S., Black, D., Carlson, M., Davies, E., Wang, Z., and W. Weiss, “An Architecture for Differentiated Services,” December 1998.) [RFC2475], these are treated as equivalent in this document, and the lists of WRR

> and the classes of a calendar queue will be referred to uniformly as "queues".

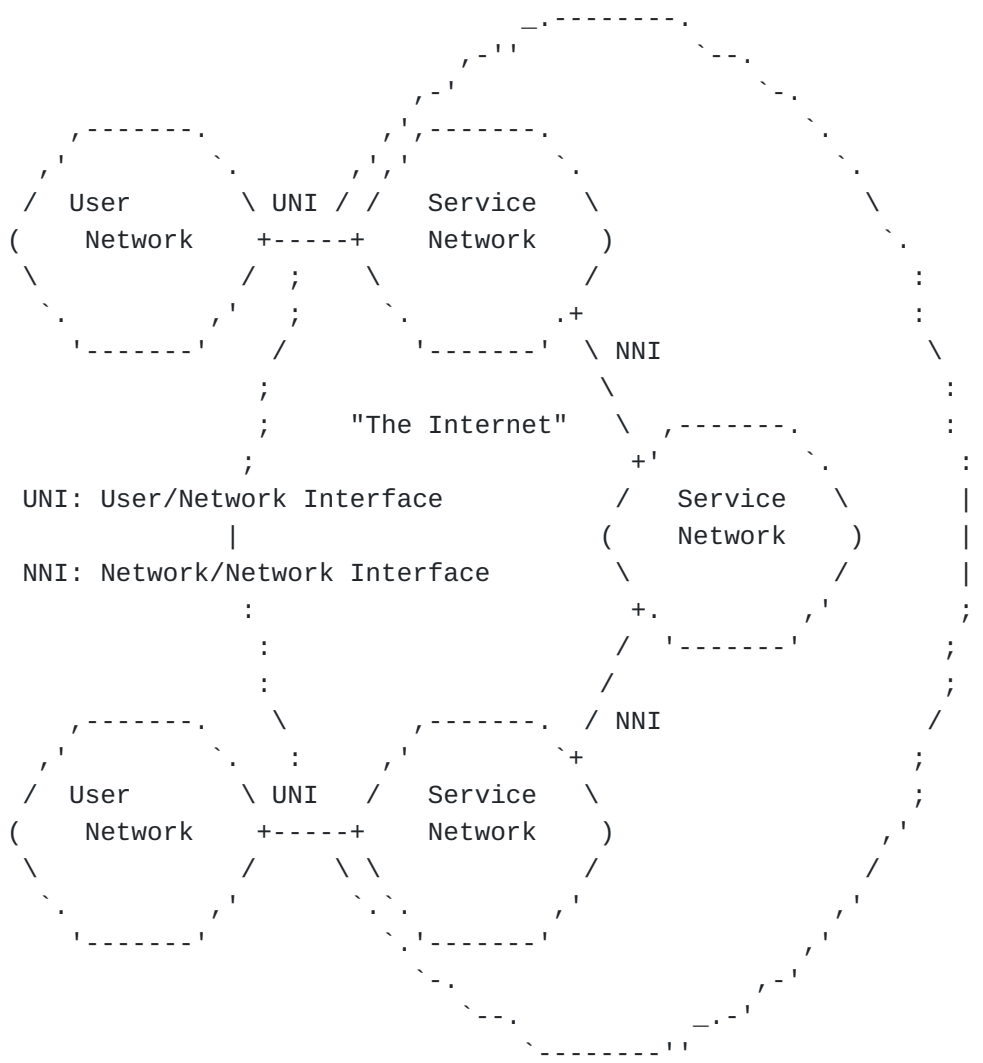

Figure 1: UNI and NNI interfaces

1.2. Problem

TOC

In short, the Telephony Service Class described in [RFC4594] (Babiarz, J., Chan, K., and F. Baker, “Configuration Guidelines for DiffServ Service Classes,” August 2006.) permits the use of capacity admission

in implementing the service, but present implementations either provide no capacity admission services or do so in a manner that depends on specific traffic engineering. In the context of the Internet backbone, the two are essentially equivalent; the edge network is depending on specific engineering by the service provider that may not be present. However, services are being requested of the network that would specifically make use of capacity admission, and would distinguish among users or the uses of available Voice-on-IP or Video-on-IP capacity in various ways. Various agencies would like to provide services as described in section 2.6 of [RFC4504] (Sinnreich, H., Lass, S., and C. Stredicke, "SIP Telephony Device Requirements and Configuration," May 2006.) or in [RFC4190] (Carlberg, K., Brown, I., and C. Beard, "Framework for Supporting Emergency Telecommunications Service (ETS) in IP Telephony," November 2005.). This requires the use of capacity admission to differentiate among users (which might be 911 call centers, other offices with preferential service contracts, or individual users gaining access with special credentials) to provide services to them that are not afforded to non-capacity admitted customer-to-customer IP telephony sessions.

1.3. Proposed Solution

TOC

The IETF is asked to differentiate, in the Telephony Service, between sessions that are originated without capacity admission or using traffic engineering and sessions that are originated using more robust capacity admission procedures. Sessions of the first type use a traffic class in which they compete without network-originated control as described in Section 2.2.1 (Capacity admission control by assumption) or Section 2.2.2 (Capacity admission control by call counting), and in the worst case lose traffic due to policing. Sessions of the second type cooperate with network control, and may be given different levels of preference depending on the policies that the network applies. In order to provide this differentiation, the IETF requests that the IANA assign a separate DSCP value to admitted sessions using the Telephony service (see Section 4 (IANA Considerations)).

---

2. Implementation of the Admitted Service Classes

TOC

TOC

2.1. Potential implementations of EF in this model

There are at least two possible ways to implement the Expedited Forwarding PHB in this model. They are to implement separate classes as a set of

- Multiple data plane traffic classes, each consisting of a policer and a queue, and the queues enjoying different priorities, or

- Multiple data plane traffic classes, each consisting of a policer but feeding into a common queue or multiple queues at the same priority.

We will explain the difference, and describe in what way they differ in operation. The reason this is necessary is that there is current confusion in the industry, including a widely reported test for NS/EP services that implemented the policing model and described it as an implementation of the multi-priority model, and discussion in other environments of the intermixing of voice and video traffic at relatively low bandwidths in the policing model.
The multi-priority model is shown in Figure 2 (Implementation as a data plane priority). In this model, traffic from each service class is placed into a separate priority queue. If data is present in both queues, traffic from one of them will always be selected for transmission. This has the effect of transferring jitter from the higher priority queue to the lower priority queue, and reordering traffic in a way that gives the higher priority traffic a smaller average queuing delay. Each queue must have its own policer, however, to protect the network from errors and attacks; if a traffic class thinks it is carrying a certain data rate but an abuse sends significantly more, the effect of simple prioritization would not preserve the lower priorities of traffic, which could cause routing to fail or otherwise impact an SLA.

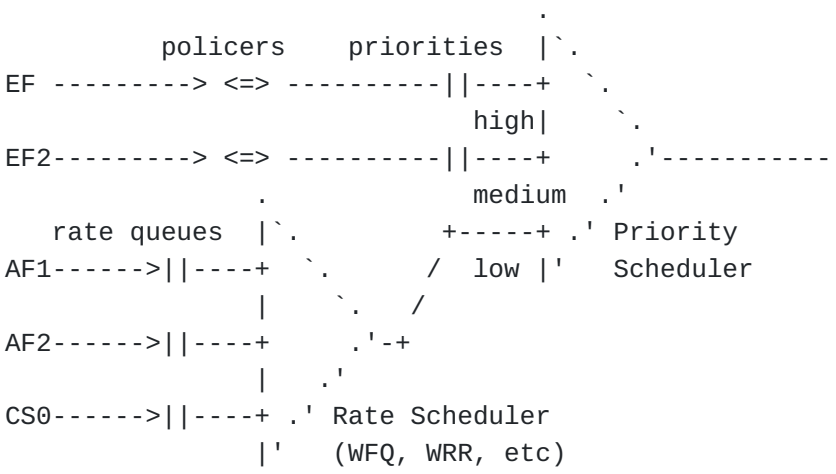

Figure 2: Implementation as a data plane priority

The multi-policer model is shown in Figure 3 (Implementation as a data plane policer). In this model, traffic from each service class is policed according to its SLA requirements, and then placed into a common priority queue. Unlike the multi-priority model, the jitter experienced by the traffic classes in this case is the same, as there is only one queue, but the sum of the traffic in this higher priority queue experiences less average jitter than the elastic traffic in the lower priority.

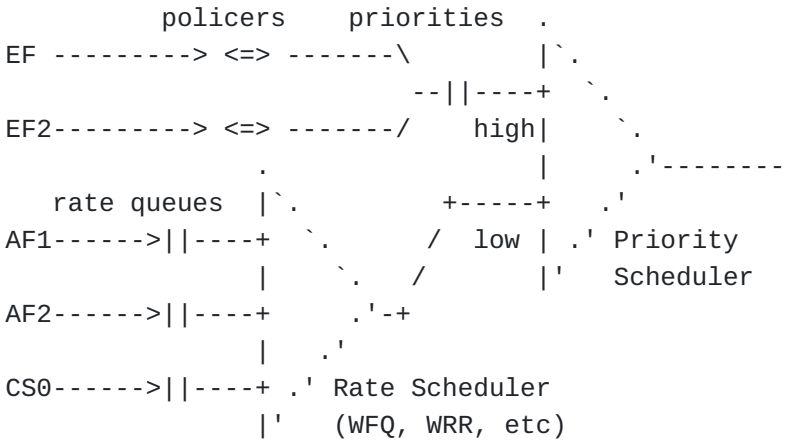

Figure 3: Implementation as a data plane policer

The difference between the two operationally is, as stated, the issues of loss due to policing and distribution of jitter.

If the two traffic classes are, for example, voice and video, datagrams containing video data are relatively large (generally the size of the path MTU) while datagrams containing voice are relatively small, on the order of only 40 to 200 bytes, depending on the codec. On lower speed links (less than 10 MBPS), the jitter introduced by video to voice can be disruptive, while at higher speeds the jitter is nominal compared to the jitter requirements of voice. At access network speeds, therefore, [RFC4594] (Babiarz, J., Chan, K., and F. Baker, “Configuration Guidelines for DiffServ Service Classes,” August 2006.) recommends separation of video and voice into separate queues, while at optical speeds [RFC5127] (Chan, K., Babiarz, J., and F. Baker, “Aggregation of DiffServ Service Classes,” February 2008.) recommends that they use a common queue.
If, on the other hand, the two traffic classes are carrying the same type of application with the same jitter requirements, then giving one preference in this sense does not benefit the higher priority traffic and may harm the lower priority traffic. In such a case, using separate policers and a common queue is a superior approach.

2.2. Capacity admission control

TOC

There are five major ways that capacity admission is done or has been proposed to be done in real-time applications:

- *Capacity admission control by assumption,
- *Capacity admission control by call counting,
- *End-point capacity admission performed by probing the network,
- *Centralized capacity admission control, and
- *Distributed capacity admission control.

There is also a mechanism that has been proposed for enhancing the probability of call completion in a preferential manner. This is not capacity admission per se, since it never actually refuses a call (although a session may be dropped by its user when the user finds continuation untenable). The central notion is that when the capacity available for a set of variable rate sessions has been overbooked, traffic may be randomly dropped from lower precedence sessions to allow a higher precedence session in. This has a number of ramifications that make it inappropriate in the Internet. A key issue is that it affects not a single session but a class of sessions - all sessions of lower precedence than the protected session(s). A video example will suffice for the present. Multimedia data streams and sensor traffic often build on information in previous frames, and their content spans multiple

datagrams in the same frame. The loss of a datagram forces the codec into a recovery mode that reduces image quality for at least one frame, and may cause the image to freeze for multiple seconds. This is readily observed on television, where screen artifacts are very visible. Scattered random datagram loss results in all sessions in the class being impacted to some degree. Hence, it is far more suitable to drop an entire session (and therefore impact only one session) than to impact all sessions in a class in a manner that consumes the available bandwidth but delivers sub-SLA service to an entire class of sessions. It also exposes the precedence level of each session in the clear.

2.2.1. Capacity admission control by assumption

TOC

The first approach is to ignore the matter entirely. If one assumes that the capacity available to the application is uniformly far in excess of its requirements, it is perhaps overhead that can be ignored. This assumption is currently made in Internet VoIP offerings such as Skype and Vonage; the end user is responsible to place his service on a LAN connected to the Internet backbone by a high speed broadband connection and use capable ISPs to deliver the service. The only "authorization" verified is that the user pays his bills; no capacity admission is considered because there is a clear separation from the application service provider admitting the calls and the access network provider admitting the traffic. The two have no way of knowing about each other, except in the abstract sense.

2.2.2. Capacity admission control by call counting

TOC

The H.323 gatekeeper, originally specified in 1996, operates on the model that the considerations of Section 2.2.1 (Capacity admission control by assumption) generally apply, and that it is therefore sufficient to count calls in order to ensure that any bottlenecks in the network are never overloaded. Which phone is calling which phone is configured information into the Gatekeeper, ensuring it doesn't admit too many calls across a low speed link. The area of influence of a Gatekeeper is called a Zone, and limits how far away a Gatekeeper can influence calls. This is because call counting doesn't scale when more than one server is admitting flows across the same limited speed links. This approach is consistent with the original design of H.323, which in 1996 was a mechanism for connecting H.320 media gateways across a LAN. VoIP has come a long way since then, however, and the engineering trade-offs this approach requires in complex networks are unsatisfactory.

SIP provides the option to go down another path, to admit its servers at layer 7, have no awareness of lower layer connectivity, resulting in a divorce from infrastructure knowledge - save for [RFC3312] (Camarillo, G., Marshall, W., and J. Rosenberg, “Integration of Resource Management and Session Initiation Protocol (SIP),” October 2002.), which binds the two, but only at the endpoints. In short, if there is a bottleneck anywhere in the network that might be used to connect two gatekeepers, SIP proxies that do not implement or do not configure the use of [RFC3312] (Camarillo, G., Marshall, W., and J. Rosenberg, “Integration of Resource Management and Session Initiation Protocol (SIP),” October 2002.), or other call management systems, the amount of traffic between the two must be contained below that bottleneck even if the normal path is of much higher bandwidth. In addition, the multiplexing of traffic streams between different pairs of gatekeepers over a common LAN infrastructure is not handled by the application, and so must be managed in the engineering of the network.

2.2.3. End-point capacity admission performed by probing the network

TOC

The IETF started looking into the use of Pre-Congestion Notification mechanism to full fill the need of admission control for real-time traffic. The main contribution of this work for admission control is to allow the network to provide the network's pre-congestion information using encoding of a field in the IP header. This network pre-congestion information is then used for making admission control decisions. With the decision influenced by this network pre-congestion notification information and any applicable policy information with possible user credentials and situational information. The pre-congestion notification mechanism does not limit the placement of the admission control decision point or the signaling protocol used.
The overview of one of the current proposals is provided by [I-D.chan-pcn-problem-statement] (Chan, K., “Pre-Congestion Notification Problem Statement,” October 2006.). With the pre-congestion notification encoding described in [I-D.briscoe-tsvwg-cl-phb] (Briscoe, B., “Pre-Congestion Notification marking,” October 2006.). An initial deployment model provided by [I-D.briscoe-tsvwg-cl-architecture] (Briscoe, B., “An edge-to-edge Deployment Model for Pre-Congestion Notification: Admission Control over a DiffServ Region,” October 2006.). Another proposal is embodied in [I-D.charny-pcn-single-marking] (Charny, A., Zhang, X., Faucheur, F., and V. Liatsos, “Pre-Congestion Notification Using Single Marking for Admission and Termination,” November 2007.). Similar approaches have been proposed in [I-D.morita-tsvwg-pps] (Morita, N. and G. Karlsson, “Framework of Priority Promotion Scheme,” October 2003.) and

its related drafts, by Ivars and Karlsson in their PBAC work, and many others.

2.2.4. Centralized capacity admission control

TOC

The concept of a Bandwidth Broker was first discussed in the research world surrounding ESNET and Internet II in the late 1990's, and has been discussed in the literature pertaining to the Differentiated Services Architecture (Blake, S., Black, D., Carlson, M., Davies, E., Wang, Z., and W. Weiss, “An Architecture for Differentiated Services,” December 1998.) [RFC2475]. It is, in short, a central system that performs a variety of services on behalf of clients of a network including applying AAA services (as in [RFC2904] (Vollbrecht, J., Calhoun, P., Farrell, S., Gommans, L., Gross, G., de Bruijn, B., de Laat, C., Holdrege, M., and D. Spence, “AAA Authorization Framework,” August 2000.)) and authorizing them to use specified capacity at specified times. Its strength is that it is relatively simple, at least in concept, and can keep track of simple book-keeping functions apart from network elements such as routers. Its weakness is that it has no idea what the specific routing of any stated data flow is, or its capacity apart from services such as MPLS Traffic Engineering or engineering assumptions specified by the designers of a network. Obtaining that information from the network via SNMP GET or other network management action can impose a severe network overhead, and is obviously not real-time.
For scaling reasons, operational Bandwidth Brokers generally take on a semi-distributed or fully distributed nature. They are implemented on a per-point-of-presence basis, and in satellite networks might be implemented in each terminal. At this point, they become difficult to operationally distinguish from distributed capacity admission services such as described in Section 2.2.5 (Distributed capacity admission control).

2.2.5. Distributed capacity admission control

TOC

The IETF developed the Integrated Services Model (Braden, B., Clark, D., and S. Shenker, “Integrated Services in the Internet Architecture: an Overview,” June 1994.) [RFC1633] and the RSVP capacity admission protocol (Braden, B., Zhang, L., Berson, S., Herzog, S., and S. Jamin, “Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification,” September 1997.) [RFC2205] in the early 1990's, and then integrated it with the Differentiated Services Architecture in [RFC2998] (Bernet, Y., Ford, P., Yavatkar, R., Baker, F., Zhang, L., Speer, M., Braden, R., Davie, B., Wroclawski, J., and E. Felstaine, “A

Framework for Integrated Services Operation over Diffserv Networks," November 2000.). Since then, the IETF has been working on a next generation signaling protocol called NSIS (Hancock, R., Karagiannis, G., Loughney, J., and S. Van den Bosch, "Next Steps in Signaling (NSIS): Framework," June 2005.) [RFC4080] that can be used for capacity admission protocol, and which is limited in scope to considering unicast sessions. [RFC4542] (Baker, F. and J. Polk, "Implementing an Emergency Telecommunications Service (ETS) for Real-Time Services in the Internet Protocol Suite," May 2006.) looked at the issue of providing preferential services in the Internet, and determined that RSVP with its defined extensions could provide those services to unicast and multicast sessions.

As with the Bandwidth Broker model, there are concerns regarding scaling, mentioned in [RFC2208] (Mankin, A., Baker, F., Braden, B., Bradner, S., O'Dell, M., Romanow, A., Weinrib, A., and L. Zhang, "Resource ReSerVation Protocol (RSVP) Version 1 Applicability Statement Some Guidelines on Deployment," September 1997.). Present implementations that have been measured have been found to not display the scaling concerns, however, and in any event the use of RSVP Aggregation enables the backbone to handle such sessions in a manner similar to an ATM Virtual Path, bundling sessions together for capacity management purposes.

2.3. Prioritized capacity admission control

TOC

Emergency Telecommunication Service, the US Department of Defense's Assured Service, and e-911 each call for some form of prioritization of some calls over others. Prioritization of the use of bandwidth is fundamentally a matter of choices - at a point where one has multiple choices, applying a policy that selects among them. In the PSTN, GETS operates in favor of an authorized caller either by routing a call that would otherwise be refused by a path unavailable to the general public or by queuing the call until some existing call completes and bandwidth becomes available. e-911 is similar, but the policy is based on the called party, the emergency call center. MLPP operates by preempting an existing call to make way for the new one.

In the Internet, routing is not performed on a per-call basis, so, apart from interconnections to the PSTN, re-routing isn't an option. On the other hand, in the Internet there are more classes of traffic than in the PSTN. In the PSTN, all calls are uses of circuits, while in the Internet some bandwidth is always reserved for elastic applications - at least, it must be available for routing, and there is generally significant consideration of the web, instant messaging, and other applications. In essence, any capacity admission policy that differentiates between calls has the option of temporarily borrowing bandwidth from the capacity reserved for elastic traffic by accepting

new sessions under some prioritized policy while refusing sessions of lower priority because the threshold at that priority has been reached. For example, regardless of the type of capacity admission that is used (apart from "no admission process"), one might admit prioritized sessions using a higher bandwidth threshold than one admits lower priority sessions.

If capacity admission as described in Section 2.2.2 (Capacity admission control by call counting) is in use, the thresholds must be set low enough that bandwidth would be available anywhere in the network. This greatly limits the utility of such a service due to the level of bandwidth waste that results.

If capacity admission as described in Section 2.2.3 (End-point capacity admission performed by probing the network) is in use, then multiple thresholds must be applied in marking the traffic, multiple traffic marks must be applied, or there must be multiple ways to interpret the result. In any event, this is only applicable in domains in which the law of large numbers applies.

If capacity admission as described in Section 2.2.4 (Centralized capacity admission control) is in use, thresholds can be applied related to a general policy or SLA, or related to the network ingress and egress in use. It requires them to maintain state regarding network traffic routing separate from the network; to the extent that is variable, it requires direct monitoring in the OSS.

If capacity admission as described in Section 2.2.5 (Distributed capacity admission control) is in use, thresholds can be applied to the critical points of the path that the traffic in question actually takes because one is asking the equipment that the path traverses.

---

3. Recommendations on implementation of an Admitted Telephony Service Class

TOC

It is the belief of the authors that either data plane PHB described in Section 2.1 (Potential implementations of EF in this model), if coupled with adequate AAA and capacity admission procedures as described in Section 2.2.5 (Distributed capacity admission control), are sufficient to provide the services required for an Admitted Telephony service class and an Admitted Multimedia Conferencing Service Class. If preemption is required, as described in section 2.3.5.2 of [RFC4542] (Baker, F. and J. Polk, “Implementing an Emergency Telecommunications Service (ETS) for Real-Time Services in the Internet Protocol Suite,” May 2006.), this provides the tools for carrying out the preemption. If preemption is not in view, or in addition to preemptive services, the application of different thresholds depending on call precedence has the effect of improving the probability of call completion by admitting preferred calls at a time that other calls are being refused. Routine and priority traffic can be admitted using the same DSCP value, as the

choice of which calls are admitted is handled in the admission procedure executed in the control plane, not the policing of the data plane.
On the point of what protocols and procedures are required for authentication, authorization, and capacity admission, we note that clear standards do not at this time exist for bandwidth brokers, NSIS has not at this time been finalized and in any event is limited to unicast sessions, and that RSVP has been standardized and has the relevant services. We therefore recommend the use of RSVP at the UNI. Procedures at the NNI are business matters to be discussed between the relevant networks, and are recommended but not required.

---

4. IANA Considerations

TOC

This note requests that IANA assign a DSCP value to a second EF traffic class consistent with [RFC3246] (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),” March 2002.) and [RFC3247] (Charny, A., Bennet, J., Benson, K., Boudec, J., Chiu, A., Courtney, W., Davari, S., Firoiu, V., Kalmanek, C., and K. Ramakrishnan, “Supplemental Information for the New Definition of the EF PHB (Expedited Forwarding Per-Hop Behavior),” March 2002.) in the "Differentiated Services Field Codepoints" registry. It implements the Telephony Service Class described in [RFC4594] (Babiarz, J., Chan, K., and F. Baker, “Configuration Guidelines for DiffServ Service Classes,” August 2006.) at lower speeds and is included in the Real Time Treatment Aggregate (Chan, K., Babiarz, J., and F. Baker, “Aggregation of DiffServ Service Classes,” February 2008.) [RFC5127] at higher speeds. The recommended value for the code point 101100, paralleling the EF code point, which is 101110. The code point should be referred to as VOICE-ADMIT.
This traffic class requires the use of capacity admission such as RSVP services together with AAA services at the User/Network Interface (UNI); the use of such services at the NNI is at the option of the interconnected networks.

---

5. Security Considerations

TOC

A major requirement of this service is effective use of a signaling protocol such as RSVP, with the capabilities to identify its user either as an individual or as a member of some corporate entity, and assert a policy such as "routine" or "priority".
This capability, one has to believe, will be abused by script kiddies and others if the proof of identity is not adequately strong or if

policies are written or implemented improperly by the carriers. This goes without saying, but this section is here for it to be said...

---

6. Acknowledgements

TOC

Kwok Ho Chan offered some textual comments and rewrote Section 2.2.3 (End-point capacity admission performed by probing the network). Georgios Karagiannis offered additional comments on the same section. The impetus for including Video in the discussion, which initially only targeted voice, is from Dave McDysan, and text he suggested was included. Dan Voce also commented.

---

7. References

TOC

7.1. Normative References

TOC

[RFC2119]	Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," BCP 14, RFC 2119, March 1997 (TXT, HTML, XML).
[RFC2474]	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 (TXT, HTML, XML).
[RFC3246]	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 (TXT).

7.2. Informative References

TOC

[I-D.briscoe-tsvwg-cl-architecture]	Briscoe, B., "An edge-to-edge Deployment Model for Pre-Congestion Notification: Admission Control over a DiffServ Region," draft-briscoe-tsvwg-cl-architecture-04 (work in progress), October 2006 (TXT).
[I-D.briscoe-tsvwg-cl-phb]	Briscoe, B., "Pre-Congestion Notification marking," draft-briscoe-tsvwg-cl-phb-03 (work in progress), October 2006 (TXT).

[I-D.chan-pcn-problem-statement]	Chan, K., "Pre-Congestion Notification Problem Statement," draft-chan-pcn-problem-statement-01 (work in progress), October 2006 (TXT).
[I-D.charny-pcn-single-marking]	Charny, A., Zhang, X., Faucheur, F., and V. Liatsos, "Pre-Congestion Notification Using Single Marking for Admission and Termination," draft-charny-pcn-single-marking-03 (work in progress), November 2007 (TXT).
[I-D.morita-tsvwg-pps]	Morita, N. and G. Karlsson, "Framework of Priority Promotion Scheme," draft-morita-tsvwg-pps-01 (work in progress), October 2003 (TXT).
[ITU.MLPP.1990]	International Telecommunications Union, "Multilevel Precedence and Preemption Service," ITU-T Recommendation I.255.3, 1990.
[RFC1633]	Braden, B., Clark, D., and S. Shenker, "Integrated Services in the Internet Architecture: an Overview," RFC 1633, June 1994 (TXT, PS, PDF).
[RFC2205]	Braden, B., Zhang, L., Berson, S., Herzog, S., and S. Jamin, "Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification," RFC 2205, September 1997 (TXT, HTML, XML).
[RFC2208]	Mankin, A., Baker, F., Braden, B., Bradner, S., O'Dell, M., Romanow, A., Weinrib, A., and L. Zhang, "Resource ReSerVation Protocol (RSVP) Version 1 Applicability Statement Some Guidelines on Deployment," RFC 2208, September 1997 (TXT, HTML, XML).
[RFC2475]	Blake, S., Black, D., Carlson, M., Davies, E., Wang, Z., and W. Weiss, "An Architecture for Differentiated Services," RFC 2475, December 1998 (TXT, HTML, XML).
[RFC2904]	Vollbrecht, J., Calhoun, P., Farrell, S., Gommans, L., Gross, G., de Bruijn, B., de Laat, C., Holdrege, M., and D. Spence, "AAA Authorization Framework," RFC 2904, August 2000 (TXT).
[RFC2998]	Bernet, Y., Ford, P., Yavatkar, R., Baker, F., Zhang, L., Speer, M., Braden, R., Davie, B., Wroclawski, J., and E. Felstaine, "A Framework for Integrated Services Operation over Diffserv Networks," RFC 2998, November 2000 (TXT).
[RFC3247]	Charny, A., Bennet, J., Benson, K., Boudec, J., Chiu, A., Courtney, W., Davari, S., Firoiu, V., Kalmanek, C., and K. Ramakrishnan, "Supplemental Information for the New Definition of the EF PHB (Expedited Forwarding Per-Hop Behavior)," RFC 3247, March 2002 (TXT).
[RFC3260]	Grossman, D., "New Terminology and Clarifications for Diffserv," RFC 3260, April 2002 (TXT).

[RFC3312]	Camarillo, G., Marshall, W., and J. Rosenberg, "Integration of Resource Management and Session Initiation Protocol (SIP)," RFC 3312, October 2002 (TXT, PS, PDF).
[RFC4080]	Hancock, R., Karagiannis, G., Loughney, J., and S. Van den Bosch, "Next Steps in Signaling (NSIS): Framework," RFC 4080, June 2005 (TXT).
[RFC4190]	Carlberg, K., Brown, I., and C. Beard, "Framework for Supporting Emergency Telecommunications Service (ETS) in IP Telephony," RFC 4190, November 2005 (TXT).
[RFC4504]	Sinnreich, H., Lass, S., and C. Stredicke, "SIP Telephony Device Requirements and Configuration," RFC 4504, May 2006 (TXT).
[RFC4542]	Baker, F. and J. Polk, "Implementing an Emergency Telecommunications Service (ETS) for Real-Time Services in the Internet Protocol Suite," RFC 4542, May 2006 (TXT).
[RFC4594]	Babiarz, J., Chan, K., and F. Baker, "Configuration Guidelines for DiffServ Service Classes," RFC 4594, August 2006 (TXT).
[RFC5127]	Chan, K., Babiarz, J., and F. Baker, "Aggregation of DiffServ Service Classes," RFC 5127, February 2008 (TXT).

Authors' Addresses

TOC

	Fred Baker
	Cisco Systems
	Santa Barbara, California 93117
	USA
Phone:	+1-408-526-4257
Email:	fred@cisco.com
	James Polk
	Cisco Systems
	Richardson, Texas 75082
	USA
Phone:	+1-817-271-3552
Email:	jmpolk@cisco.com
	Martin Dolly
	AT&T Labs
	Middletown Township, New Jersey 07748
	USA
Phone:	+1-732-420-4574

Email: mdolly@att.com

Full Copyright Statement

TOC

Intellectual Property