Network WG James Polk
Internet-Draft Subha Dhesikan
Expires: August 18, 2013 Paul Jones
Intended Status: Standards Track (PS) Cisco Systems
Feb 18, 2013

The Session Description Protocol (SDP) 'trafficclass' Attribute
draft-ietf-mmusic-traffic-class-for-sdp-03

Abstract

This document proposes a new Session Description Protocol (SDP) attribute to identify the traffic class a session is requesting in its offer/answer exchange.

Status of this Memo

Copyright Notice

Table of Contents

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 [RFC2119].

1. Introduction

The Session Description Protocol (SDP) [RFC4566] provides a means for an offerer to describe the specifics of a session to an answerer, and for the answerer to respond back with its session specifics to the offerer. These session specifics include offering the codec or codecs to choose from, the specific IP address and port number the offerer wants to receive the RTP stream(s) on/at, the particulars about the codecs the offerer wants considered or mandated, and so on.

There are many facets within SDP to determine the Real-time Transport Protocol (RTP) [RFC3550] details for the session establishment between one or more endpoints, but identifying how the underlying network should process each stream still remains under-specified.

The ability to identify a traffic flow by port number gives an indication to underlying network elements to treat traffic with dissimilar ports in a different way, the same or in groups the same - but different from other ports or groups of ports.

Within the context of realtime communications, the labeling of an RTP session based on media descriptor lines as just a voice and/or video session is insufficient, and provides no guidelines to the underlying network on how to treat the traffic. A more granular labeling helps on several fronts to

- inform application layer elements in the signaling path the intent of this session.

- inform the network on how to treat the traffic if the network is configured to differentiate session treatments based on the type of session the RTP is, including the ability to provide call admission control based on the type of traffic in the network.

- allow network monitoring/management of traffic types realtime and after-the-fact analysis.

Some network operators want the ability to guarantee certain traffic gets a minimum amount of network bandwidth per link or through a series of links that make up a network such as a campus or WAN, or a backbone. For example, a call center voice application might get at least 20% of the available link bandwidth.

Some network operators want the ability to allow certain users or devices access to greater bandwidth during non-busy hours than during busy hours of the day. For example, all desktop video might operate at 1080p during non-peak times, but a similar session might be curtailed between the same users or devices to 720p or 360p during peak hours. Another example would be to reduce the frames per second (fps) rate, say from 30fps to 15fps. This case is not as clear as accepting or denying similar sessions during different times of the day, but tuning the access to the bandwidth based on the type of session. In other words, tune down the bandwidth for desktop video during peak hours to allow a 3-screen Telepresence session that would otherwise look like the same type of traffic (RTP, and more granular, video).

RFC 4594 established a guideline for classifying the various flows in the network and the Differentiated Services Codepoint (DSCP) values that apply to many traffic types (table 3 of [RFC4594]), including RTP based voice and video traffic sessions. The RFC also defined the per hop network behavior that is strongly encouraged for each of these application traffic types based on the traffic characteristics and tolerances to delay, loss and jitter within each traffic class.

Video was broken down into four categories in that RFC, and voice in another single category. We do not believe this satisfies the technical and business requirements to accomplish sufficiently unique labeling of RTP traffic.

If the application becomes aware of traffic labeling,

- this can be coded into layer 3 mechanisms.

- this can be coded into layer 4 protocols and/or mechanisms.

- this can be coded into a combination of mechanisms and protocols.

The layer 3 mechanism for differentiating traffic is either the port number or the Differentiated Services Codepoint (DSCP) value [RFC2474]. Within the public Internet, if the application is not part of a managed service, the DSCP value likely will be best effort (BE), or reset to BE when ingressing a provider's network. Within the corporate LAN, this is usually completely configurable and a local IT department can take full advantage of this labeling to shape and manage their network as they see fit.

Within a network core, DiffServ typically does not apply. That said, DiffServ can be used to identify which traffic goes into which MPLS tunnel [RFC4124].

Labeling realtime traffic types using a layer 4 protocol would likely involve RSVP [RFC2205] or NSIS [RFC4080]. RSVP has an Application Identifier (app-ID) defined in [RFC2872] that provides a means for carrying a traffic class label along the media path. An advantage of this mechanism is that the label can inform each domain along the media path what type of traffic this traffic flow is, and allow each domain to adjust the appropriate DSCP value (set by each domain for use within that domain). Meaning, if a DSCP value is set by an endpoint or a router in the first domain and gets reset by a service provider, the far-end domain will be able to reset the DSCP value appropriate for the intended traffic class. There is a proposed extension to RSVP which creates individual profiles for what goes into each app-ID field to describe these traffic classes [ID-RSVP-PROF], which will take advantage of what is described in this document.

There are several proprietary mechanisms that can take advantage of this labeling, but none of those will be discussed here.

The idea of traffic - or service - identification is not new; it has been described in [RFC5897]. If that RFC is used as a guideline, identification that leads to stream differentiation can be quite useful. One of the points within RFC 5897 is that users cannot be allowed to assign any identification (fraud is one reason given). In addition, RFC 5897 recommends that service identification should be done in signaling, rather than guessing or deep packet inspection. Currently, any network would have to guess or perform deep packet inspection to classify traffic and offer the service as per RFC 4594 as such service identification information is currently not available in SDP and therefore to the network elements. Since SDP understands how each stream is created (i.e., the particulars of the RTP stream), this is the right place to have this service differentiated. Such service differentiation can then be communicated to and leveraged by the network.

[Editor's Note: the words "traffic" and "service" are similar enough that the above paragraph talks about RFC 5897's "service identification", but this document only discuss and propose traffic indications in SDP.]

This document proposes a simple attribute line to identify the application a session is requesting in its offer/answer exchange. This document uses previously defined service class strings for consistency between IETF documents.

This document modifies the traffic classes originally created in RFC 4594 in Section 2, incrementing each class with application identifiers and optional adjective strings. Section 3 defines the new SDP attribute "trafficclass". Section 4 discusses the offerer and answerer behavior when generating or receiving this attribute.

2. Traffic Class Framework and Component Definitions

The framework of the traffic class attribute will have at least two parts, called components, allowing for several more to be included further distinguishing a particular session's traffic classification from another session's traffic classification. The amount of indicated differentiation between sessions is not a goal, and should only have additional components for differentiation if there is a need to uniquely identify traffic in different sessions.

The intention is to have a category component (e.g., conversational) that identifies the traffic pattern for a session. Is the traffic within a session one-way or two-way? Can the traffic be buffered before reaching the destination or not? What is this session's tolerance to packet loss and can there be retransmissions?

The application component (e.g., video) identifies the basic type of traffic within a category. Is it media or data packets? If media, which type of media? If data packets, which application of data packets are in this session?

The optional adjective component(s) (e.g., immersive) help to further refine the traffic within a session by providing more description. For instance, if a session is two-way voice, what additional information can be given about this particular session to refine its description? Is it part of a conference or telepresence session? Is it just standalone voice call? Has a capacity admission protocol or mechanism been applied to this session?

The traffic class label will have the following structure,

```
category.application(.adjective)(.adjective)...
```

[Editor's Note: the above is not the exact ABNF to be used. The order is right. The category and application MUST appear first (each only once) and zero or more adjectives can appear following the application component.]

Where
1) the 1st component is the category, and is mandatory;
2) the 2nd component is the application, and is mandatory;
3) an optional 3rd component or series of components are adjective(s) used to further refine the application component;

The construction of the traffic class label for Telepresence video would follow the minimum form of:

```
conversational.video.immersive
```

where there might be one or more adjective after '.immersive'.

There is no traffic class or DSCP value associated with just "conversational". There is a traffic class associated with "conversational.video", creating a differentiation between it and a "conversational.video.immersive" traffic class, which would have DSCP associated with the latter traffic class, depending on local policy. Each category component is defined below, as are several of application and adjective strings.

3. Traffic Class Attribute Definition

This document proposes the 'trafficclass' session and media-level SDP attribute. The following is the Augmented Backus-Naur Form (ABNF) [RFC5234] syntax for this attribute, which is based on the SDP [RFC4566] grammar:

```
attribute              =/ traffic-class-label

traffic-class-label     = "trafficclass" ":" [SP] category
                          "." application *( "." adjective )

category                = "broadcast" /
                          "realtime-interactive" /
                          "multimedia-conferencing" /
                          "multimedia-streaming" /
```

"conversational" / tcl-token

```
   application            = tcl-token

   adjective              = classified-adjective /
                            unclassified-adjective

   classified-adjective   = tcl-token ":" tcl-token

   unclassified-adjective = tcl-token

   tcl-token              = ALPHA *( [ "-" ] ALPHA / DIGIT )
```

The attribute is named "trafficclass", for traffic classification, identifying which one of the five categories applies to the media stream associated with this m-line. There MUST NOT be more than one category component per media line.

The categories in this document are an augmented version of the application labels introduced by table 3 of RFC 4595 (which will be rewritten based on the updated labels and treatments expected for each traffic class defined in this document).

Application Labels Defined in RFC 4594	Category Classes Defined in this document
broadcast-video	broadcast
realtime-interactive	realtime-interactive
multimedia-conferencing	multimedia-conferencing
multimedia-streaming	multimedia-streaming
telephony	conversational

Figure 1. Label Differences from RFC 4594

As is evident from the changes above, from left to right, two labels are different and each of the meanings are different in this document relative to how RFC 4594 defined them. These differences are articulated in Section 4 of this document.

Applications and adjectives are defined using the syntax of "tcl-token" defined above.

RFC 4566 defined SDP as case sensitive. Everything is here as well.

An algorithm such as alphabetizing the list of components and matching the understood strings SHOULD be used for determining the traffic within a session.

Any category, application, or adjective string component within this attribute that is not understood MUST be ignored, leaving all that is understood to be processed. Ignored components SHOULD NOT be deleted, as a downstream entity could understand the component(s) and use it/them during processing.

The following is an example of media level description with a 'trafficclass' attribute:

```
m=video 50000 RTP/AVP 112
a=trafficclass conversational.video.immersive.aq:admitted
```

The above indicates the video part of a Telepresence session that has had capacity admission process applied to its media flow.

3.1 Categories within the SDP Traffic Class Label

The category component within the traffic class attribute describes the type of communication that will occur within that session. It answers these questions, is the traffic

- one-way or two-or-more-way interactive?

- elastic or inelastic (as far as retransmissions)?

- buffered or (virtually) non-buffered?

- media or non-media (data)?

The five category components of the traffic class attribute defined within this specification are as follows:

o conversational
o multimedia-conferencing
o realtime-interactive
o multimedia-streaming
o broadcast

Sections 3.1 through 3.5 define each of the above.

The category component MUST NOT be the only component present in a traffic class attribute. The category component MUST BE paired with an application component to give enough meaning to the traffic class labeling goal.

Not understanding the category component SHOULD mean that this attribute is ignored, because of the information about the communication flow within that component.

3.2 Applications within the SDP Traffic Class Label

The application component identifies the application of a particular traffic flow, for example, audio or video. The application types are listed and defined in Section 2 of this document. Not every category is paired with every application listed, at least as defined in this document. One or more applications are inappropriate in one or more categories. For example, iptv is a single directional traffic application that is suited for the broadcast (one-way) category rather than categories like realtime-interactive or conversational.

Section 4.1 through 4.5 list many of the expected combinations.

3.3 Adjectives within the SDP Traffic Class Label

For additional application type granularity, adjective components can be added. One or more adjectives can be within the same traffic class attribute to provide more differentiation.

It is important to note that while the order of component types matter, the order of the adjective components do not. There might be local significance to the ordering of adjectives though, such as having a pattern matching algorithm in which labels are matched exactly (i.e., the order matters), or not at all. In other words, the category class component MUST be before the application component, which MUST be before any and all adjective component(s).

There is no limit to the number of adjectives allowed.

Adjective components come in two versions, unqualified and qualified. One has a prefix (qualified), the other (unqualified) does not. A defined qualified adjective MUST NOT appear without its qualifier name, even in future extensions to this specification. Some implementations will likely perform a search within this attribute for the presence of qualifiers, which might be as simple as searching for the ":" COLON character. Implementations will be confused with inconsistent coding, therefore strict adherence is necessary.

3.3.1 Qualified Adjectives

Adjectives can be either unqualified or qualified. Qualified adjectives have a delimiter ":" character between the "qualifier name" and the "qualifier value". As one example, we introduce in this specification the "admission qualifier" and it has a qualifier name of "aq". We also define several possible qualifier values for the admission qualifier, namely "admitted", "non-admitted", "partial", and "none". When present in a TCL string, the qualified adjectives look like these admission qualifier adjectives:

```
aq:admitted
aq:non-admitted
aq:partial
aq:none
```

Defining some adjectives as qualified adjectives allows entities processing the traffic class label to potentially recognize a particular qualifier name and act on it, even if it does not understand the qualifier value. In the future, a new admission qualifier value might be defined, e.g. "foo", and entities could at least recognize the admission qualifier adjective, even if it did not understand the qualifier value "foo".

Like all adjectives, it is OPTIONAL to include the admission qualifier adjective in any trafficclass attribute.

The admission qualifier and its qualifier values are defined as:

- aq - 'admission qualifier' - this is the qualifier name for the admission qualifier adjectives, wherein the following qualifier values indicate the admission status for the traffic flow described by this m-line.

- admitted - capacity admission mechanisms or protocols are to be or were used for the full amount of bandwidth in relation to this m= line.

- non-admitted - capacity admission mechanisms or protocols were attempted but failed in relation to this m= line. This does not mean the flow described by this m= line failed. It just failed to attain the capacity admission mechanism or protocol necessary for a predictable quality of service, and is likely to continue with only a class of service marking or best effort.

- partial - capacity admission mechanisms or protocols are to be or were used for the part of the amount of bandwidth in relation to this m= line. All traffic above a certain amount will have no capacity admission mechanisms applied. In other words, there is more traffic sent than was agreed to. The burden is on the sender and receiver to deal with any sent and lost information.

- none - no capacity admission mechanisms or protocols are or were attempted in relation to this m= line.

The default for any flow generated from an m-line not having a trafficclass adjective of 'aq:admitted' or 'aq:non-admitted' MUST be the equivalent of 'aq:none', whether or not it is present.

4. Matching Categories with Applications and Adjectives

This section describes each component within this document, as well as provides the combinations of categories and applications and adjectives. Given that not every combination makes sense, we express the limits here - which will be IANA registered.

4.1 Conversational Category Traffic Class

The "conversational" traffic class is best suited for applications that require very low delay variation and generally intended to enable realtime, bi-directional person-to-person or multi-directional via an MCU communication. Conversational flows are inelastic, and with few exceptions, use a UDP transport.

Traffic Class Name	Traffic Characteristics	Tolerance to Loss	Tolerance to Delay	Tolerance to Jitter
conversational	High priority, typically small packets (large video frames produce large packets), generally sustained high packet rate, low inter-packet transmission interval, usually UDP framed in (S)RTP	Very Low	Very Low	Very Low

Figure 2. Conversational Traffic Characteristics

The following application components are appropriate for use with the Conversational category:

o audio (voice)

o video

o text (i.e., real-time text required by deaf users)

o multiplex (i.e., combined a/v streams)

With adjective substrings to the above

immersive (TP) - An interactive audio-visual communications experience between remote locations, where the users enjoy a strong sense of realism and presence between all participants by optimizing a variety of attributes such as audio and video quality, eye contact, body language, spatial audio, coordinated environments and natural image size.

avconf - An interactive audio-visual communication experience that is not immersive in nature, though can have a high resolution video component.

text - a term for real-time transmission of text in a character-by-character fashion for use in conversational services, often as a text equivalent to voice-based conversational services. Conversational text is defined in the ITU-T Framework for multimedia services, Recommendation F.700 [RFC5194].

Multiplex - an application wherein media of different forms (e.g., audio and video) is multiplexed within the same media flow.

Category	Application	Adjective
conversational	audio	immersive
		avconf
		aq:admitted
		aq:non-admitted
		aq:partial
		aq:none
	video	immersive
		avconf
		aq:admitted
		aq:non-admitted
		aq:partial
		aq:none
	text	aq:admitted
		aq:non-admitted
		aq:partial
		aq:none
	multiplex	aq:admitted
		aq:non-admitted
		aq:partial
		aq:none

Figure 3. Conversational Applications and Adjective Combinations

4.2 Multimedia-Conferencing Category Traffic Class

The "multimedia-conferencing" traffic class is best suited for applications that are generally intended for communication between human users, but are less demanding in terms of delay, packet loss, and jitter than what conversational applications require. These applications require low to medium delay and may have the ability to change encoding rate (rate adaptive) or transmit data at varying rates.

Traffic Class Name	Traffic Characteristics	Tolerance to Loss	Tolerance to Delay	Tolerance to Jitter
multimedia-conferencing	Variable size packets, Variable transmit interval, rate adaptive, reacts to loss, usually TCP-based	Low - Medium	Low - Medium	Low - Medium

Figure 4. Multimedia Conferencing Traffic Characteristics

Multimedia-conferencing flows are not to be media based. Media sessions use other categories. Multimedia-conferencing flows are those data flows that are typically transmitted in parallel to currently active media flows. For example, a two-way conference session in which the users share a presentation. The presentation part of that conference call uses the Multimedia-conferencing category, whereas the audio and any video uses the conversational category indication.

The following application components are appropriate for use with the Multimedia-Conferencing category:

o application-sharing (that webex does or protocols like T.128) - An application that shares the output of one or more running applications or the desktop on a host. This can utilize vector graphics, raster graphics or video.

o presentation-data - can be a series of still images or motion video.

o whiteboarding - an application enabling the exchange of graphical information including images, pointers and filled and unfilled parametric drawing elements (points, lines, polygons and ellipses).

o (RTP-based) file-transfer

o instant messaging

Category	Application	Adjective
multimedia-	application-sharing	aq:admitted

conferencing		aq:non-admitted
		aq:partial

		aq:none
	whiteboarding	aq:admitted
		aq:non-admitted
		aq:partial
		aq:none
	presentation-data	aq:admitted
		aq:non-admitted
		aq:partial
		aq:none
	instant-messaging	aq:admitted
		aq:non-admitted
		aq:partial
		aq:none
	file-transfer	aq:admitted
		aq:non-admitted
		aq:partial
		aq:none

Figure 5. Multimedia Conferencing Applications and Adjective Combinations

4.3 Realtime-Interactive Category Traffic Class

The "Realtime-Interactive" traffic class is intended for interactive variable rate inelastic applications that require low jitter and loss and very low delay. Many of the applications that use the Realtime-Interactive category use TCP or SCTP, even gaming, because lost packets is information that is still required - therefore it is retransmitted.

Traffic Class Name	Traffic Characteristics	Tolerance to Loss	Tolerance to Delay	Tolerance to Jitter
realtime-interactive	Inelastic, mostly variable rate, rate increases with user activity	Low	Very Low	Low

Figure 6. Realtime Interactive Traffic Characteristics

The following application components are appropriate for use with the Realtime-Interactive category:

o gaming - interactive player video games with other users on other hosts (e.g., Doom)

- o remote-desktop - controlling a remote node with local peripherals (i.e., monitor, keyboard and mouse)

- o telemetry - a communication that allows remote measurement and reporting of information (e.g., post launch missile status or energy monitoring)

With adjective substrings to the above

- o virtual - To be used with the remote-desktop application component specifically when the traffic is a virtual desktop similar to an X-windows station, has no local hard drive, or is operating an computer application with no local storage.

Category	Application	Adjective
realtime-interactive	gaming	aq:admitted
		aq:non-admitted
		aq:partial
		aq:none
	remote-desktop	virtual
		aq:admitted
		aq:non-admitted
		aq:partial
		aq:none
	telemetry	aq:admitted
		aq:non-admitted
		aq:partial
		aq:none

Figure 7. Realtime-Interactive Applications and Adjective Combinations

4.4 Multimedia-Streaming Category Traffic Class

The "multimedia-streaming" traffic class is best suited for variable rate elastic streaming media applications where a human is waiting for output and where the application has the capability to react to packet loss by reducing its transmission rate.

Traffic Class Name	Traffic Characteristics	Tolerance to Loss	Delay	Jitter

```
|==============+==============================+======+======+======|
|  multimedia-  | Variable size packets,        |Low - |Medium| High |
```

streaming	elastic with variable rate	Medium	- High	

Figure 8. Multimedia Streaming Traffic Characteristics

The following application components are appropriate for use with the Multimedia-Streaming category:

o audio (see Section 4.1)

o video (see Section 4.1)

o webcast

o multiplex (see Section 4.1)

The primary difference from the multimedia-streaming category and the broadcast category is about the length of time for buffering. Buffered streaming audio and/or video which are initiated by SDP, and not HTTP. Buffering here can be from many seconds to hours, and is typically at the destination end (as opposed to Broadcast buffering which is minimal at the destination). The buffering aspect is what differentiates this category class from the broadcast category (which has minimal or no buffering).

Category	Application	Adjective
multimedia-streaming	audio	aq:admitted
		aq:non-admitted
		aq:partial
		aq:none
	video	aq:admitted
		aq:non-admitted
		aq:partial
		aq:none
	webcast	live
		aq:admitted
		aq:non-admitted
		aq:partial
		aq:none
	multiplex	aq:admitted
		aq:non-admitted
		aq:partial
		aq:none

```
   +----------------------+---------------------+---------------------+
```

Figure 9. Multimedia Streaming Applications and Adjective Combinations

4.5 Broadcast Category Traffic Class

The "broadcast" traffic class is best suited for inelastic streaming media Applications, which might have a 'wardrobe malfunction' delay at or near the source but not typically at the destination, that may be of constant or variable rate, requiring low jitter and very low packet loss.

See Section 4.4 for the difference between Multimedia-Streaming and Broadcast; it all has to do with buffering.

Traffic Class Name	Traffic Characteristics	Tolerance to Loss	Tolerance to Delay	Tolerance to Jitter
broadcast	Constant and variable rate, inelastic, generally non-bursty flows, generally sustained high packet rate, low inter-packet transmission interval, usually UDP framed in (S)RTP	Very Low	Low - Medium	Low - Medium

Figure 10. Broadcast Traffic Characteristics

The following application components are appropriate for use with the Broadcast category:

o audio (see Section 4.1)

o video (see Section 4.1)

o iptv

o multiplex (see Section 4.1)

With adjective substrings to the above:

o live (non-buffered)

o surveillance - one way audio from a microphone or video from a camera (e.g., observing a parking lot or building exit), typically enabled for long periods of time, usually stored at the destination.

Category	Application	Adjective
broadcast	audio	surveillance
		live
		aq:admitted
		aq:non-admitted
		aq:partial
		aq:none
	video	surveillance
		live
		aq:admitted
		aq:non-admitted
		aq:partial
		aq:none
	iptv	live
		aq:admitted
		aq:non-admitted
		aq:partial
		aq:none
	multiplex	aq:admitted
		aq:non-admitted
		aq:partial
		aq:none

Figure 11. Broadcast Applications and Adjective Combinations

5. Offer/Answer Behavior

Through the inclusion of the 'trafficclass' attribute, an offer/answer exchange identifies the application type for use by endpoints within a session. Policy elements can use this attribute to determine the acceptability and/or treatment of that session through lower layers. One specific use-case is for setting of the DSCP specific for that application type (say a broadcast instead of a conversational video), decided on a per domain basis - instead of exclusively by the offering domain.

5.1 Offer Behavior

Offerers include the 'trafficclass' attribute with a single string comprised of two or more components (from the list in Section 2) to obtain configurable and predictable classification between the answerer and the offerer. The offerer can also include a private set of components, or a combination of IANA registered and private components within a single domain (e.g., enterprise networks).

Offerers of this 'trafficclass' attribute MUST NOT change the label in transit (e.g., wrt to B2BUAs). Session Border Controllers (SBC) at domain boundaries can change this attribute through local policy.

Offers containing a 'trafficclass' label not understood are ignored by default (i.e., as if there was no 'trafficclass' attribute in the offer).

5.2 Answer Behavior

Upon receiving an offer containing a 'trafficclass' attribute, if the offer is accepted, the answerer will use this attribute to classify the session or media (level) traffic accordingly towards the offerer. This answer does not need to match the traffic class in the offer, though this will likely be the case most of the time.

In order to understand the traffic class attribute, the answerer MUST check several components within the attribute, such as

1 - does the answerer understand the category component?

If not, the attribute SHOULD be ignored.

If yes, it checks the application component.

2 - does the answerer understand the application component?

If not, the answerer needs to check if it has a local policy to proceed without an application component. The default for this situation is as if the category component was not understand, the attribute SHOULD be ignored.

If yes, it checks to see if there are any adjective components present in this attribute to start its classification.

3 - does the answerer understand the adjective component or components if any are present?

If not present, process and match the trafficclass label value as is.

If yes, determine if there is more than one. Search for each that is understood. Any adjectives not understood are to be ignored, as if they are not present. Match all remaining understood components according to local policy and process attribute.

The answerer will answer the offer with its own 'trafficclass' attribute, which will likely be the same value, although this is not mandatory (at this time). The Offerer will process the received answer just as the answerer processed the offer. In other words, the processing steps and rules are identical for each end.

The answerer should expect to receive RTP packets marked as indicated by its 'trafficclass' attribute in the answer itself.

An Answer MAY have a 'trafficclass' attribute when one was not in the offer. This will at least aid the local domain, and perhaps each domain the session transits, to categorize the application type of this RTP session.

Answerers that are middleboxes can use the 'trafficclass' attribute to classify the RTP traffic within this session however local policy determines. In other words, this attribute can help in deciding which DSCP an RTP stream is assigned within a domain, if the answerer were an inbound SBC to a domain.

6. Security considerations

RFC 5897 [RFC5897] discusses many of the pitfalls of service classification, which is similar enough to this idea of traffic classification to apply here as well. That document highly recommends the user not being able to set any classification. Barring a hack within an endpoint (i.e., to intentionally misclassifying (i.e., lying) about which classification an RTP stream is), this document's solution makes the classification part of the signaling between endpoints, which is recommended by RFC 5897.

7. IANA considerations

7.1 Registration of the SDP 'trafficclass' Attribute

This document requests IANA to register the following SDP att-field under the Session Description Protocol (SDP) Parameters registry:

Contact name: jmpolk@cisco.com

Attribute name: trafficclass

Long-form attribute name: Traffic Classification

Type of attribute: Session and Media levels

Subject to charset: No

Purpose of attribute: To indicate the Traffic Classification application for this session

Allowed attribute values: IANA Registered Tokens

Registration Procedures: Specification Required

Type	SDP Name	Reference
att-field (both session and media level)		
	trafficclass	[this document]

7.2 The Traffic Classification Category Registration

This document requests IANA to create a new registry for the traffic Category classes similar to the following table within the Session Description Protocol (SDP) Parameters registry:

Registry Name: "trafficclass" SDP Category Attribute Values
Reference: [this document]
Registration Procedures: Standards-Track document Required

Category Values	Reference
broadcast	[this document]
realtime-interactive	[this document]
multimedia-conferencing	[this document]
multimedia-streaming	[this document]
conversational	[this document]

7.3 The Traffic Classification Application Type Registration

This document requests IANA to create a new registry for the traffic application classes similar to the following table within the Session Description Protocol (SDP) Parameters registry:

Registry Name: "trafficclass" SDP Application Attribute Type Values
Reference: [this document]
Registration Procedures: Specification Required

Application Values	Reference
audio	[this document]
video	[this document]
text	[this document]
application-sharing	[this document]
presentation-data	[this document]
whiteboarding	[this document]
instant-messaging	[this document]
gaming	[this document]
remote-desktop	[this document]

```
   telemetry                         [this document]
   multiplex                         [this document]
```

```
webcast                        [this document]
iptv                           [this document]
```

7.4 The Traffic Classification Adjective Registration

This document requests IANA to create a new registry for the traffic adjective values similar to the following table within the Session Description Protocol (SDP) Parameters registry:

Registry Name: "trafficclass" SDP Adjective Attribute Values
Reference: [this document]
Registration Procedures: Specification Required

Adjective Values	Reference
immersive	[this document]
avconf	[this document]
realtime	[this document]
web	[this document]
virtual	[this document]
live	[this document]
surveillance	[this document]
aq:admitted	[this document]
aq:non-admitted	[this document]
aq:partial	[this document]
aq:none	[this document]

7.5 The Traffic Classification Component Mapping

7.5.1 Broadcast Applications and Adjective Combinations

This document requests IANA to create a new registry for the Broadcast category mapping similar to Table 11 in Section 4.5 of this document within the Session Description Protocol (SDP) Parameters registry:

Registry Name: Broadcast Applications and Adjective Combinations Table
Reference: [this document]
Registration Procedures: TBD

7.5.2 Realtime Interactive Applications and Adjective Combinations

This document requests IANA to create a new registry for the Realtime Interactive category mapping similar to Table 7 in Section 4.3 of this document within the Session Description Protocol (SDP) Parameters registry:

Registry Name: Realtime Interactive Applications and Adjective

Combinations Table
Reference: [this document]
Registration Procedures: TBD

7.5.3 Multimedia Conferencing Applications and Adjective Combinations

This document requests IANA to create a new registry for the Multimedia Conferencing category mapping similar to Table 5 in Section 4.2 of this document within the Session Description Protocol (SDP) Parameters registry:

Registry Name: Multimedia Conferencing Applications and Adjective
               Combinations Table
Reference: [this document]
Registration Procedures: TBD

7.5.4 Multimedia-Streaming

This document requests IANA to create a new registry for the Multimedia-Streaming category mapping similar to Table 9 in Section 4.4 of this document within the Session Description Protocol (SDP) Parameters registry:

Registry Name: Multimedia-Streaming Applications and Adjective
               Combinations Table
Reference: [this document]
Registration Procedures: TBD

7.5.5 Conversational Applications and Adjective Combinations

This document requests IANA to create a new registry for the conversational category mapping similar to Table 3 in Section 4.1 of this document within the Session Description Protocol (SDP) Parameters registry:

Registry Name: Conversational Applications and Adjective
               Combinations Table
Reference: [this document]
Registration Procedures: TBD

8. Acknowledgments

To Dave Oran, Toerless Eckert, Henry Chen, David Benham, David Benham, Mo Zanty, Michael Ramalho, Glen Lavers, Charles Ganzhorn, Paul Kyzivat, Greg Edwards, Charles Eckel, Dan Wing, Cullen Jennings and Peter Saint-Andre for their comments and suggestions.

9. References

9.1. Normative References

[RFC2119] S. Bradner, "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, March 1997

[RFC2205] R. Braden, Ed., L. Zhang, S. Berson, S. Herzog, S. Jamin, "Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification", RFC 2205, September 1997

[RFC2474] K. Nichols, S. Blake, F. Baker, D. Black, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers ", RFC 2474, December 1998

[RFC2872] Y. Bernet, R. Pabbati, "Application and Sub Application Identity Policy Element for Use with RSVP", RFC 2872, June 2000

[RFC3550] Schulzrinne, H., Casner, S., Frederick, R., and V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications", STD 64, RFC 3550, July 2003.

[RFC4080] R. Hancock, G. Karagiannis, J. Loughney, S. Van den Bosch, "Next Steps in Signaling (NSIS): Framework", RFC 4080, June 2005

[RFC4124] F. Le Faucheur, Ed., " Protocol Extensions for Support of Diffserv-aware MPLS Traffic Engineering ", RFC 4124, June 2005

[RFC4566] M. Handley, V. Jacobson, C. Perkins, "SDP: Session

Description Protocol", RFC 4566, July 2006

[RFC5234] Crocker, D., Ed., and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, January 2008.

[RFC5865] F. Baker, J. Polk, M. Dolly, "A Differentiated Services Code Point (DSCP) for Capacity-Admitted Traffic", RFC 5865, May 2010

[RFC5897] J. Rosenberg, "Identification of Communications Services in the Session Initiation Protocol (SIP)", RFC 5897, June 2010

9.2. Informative References

[RFC4594] J. Babiarz, K. Chan, F Baker, "Configuration Guidelines for

Diffserv Service Classes", RFC 4594, August 2006

[ID-RSVP-PROF] J. Polk, S. Dhesikan, "Resource Reservation Protocol (RSVP) Application-ID Profiles for Voice and Video Streams", work in progress, Feb 2013

Author's Addresses

James Polk
3913 Treemont Circle
Colleyville, Texas, USA
+1.818.271.3552

mailto: jmpolk@cisco.com

Subha Dhesikan
170 W Tasman St
San Jose, CA, USA
+1.408-902-3351

mailto: sdhesika@cisco.com

Paul E. Jones
7025 Kit Creek Rd.
Research Triangle Park, NC, USA
+1 919 476 2048

mailto: paulej@packetizer.com

Appendix - Changes from Previous Versions

A.1 From -02 to -03

These are the following changes made between the WG -02 version and the -03 version:

- Rearranged a fair amount of text

- Separated and defined the components into separate subsections.

- built 5 different tables, one per category, that lists within each category - what applications are appropriate as well as what adjectives are appropriate for each application within that category.

- added the 'partial' admission qualifier for those flows that have only part of their respective flow admitted (i.e., CAC'd).

A.2 From -01 to -02

These are the following changes made between the WG -01 version and the -02 version:

- converged the use of terms 'parent' and 'category' to just 'category' for consistency.

- changed ABNF to reflect extensibility by not having applications and adjectives named in the ABNF, rather have them merely IANA registered.

- merged the qualified and unqualified adjective sections into a single section on adjectives, but allowing some to have a preceding qualifier.

- text clean-up

A.3 From -00 to -01

These are the following changes made between the WG -00 version and the -01 version:

- removed the non-SDP applications Netflix and VOD

- switched the adjective 'desktop' to 'avconf'

- Labeled each of the figures.

- clarified the differences between Multimedia-Streaming and Broadcast category categories.

- defined Video surveillance

- added the concept of a 'qualified' adjective, and modified the ABNF.

- deleted the idea of a 'cac-class' as a separate component, and made the equivalent a qualified adjective.

- modified the answerer behavior because of the removal of the

  'cac-class' component.

- created an IANA registry for qualified adjectives

- general clean-up of the doc.

Did *not* do the following in this version:

- add the ability to have more than one trafficclass attribute based on the codec chosen, as feedback indicated this was a bad idea.

- no swap of the Multimedia-Conferencing category with the offered Collaboration category, as doing this did not solve any perceived problems.

- add more to the 'how does this get processed' portion of Section 3. That will come in the next revision.