Internet Engineering Task Force (IETF)
Request for Comments: 9143
Obsoletes: 8843
Updates: 3264, 5888, 7941
Category: Standards Track
ISSN: 2070-1721

C. Holmberg
Ericsson
H. Alvestrand
Google
C. Jennings
Cisco

February 2022

Negotiating Media Multiplexing Using the Session Description Protocol (SDP)

Abstract

This specification defines a new Session Description Protocol (SDP) Grouping Framework extension called 'BUNDLE'. The extension can be used with the SDP offer/answer mechanism to negotiate the usage of a single transport (5-tuple) for sending and receiving media described by multiple SDP media descriptions ("m=" sections). Such transport is referred to as a "BUNDLE transport", and the media is referred to as "bundled media". The "m=" sections that use the BUNDLE transport form a BUNDLE group.

This specification defines a new RTP Control Protocol (RTCP) Source Description (SDES) item and a new RTP header extension.

This specification updates RFCs 3264, 5888, and 7941.

This specification obsoletes RFC 8843.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9143.

Table of Contents

1. Introduction

1.1. Background

When the SDP offer/answer mechanism [RFC3264] is used to negotiate the establishment of multimedia communication sessions, if separate transports (5-tuples) are negotiated for each individual media stream, each transport consumes additional resources (especially when Interactive Connectivity Establishment (ICE) [RFC8445] is used). For this reason, it is attractive to use a single transport for multiple media streams.

1.2. BUNDLE Mechanism

This specification defines a way to use a single transport (BUNDLE transport) for sending and receiving media (bundled media) described by multiple SDP media descriptions ("m=" sections). The address:port combination used by an endpoint for sending and receiving bundled media is referred to as the "BUNDLE address:port". The set of SDP attributes that are applied to each "m=" section within a BUNDLE group is referred to as "BUNDLE attributes". The same BUNDLE transport is used for sending and receiving bundled media, which means that the symmetric Real-time Transport Protocol (RTP) mechanism [RFC4961] is always used for RTP-based bundled media.

This specification defines a new SDP Grouping Framework [RFC5888] extension called 'BUNDLE'. The extension can be used with the Session Description Protocol (SDP) offer/answer mechanism [RFC3264] to negotiate which "m=" sections will become part of a BUNDLE group. In addition, the offerer and answerer [RFC3264] use the BUNDLE extension to negotiate the BUNDLE addresses:ports (offerer BUNDLE address:port and answerer BUNDLE address:port) and the set of BUNDLE attributes (offerer BUNDLE attributes and answerer BUNDLE attributes) that will be applied to each "m=" section within the BUNDLE group.

The use of a BUNDLE transport allows the usage of a single set of ICE candidates [RFC8445] for the whole BUNDLE group.

A given BUNDLE address:port MUST only be associated with a single BUNDLE group. If an SDP offer or SDP answer (hereafter referred to as "offer" and "answer") contains multiple BUNDLE groups, the procedures in this specification apply to each group independently. All RTP-based bundled media associated with a given BUNDLE group belong to a single RTP session [RFC3550].

The BUNDLE extension is backward compatible. Endpoints that do not support the extension are expected to generate offers and answers without an SDP 'group:BUNDLE' attribute and assign a unique address:port to each "m=" section within an offer and answer, according to the procedures in [RFC3264] and [RFC4566].

1.3. Protocol Extensions

In addition to defining the new SDP Grouping Framework extension, this specification defines the following protocol extensions and makes the following updates to RFCs. This specification:

* defines a new SDP attribute, 'bundle-only', which can be used to request that a specific "m=" section (and the associated media) be used only if kept within a BUNDLE group.

* updates RFC 3264 [RFC3264] to also allow assigning a zero port value to an "m=" section in cases where the media described by the "m=" section is not disabled or rejected.

* defines a new RTCP [RFC3550] SDES item, Media Identification ('MID'), and a new RTP SDES header extension that can be used to associate RTP streams with "m=" sections.

* updates [RFC7941] by adding an exception, for the MID RTP header extension, to the requirement regarding protection of an SDES RTP header extension carrying an SDES item for the MID RTP header extension.

* updates [RFC5888] by allowing an SDP 'group' attribute to contain an identification-tag that identifies an "m=" section with the port value set to zero.

1.4. Changes from RFC 8843

When [RFC8843] and [RFC8829] were published, an inconsistency between the specifications was identified. The procedures regarding assigning the port value to a bundled "m=" section in an answer (initial or subsequent) and a subsequent offer were inconsistent. This specification removes the inconsistency by aligning the port value assignment procedure with the procedure in [RFC8829].

In addition, this document implements changes from the following errata reports: [Err6431], [Err6437].

2. Terminology

"m=" section: SDP bodies contain one or more media descriptions, referred to as "m=" sections. Each "m=" section is represented by an SDP "m=" line and zero or more SDP attributes associated with the "m=" line. A local address:port combination is assigned to each "m=" section.

5-tuple: A collection of the following values: source address, source port, destination address, destination port, and transport-layer protocol.

Unique address:port: An address:port combination that is assigned to only one "m=" section in an offer or answer.

Offerer BUNDLE-tag: The first identification-tag in a given SDP 'group:BUNDLE' attribute identification-tag list in an offer.

Answerer BUNDLE-tag: The first identification-tag in a given SDP 'group:BUNDLE' attribute identification-tag list in an answer.

Suggested offerer-tagged "m=" section: The bundled "m=" section identified by the offerer BUNDLE-tag in an initial BUNDLE offer, before a BUNDLE group has been negotiated.

Offerer-tagged "m=" section: The bundled "m=" section identified by the offerer BUNDLE-tag in a subsequent offer. The "m=" section contains characteristics (offerer BUNDLE address:port and offerer BUNDLE attributes) that are applied to each "m=" section within the BUNDLE group.

Answerer-tagged "m=" section: The bundled "m=" section identified by the answerer BUNDLE-tag in an answer (initial BUNDLE answer or subsequent). The "m=" section contains characteristics (answerer BUNDLE address:port and answerer BUNDLE attributes) that are

applied to each "m=" section within the BUNDLE group.

BUNDLE address:port: An address:port combination that an endpoint uses for sending and receiving bundled media.

Offerer BUNDLE address:port: The address:port combination used by the offerer for sending and receiving media.

Answerer BUNDLE address:port: The address:port combination used by the answerer for sending and receiving media.

BUNDLE attributes: IDENTICAL and TRANSPORT multiplexing category SDP attributes. Once a BUNDLE group has been created, the attribute values apply to each bundled "m=" section within the BUNDLE group.

Offerer BUNDLE attributes: IDENTICAL and TRANSPORT multiplexing category SDP attributes included in the offerer-tagged "m=" section.

Answerer BUNDLE attributes: IDENTICAL and TRANSPORT multiplexing category SDP attributes included in the answerer-tagged "m=" section.

BUNDLE transport: The transport (5-tuple) used by all media described by the "m=" sections within a BUNDLE group.

BUNDLE group: A set of bundled "m=" sections, created using an SDP offer/answer exchange, that uses a single BUNDLE transport and a single set of BUNDLE attributes for sending and receiving all media (bundled media) described by the set of "m=" sections. The same BUNDLE transport is used for sending and receiving bundled media.

Bundled "m=" section: An "m=" section, whose identification-tag is placed in an SDP 'group:BUNDLE' attribute identification-tag list in an offer or answer.

Bundle-only "m=" section: A bundled "m=" section that contains an SDP 'bundle-only' attribute.

Bundled media: All media associated with a given BUNDLE group.

Initial BUNDLE offer: The first offer, within an SDP session (e.g., a SIP dialog when SIP [RFC3261] is used to carry SDP), in which the offerer indicates that it wants to negotiate a given BUNDLE group.

Initial BUNDLE answer: The answer to an initial BUNDLE offer in which the offerer indicates that it wants to negotiate a BUNDLE group, and the answerer accepts the creation of the BUNDLE group. The BUNDLE group is created once the answerer sends the initial BUNDLE answer.

Subsequent offer: An offer that contains a BUNDLE group that has been created as part of a previous offer/answer exchange.

Subsequent answer: An answer to a subsequent offer.

Identification-tag: A unique token value that is used to identify an "m=" section. The SDP 'mid' attribute [RFC5888] in an "m=" section carries the unique identification-tag assigned to that "m=" section. The session-level SDP 'group' attribute [RFC5888] carries a list of identification-tags, identifying the "m=" sections associated with that particular 'group' attribute.

3. Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

4. Applicability Statement

The mechanism in this specification only applies to SDP [RFC4566], when used together with the SDP offer/answer mechanism [RFC3264]. Declarative usage of SDP is out of scope of this document and is thus undefined.

5. SDP Grouping Framework BUNDLE Extension

This section defines a new SDP Grouping Framework [RFC5888] extension, 'BUNDLE'. The BUNDLE extension can be used with the SDP offer/answer mechanism to negotiate a set of "m=" sections that will become part of a BUNDLE group. Within a BUNDLE group, each "m=" section uses a BUNDLE transport for sending and receiving bundled media. Each endpoint uses a single address:port combination for sending and receiving the bundled media.

The BUNDLE extension is indicated using an SDP 'group' attribute with a semantics value [RFC5888] of "BUNDLE". An identification-tag is assigned to each bundled "m=" section, and each identification-tag is listed in the SDP 'group:BUNDLE' attribute identification-tag list. Each "m=" section whose identification-tag is listed in the identification-tag list is associated with a given BUNDLE group.

SDP bodies can contain multiple BUNDLE groups. Any given bundled "m=" section MUST NOT be associated with more than one BUNDLE group at any given time.

NOTE: The order of the "m=" sections listed in the SDP 'group:BUNDLE' attribute identification-tag list does not have to be the same as the order in which the "m=" sections occur in the SDP.

The multiplexing category [RFC8859] for the 'group:BUNDLE' attribute is 'NORMAL'.

Section 7 defines the detailed SDP offer/answer procedures for the BUNDLE extension.

6. SDP 'bundle-only' Attribute

This section defines a new SDP media-level attribute [RFC4566], 'bundle-only'. 'bundle-only' is a property attribute [RFC4566]; hence, it has no value.

In order to ensure that an answerer that does not support the BUNDLE extension always rejects a bundled "m=" section in an offer, the offerer can assign a zero port value to the "m=" section. According to [RFC3264], an answerer will reject such an "m=" section. By including an SDP 'bundle-only' attribute in a bundled "m=" section, the offerer can request that the answerer accept the "m=" section only if the answerer supports the BUNDLE extension and if the answerer keeps the "m=" section within the associated BUNDLE group.

Name: bundle-only

Value: N/A

Usage Level: media

Charset Dependent: no

Example: a=bundle-only

The usage of the 'bundle-only' attribute is only defined for a bundled "m=" section with a zero port value. Other usage is unspecified. If an offerer or answerer receives a 'bundle-only' attribute in a non-bundled "m=" section, the offerer or answerer MUST discard the attribute.

Section 7 defines the detailed SDP offer/answer procedures for the 'bundle-only' attribute.

7. SDP Offer/Answer Procedures

This section describes the SDP offer/answer [RFC3264] procedures for:

* Negotiating a BUNDLE group;

* Suggesting and selecting the tagged "m=" sections (offerer-tagged "m=" section and answerer-tagged "m=" section);

* Adding an "m=" section to a BUNDLE group;

* Moving an "m=" section out of a BUNDLE group; and

* Disabling an "m=" section within a BUNDLE group.

The generic rules and procedures defined in [RFC3264] and [RFC5888] also apply to the BUNDLE extension. For example, if an offer is rejected by the answerer, the previously negotiated addresses:ports, SDP parameters, and characteristics (including those associated with a BUNDLE group) apply. Hence, if an offerer generates an offer in order to negotiate a BUNDLE group and the answerer rejects the offer, the BUNDLE group is not created.

The procedures in this section are independent of the media type or "m=" line proto value assigned to a bundled "m=" section. Section 6 defines additional considerations for the usage of the SDP 'bundle-only' attribute. Section 9 defines additional considerations for RTP-based media. Section 10 defines additional considerations for the usage of the ICE mechanism [RFC8445].

Offers and answers can contain multiple BUNDLE groups. The procedures in this section apply independently to a given BUNDLE group.

7.1. Generic SDP Considerations

This section describes generic restrictions associated with the usage of SDP parameters within a BUNDLE group. It also describes how to calculate a value for the whole BUNDLE group, when parameter and attribute values have been assigned to each bundled "m=" section.

7.1.1. Connection Data ("c=")

The "c=" line nettype value [RFC4566] associated with a bundled "m=" section MUST be 'IN'.

The "c=" line addrtype value [RFC4566] associated with a bundled "m=" section MUST be 'IP4' or 'IP6'. The same value MUST be associated with each "m=" section.

> NOTE: Extensions to this specification can specify usage of the BUNDLE mechanism for other nettype and addrtype values than the ones listed above.

7.1.2. Bandwidth ("b=")

An offerer and answerer MUST use the rules and restrictions defined in [RFC8859] for associating the SDP bandwidth ("b=") line with bundled "m=" sections.

7.1.3. Attributes ("a=")

An offerer and answerer MUST include SDP attributes in every bundled "m=" section where applicable, following the normal offer/answer procedures for each attribute, with the following exceptions:

* In the initial BUNDLE offer, the offerer MUST NOT include IDENTICAL and TRANSPORT multiplexing category SDP attributes (BUNDLE attributes) in bundle-only "m=" sections. The offerer MUST include such attributes in all other bundled "m=" sections. In the initial BUNDLE offer, each bundled "m=" line can contain a different set of BUNDLE attributes and attribute values. Once the offerer-tagged "m=" section has been selected, the BUNDLE attributes contained in the offerer-tagged "m=" section will apply to each bundled "m=" section within the BUNDLE group.

* In a subsequent offer or in an answer (initial or subsequent), the offerer and answerer MUST include IDENTICAL and TRANSPORT multiplexing category SDP attributes (BUNDLE attributes) only in

the tagged "m=" section (offerer-tagged "m=" section or answerer-tagged "m=" section). The offerer and answerer MUST NOT include such attributes in any other bundled "m=" section. The BUNDLE attributes contained in the tagged "m=" section will apply to each bundled "m=" section within the BUNDLE group.

* In an offer (initial BUNDLE offer or subsequent) or in an answer (initial BUNDLE answer or subsequent), the offerer and answerer MUST include SDP attributes from categories other than IDENTICAL and TRANSPORT in each bundled "m=" section that a given attribute applies to. Each bundled "m=" line can contain a different set of such attributes and attribute values, as such attributes only apply to the given bundled "m=" section in which they are included.

  NOTE: A consequence of the rules above is that media-specific IDENTICAL and TRANSPORT multiplexing category SDP attributes that are applicable only to some of the bundled "m=" sections within the BUNDLE group might appear in the tagged "m=" section for which they are not applicable. For instance, the tagged "m=" section might contain an SDP 'rtcp-mux' attribute even if the tagged "m=" section does not describe RTP-based media (but another bundled "m=" section within the BUNDLE group does describe RTP-based media).

7.2. Generating the Initial BUNDLE Offer

The procedures in this section apply to the first offer within an SDP session (e.g., a SIP dialog when SIP [RFC3261] is used to carry SDP) in which the offerer indicates that it wants to negotiate a given BUNDLE group. This could occur in the initial offer, or in a subsequent offer, of the SDP session.

When an offerer generates an initial BUNDLE offer, in order to negotiate a BUNDLE group, it MUST:

* Assign a unique address:port to each bundled "m=" section following the procedures in [RFC3264], excluding any bundle-only "m=" sections (see below);

* Pick a bundled "m=" section as the suggested offerer-tagged "m=" (Section 7.2.1);

* Include SDP attributes in the bundled "m=" sections following the rules in Section 7.1.3;

* Include an SDP 'group:BUNDLE' attribute in the offer; and

* Place the identification-tag of each bundled "m=" section in the SDP 'group:BUNDLE' attribute identification-tag list. The offerer BUNDLE-tag indicates the suggested offerer-tagged "m=" section.

  NOTE: When the offerer assigns unique addresses:ports to multiple bundled "m=" sections, the offerer needs to be prepared to receive bundled media on each unique address:port until it receives the associated answer and finds out which bundled "m=" section (and

associated address:port combination) the answerer has selected as the offerer-tagged "m=" section.

If the offerer wants to request that the answerer accept a given bundled "m=" section only if the answerer keeps the "m=" section within the negotiated BUNDLE group, the offerer MUST:

* Include an SDP 'bundle-only' attribute (Section 7.2.1) in the "m=" section, and

* Assign a zero port value to the "m=" section.

  NOTE: If the offerer assigns a zero port value to a bundled "m=" section but does not include an SDP 'bundle-only' attribute in the "m=" section, it is an indication that the offerer wants to disable the "m=" section (Section 7.5.3).

Sections 7.2.2 and 18.1 show an example of an initial BUNDLE offer.

7.2.1. Suggesting the Offerer-Tagged "m=" Section

In the initial BUNDLE offer, the bundled "m=" section indicated by the offerer BUNDLE-tag is the suggested offerer-tagged "m=" section. The address:port combination associated with the "m=" section will be used by the offerer for sending and receiving bundled media if the answerer selects the "m=" section as the offerer-tagged "m=" section (Section 7.3.1). In addition, if the answerer selects the "m=" section as the offerer-tagged "m=" section, the BUNDLE attributes included in the "m=" section will be applied to each "m=" section within the negotiated BUNDLE group.

The offerer MUST NOT suggest a bundle-only "m=" section as the offerer-tagged "m=" section.

It is RECOMMENDED that the suggested offerer-tagged "m=" section be a bundled "m=" section which the offerer believes is unlikely to be rejected or moved out of the BUNDLE group by the answerer. How such an assumption is made is outside the scope of this document.

7.2.2. Example: Initial BUNDLE Offer

The following example shows an initial BUNDLE offer. The offer includes two "m=" sections in the offer and suggests that both "m=" sections be included in a BUNDLE group. The audio "m=" section is the suggested offerer-tagged "m=" section, indicated by placing the identification-tag associated with the "m=" section (offerer BUNDLE-tag) first in the SDP 'group:BUNDLE' attribute identification-id list.

SDP Offer

```
v=0
o=alice 2890844526 2890844526 IN IP6 2001:db8::3
s=
c=IN IP6 2001:db8::3
t=0 0
```

```
  a=group:BUNDLE foo bar

  m=audio 10000 RTP/AVP 0 8 97
  b=AS:200
  a=mid:foo
  a=rtcp-mux
  a=rtpmap:0 PCMU/8000
  a=rtpmap:8 PCMA/8000
  a=rtpmap:97 iLBC/8000
  a=extmap:1 urn:ietf:params:rtp-hdrext:sdes:mid

  m=video 10002 RTP/AVP 31 32
  b=AS:1000
  a=mid:bar
  a=rtcp-mux
  a=rtpmap:31 H261/90000
  a=rtpmap:32 MPV/90000
  a=extmap:1 urn:ietf:params:rtp-hdrext:sdes:mid
```

The following example shows an initial BUNDLE offer. The offer includes two "m=" sections in the offer and suggests that both "m=" sections are included in a BUNDLE group. The offerer includes an SDP 'bundle-only' attribute in the video "m=" section to request that the answerer accept the "m=" section only if the answerer supports the BUNDLE extension and if the answerer keeps the "m=" section within the associated BUNDLE group. The audio "m=" section is the suggested offerer-tagged "m=" section, indicated by placing the identification-tag associated with the "m=" section (offerer BUNDLE-tag) first in the SDP 'group:BUNDLE' attribute identification-id list.

SDP Offer

```
  v=0
  o=alice 2890844526 2890844526 IN IP6 2001:db8::3
  s=
  c=IN IP6 2001:db8::3
  t=0 0
  a=group:BUNDLE foo bar

  m=audio 10000 RTP/AVP 0 8 97
  b=AS:200
  a=mid:foo
  a=rtcp-mux
  a=rtpmap:0 PCMU/8000
  a=rtpmap:8 PCMA/8000
  a=rtpmap:97 iLBC/8000
  a=extmap:1 urn:ietf:params:rtp-hdrext:sdes:mid

  m=video 0 RTP/AVP 31 32
  b=AS:1000
  a=mid:bar
  a=bundle-only
  a=rtpmap:31 H261/90000
  a=rtpmap:32 MPV/90000
  a=extmap:1 urn:ietf:params:rtp-hdrext:sdes:mid
```

7.3. Generating the SDP Answer

When an answerer generates an answer (initial BUNDLE answer or subsequent) that contains a BUNDLE group, the following general SDP Grouping Framework restrictions, defined in [RFC5888], also apply to the BUNDLE group:

* The answerer is only allowed to include a BUNDLE group in an initial BUNDLE answer if the offerer requested the BUNDLE group to be created in the corresponding initial BUNDLE offer;

* The answerer is only allowed to include a BUNDLE group in a subsequent answer if the corresponding subsequent offer contains a previously negotiated BUNDLE group;

* The answerer is only allowed to include a bundled "m=" section in an answer if the "m=" section was indicated as bundled in the corresponding offer; and

* The answerer is only allowed to include a bundled "m=" section in the same BUNDLE group as the bundled "m=" line in the corresponding offer.

In addition, when an answerer generates an answer (initial BUNDLE answer or subsequent) that contains a BUNDLE group, the answerer MUST:

* In case of an initial BUNDLE answer, select the offerer-tagged "m=" section using the procedures in Section 7.3.1. In case of a subsequent answer, the offerer-tagged "m=" section is indicated in the corresponding subsequent offer and MUST NOT be changed by the answerer;

* Select the answerer-tagged "m=" section (Section 7.3.1);

* Assign the answerer BUNDLE address:port to the answerer-tagged "m=" section and to every other bundled "m=" section within the BUNDLE group;

* Include SDP attributes in the bundled "m=" sections following the rules in Section 7.1.3;

* Include an SDP 'group:BUNDLE' attribute in the answer; and

* Place the identification-tag of each bundled "m=" section in the SDP 'group:BUNDLE' attribute identification-tag list. The answerer BUNDLE-tag indicates the answerer-tagged "m=" section (Section 7.3.1).

If the answerer does not want to keep an "m=" section within a BUNDLE group, it MUST:

* Move the "m=" section out of the BUNDLE group (Section 7.3.2); or

* Reject the "m=" section (Section 7.3.3).

The answerer can modify the answerer BUNDLE address:port, add and remove SDP attributes, or modify SDP attribute values in a subsequent answer. Changes to the answerer BUNDLE address:port and the answerer BUNDLE attributes will be applied to each bundled "m=" section within the BUNDLE group.

NOTE: If a bundled "m=" section in an offer contains a zero port value, but the "m=" section does not contain an SDP 'bundle-only' attribute, it is an indication that the offerer wants to disable the "m=" section (Section 7.5.3).

7.3.1. Answerer Selection of Tagged "m=" Sections

When selecting the offerer-tagged "m=" section, the answerer MUST first check whether the "m=" section fulfills the following criteria (Section 7.2.1):

* The answerer will not move the "m=" section out of the BUNDLE group (Section 7.3.2);

* The answerer will not reject the "m=" section (Section 7.3.3); and

* The "m=" section does not contain a zero port value.

If all of the criteria above are fulfilled, the answerer MUST select the "m=" section as the offerer-tagged "m=" section and MUST also mark the corresponding "m=" section in the answer as the answerer-tagged "m=" section. In the answer, the answerer BUNDLE-tag indicates the answerer-tagged "m=" section.

If one or more of the criteria are not fulfilled, the answerer MUST pick the next identification-tag in the identification-tag list in the offer and perform the same criteria check for the "m=" section indicated by that identification-tag. If there are no more identification-tags in the identification-tag list, the answerer MUST NOT create the BUNDLE group. In addition, unless the answerer rejects the whole offer, the answerer MUST apply the answerer procedures for moving an "m=" section out of a BUNDLE group (Section 7.3.2) or rejecting an "m=" section within a BUNDLE group (Section 7.3.3) to every bundled "m=" section in the offer when creating the answer.

Section 18.1 shows an example of an offerer BUNDLE address:port selection.

Sections 7.3.4 and 18.1 show an example of an answerer-tagged "m=" section selection.

7.3.2. Moving a Media Description Out of a BUNDLE Group

When an answerer generates the answer, the answerer MUST first check the following criteria if it wants to move a bundled "m=" section out of the negotiated BUNDLE group:

* In the corresponding offer, the "m=" section is within a previously negotiated BUNDLE group, and

* In the corresponding offer, the "m=" section contains an SDP 'bundle-only' attribute.

If either criterion above is fulfilled, the answerer cannot move the "m=" section out of the BUNDLE group in the answer. The answerer can reject the whole offer, reject each bundled "m=" section within the BUNDLE group (Section 7.3.3), or keep the "m=" section within the BUNDLE group in the answer and later create an offer where the "m=" section is moved out of the BUNDLE group (Section 7.5.2).

NOTE: One consequence of the rules above is that, once a BUNDLE group has been negotiated, a bundled "m=" section cannot be moved out of the BUNDLE group in an answer. Instead, an offer is needed.

When the answerer generates an answer in which it moves a bundled "m=" section out of a BUNDLE group, the answerer:

* MUST assign a unique address:port to the "m=" section;

* MUST include any applicable SDP attribute in the "m=" section using the normal offer/answer procedures for each attribute;

* MUST NOT place the identification-tag associated with the "m=" section in the SDP 'group:BUNDLE' attribute identification-tag list associated with the BUNDLE group; and

* MUST NOT include an SDP 'bundle-only' attribute to the "m=" section.

Because an answerer is not allowed to move an "m=" section from one BUNDLE group to another within an answer (Section 7.3), if the answerer wants to move an "m=" section from one BUNDLE group to another, it MUST first move the "m=" section out of the current BUNDLE group and then generate an offer where the "m=" section is added to another BUNDLE group (Section 7.5.1).

7.3.3. Rejecting a Media Description in a BUNDLE Group

When an answerer wants to reject a bundled "m=" section in an answer, it MUST first check the following criterion:

* In the corresponding offer (subsequent), the "m=" section is the offerer-tagged "m=" section.

If the criterion above is fulfilled, the answerer cannot reject the "m=" section in the answer. The answerer can reject the whole offer, reject each bundled "m=" section within the BUNDLE group, or keep the "m=" section within the BUNDLE group in the answer and later create an offer where the "m=" section is disabled within the BUNDLE group (Section 7.5.3).

When an answerer generates an answer in which it rejects a bundled "m=" section, the answerer:

* MUST assign a zero port value to the "m=" section, according to the procedures in [RFC3264];

* MUST NOT place the identification-tag associated with the "m=" section in the SDP 'group:BUNDLE' attribute identification-tag list associated with the BUNDLE group; and

* MUST NOT include an SDP 'bundle-only' attribute in the "m=" section.

7.3.4. Example: SDP Answer

The example below shows an answer based on the corresponding offer in Section 7.2.2. The answerer accepts both bundled "m=" sections within the created BUNDLE group. The audio "m=" section is the answerer-tagged "m=" section, indicated by placing the identification-tag associated with the "m=" section (answerer BUNDLE-tag) first in the SDP 'group:BUNDLE' attribute identification-id list.

SDP Answer

```
v=0
o=bob 2808844564 2808844564 IN IP6 2001:db8::1
s=
c=IN IP6 2001:db8::1
t=0 0
a=group:BUNDLE foo bar

m=audio 20000 RTP/AVP 0
b=AS:200
a=mid:foo
a=rtcp-mux
a=rtpmap:0 PCMU/8000
a=extmap:1 urn:ietf:params:rtp-hdrext:sdes:mid

m=video 20000 RTP/AVP 32
b=AS:1000
a=mid:bar
a=rtpmap:32 MPV/90000
a=extmap:1 urn:ietf:params:rtp-hdrext:sdes:mid
```

7.3.5. RFC 8843 Considerations

In [RFC8843], instead of assigning the offerer BUNDLE address:port to each "m=" section within the BUNDLE group when modifying the session (Section 7.5), the offerer only assigned the offerer BUNDLE address:port to the offerer-tagged "m=" section. For every other "m=" section within the BUNDLE group, the offerer included an SDP 'bundle-only' attribute in, and assigned a zero port value to, the "m=" section. The way an answerer compliant with this specification processes such offer is considered an implementation issue (e.g., based on whether the answerer needs to be backward compatible with offerers compliant with [RFC8843]) and is outside the scope of this specification. The example below shows such an SDP Offer:

SDP Offer

```
v=0
o=alice 2890844526 2890844526 IN IP6 2001:db8::3
s=
c=IN IP6 2001:db8::3
t=0 0
a=group:BUNDLE foo bar

m=audio 10000 RTP/AVP 0 8 97
b=AS:200
a=mid:foo
a=rtcp-mux
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:97 iLBC/8000
a=extmap:1 urn:ietf:params:rtp-hdrext:sdes:mid

m=video 0 RTP/AVP 31 32
b=AS:1000
a=mid:bar
a=bundle-only
a=rtpmap:31 H261/90000
a=rtpmap:32 MPV/90000
a=extmap:1 urn:ietf:params:rtp-hdrext:sdes:mid
```

7.4. Offerer Processing of the SDP Answer

When an offerer receives an answer, if the answer contains a BUNDLE group, the offerer MUST check that any bundled "m=" section in the answer was indicated as bundled in the corresponding offer (for the same BUNDLE group). If there is no mismatch, the offerer MUST apply the properties (BUNDLE address:port, BUNDLE attributes, etc.) of the offerer-tagged "m=" section (selected by the answerer; see Section 7.3.1) to each bundled "m=" section within the BUNDLE group.

> NOTE: As the answerer might reject one or more bundled "m=" sections in an initial BUNDLE offer or move a bundled "m=" section out of a BUNDLE group, a given bundled "m=" section in the offer might not be indicated as bundled in the corresponding answer.

If the answer does not contain a BUNDLE group, the offerer MUST process the answer as a normal answer.

7.4.1. RFC 8843 Considerations

In [RFC8843], instead of assigning the answerer BUNDLE address:port to each "m=" section within the BUNDLE group when generating the SDP Answer (Section 7.3), the answerer only assigned the answerer BUNDLE address:port to the answerer-tagged "m=" section. For every other "m=" section within the BUNDLE group, the answerer included an SDP 'bundle-only' attribute in, and assigned a zero port value to, the "m=" section. The way an offerer compliant with this specification processes such an SDP Answer is considered an implementation issue (e.g., based on whether the answerer needs to be backward compatible with offerers compliant with [RFC8843]) and is outside the scope of

this specification. The example below shows such an SDP Answer:

SDP Answer

```
v=0
o=bob 2808844564 2808844564 IN IP6 2001:db8::1
s=
c=IN IP6 2001:db8::1
t=0 0
a=group:BUNDLE foo bar

m=audio 20000 RTP/AVP 0
b=AS:200
a=mid:foo
a=rtcp-mux
a=rtpmap:0 PCMU/8000
a=extmap:1 urn:ietf:params:rtp-hdrext:sdes:mid

m=video 0 RTP/AVP 32
b=AS:1000
a=mid:bar
a=bundle-only
a=rtpmap:32 MPV/90000
a=extmap:1 urn:ietf:params:rtp-hdrext:sdes:mid
```

7.5. Modifying the Session

When a BUNDLE group has been previously negotiated and an offerer generates a subsequent offer, the offerer MUST:

* Pick one bundled "m=" section as the offerer-tagged "m=" section. The offerer can pick either the "m=" section that was previously selected by the answerer as the offerer-tagged "m=" section or another bundled "m=" section within the BUNDLE group;

* Assign a BUNDLE address:port (previously negotiated or newly suggested) to the offerer-tagged "m=" section and to every other bundled "m=" section within the BUNDLE group;

* Include SDP attributes in the bundled "m=" sections following the rules in Section 7.1.3;

* Include an SDP 'group:BUNDLE' attribute in the offer; and

* Place the identification-tag of each bundled "m=" section in the SDP 'group:BUNDLE' attribute identification-tag list. The offerer BUNDLE-tag indicates the offerer-tagged "m=" section.

The offerer MUST NOT pick a given bundled "m=" section as the offerer-tagged "m=" section if:

* The offerer wants to move the "m=" section out of the BUNDLE group (Section 7.5.2), or

* The offerer wants to disable the "m=" section (Section 7.5.3).

The offerer can modify the offerer BUNDLE address:port, add and remove SDP attributes, or modify SDP attribute values in the subsequent offer. Changes to the offerer BUNDLE address:port and the offerer BUNDLE attributes will (if the offer is accepted by the answerer) be applied to each bundled "m=" section within the BUNDLE group.

7.5.1. Adding a Media Description to a BUNDLE Group

When an offerer generates a subsequent offer in which it wants to add a bundled "m=" section to a previously negotiated BUNDLE group, the offerer follows the procedures in Section 7.5. The offerer picks either the added "m=" section or an "m=" section previously added to the BUNDLE group as the offerer-tagged "m=" section.

> NOTE: As described in Section 7.3.2, the answerer cannot move the added "m=" section out of the BUNDLE group in its answer. If the answerer wants to move the "m=" section out of the BUNDLE group, it will have to first accept it into the BUNDLE group in the answer and then send a subsequent offer where the "m=" section is moved out of the BUNDLE group (Section 7.5.2).

7.5.2. Moving a Media Description Out of a BUNDLE Group

When an offerer generates a subsequent offer in which it wants to remove a bundled "m=" section from a BUNDLE group, the offerer:

* MUST assign a unique address:port to the "m=" section;
* MUST include SDP attributes in the "m=" section following the normal offer/answer rules for each attribute;
* MUST NOT place the identification-tag associated with the "m=" section in the SDP 'group:BUNDLE' attribute identification-tag list associated with the BUNDLE group; and
* MUST NOT assign an SDP 'bundle-only' attribute to the "m=" section.

For the other bundled "m=" sections within the BUNDLE group, the offerer follows the procedures in Section 7.5.

An offerer MUST NOT move an "m=" section from one BUNDLE group to another within a single offer. If the offerer wants to move an "m=" section from one BUNDLE group to another, it MUST first move the BUNDLE group out of the current BUNDLE group and then generate a second offer where the "m=" section is added to another BUNDLE group (Section 7.5.1).

Section 18.4 shows an example of an offer for moving an "m=" section out of a BUNDLE group.

7.5.3. Disabling a Media Description in a BUNDLE Group

When an offerer generates a subsequent offer in which it wants to disable a bundled "m=" section from a BUNDLE group, the offerer:

* MUST assign a zero port value to the "m=" section, following the procedures in [RFC4566];

* MUST NOT place the identification-tag associated with the "m=" section in the SDP 'group:BUNDLE' attribute identification-tag list associated with the BUNDLE group; and

* MUST NOT assign an SDP 'bundle-only' attribute to the "m=" section.

For the other bundled "m=" sections within the BUNDLE group, the offerer follows the procedures in Section 7.5.

Section 18.5 shows an example of an offer and answer for disabling an "m=" section within a BUNDLE group.

7.6. 3PCC Considerations

In some third-party call control (3PCC) scenarios, a new session will be established between an endpoint that is currently part of an ongoing session and an endpoint that is not currently part of an ongoing session. In this situation, the endpoint that is not part of a session, while expecting an initial offer, can receive an SDP offer created as a subsequent offer. The text below describes how this can occur with the Session Initiation Protocol (SIP) [RFC3261].

SIP [RFC3261] allows a User Agent Client (UAC) to send a re-INVITE request without an SDP body (sometimes referred to as an "empty re-INVITE"). In such cases, the User Agent Server (UAS) will include an SDP Offer in the associated 200 (OK) response; when the UAS is a part of an ongoing SIP session, this offer will be a subsequent offer. This offer will be received by the 3PCC controller (UAC) and then forwarded to another User Agent (UA). When that UA is not part of an ongoing SIP session, as noted above, it will process the offer as an initial SDP offer.

When the BUNDLE mechanism is used, an initial BUNDLE offer is constructed using different rules than subsequent BUNDLE offers, and it cannot be assumed that a UA is able to correctly process a subsequent BUNDLE offer as an initial BUNDLE offer. Therefore, the 3PCC controller SHOULD take action to mitigate this problem, e.g., rewrite the subsequent BUNDLE offer into a valid initial BUNDLE offer (Section 7.2), before it forwards the BUNDLE offer to a UA.

8. Protocol Identification

Each "m=" section within a BUNDLE group MUST use the same transport-layer protocol. If bundled "m=" sections use different upper-layer protocols on top of the transport-layer protocol, there MUST exist a publicly available specification that describes how a mechanism associates received data with the correct protocol for this particular protocol combination.

In addition, if received data can be associated with more than one bundled "m=" section, there MUST exist a publicly available

specification that describes a mechanism for associating the received data with the correct "m=" section.

This document describes a mechanism to identify the protocol of received data among the Session Traversal Utilities for NAT (STUN), Datagram Transport Layer Security (DTLS), and the Secure Real-time Transport Protocol (SRTP) (in any combination) when UDP is used as a transport-layer protocol, but it does not describe how to identify different protocols transported on DTLS. While the mechanism is generally applicable to other protocols and transport-layer protocols, any such use requires further specification that encompasses how to multiplex multiple protocols on a given transport-layer protocol and how to associate received data with the correct protocols.

8.1. STUN, DTLS, and SRTP

Section 5.1.2 of [RFC5764] describes a mechanism to identify the protocol of a received packet among the STUN, DTLS, and SRTP protocols (in any combination). If an offer or answer includes a bundled "m=" section that represents these protocols, the offerer or answerer MUST support the mechanism described in [RFC5764], and no explicit negotiation is required in order to indicate support and usage of the mechanism.

[RFC5764] does not describe how to identify different protocols transported on DTLS, only how to identify the DTLS protocol itself. If multiple protocols are transported on DTLS, there MUST exist a specification describing a mechanism for identifying each individual protocol. In addition, if a received DTLS packet can be associated with more than one "m=" section, there MUST exist a specification that describes a mechanism for associating the received DTLS packets with the correct "m=" section.

Section 9.2 describes how to associate the packets in a received SRTP stream with the correct "m=" section.

9. RTP Considerations

9.1. Single RTP Session

All RTP-based media within a single BUNDLE group belong to a single RTP session [RFC3550].

Since a single BUNDLE transport is used for sending and receiving bundled media, the symmetric RTP mechanism [RFC4961] MUST be used for RTP-based bundled media.

Since a single RTP session is used for each BUNDLE group, all "m=" sections representing RTP-based media within a BUNDLE group will share a single synchronization source (SSRC) numbering space [RFC3550].

The following rules and restrictions apply for a single RTP session:

* A specific payload type value can be used in multiple bundled "m="

sections only if each codec associated with the payload type number shares an identical codec configuration (Section 9.1.1).

* The proto value in each bundled RTP-based "m=" section MUST be identical (e.g., RTP/AVPF).

* The RTP MID header extension MUST be enabled by including an SDP 'extmap' attribute [RFC8285], with a 'urn:ietf:params:rtp-hdrext:sdes:mid' URI value defined in this specification in each bundled RTP-based "m=" section in every offer and answer.

* A given SSRC MUST NOT transmit RTP packets using payload types that originate from different bundled "m=" sections.

  NOTE: The last bullet above is to avoid sending multiple media types from the same SSRC. If transmission of multiple media types is done with time overlap, RTP and RTCP fail to function. Even if done in the proper sequence, this causes RTP timestamp rate switching issues [RFC7160]. However, once an SSRC has left the RTP session (by sending an RTCP BYE packet), that SSRC can be reused by another source (possibly associated with a different bundled "m=" section) after a delay of 5 RTCP reporting intervals (the delay is to ensure the SSRC has timed out in case the RTCP BYE packet was lost [RFC3550]).

[RFC7657] defines Differentiated Services (Diffserv) considerations for RTP-based bundled media sent using a mixture of Diffserv Codepoints.

9.1.1. Payload Type (PT) Value Reuse

Multiple bundled "m=" sections might describe RTP-based media. As all RTP-based media associated with a BUNDLE group belong to the same RTP session, in order for a given payload type value to be used inside more than one bundled "m=" section, all codecs associated with the payload type number MUST share an identical codec configuration. This means that the codecs MUST share the same media type, encoding name, clock rate, and any parameter that can affect the codec configuration and packetization. [RFC8859] lists SDP attributes whose attribute values are required to be identical for all codecs that use the same payload type value.

9.2. Associating RTP/RTCP Streams with the Correct SDP Media Description

As described in [RFC3550], RTP packets are associated with RTP streams [RFC7656]. Each RTP stream is identified by an SSRC value, and each RTP packet includes an SSRC field that is used to associate the packet with the correct RTP stream. RTCP packets also use SSRCs to identify which RTP streams the packet relates to. However, an RTCP packet can contain multiple SSRC fields in the course of providing feedback or reports on different RTP streams; therefore, they can be associated with multiple such streams.

In order to be able to process received RTP/RTCP packets correctly, it MUST be possible to associate an RTP stream with the correct "m="

section, as the "m=" section and SDP attributes associated with the "m=" section contain information needed to process the packets.

As all RTP streams associated with a BUNDLE group use the same transport for sending and receiving RTP/RTCP packets, the local address:port combination part of the transport cannot be used to associate an RTP stream with the correct "m=" section. In addition, multiple RTP streams might be associated with the same "m=" section.

An offerer and answerer can inform each other which SSRC values they will use for an RTP stream by using the SDP 'ssrc' attribute [RFC5576]. However, an offerer will not know which SSRC values the answerer will use until the offerer has received the answer providing that information. Due to this, before the offerer has received the answer, the offerer will not be able to associate an RTP stream with the correct "m=" section using the SSRC value associated with the RTP stream. In addition, the offerer and answerer may start using new SSRC values mid-session, without informing each other about using the SDP 'ssrc' attribute.

In order for an offerer and answerer to always be able to associate an RTP stream with the correct "m=" section, the offerer and answerer using the BUNDLE extension MUST support the mechanism defined in Section 15, where the offerer and answerer insert the identification-tag associated with an "m=" section (provided by the remote peer) into RTP and RTCP packets associated with a BUNDLE group.

When using this mechanism, the mapping from an SSRC to an identification-tag is carried in RTP header extensions or RTCP SDES packets, as specified in Section 15. Since a compound RTCP packet can contain multiple RTCP SDES packets and each RTCP SDES packet can contain multiple chunks, a single RTCP packet can contain several mappings of SSRC to identification-tag. The offerer and answerer maintain tables used for routing that are updated each time an RTP/RTCP packet contains new information that affects how packets are to be routed.

However, some legacy implementations may not include this identification-tag in their RTP and RTCP traffic when using the BUNDLE mechanism and instead use a mechanism based on the payload type to associate RTP streams with SDP "m=" sections. In this situation, each "m=" section needs to use unique payload type values in order for the payload type to be a reliable indicator of the relevant "m=" section for the RTP stream. If an implementation fails to ensure unique payload type values, it will be impossible to associate the RTP stream using that payload type value to a particular "m=" section. Note that when using the payload type to associate RTP streams with "m=" sections, an RTP stream, identified by its SSRC, will be mapped to an "m=" section when the first packet of that RTP stream is received, and the mapping will not be changed even if the payload type used by that RTP stream changes. In other words, the SSRC cannot "move" to a different "m=" section simply by changing the payload type.

Applications can implement RTP stacks in different ways. The algorithm below details one way that RTP streams can be associated

with "m=" sections, but it is not meant to be prescriptive about exactly how an RTP stack needs to be implemented. Applications MAY use any algorithm that achieves equivalent results to those described in the algorithm below.

To prepare to associate RTP streams with the correct "m=" section, the following steps MUST be followed for each BUNDLE group:

* Construct a table mapping a MID to an "m=" section for each "m=" section in this BUNDLE group. Note that an "m=" section may only have one MID.

* Construct a table mapping SSRCs of incoming RTP streams to an "m=" section for each "m=" section in this BUNDLE group and for each SSRC configured for receiving in that "m=" section.

* Construct a table mapping the SSRC of each outgoing RTP stream to an "m=" section for each "m=" section in this BUNDLE group and for each SSRC configured for sending in that "m=" section.

* Construct a table mapping a payload type to an "m=" section for each "m=" section in the BUNDLE group and for each payload type configured for receiving in that "m=" section. If any payload type is configured for receiving in more than one "m=" section in the BUNDLE group, do not include it in the table, as it cannot be used to uniquely identify an "m=" section.

* Note that for each of these tables, there can only be one mapping for any given key (MID, SSRC, or PT). In other words, the tables are not multimaps.

As "m=" sections are added or removed from the BUNDLE groups or their configurations are changed, the tables above MUST also be updated.

When an RTP packet is received, it MUST be delivered to the RTP stream corresponding to its SSRC. That RTP stream MUST then be associated with the correct "m=" section within a BUNDLE group for additional processing, according to the following steps:

* If the MID associated with the RTP stream is not in the table mapping a MID to an "m=" section, then the RTP stream is not decoded, and the payload data is discarded.

* If the packet has a MID and the packet's extended sequence number is greater than that of the last MID update, as discussed in [RFC7941], Section 4.2.6, update the MID associated with the RTP stream to match the MID carried in the RTP packet and then update the mapping tables to include an entry that maps the SSRC of that RTP stream to the "m=" section for that MID.

* If the SSRC of the RTP stream is in the incoming SSRC mapping table, check that the payload type used by the RTP stream matches a payload type included in the matching "m=" section. If so, associate the RTP stream with that "m=" section. Otherwise, the RTP stream is not decoded, and the payload data is discarded.

* If the payload type used by the RTP stream is in the payload type table, update the incoming SSRC mapping table to include an entry that maps the RTP stream's SSRC to the "m=" section for that payload type. Associate the RTP stream with the corresponding "m=" section.

* Otherwise, mark the RTP stream as "not for decoding" and discard the payload.

If the RTP packet contains one or more contributing source (CSRC) identifiers, then each CSRC is looked up in the incoming SSRC table, and a copy of the RTP packet is associated with the corresponding "m=" section for additional processing.

For each RTCP packet received (including each RTCP packet that is part of a compound RTCP packet), the packet is processed as usual by the RTP layer, then associated with the appropriate "m=" sections and processed for the RTP streams represented by those "m=" sections. This routing is type dependent, as each kind of RTCP packet has its own mechanism for associating it with the relevant RTP streams.

RTCP packets that cannot be associated with an appropriate "m=" section MUST still be processed as usual by the RTP layer, which updates the metadata associated with the corresponding RTP streams. This situation can occur with certain multiparty RTP topologies or when RTCP packets are sent containing a subset of the SDES information.

Additional rules for processing various types of RTCP packets are explained below.

* If the RTCP packet is of type SDES, for each chunk in the packet whose SSRC is found in the incoming SSRC table, deliver a copy of the SDES packet to the "m=" section associated with that SSRC. In addition, for any SDES MID items contained in these chunks, if the MID is found in the table mapping a MID to an "m=" section, update the incoming SSRC table to include an entry that maps the RTP stream associated with the chunk's SSRC to the "m=" section associated with that MID, unless the packet is older than the packet that most recently updated the mapping for this SSRC, as discussed in [RFC7941], Section 4.2.6.

* Note that if an SDES packet is received as part of a compound RTCP packet, the SSRC to "m=" section mapping might not exist until the SDES packet is handled (e.g., in the case where RTCP for a source is received before any RTP packets). Therefore, it can be beneficial for an implementation to delay RTCP packet routing, such that it either prioritizes processing of the SDES item to generate or update the mapping or buffers the RTCP information that needs to be routed until the SDES item(s) has been processed. If the implementation is unable to follow this recommendation, the consequence could be that some RTCP information from this particular RTCP compound packet is not provided to higher layers. The impact from this is likely minor when this information relates to a future incoming RTP stream.

* If the RTCP packet is of type BYE, it indicates that the RTP streams referenced in the packet are ending. Therefore, for each SSRC indicated in the packet that is found in the incoming SSRC table, first deliver a copy of the BYE packet to the "m=" section associated with that SSRC, and then remove the entry for that SSRC from the incoming SSRC table after an appropriate delay to account for "straggler packets", as specified in [RFC3550], Section 6.2.1.

* If the RTCP packet is of type sender report (SR) or receiver report (RR), for each report block in the report whose "SSRC of source" is found in the outgoing SSRC table, deliver a copy of the SR or RR packet to the "m=" section associated with that SSRC. In addition, if the packet is of type SR and the sender SSRC for the packet is found in the incoming SSRC table, deliver a copy of the SR packet to the "m=" section associated with that SSRC.

* If the implementation supports the RTCP Extended Report (XR) and the packet is of type XR, as defined in [RFC3611], for each report block in the report whose "SSRC of source" is found in the outgoing SSRC table, deliver a copy of the XR packet to the "m=" section associated with that SSRC. In addition, if the sender SSRC for the packet is found in the incoming SSRC table, deliver a copy of the XR packet to the "m=" section associated with that SSRC.

* If the RTCP packet is a feedback message of type RTPFB (transport-layer FB message) or PSFB (payload-specific FB message), as defined in [RFC4585], it will contain a media source SSRC, and this SSRC is used for routing certain subtypes of feedback messages. However, several subtypes of PSFB and RTPFB messages include a target SSRC(s) in a section called Feedback Control Information (FCI). For these messages, the target SSRC(s) is used for routing.

* If the RTCP packet is a feedback packet that does not include target SSRCs in its FCI section, and the media source SSRC is found in the outgoing SSRC table, deliver the feedback packet to the "m=" section associated with that SSRC. RTPFB and PSFB types that are handled in this way include:

  Generic NACK: (PT=RTPFB, FMT=1) [RFC4585]

  Picture Loss Indication (PLI): (PT=PSFB, FMT=1) [RFC4585]

  Slice Loss Indication (SLI): (PT=PSFB, FMT=2) [RFC4585]

  Reference Picture Selection Indication (RPSI): (PT=PSFB, FMT=3) [RFC4585]

* If the RTCP packet is a feedback message that does include a target SSRC(s) in its FCI section, it can either be a request or a notification. Requests reference an RTP stream that is being sent by the message recipient, whereas notifications are responses to an earlier request and therefore reference an RTP stream that is being received by the message recipient.

* If the RTCP packet is a feedback request that includes a target SSRC(s), for each target SSRC that is found in the outgoing SSRC table, deliver a copy of the RTCP packet to the "m=" section associated with that SSRC. PSFB and RTPFB types that are handled in this way include:

  Full Intra Request (FIR): (PT=PSFB, FMT=4) [RFC5104]

  Temporal-Spatial Trade-off Request (TSTR): (PT=PSFB, FMT=5) [RFC5104]

  H.271 Video Back Channel Message (VBCM): (PT=PSFB, FMT=7) [RFC5104]

  Temporary Maximum Media Stream Bit Rate Request (TMMBR): (PT=RTPFB, FMT=3) [RFC5104]

  Layer Refresh Request (LRR): (PT=PSFB, FMT=10) [LLR-RTCP].

* If the RTCP packet is a feedback notification that includes a target SSRC(s), for each target SSRC that is found in the incoming SSRC table, deliver a copy of the RTCP packet to the "m=" section associated with the RTP stream with a matching SSRC. PSFB and RTPFB types that are handled in this way include:

  Temporal-Spatial Trade-off Notification (TSTN): (PT=PSFB, FMT=6) [RFC5104]. This message is a notification in response to a prior TSTR.

  Temporary Maximum Media Stream Bit Rate Notification (TMMBN): (PT=RTPFB, FMT=4) [RFC5104]. This message is a notification in response to a prior TMMBR, but it can also be sent unsolicited.

  If the RTCP packet is of type APP, then it is handled in an application-specific manner. If the application does not recognize the APP packet, then it MUST be discarded.

9.3. RTP/RTCP Multiplexing

Within a BUNDLE group, the offerer and answerer MUST enable RTP/RTCP multiplexing [RFC5761] for the RTP-based bundled media (i.e., the same transport will be used for both RTP packets and RTCP packets). In addition, the offerer and answerer MUST support the SDP 'rtcp-mux-only' attribute [RFC8858].

9.3.1. SDP Offer/Answer Procedures

This section describes how an offerer and answerer use the SDP 'rtcp-mux' [RFC5761] and SDP 'rtcp-mux-only' attributes [RFC8858] to negotiate usage of RTP/RTCP multiplexing for RTP-based bundled media.

RTP/RTCP multiplexing only applies to RTP-based media. However, as described in Section 7.1.3, within an offer or answer, the SDP 'rtcp-mux' and SDP 'rtcp-mux-only' attributes might be included in a bundled "m=" section for non-RTP-based media (if such an "m=" section is the offerer-tagged "m=" section or answerer-tagged "m=" section).

9.3.1.1. Generating the Initial BUNDLE Offer

When an offerer generates an initial BUNDLE offer, if the offer contains one or more bundled "m=" sections for RTP-based media (or if there is a chance that "m=" sections for RTP-based media will later be added to the BUNDLE group), the offerer MUST include an SDP 'rtcp-mux' attribute [RFC5761] in each bundled "m=" section (excluding any bundle-only "m=" sections). In addition, the offerer MAY include an SDP 'rtcp-mux-only' attribute [RFC8858] in one or more bundled "m=" sections for RTP-based media.

> NOTE: Whether the offerer includes the SDP 'rtcp-mux-only' attribute depends on whether the offerer supports fallback to usage of a separate port for RTCP in case the answerer moves one or more "m=" sections for RTP-based media out of the BUNDLE group in the answer.
>
> NOTE: If the offerer includes an SDP 'rtcp-mux' attribute in the bundled "m=" sections but does not include an SDP 'rtcp-mux-only' attribute, the offerer can also include an SDP 'rtcp' attribute [RFC3605] in one or more RTP-based bundled "m=" sections in order to provide a fallback port for RTCP, as described in [RFC5761]. However, the fallback port will only be applied to "m=" sections for RTP-based media that are moved out of the BUNDLE group by the answerer.

In the initial BUNDLE offer, the address:port combination for RTCP MUST be unique in each bundled "m=" section for RTP-based media (excluding a bundle-only "m=" section), similar to RTP.

9.3.1.2. Generating the SDP Answer

When an answerer generates an answer, if the answerer supports RTP-based media and if a bundled "m=" section in the corresponding offer contained an SDP 'rtcp-mux' attribute, the answerer MUST enable usage of RTP/RTCP multiplexing, even if there currently are no bundled "m=" sections for RTP-based media within the BUNDLE group. The answerer MUST include an SDP 'rtcp-mux' attribute in the answerer-tagged "m=" section, following the procedures for BUNDLE attributes (Section 7.1.3). In addition, if the "m=" section that is selected as the offerer-tagged "m=" section contained an SDP 'rtcp-mux-only' attribute, the answerer MUST include an SDP 'rtcp-mux-only' attribute in the answerer-tagged "m=" section.

In an initial BUNDLE offer, if the suggested offerer-tagged "m=" section contained an SDP 'rtcp-mux-only' attribute, the "m=" section was for RTP-based media. If the answerer does not accept the "m=" section in the created BUNDLE group and moves the "m=" section out of the BUNDLE group (Section 7.3.2), the answerer MUST include the attribute in the moved "m=" section and enable RTP/RTCP multiplexing for the media associated with the "m=" section. If the answerer rejects the "m=" section (Section 7.3.3), the answerer MUST NOT include the attribute.

The answerer MUST NOT include an SDP 'rtcp' attribute in any bundled

"m=" section in the answer. The answerer will use the port value of the offerer-tagged "m=" section sending RTP and RTCP packets associated with RTP-based bundled media towards the offerer.

If the usage of RTP/RTCP multiplexing within a BUNDLE group has been negotiated in a previous offer/answer exchange, the answerer MUST include an SDP 'rtcp-mux' attribute in the answerer-tagged "m=" section. It is not possible to disable RTP/RTCP multiplexing within a BUNDLE group.

9.3.1.3. Offerer Processing of the SDP Answer

When an offerer receives an answer, if the answerer has accepted the usage of RTP/RTCP multiplexing (Section 9.3.1.2), the answerer follows the procedures for RTP/RTCP multiplexing defined in [RFC5761]. The offerer will use the port value of the answerer-tagged "m=" section for sending RTP and RTCP packets associated with RTP-based bundled media towards the answerer.

> NOTE: It is considered a protocol error if the answerer has not accepted the usage of RTP/RTCP multiplexing for RTP-based "m=" sections that the answerer included in the BUNDLE group.

9.3.1.4. Modifying the Session

When an offerer generates a subsequent offer, the offerer MUST include an SDP 'rtcp-mux' attribute in the offerer-tagged "m=" section, following the procedures for IDENTICAL multiplexing category attributes in Section 7.1.3.

10. ICE Considerations

This section describes how to use the BUNDLE grouping extension together with the ICE mechanism [RFC8445].

The generic procedures for negotiating the usage of ICE using SDP, defined in [RFC8839], also apply to the usage of ICE with BUNDLE, with the following exceptions:

* When the BUNDLE transport has been established, ICE connectivity checks and keepalives only need to be performed for the BUNDLE transport, instead of per individual bundled "m=" section within the BUNDLE group.

* The generic SDP attribute offer/answer considerations (Section 7.1.3) also apply to ICE-related attributes. Therefore, when an offerer sends an initial BUNDLE offer (in order to negotiate a BUNDLE group), the offerer includes ICE-related media-level attributes in each bundled "m=" section (excluding any bundle-only "m=" sections), and each "m=" section MUST contain unique ICE properties. When an answerer generates an answer (initial BUNDLE answer or subsequent) that contains a BUNDLE group and when an offerer sends a subsequent offer that contains a BUNDLE group, ICE-related media-level attributes are only included in the tagged "m=" section (suggested offerer-tagged "m=" section or answerer-tagged "m=" section), and the ICE properties are

applied to each bundled "m=" section within the BUNDLE group.

NOTE: Most ICE-related media-level SDP attributes belong to the TRANSPORT multiplexing category [RFC8859], and the generic SDP attribute offer/answer considerations for the TRANSPORT multiplexing category apply to the attributes. However, in the case of ICE-related attributes, the same considerations also apply to ICE-related media-level attributes that belong to other multiplexing categories.

NOTE: The following ICE-related media-level SDP attributes are defined in [RFC8839]: 'candidate', 'remote-candidates', 'ice-mismatch', 'ice-ufrag', 'ice-pwd', and 'ice-pacing'.

Initially, before ICE has produced selected candidate pairs that will be used for media, there might be multiple transports established (if multiple candidate pairs are tested). Once ICE has selected candidate pairs, they form the BUNDLE transport.

Support and usage of the ICE mechanism together with the BUNDLE extension is OPTIONAL, and the procedures in this section only apply when the ICE mechanism is used. Note that applications might mandate usage of the ICE mechanism even if the BUNDLE extension is not used.

NOTE: If the Trickle ICE mechanism [RFC8840] is used, an offerer and answerer might assign a port value of '9' and an IPv4 address of '0.0.0.0' (or, the IPv6 equivalent '::') to multiple bundled "m=" sections in the initial BUNDLE offer. The offerer and answerer will follow the normal procedures for generating the offers and answers, including picking a bundled "m=" section as the suggested offerer-tagged "m=" section, selecting the tagged "m=" sections, etc. The only difference is that media cannot be sent until one or more candidates have been provided. Once a BUNDLE group has been negotiated, trickled candidates associated with a bundled "m=" section will be applied to all bundled "m=" sections within the BUNDLE group.

11. DTLS Considerations

One or more media streams within a BUNDLE group might use the DTLS protocol [RFC6347] in order to encrypt the data or negotiate encryption keys if another encryption mechanism is used to encrypt media.

When DTLS is used within a BUNDLE group, the following rules apply:

* There can only be one DTLS association [RFC6347] associated with the BUNDLE group;

* Each usage of the DTLS association within the BUNDLE group MUST use the same mechanism for determining which endpoints (the offerer or answerer) become DTLS client and DTLS server;

* Each usage of the DTLS association within the BUNDLE group MUST use the same mechanism for determining whether an offer or answer will trigger the establishment of a new DTLS association or if an

existing DTLS association will be used instead; and

* If the DTLS client supports DTLS-SRTP, it MUST include the 'use_srtp' extension in the DTLS ClientHello message [RFC5764]. The client MUST include the extension even if the usage of DTLS-SRTP is not negotiated as part of the multimedia session (e.g., the SIP session [RFC3261]).

  NOTE: The inclusion of the 'use_srtp' extension during the initial DTLS handshake ensures that a DTLS renegotiation will not be required in order to include the extension in case DTLS-SRTP encrypted media is added to the BUNDLE group later during the multimedia session.

12. RTP Header Extensions Consideration

When RTP header extensions [RFC8285] are used in the context of this specification, the identifier used for a given extension MUST identify the same extension across all the bundled media descriptions.

13. Updates to RFC 3264

This section updates [RFC3264] in order to allow extensions to define the usage of a zero port value in offers and answers for purposes other than removing or disabling media streams. The following sections are being updated:

* "Unicast Streams"; see Section 5.1 of [RFC3264].

* "Putting a Unicast Media Stream on Hold"; see Section 8.4 of [RFC3264].

13.1. Original Text from RFC 3264, Section 5.1, Paragraph 2

> For recvonly and sendrecv streams, the port number and address in the offer indicate where the offerer would like to receive the media stream. For sendonly RTP streams, the address and port number indirectly indicate where the offerer wants to receive RTCP reports. Unless there is an explicit indication otherwise, reports are sent to the port number one higher than the number indicated. The IP address and port present in the offer indicate nothing about the source IP address and source port of RTP and RTCP packets that will be sent by the offerer. A port number of zero in the offer indicates that the stream is offered but MUST NOT be used. This has no useful semantics in an initial offer, but is allowed for reasons of completeness, since the answer can contain a zero port indicating a rejected stream (Section 6). Furthermore, existing streams can be terminated by setting the port to zero (Section 8). In general, a port number of zero indicates that the media stream is not wanted.

13.2. New Text Replacing RFC 3264, Section 5.1, Paragraph 2

> For recvonly and sendrecv streams, the port number and address in the offer indicate where the offerer would like to receive the

> media stream. For sendonly RTP streams, the address and port number indirectly indicate where the offerer wants to receive RTCP reports. Unless there is an explicit indication otherwise, reports are sent to the port number one higher than the number indicated. The IP address and port present in the offer indicate nothing about the source IP address and source port of the RTP and RTCP packets that will be sent by the offerer. By default, a port number of zero in the offer indicates that the stream is offered but MUST NOT be used, but an extension mechanism might specify different semantics for the usage of a zero port value. Furthermore, existing streams can be terminated by setting the port to zero (Section 8). In general, a port number of zero by default indicates that the media stream is not wanted.

13.3. Original Text from RFC 3264, Section 8.4, Paragraph 6

> RFC 2543 [10] specified that placing a user on hold was accomplished by setting the connection address to 0.0.0.0. Its usage for putting a call on hold is no longer recommended, since it doesn't allow for RTCP to be used with held streams, doesn't work with IPv6, and breaks with connection oriented media. However, it can be useful in an initial offer when the offerer knows it wants to use a particular set of media streams and formats, but doesn't know the addresses and ports at the time of the offer. Of course, when used, the port number MUST NOT be zero, which would specify that the stream has been disabled. An agent MUST be capable of receiving SDP with a connection address of 0.0.0.0, in which case it means that neither RTP nor RTCP should be sent to the peer.

13.4. New Text Replacing RFC 3264, Section 8.4, Paragraph 6

> RFC 2543 [RFC2543] specifies that placing a user on hold was accomplished by setting the connection address to 0.0.0.0. Its usage for putting a call on hold is no longer recommended, since it doesn't allow for RTCP to be used with held streams, doesn't work with IPv6, and breaks with connection oriented media. However, it can be useful in an initial offer when the offerer knows it wants to use a particular set of media streams and formats, but doesn't know the addresses and ports at the time of the offer. Of course, when used, the port number MUST NOT be zero, if it would specify that the stream has been disabled. However, an extension mechanism might specify different semantics of the zero port number usage. An agent MUST be capable of receiving SDP with a connection address of 0.0.0.0, in which case it means that neither RTP nor RTCP is to be sent to the peer.

14. Update to RFC 5888

This section updates RFC 5888 [RFC5888] in order for extensions to allow an SDP 'group' attribute containing an identification-tag that identifies an "m=" section with the port set to zero. "Group Value in Answers" (Section 9.2 of [RFC5888]) is updated.

14.1. Original Text from RFC 5888, Section 9.2, Paragraph 3

> SIP entities refuse media streams by setting the port to zero in the corresponding "m" line. "a=group" lines MUST NOT contain identification-tags that correspond to "m" lines with the port set to zero.

14.2. New Text Replacing RFC 5888, Section 9.2, Paragraph 3

> SIP entities refuse media streams by setting the port to zero in the corresponding "m" line. "a=group" lines MUST NOT contain identification-tags that correspond to "m" lines with the port set to zero, but an extension mechanism might specify different semantics for including identification-tags that correspond to such "m=" lines.

15. RTP/RTCP Extensions for identification-tag Transport

Offerers and answerers [RFC3264] can associate identification-tags with "m=" sections within offers and answers using the procedures in [RFC5888]. Each identification-tag uniquely represents an "m=" section.

This section defines a new RTCP SDES item [RFC3550], 'MID', which is used to carry identification-tags within RTCP SDES packets. This section also defines a new RTP SDES header extension [RFC7941], which is used to carry the 'MID' RTCP SDES item in RTP packets.

The SDES item and RTP SDES header extension make it possible for a receiver to associate each RTP stream with a specific "m=" section with which the receiver has associated an identification-tag, even if those "m=" sections are part of the same RTP session. The RTP SDES header extension also ensures that the media recipient gets the identification-tag upon receipt of the first decodable media and is able to associate the media with the correct application.

A media recipient informs the media sender about the identification-tag associated with an "m=" section through the use of a 'mid' attribute [RFC5888]. The media sender then inserts the identification-tag in RTCP and RTP packets sent to the media recipient.

> NOTE: The text above defines how identification-tags are carried in offers and answers. The usage of other signaling protocols for carrying identification-tags is not prevented, but the usage of such protocols is outside the scope of this document.

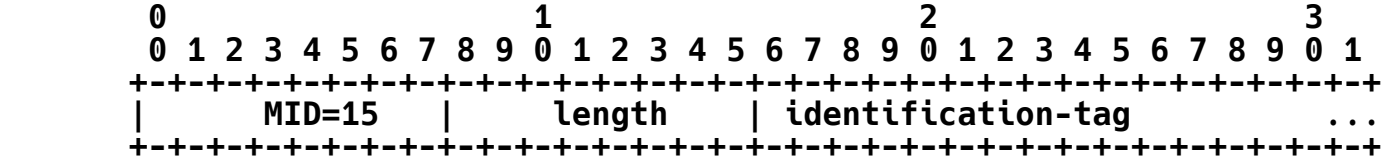
[RFC3550] defines general procedures regarding the RTCP transmission interval. The RTCP MID SDES item SHOULD be sent in the first few RTCP packets after joining the session and SHOULD be sent regularly thereafter. The exact number of RTCP packets in which this SDES item is sent is intentionally not specified here, as it will depend on the expected packet-loss rate, the RTCP reporting interval, and the allowable overhead.

The RTP SDES header extension for carrying the 'MID' RTCP SDES SHOULD be included in some RTP packets at the start of the session and whenever the SSRC changes. It might also be useful to include the

header extension in RTP packets that comprise access points in the media (e.g., with video I-frames). The exact number of RTP packets in which this header extension is sent is intentionally not specified here, as it will depend on expected packet-loss rate and loss patterns, the overhead the application can tolerate, and the importance of immediate receipt of the identification-tag.

For robustness, endpoints need to be prepared for situations where the reception of the identification-tag is delayed and SHOULD NOT terminate sessions in such cases, as the identification-tag is likely to arrive soon.

15.1. RTCP MID SDES Item



The identification-tag payload is UTF-8 encoded [RFC3629], as in SDP.

The identification-tag is not zero terminated.

15.2. RTP SDES Header Extension for MID

The payload, containing the identification-tag, of the RTP SDES header extension element can be encoded using either the 1-byte or the 2-byte header [RFC7941]. The identification-tag payload is UTF-8 encoded, as in SDP.

The identification-tag is not zero terminated. Note that the set of header extensions included in the packet needs to be padded to the next 32-bit boundary using zero bytes [RFC8285].

As the identification-tag is included in an RTCP SDES item, an RTP SDES header extension, or both, there needs to be some consideration about the packet expansion caused by the identification-tag. To avoid Maximum Transmission Unit (MTU) issues for the RTP packets, the header extension's size needs to be taken into account when encoding the media.

It is recommended that the identification-tag be kept short. Due to the properties of the RTP header extension mechanism, when using the 1-byte header, a tag that is 1-3 bytes will result in a minimal number of 32-bit words used for the RTP SDES header extension, in case no other header extensions are included at the same time. Note: do take into account that some single characters when UTF-8 encoded will result in multiple octets. The identification-tag MUST NOT contain any user information, and applications SHALL avoid generating the identification-tag using a pattern that enables user or application identification.

16. IANA Considerations

NOTE: Apart from the references, the IANA considerations in this

section are identical to those in [RFC8843].

16.1. SDES Item

This document updates the MID SDES entry in the "RTP SDES Item Types" registry as follows:

Value: 15
Abbrev.: MID
Name: Media Identification
Reference: RFC 9143

16.2. RTP SDES Header Extension URI

This document updates the extension URI in the "RTP SDES Compact Header Extensions" subregistry of the "RTP Compact Header Extensions" sub-registry, according to the following data:

Extension URI: urn:ietf:params:rtp-hdrext:sdes:mid
Description: Media identification
Contact: IESG (iesg@ietf.org)
Reference: RFC 9143

The SDES item does not reveal privacy information about the users. It is simply used to associate RTP-based media with the correct SDP media description ("m=" section) in the SDP used to negotiate the media.

The purpose of the extension is for the offerer to be able to associate received multiplexed RTP-based media before the offerer receives the associated answer.

16.3. SDP Attribute

This document updates the SDP media-level attribute, 'bundle-only', in the "attribute-name (formerly 'att-field')" subregistry of the "Session Description Protocol (SDP) Parameters" registry according to the following data:

Attribute name: bundle-only
Type of attribute: media
Subject to charset: No
Purpose: Request a media description to be accepted in the answer only if kept within a BUNDLE group by the answerer.
Appropriate values: N/A
Contact name: IESG
Contact e-mail: iesg@ietf.org
Reference: RFC 9143
Mux category: NORMAL

16.4. SDP Group Semantics

This document updates the following semantics in the "Semantics for the 'group' SDP Attribute" subregistry (under the "Session Description Protocol (SDP) Parameters" registry):

Semantics	Token	Mux Category	Reference
Media bundling	BUNDLE	NORMAL	RFC 9143

Table 1: Update to SDP Group Semantics

17. Security Considerations

The security considerations defined in [RFC3264] and [RFC5888] apply to the BUNDLE extension. BUNDLE does not change which information, e.g., RTP streams, flows over the network, except for the usage of the MID SDES item as discussed below. Primarily, it changes which addresses and ports, and thus in which (RTP) sessions, the information flows to. This affects the security contexts being used and can cause previously separated information flows to share the same security context. This has very little impact on the performance of the security mechanism of the RTP sessions. In cases where one would have applied different security policies on the different RTP streams being bundled or where the parties having access to the security contexts would have differed between the RTP streams, additional analysis of the implications is needed before selecting to apply BUNDLE.

The identification-tag, independent of transport, RTCP SDES packet, or RTP header extension, can expose the value to parties beyond the signaling chain. Therefore, the identification-tag values MUST be generated in a fashion that does not leak user information, e.g., randomly or using a per-bundle group counter, and SHOULD be 3 bytes or fewer to allow them to efficiently fit into the MID RTP header extension. Note that if implementations use different methods for generating identification-tags, this could enable fingerprinting of the implementation, making it vulnerable to targeted attacks. The identification-tag is exposed on the RTP stream level when included in the RTP header extensions; however, what it reveals of the RTP media stream structure of the endpoint and application was already possible to deduce from the RTP streams without the MID SDES header extensions. As the identification-tag is also used to route the media stream to the right application functionality, it is important that the value received is the one intended by the sender; thus, integrity and the authenticity of the source are important to prevent denial of service on the application. Existing SRTP configurations and other security mechanisms protecting the whole RTP/RTCP packets will provide the necessary protection.

When the BUNDLE extension is used, the set of configurations of the security mechanism used in all the bundled media descriptions will need to be compatible so that they can be used simultaneously, at least per direction or endpoint. When using SRTP, this will be the case, at least for the IETF-defined key-management solutions due to their SDP attributes ("a=crypto", "a=fingerprint", "a=mikey") and their classification in [RFC8859].

The security considerations of "RTP Header Extension for the RTP Control Protocol (RTCP) Source Description Items" [RFC7941] require

that when RTCP is confidentiality protected, any SDES RTP header extension carrying an SDES item, such as the MID RTP header extension, is also protected using commensurate strength algorithms. However, assuming the above requirements and recommendations are followed, there are no known significant security risks with leaving the MID RTP header extension without confidentiality protection. Therefore, this specification updates [RFC7941] by adding the exception that this requirement MAY be ignored for the MID RTP header extension. Security mechanisms for RTP/RTCP are discussed in "Options for Securing RTP Sessions" [RFC7201]; for example, SRTP [RFC3711] can provide the necessary security functions of ensuring the integrity and source authenticity.

18. Examples

18.1. Example: Tagged "m=" Section Selections

The example below shows:

* An initial BUNDLE offer, in which the offerer wants to negotiate a BUNDLE group and indicates the audio "m=" section as the suggested offerer-tagged "m=" section.

* An initial BUNDLE answer, in which the answerer accepts the creation of the BUNDLE group, selects the audio "m=" section in the offer as the offerer-tagged "m=" section, selects the audio "m=" section in the answer as the answerer-tagged "m=" section, and assigns the answerer BUNDLE address:port to that "m=" section.

SDP Offer (1)

```
v=0
o=alice 2890844526 2890844526 IN IP6 2001:db8::3
s=
c=IN IP6 2001:db8::3
t=0 0
a=group:BUNDLE foo bar

m=audio 10000 RTP/AVP 0 8 97
b=AS:200
a=mid:foo
a=rtcp-mux
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:97 iLBC/8000
a=extmap:1 urn:ietf:params:rtp-hdrext:sdes:mid

m=video 10002 RTP/AVP 31 32
b=AS:1000
a=mid:bar
a=rtcp-mux
a=rtpmap:31 H261/90000
a=rtpmap:32 MPV/90000
a=extmap:1 urn:ietf:params:rtp-hdrext:sdes:mid
```

SDP Answer (2)

```
v=0
o=bob 2808844564 2808844564 IN IP6 2001:db8::1
s=
c=IN IP6 2001:db8::1
t=0 0
a=group:BUNDLE foo bar

m=audio 20000 RTP/AVP 0
b=AS:200
a=mid:foo
a=rtcp-mux
a=rtpmap:0 PCMU/8000
a=extmap:1 urn:ietf:params:rtp-hdrext:sdes:mid

m=video 20000 RTP/AVP 32
b=AS:1000
a=mid:bar
a=rtpmap:32 MPV/90000
a=extmap:1 urn:ietf:params:rtp-hdrext:sdes:mid
```

18.2. Example: BUNDLE Group Rejected

The example below shows:

* An initial BUNDLE offer, in which the offerer wants to negotiate a BUNDLE group and indicates the audio "m=" section as the suggested offerer-tagged "m=" section.

* An initial BUNDLE answer, in which the answerer rejects the creation of the BUNDLE group, generates a normal answer, and assigns a unique address:port to each "m=" section in the answer.

SDP Offer (1)

```
v=0
o=alice 2890844526 2890844526 IN IP6 2001:db8::3
s=
c=IN IP6 2001:db8::3
t=0 0
a=group:BUNDLE foo bar

m=audio 10000 RTP/AVP 0 8 97
b=AS:200
a=mid:foo
a=rtcp-mux
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:97 iLBC/8000
a=extmap:1 urn:ietf:params:rtp-hdrext:sdes:mid

m=video 10002 RTP/AVP 31 32
b=AS:1000
a=mid:bar
a=rtcp-mux
a=rtpmap:31 H261/90000
```

```
    a=rtpmap:32 MPV/90000
    a=extmap:1 urn:ietf:params:rtp-hdrext:sdes:mid
```

SDP Answer (2)

```
    v=0
    o=bob 2808844564 2808844564 IN IP6 2001:db8::1
    s=
    c=IN IP6 2001:db8::1
    t=0 0

    m=audio 20000 RTP/AVP 0
    b=AS:200
    a=rtcp-mux
    a=rtpmap:0 PCMU/8000

    m=video 30000 RTP/AVP 32
    b=AS:1000
    a=rtcp-mux
    a=rtpmap:32 MPV/90000
```

18.3. Example: Offerer Adds a Media Description to a BUNDLE Group

The example below shows:

* A subsequent offer, in which the offerer adds a new bundled "m=" section (video), indicated by the "zen" identification-tag, to a previously negotiated BUNDLE group; indicates the new "m=" section as the offerer-tagged "m=" section; and assigns the offerer BUNDLE address:port to that "m=" section.

* A subsequent answer, in which the answerer indicates the new video "m=" section in the answer as the answerer-tagged "m=" section and assigns the answerer BUNDLE address:port to that "m=" section.

SDP Offer (1)

```
    v=0
    o=alice 2890844526 2890844526 IN IP6 2001:db8::3
    s=
    c=IN IP6 2001:db8::3
    t=0 0
    a=group:BUNDLE zen foo bar

    m=audio 10000 RTP/AVP 0 8 97
    b=AS:200
    a=mid:foo
    a=rtpmap:0 PCMU/8000
    a=rtpmap:8 PCMA/8000
    a=rtpmap:97 iLBC/8000
    a=extmap:1 urn:ietf:params:rtp-hdrext:sdes:mid

    m=video 10000 RTP/AVP 31 32
    b=AS:1000
    a=mid:bar
    a=rtpmap:31 H261/90000
```

```
a=rtpmap:32 MPV/90000
a=extmap:1 urn:ietf:params:rtp-hdrext:sdes:mid

m=video 10000 RTP/AVP 66
b=AS:1000
a=mid:zen
a=rtcp-mux
a=rtpmap:66 H261/90000
a=extmap:1 urn:ietf:params:rtp-hdrext:sdes:mid
```

SDP Answer (2)

```
v=0
o=bob 2808844564 2808844564 IN IP6 2001:db8::1
s=
c=IN IP6 2001:db8::1
t=0 0
a=group:BUNDLE zen foo bar

m=audio 20000 RTP/AVP 0
b=AS:200
a=mid:foo
a=rtpmap:0 PCMU/8000
a=extmap:1 urn:ietf:params:rtp-hdrext:sdes:mid

m=video 20000 RTP/AVP 32
b=AS:1000
a=mid:bar
a=rtpmap:32 MPV/90000
a=extmap:1 urn:ietf:params:rtp-hdrext:sdes:mid

m=video 20000 RTP/AVP 66
b=AS:1000
a=mid:zen
a=rtcp-mux
a=rtpmap:66 H261/90000
a=extmap:1 urn:ietf:params:rtp-hdrext:sdes:mid
```

18.4. Example: Offerer Moves a Media Description Out of a BUNDLE Group

The example below shows:

* A subsequent offer, in which the offerer removes an "m=" section (video), indicated by the "zen" identification-tag, from a previously negotiated BUNDLE group; indicates one of the bundled "m=" sections (audio) remaining in the BUNDLE group as the offerer-tagged "m=" section; and assigns the offerer BUNDLE address:port to that "m=" section.

* A subsequent answer, in which the answerer removes the "m=" section from the BUNDLE group, indicates the audio "m=" section in the answer as the answerer-tagged "m=" section, and assigns the answerer BUNDLE address:port to that "m=" section.

SDP Offer (1)

```
    v=0
    o=alice 2890844526 2890844526 IN IP6 2001:db8::3
    s=
    c=IN IP6 2001:db8::3
    t=0 0
    a=group:BUNDLE foo bar

    m=audio 10000 RTP/AVP 0 8 97
    b=AS:200
    a=mid:foo
    a=rtcp-mux
    a=rtpmap:0 PCMU/8000
    a=rtpmap:8 PCMA/8000
    a=rtpmap:97 iLBC/8000
    a=extmap:1 urn:ietf:params:rtp-hdrext:sdes:mid

    m=video 10000 RTP/AVP 31 32
    b=AS:1000
    a=mid:bar
    a=rtpmap:31 H261/90000
    a=rtpmap:32 MPV/90000
    a=extmap:1 urn:ietf:params:rtp-hdrext:sdes:mid

    m=video 50000 RTP/AVP 66
    b=AS:1000
    a=mid:zen
    a=rtcp-mux
    a=rtpmap:66 H261/90000
```

SDP Answer (2)

```
    v=0
    o=bob 2808844564 2808844564 IN IP6 2001:db8::1
    s=
    c=IN IP6 2001:db8::1
    t=0 0
    a=group:BUNDLE foo bar

    m=audio 20000 RTP/AVP 0
    b=AS:200
    a=mid:foo
    a=rtcp-mux
    a=rtpmap:0 PCMU/8000
    a=extmap:1 urn:ietf:params:rtp-hdrext:sdes:mid

    m=video 20000 RTP/AVP 32
    b=AS:1000
    a=mid:bar
    a=rtpmap:32 MPV/90000
    a=extmap:1 urn:ietf:params:rtp-hdrext:sdes:mid

    m=video 60000 RTP/AVP 66
    b=AS:1000
    a=mid:zen
    a=rtcp-mux
    a=rtpmap:66 H261/90000
```

18.5. Example: Offerer Disables a Media Description within a BUNDLE Group

The example below shows:

* A subsequent offer, in which the offerer disables (by assigning a zero port value) an "m=" section (video), indicated by the "zen" identification-tag, from a previously negotiated BUNDLE group; indicates one of the bundled "m=" sections (audio) remaining active in the BUNDLE group as the offerer-tagged "m=" section; and assigns the offerer BUNDLE address:port to that "m=" section.

* A subsequent answer, in which the answerer disables the "m=" section, indicates the audio "m=" section in the answer as the answerer-tagged "m=" section, and assigns the answerer BUNDLE address:port to that "m=" section.

SDP Offer (1)

```
v=0
o=alice 2890844526 2890844526 IN IP6 2001:db8::3
s=
t=0 0
a=group:BUNDLE foo bar

m=audio 10000 RTP/AVP 0 8 97
c=IN IP6 2001:db8::3
b=AS:200
a=mid:foo
a=rtcp-mux
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:97 iLBC/8000
a=extmap:1 urn:ietf:params:rtp-hdrext:sdes:mid

m=video 10000 RTP/AVP 31 32
c=IN IP6 2001:db8::3
b=AS:1000
a=mid:bar
a=rtpmap:31 H261/90000
a=rtpmap:32 MPV/90000
a=extmap:1 urn:ietf:params:rtp-hdrext:sdes:mid

m=video 0 RTP/AVP 66
a=mid:zen
a=rtpmap:66 H261/90000
```

SDP Answer (2)

```
v=0
o=bob 2808844564 2808844564 IN IP6 2001:db8::1
s=
t=0 0
a=group:BUNDLE foo bar
```

```
m=audio 20000 RTP/AVP 0
c=IN IP6 2001:db8::1
b=AS:200
a=mid:foo
a=rtcp-mux
a=rtpmap:0 PCMU/8000
a=extmap:1 urn:ietf:params:rtp-hdrext:sdes:mid

m=video 20000 RTP/AVP 32
c=IN IP6 2001:db8::1
b=AS:1000
a=mid:bar
a=rtpmap:32 MPV/90000
a=extmap:1 urn:ietf:params:rtp-hdrext:sdes:mid

m=video 0 RTP/AVP 66
a=mid:zen
a=rtpmap:66 H261/90000
```

19. References

19.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC3264] Rosenberg, J. and H. Schulzrinne, "An Offer/Answer Model with Session Description Protocol (SDP)", RFC 3264, DOI 10.17487/RFC3264, June 2002, <https://www.rfc-editor.org/info/rfc3264>.

[RFC3550] Schulzrinne, H., Casner, S., Frederick, R., and V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications", STD 64, RFC 3550, DOI 10.17487/RFC3550, July 2003, <https://www.rfc-editor.org/info/rfc3550>.

[RFC3605] Huitema, C., "Real Time Control Protocol (RTCP) attribute in Session Description Protocol (SDP)", RFC 3605, DOI 10.17487/RFC3605, October 2003, <https://www.rfc-editor.org/info/rfc3605>.

[RFC3629] Yergeau, F., "UTF-8, a transformation format of ISO 10646", STD 63, RFC 3629, DOI 10.17487/RFC3629, November 2003, <https://www.rfc-editor.org/info/rfc3629>.

[RFC3711] Baugher, M., McGrew, D., Naslund, M., Carrara, E., and K. Norrman, "The Secure Real-time Transport Protocol (SRTP)", RFC 3711, DOI 10.17487/RFC3711, March 2004, <https://www.rfc-editor.org/info/rfc3711>.

[RFC4566] Handley, M., Jacobson, V., and C. Perkins, "SDP: Session Description Protocol", RFC 4566, DOI 10.17487/RFC4566, July 2006, <https://www.rfc-editor.org/info/rfc4566>.

[RFC4961] Wing, D., "Symmetric RTP / RTP Control Protocol (RTCP)", BCP 131, RFC 4961, DOI 10.17487/RFC4961, July 2007, <https://www.rfc-editor.org/info/rfc4961>.

[RFC5761] Perkins, C. and M. Westerlund, "Multiplexing RTP Data and Control Packets on a Single Port", RFC 5761, DOI 10.17487/RFC5761, April 2010, <https://www.rfc-editor.org/info/rfc5761>.

[RFC5764] McGrew, D. and E. Rescorla, "Datagram Transport Layer Security (DTLS) Extension to Establish Keys for the Secure Real-time Transport Protocol (SRTP)", RFC 5764, DOI 10.17487/RFC5764, May 2010, <https://www.rfc-editor.org/info/rfc5764>.

[RFC5888] Camarillo, G. and H. Schulzrinne, "The Session Description Protocol (SDP) Grouping Framework", RFC 5888, DOI 10.17487/RFC5888, June 2010, <https://www.rfc-editor.org/info/rfc5888>.

[RFC6347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security Version 1.2", RFC 6347, DOI 10.17487/RFC6347, January 2012, <https://www.rfc-editor.org/info/rfc6347>.

[RFC7941] Westerlund, M., Burman, B., Even, R., and M. Zanaty, "RTP Header Extension for the RTP Control Protocol (RTCP) Source Description Items", RFC 7941, DOI 10.17487/RFC7941, August 2016, <https://www.rfc-editor.org/info/rfc7941>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8285] Singer, D., Desineni, H., and R. Even, Ed., "A General Mechanism for RTP Header Extensions", RFC 8285, DOI 10.17487/RFC8285, October 2017, <https://www.rfc-editor.org/info/rfc8285>.

[RFC8445] Keranen, A., Holmberg, C., and J. Rosenberg, "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal", RFC 8445, DOI 10.17487/RFC8445, July 2018, <https://www.rfc-editor.org/info/rfc8445>.

[RFC8839] Petit-Huguenin, M., Nandakumar, S., Holmberg, C., Keränen, A., and R. Shpount, "Session Description Protocol (SDP) Offer/Answer Procedures for Interactive Connectivity Establishment (ICE)", RFC 8839, DOI 10.17487/RFC8839, January 2021, <https://www.rfc-editor.org/info/rfc8839>.

[RFC8840] Ivov, E., Stach, T., Marocco, E., and C. Holmberg, "A Session Initiation Protocol (SIP) Usage for Incremental Provisioning of Candidates for the Interactive Connectivity Establishment (Trickle ICE)", RFC 8840, DOI 10.17487/RFC8840, January 2021, <https://www.rfc-editor.org/info/rfc8840>.

[RFC8858] Holmberg, C., "Indicating Exclusive Support of RTP and RTP Control Protocol (RTCP) Multiplexing Using the Session Description Protocol (SDP)", RFC 8858, DOI 10.17487/RFC8858, January 2021, <https://www.rfc-editor.org/info/rfc8858>.

[RFC8859] Nandakumar, S., "A Framework for Session Description Protocol (SDP) Attributes When Multiplexing", RFC 8859, DOI 10.17487/RFC8859, January 2021, <https://www.rfc-editor.org/info/rfc8859>.

19.2. Informative References

[Err6431] RFC Errata, Erratum ID 6431, RFC 8843, <https://www.rfc-editor.org/errata/eid6431>.

[Err6437] RFC Errata, Erratum ID 6437, RFC 8843, <https://www.rfc-editor.org/errata/eid6437>.

[LLR-RTCP] Lennox, J., Hong, D., Uberti, J., Holmer, S., and M. Flodman, "The Layer Refresh Request (LRR) RTCP Feedback Message", Work in Progress, Internet-Draft, draft-ietf-avtext-lrr-07, 2 July 2017, <https://datatracker.ietf.org/doc/html/draft-ietf-avtext-lrr-07>.

[RFC2543] Handley, M., Schulzrinne, H., Schooler, E., and J. Rosenberg, "SIP: Session Initiation Protocol", RFC 2543, DOI 10.17487/RFC2543, March 1999, <https://www.rfc-editor.org/info/rfc2543>.

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, DOI 10.17487/RFC3261, June 2002, <https://www.rfc-editor.org/info/rfc3261>.

[RFC3611] Friedman, T., Ed., Caceres, R., Ed., and A. Clark, Ed., "RTP Control Protocol Extended Reports (RTCP XR)", RFC 3611, DOI 10.17487/RFC3611, November 2003, <https://www.rfc-editor.org/info/rfc3611>.

[RFC4585] Ott, J., Wenger, S., Sato, N., Burmeister, C., and J. Rey, "Extended RTP Profile for Real-time Transport Control Protocol (RTCP)-Based Feedback (RTP/AVPF)", RFC 4585, DOI 10.17487/RFC4585, July 2006, <https://www.rfc-editor.org/info/rfc4585>.

[RFC5104] Wenger, S., Chandra, U., Westerlund, M., and B. Burman, "Codec Control Messages in the RTP Audio-Visual Profile with Feedback (AVPF)", RFC 5104, DOI 10.17487/RFC5104, February 2008, <https://www.rfc-editor.org/info/rfc5104>.

[RFC5576] Lennox, J., Ott, J., and T. Schierl, "Source-Specific Media Attributes in the Session Description Protocol

(SDP)", RFC 5576, DOI 10.17487/RFC5576, June 2009,
<https://www.rfc-editor.org/info/rfc5576>.

[RFC7160] Petit-Huguenin, M. and G. Zorn, Ed., "Support for Multiple Clock Rates in an RTP Session", RFC 7160, DOI 10.17487/RFC7160, April 2014, <https://www.rfc-editor.org/info/rfc7160>.

[RFC7201] Westerlund, M. and C. Perkins, "Options for Securing RTP Sessions", RFC 7201, DOI 10.17487/RFC7201, April 2014, <https://www.rfc-editor.org/info/rfc7201>.

[RFC7656] Lennox, J., Gross, K., Nandakumar, S., Salgueiro, G., and B. Burman, Ed., "A Taxonomy of Semantics and Mechanisms for Real-Time Transport Protocol (RTP) Sources", RFC 7656, DOI 10.17487/RFC7656, November 2015, <https://www.rfc-editor.org/info/rfc7656>.

[RFC7657] Black, D., Ed. and P. Jones, "Differentiated Services (Diffserv) and Real-Time Communication", RFC 7657, DOI 10.17487/RFC7657, November 2015, <https://www.rfc-editor.org/info/rfc7657>.

[RFC8829] Uberti, J., Jennings, C., and E. Rescorla, Ed., "JavaScript Session Establishment Protocol (JSEP)", RFC 8829, DOI 10.17487/RFC8829, January 2021, <https://www.rfc-editor.org/info/rfc8829>.

[RFC8838] Ivov, E., Uberti, J., and P. Saint-Andre, "Trickle ICE: Incremental Provisioning of Candidates for the Interactive Connectivity Establishment (ICE) Protocol", RFC 8838, DOI 10.17487/RFC8838, January 2021, <https://www.rfc-editor.org/info/rfc8838>.

[RFC8843] Holmberg, C., Alvestrand, H., and C. Jennings, "Negotiating Media Multiplexing Using the Session Description Protocol (SDP)", RFC 8843, DOI 10.17487/RFC8843, January 2021, <https://www.rfc-editor.org/info/rfc8843>.

Appendix A. Design Considerations

One of the main issues regarding the BUNDLE grouping extensions has been whether, in offers and answers, the same port value can be inserted in "m=" lines associated with a BUNDLE group, as the purpose of the extension is to negotiate the usage of a single transport for media specified by the "m=" sections. Issues with both approaches, discussed in Appendix A, have been raised. The outcome was to specify a mechanism that uses offers with both different and identical port values.

Below are the primary issues that have been considered when defining the "BUNDLE" grouping extension:

1) Interoperability with existing User Agents (UAs).

2) Interoperability with intermediary Back-to-Back User Agent (B2BUA) and proxy entities.

3) The number of ICE candidates and the time to gather them.

4) Different error scenarios and when they occur.

5) SDP offer/answer impacts, including usage of port number value zero.

A.1. UA Interoperability

Consider the following SDP offer/answer exchange, where Alice sends an offer to Bob:

SDP Offer

```
v=0
o=alice 2890844526 2890844526 IN IP4 atlanta.example.com
s=
c=IN IP4 atlanta.example.com
t=0 0

m=audio 10000 RTP/AVP 97
a=rtpmap:97 iLBC/8000
m=video 10002 RTP/AVP 97
a=rtpmap:97 H261/90000
```

SDP Answer

```
v=0
o=bob 2808844564 2808844564 IN IP4 biloxi.example.com
s=
c=IN IP4 biloxi.example.com
t=0 0

m=audio 20000 RTP/AVP 97
a=rtpmap:97 iLBC/8000
m=video 20002 RTP/AVP 97
a=rtpmap:97 H261/90000
```

[RFC4961] specifies a way of doing symmetric RTP, but that is a later extension to RTP, and Bob cannot assume that Alice supports [RFC4961]. This means that Alice may be sending RTP from a different port than 10000 or 10002 -- some implementations simply send the RTP from an ephemeral port. When Bob's endpoint receives an RTP packet, the only way that Bob knows if the packet is to be passed to the video or audio codec is by looking at the port it was received on. This prompted some SDP implementations to use a port number as an index to find the correct "m=" line in the SDP, since each "m"= section contains a different port number. As a result, some implementations that do support symmetric RTP and ICE still use an SDP data structure where SDP with "m=" sections with the same port such as:

SDP Offer

```
v=0
o=alice 2890844526 2890844526 IN IP4 atlanta.example.com
s=
c=IN IP4 atlanta.example.com
t=0 0

m=audio 10000 RTP/AVP 97
a=rtpmap:97 iLBC/8000
m=video 10000 RTP/AVP 98
a=rtpmap:98 H261/90000
```

will result in the second "m=" section being considered an SDP error because it has the same port as the first line.

A.2. Usage of Port Number Value Zero

In an offer or answer, the media specified by an "m=" section can be disabled/rejected by setting the port number value to zero. This is different from, e.g., using the SDP direction attributes, where RTCP traffic will continue even if the SDP 'inactive' attribute is indicated for the associated "m=" section.

If each "m=" section associated with a BUNDLE group were to contain different port values and one of those port values were used for a BUNDLE address:port associated with the BUNDLE group, problems would occur if an endpoint wants to disable/reject the "m=" section associated with that port by setting the port value to zero. After that, no "m=" section would contain the port value that is used for the BUNDLE address:port. In addition, it is unclear what would happen to the ICE candidates associated with the "m=" section, as they are also used for the BUNDLE address:port.

A.3. B2BUA and Proxy Interoperability

Some back-to-back user agents may be configured in a mode where if the incoming call leg contains an SDP attribute the B2BUA does not understand, the B2BUA still generates that SDP attribute in the Offer for the outgoing call leg. Consider a B2BUA that did not understand the SDP 'rtcp' attribute, defined in [RFC3605], yet acted this way. Further, assume that the B2BUA was configured to tear down any call where it did not see any RTCP for 5 minutes. In this case, if the B2BUA received an Offer like:

SDP Offer

```
v=0
o=alice 2890844526 2890844526 IN IP4 atlanta.example.com
s=
c=IN IP4 atlanta.example.com
t=0 0

m=audio 49170 RTP/AVP 0
a=rtcp:53020
```

it would be looking for RTCP on port 49171 but would not see any

because the RTCP would be on port 53020, and after five minutes, it would tear down the call. Similarly, a B2BUA that did not understand BUNDLE yet put it in its offer may be looking for media on the wrong port and tear down the call. It is worth noting that a B2BUA that generated an Offer with capabilities it does not understand is not compliant with the specifications.

A.3.1. Traffic Policing

Sometimes intermediaries do not act as B2BUAs, in the sense that they don't modify SDP bodies nor do they terminate SIP dialogs. However, they may still use SDP information (e.g., IP address and port) in order to control traffic gating functions and to set traffic policing rules. There might be rules that will trigger a session to be terminated in case media is not sent or received on the ports retrieved from the SDP. This typically occurs once the session is already established and ongoing.

A.3.2. Bandwidth Allocation

Sometimes, intermediaries do not act as B2BUAs, in the sense that they don't modify SDP bodies nor do they terminate SIP dialogs. However, they may still use SDP information (e.g., codecs and media types) in order to control bandwidth allocation functions. The bandwidth allocation is done per "m=" section, which means that it might not be enough if media specified by all "m=" sections try to use that bandwidth. That may simply lead to either a bad user experience or termination of the call.

A.4. Candidate Gathering

When using ICE, a candidate needs to be gathered for each port. This takes approximately 20 ms extra for each extra "m=" section due to the NAT pacing requirements. All of this gathering can be overlapped with other things while, e.g., a web page is loading to minimize the impact. If the client only wants to generate Traversal Using Relays around NAT (TURN) or STUN ICE candidates for one of the "m=" lines and then use Trickle ICE [RFC8838] to get the non-host ICE candidates for the rest of the "m=" sections, it MAY do that and will not need any additional gathering time.

Some people have suggested a TURN extension to get a bunch of TURN allocations at once. This would only provide a single STUN result, so in cases where the other end did not support BUNDLE, it may cause more use of the TURN server, but it would be quick in the cases where both sides supported BUNDLE and would fall back to a successful call in the other cases.

Acknowledgements

The usage of the SDP grouping extension for negotiating bundled media is based on similar alternatives proposed by Harald Alvestrand and Cullen Jennings. The BUNDLE extension described in this document is based on the different alternative proposals, and text (e.g., SDP examples) has been borrowed (and, in some cases, modified) from those alternative proposals.

The SDP examples are also modified versions from the ones in the Alvestrand proposal.

Thanks to Paul Kyzivat, Martin Thomson, Flemming Andreasen, Thomas Stach, Ari Keränen, Adam Roach, Christian Groves, Roman Shpount, Suhas Nandakumar, Nils Ohlmeier, Jens Guballa, Raju Makaraju, Justin Uberti, Taylor Brandstetter, Byron Campen, and Eric Rescorla for reading the text and providing useful feedback.

Thanks to Bernard Aboba, Peter Thatcher, Justin Uberti, and Magnus Westerlund for providing the text for the section on RTP/RTCP stream association.

Thanks to Magnus Westerlund, Colin Perkins, and Jonathan Lennox for providing help and text on the RTP/RTCP procedures.

Thanks to Charlie Kaufman for performing the Sec-Dir review.

Thanks to Linda Dunbar for performing the Gen-ART review.

Thanks to Spotify for providing music for the countless hours of document editing.

Authors' Addresses

Christer Holmberg
Ericsson
Hirsalantie 11
FI-02420 Jorvas
Finland
Email: christer.holmberg@ericsson.com

Harald Tveit Alvestrand
Google
Kungsbron 2
SE-11122 Stockholm
Sweden
Email: harald@alvestrand.no

Cullen Jennings
Cisco
Suite 350
400 3rd Avenue SW
Calgary AB T2P 4H2
Canada
Email: fluffy@iii.ca