[MS-TURNBWM]: Traversal using Relay NAT (TURN) Bandwidth Management Extensions

---

Intellectual Property Rights Notice for Open Specifications Documentation

- **Technical Documentation.** Microsoft publishes Open Specifications documentation for protocols, file formats, languages, standards as well as overviews of the interaction among each of these technologies.
- **Copyrights.** This documentation is covered by Microsoft copyrights. Regardless of any other terms that are contained in the terms of use for the Microsoft website that hosts this documentation, you may make copies of it in order to develop implementations of the technologies described in the Open Specifications and may distribute portions of it in your implementations using these technologies or your documentation as necessary to properly document the implementation. You may also distribute in your implementation, with or without modification, any schema, IDL's, or code samples that are included in the documentation. This permission also applies to any documents that are referenced in the Open Specifications.
- **No Trade Secrets.** Microsoft does not claim any trade secret rights in this documentation.
- **Patents.** Microsoft has patents that may cover your implementations of the technologies described in the Open Specifications. Neither this notice nor Microsoft's delivery of the documentation grants any licenses under those or any other Microsoft patents. However, a given Open Specification may be covered by Microsoft's Open Specification Promise (available here: http://www.microsoft.com/interop/osp) or the Community Promise (available here: http://www.microsoft.com/interop/cp/default.mspx). If you would prefer a written license, or if the technologies described in the Open Specifications are not covered by the Open Specifications Promise or Community Promise, as applicable, patent licenses are available by contacting iplg@microsoft.com.
- **Trademarks.** The names of companies and products contained in this documentation may be covered by trademarks or similar intellectual property rights. This notice does not grant any licenses under those rights.
- **Fictitious Names.** The example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted in this documentation are fictitious. No association with any real company, organization, product, domain name, email address, logo, person, place, or event is intended or should be inferred.

Reservation of Rights. All other rights are reserved, and this notice does not grant any rights other than specifically described above, whether by implication, estoppel, or otherwise.

Tools. The Open Specifications do not require the use of Microsoft programming tools or programming environments in order for you to develop an implementation. If you have access to Microsoft programming tools and environments you are free to take advantage of them. Certain Open Specifications are intended for use in conjunction with publicly available standard specifications and network programming art, and assumes that the reader either is familiar with the aforementioned material or has immediate access to it.

Revision Summary

Date	Revision History	Revision Class	Comments
03/31/2010	0.1	Major	Initial Availability
04/30/2010	0.2	Editorial	Revised and edited the technical content
06/07/2010	0.3	Editorial	Revised and edited the technical content
06/29/2010	0.4	Editorial	Changed language and formatting in the technical content.
07/23/2010	0.4	No change	No changes to the meaning, language, or formatting of the technical content.
09/27/2010	1.0	Major	Significantly changed the technical content.
11/15/2010	1.0	No change	No changes to the meaning, language, or formatting of the technical content.
12/17/2010	1.0	No change	No changes to the meaning, language, or formatting of the technical content.
03/18/2011	1.0	No change	No changes to the meaning, language, or formatting of the technical content.
06/10/2011	1.0	No change	No changes to the meaning, language, or formatting of the technical content.

Table of Contents

1 Introduction

This document specifies extensions to the Traversal Using Relay NAT (TURN) protocol, as described in [MS-TURN], to provide support for controlling access to network bandwidth.

1.1 Glossary

The following terms are defined in [MS-GLOS]:

Internet Protocol version 4 (IPv4)
server
Transmission Control Protocol (TCP)
type-length-value (TLV)
User Datagram Protocol (UDP)

The following terms are defined in [MS-OFCGLOS]:

200 OK
call
connectivity check
dialog
federation
INVITE
public switched telephone network (PSTN)
Session Description Protocol (SDP)
Session Initiation Protocol (SIP)
Simple Traversal of UDP through NAT (STUN)
SIP message
transport address
Traversal Using Relay NAT (TURN)
TURN client
TURN server

The following terms are specific to this document:

MAY, SHOULD, MUST, SHOULD NOT, MUST NOT: These terms (in all caps) are used as described in [RFC2119]. All statements of optional behavior use either MAY, SHOULD, or SHOULD NOT.

1.2 References

1.2.1 Normative References

We conduct frequent surveys of the normative references to assure their continued availability. If you have any issue with finding a normative reference, please contact dochelp@microsoft.com. We will assist you in finding the relevant information. Please check the archive site, http://msdn2.microsoft.com/en-us/library/E4BD6494-06AD-4aed-9823-445E921C9624, as an additional source.

[MS-TURN] Microsoft Corporation, "Traversal Using Relay NAT (TURN) Extensions"

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

1.2.2 Informative References

[MS-GLOS] Microsoft Corporation, "Windows Protocols Master Glossary".

[MS-OFCGLOS] Microsoft Corporation, "Microsoft Office Master Glossary".

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and Schooler, E., "SIP: Session Initiation Protocol", RFC 3261, June 2002, http://www.ietf.org/rfc/rfc3261.txt

[RFC4566] Handley, M., Jacobson, V., and Perkins, C., "SDP: Session Description Protocol", RFC 4566, July 2006, http://www.ietf.org/rfc/rfc4566.txt

1.3 Protocol Overview (Synopsis)

Managing and controlling the utilization of network bandwidth is important for an enterprise to reduce cost and to ensure quality of service for applications using network resources. Media communication traffic has the potential to congest and over-utilize the available bandwidth on network links unless the utilization is closely monitored and bandwidth policy restrictions are actively enforced. Even if the bandwidth utilization is known, enforcing the bandwidth policy is difficult because the clients involved in the media session could be dispersed across the enterprise and can be in different geographical or network regions.

This protocol is a proprietary extension to the **Traversal Using Relay NAT (TURN)** protocol, as described in [MS-TURN], which provides support for controlling access to network bandwidth. This extension uses the optional attribute space of the **Simple Traversal of UDP through NAT (STUN)** /TURN protocol to define new attributes that a **TURN client** can use to check for the availability of, and reserve, network bandwidth to be used for the transport of its media streams.

A typical deployment supported by this extension where a client is communicating with a peer over a bandwidth managed network link is shown in the following diagram.

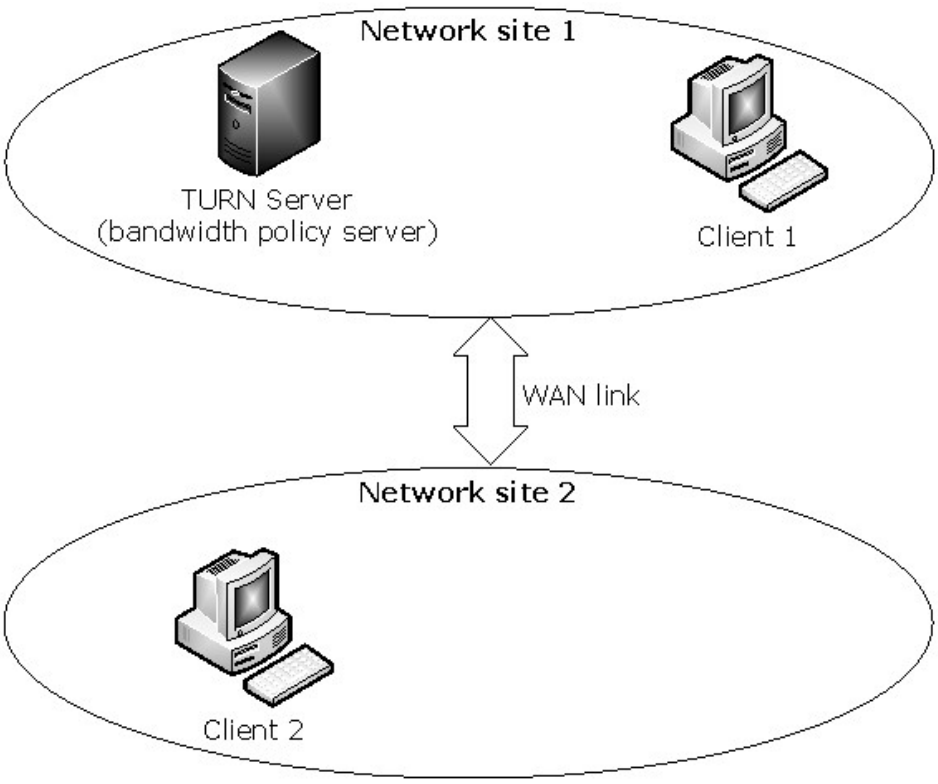


Figure 1: Client communicating with peer

The preceding diagram shows two clients in two different network sites where a network site is made up of a collection of **Internet Protocol version 4 (IPv4)** subnets. Network Site1 might be a corporation's home office while Network Site2 is a regional branch office. Network Site2 connects back to the home office over a WAN Link which has limited bandwidth capacity.

The TURN client named Client1 in Network Site1 is attempting to communicate with the TURN client named Client2 in Network Site2. Client1 allocates a public **transport address** from its **TURN server**. It then uses a signaling protocol, such as the **Session Initiation Protocol (SIP)**, to communicate its local transport address and relay allocated transport address, which is the transport address allocated by the TURN server, to Client2.

When Client2 receives Client1's media transport addresses, it attempts to allocate a public transport address from its TURN server. As part of the allocation attempt, Client2 checks for bandwidth availability across the WAN link. To check for bandwidth availability, Client2 includes the following attributes in its **Allocate Request** message:

- A **Bandwidth Access Control Message** attribute, as specified in section 2.2.1, with a value of "Reservation Check".
- A **Bandwidth Reservation Amount** attribute, as specified in section 2.2.3, with values that cover the bandwidth range required for the media stream.
- A **Remote Site Address** attribute, as specified in section 2.2.4, containing the transport address of Client1.

- A **Remote Relay Site Address** attribute, as specified in section 2.2.5, containing the transport address allocated by Client1's TURN server.
- A **Local Site Address** attribute, as specified in section 2.2.6, containing the local transport address of Client2.
- A **MS-Service Quality** attribute, as specified in [MS-TURN] section 2.2.2.18, containing the type and service quality of the media stream.

The TURN server implementing these extensions uses the transport addresses from the **Reservation Check**, along with the transport address that it allocates on behalf of Client2, to identify the network location of the two clients and their respective TURN servers in the bandwidth admission control network topology. Once it has the network locations of the clients and the TURN servers, it identifies the following network paths; Client1 to Client1 TURN server, Client2 to Client2 TURN server, Client1 to Client2. The **server (2)** checks the policy and available bandwidth for each of these network paths to see if the **Reservation Check** can be satisfied.

When the server (2) finishes checking the network paths, it responds to Client2 with an **Allocate Response** message that includes the following attributes:

- A **Bandwidth Access Control Message** attribute, as specified in section 2.2.1, with a value of "Reservation Check".
- A **Remote Site Address Response** attribute, as specified in section 2.2.8, containing flags indicating the results of the bandwidth policy check along with the bandwidth range available to be used by the transport address that was included in the **Remote Site Address** attribute, as specified in section 2.2.4, of the **Reservation Check** request.
- A **Remote Relay Site Address Response** attribute, as specified in section 2.2.9, containing flags indicating the results of the bandwidth policy check along with the maximum bandwidth available to be used by the transport address that was included in the **Remote Relay Site Address** attribute, as specified in section 2.2.5, of the **Reservation Check** request.
- A **Local Site Address Response** attribute, as specified in section 2.2.10, containing flags indicating the results of the bandwidth policy check along with the maximum bandwidth available to be used by the transport address that was included in the **Local Site Address** attribute, as specified in section 2.2.6, of the **Reservation Check** request.
- A **Local Relay Site Address Response** attribute, as specified in section 2.2.11, containing flags indicating the results of the bandwidth policy check along with the maximum bandwidth available to be used by the transport address that was allocated by the TURN server as a result of the **Allocate Request** message.

Client2 can now use any of the transport addresses that were marked as valid by the server (2) to run **connectivity checks** to Client1. If none of the transport addresses were marked valid, Client2 fails the connection attempt for lack of network bandwidth resources. When Client2 finishes connectivity checks, it notifies the server (2) of the transport addresses it is using for the media stream. Client2 does this notification by including the following attributes in another **Allocate Request** message:

- A **Bandwidth Access Control Message** attribute, as specified in section 2.2.1, with a value of "Reservation Commit".
- A **Bandwidth Reservation Amount** attribute, as specified in section 2.2.3, with values that identify the bandwidth to be used for the media stream.

- A **Remote Site Address** attribute, as specified in section 2.2.4, containing the transport address of Client1.
- If Client1 is using the transport address allocated by its TURN server, a **Remote Relay Site Address** attribute, as specified in section 2.2.9, is included with the public transport address allocated by Client1's TURN server.
- A **Local Site Address** attribute, as specified in section 2.2.6, containing the transport address of Client2.
- If Client2 is using the transport address allocated by its TURN server, a **Local Relay Site Address** attribute, as specified in section 2.2.7, is included with the public transport address allocated by Client2's TURN server.

When the server (2) receives the **Reservation Commit** message from Client2, it uses the site address attributes included in the message to locate the network sites used by clients. Once it has the network locations of the clients, it identifies the network paths that will be used for this reservation and commits the bandwidth amount of the reservation against the network paths. This reduces the amount of bandwidth that is available for future calls over these network paths. After completing the bandwidth reservation, the server (2) replies to the client letting it know that the bandwidth has been reserved for the media stream. It sends this reply in an **Allocate Response** message and includes the following attributes:

- A **Bandwidth Access Control Message** attribute, as specified in section 2.2.1, with a value of "Reservation Commit".
- A **Bandwidth Reservation Identifier** attribute, as specified in section 2.2.2, with a value that identifies the reservation with the server (2). This identifier is used in all subsequent update/change, cancellation, and bandwidth update messages dealing with the reservation.

After Client2 has committed a bandwidth reservation with the server (2), it can attempt to increase or decrease the amount of bandwidth it has reserved for the media stream by sending a reservation update request to the server (2). The client notifies the server (2) of this update request by sending another authenticated **Allocate Request** message:

- A **Bandwidth Access Control Message** attribute, as specified in section 2.2.1, with a value of "Reservation Update".
- A **Bandwidth Reservation Identifier** attribute, as specified in section 2.2.2, with the reservation id value returned by the server (2) in response to the **Reservation Commit** message.
- A **Bandwidth Reservation Amount** attribute, as specified in section 2.2.3, with values that identify the bandwidth to be used for the media stream.

When the server (2) receives the **Reservation Update** message from Client2, it uses the reservation id to identify the existing bandwidth reservation and the network paths involved in the reservation. The server (2) can update the reservation with the new values requested by the client, increasing or decreasing the bandwidth as requested. After completing the bandwidth reservation update, the server (2) replies to the client letting it know the amount of bandwidth that has been reserved for the media stream. It sends this reply in an **Allocate Response** message and includes the following attributes:

- A **Bandwidth Access Control Message** attribute, as specified in section 2.2.1, with a value of **Reservation Update**.

- A **Bandwidth Reservation Identifier** attribute, as specified in section 2.2.2, with a value that identifies the reservation with the server (2).
- A **Bandwidth Reservation Amount** attribute, as specified in section 2.2.3, with values that identify the bandwidth that is reserved for the media stream.

The basic message flow for a scenario that uses SIP for signaling is shown in the following diagram.

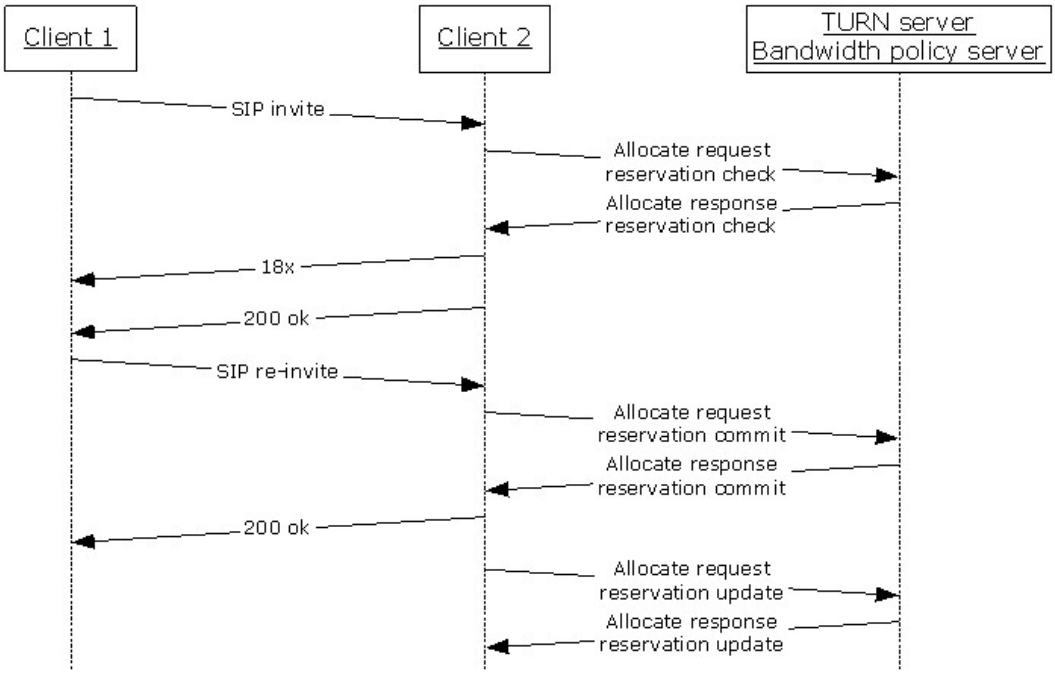


Figure 2: SIP signaling message flow

1.4 Relationship to Other Protocols

This protocol integrates with and extends the TURN protocol described in [MS-TURN].

1.5 Prerequisites/Preconditions

This protocol assumes the prerequisites/preconditions described in [MS-TURN] section 1.5.

This protocol requires that the TURN client authenticate with the TURN server.

This protocol requires that the TURN clients be able to communicate through a signaling protocol, such as SIP, to exchange transport addresses that identify the client's site address and relay site address.

This protocol requires that the TURN server be configured with appropriate network topology information. This information includes network subnets that are used to identify network sites, along with bandwidth policy for any network links used to connect the network sites. The bandwidth policy information includes configured bandwidth availability for various media stream modalities on the network link used to connect the network sites.

1.6 Applicability Statement

This protocol is designed to provide a mechanism for TURN clients that are communicating with a bandwidth policy aware TURN server to check for the availability of, and reserve, bandwidth for transmission of a media stream.

1.7 Versioning and Capability Negotiation

This protocol does not have any versioning or capability negotiation beyond that described in [MS-TURN] section 1.7.

1.8 Vendor-Extensible Fields

None.

1.9 Standards Assignments

This protocol uses the standard **User Datagram Protocol (UDP)** and **Transmission Control Protocol (TCP)** ports from [MS-TURN] section 1.9.

2 Messages

2.1 Transport

This protocol does not change the transport requirements of the TURN protocol, as specified in [MS-TURN] section 2.1.

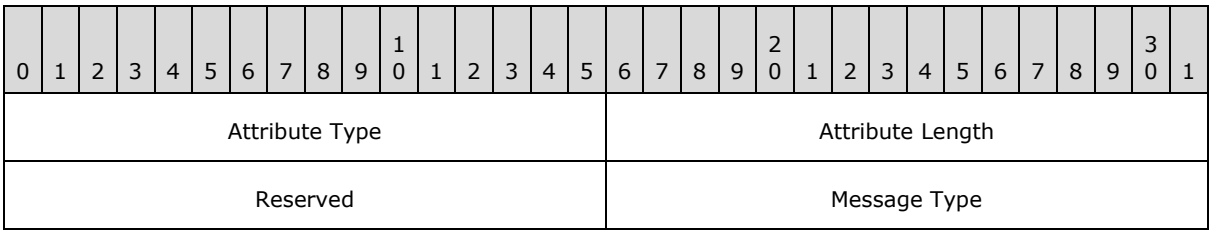
2.2 Message Syntax

All **Bandwidth Admission Control** message attributes are **type-length-value (TLV)** encoded, as specified in [MS-TURN] section 2.2.2.

2.2.1 Bandwidth Admission Control Message

The **Bandwidth Admission Control Message** attribute MUST be included in all **Allocate Request/Response** message exchanges between a client and a server (2) when a bandwidth admission control action is required. The supported bandwidth admission control actions are:

- **Reservation Check**, which is used to check bandwidth availability between a client and its peer.
- **Reservation Commit**, which is used to commit a bandwidth reservation between a client and its peer.
- **Reservation Update**, which is used to update and refresh an already committed bandwidth reservation.



Attribute Type (2 bytes): Set to "0x8056".

Attribute Length (2 bytes): Length of the following fields. Set to "0x0004".

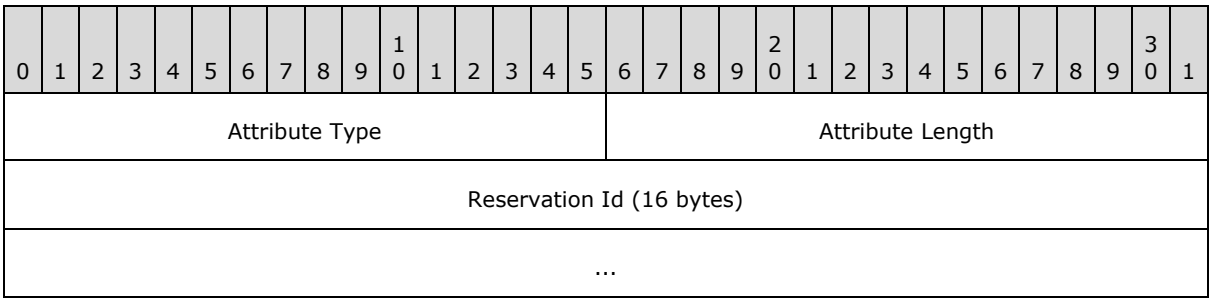
Reserved (2 bytes): These bits MUST be set to "0" on send and ignored on receive.

Message Type (2 bytes): The bandwidth admission control action that the client is requesting. The message types are defined as follows. All other message types are reserved for future use.

- **Reservation Check (0x0000):** Used by the client to request a bandwidth reservation check.
- **Reservation Commit (0x0001):** Used by the client to commit a bandwidth reservation.
- **Reservation Update (0x0002):** Used by the client to update and refresh an already-committed bandwidth reservation.

2.2.2 Bandwidth Reservation Identifier

The **Bandwidth Reservation Identifier** attribute is returned by the server (2) in response to a **Reservation Commit** message. This attribute MUST be used in all subsequent **Reservation Commit** and **Reservation Update** messages sent by the client to the server (2) for this reservation, and MUST include the value assigned by the server (2) in the response to the original **Reservation Commit** message.



Attribute Type (2 bytes): Set to "0x8057".

Attribute Length (2 bytes): Length of the **Reservation Id** field. Set to "0x0010".

Reservation Id (16 bytes): A bandwidth admission control reservation. This field is assigned by the server (2) in response to a client's **Reservation Commit** message. Once assigned, it is used by the client to identify the bandwidth reservation in all subsequent messages sent to the server (2). The server (2) can return a **Reservation Id** consisting of all zeros in response to a **Reservation Commit**. This indicates that the server (2) is not managing the network resources involved in the connection. If the client is not using the TURN session for any other purposes, such as data transport, it SHOULD disconnect the session when it receives a **Reservation Id** of all zeros.

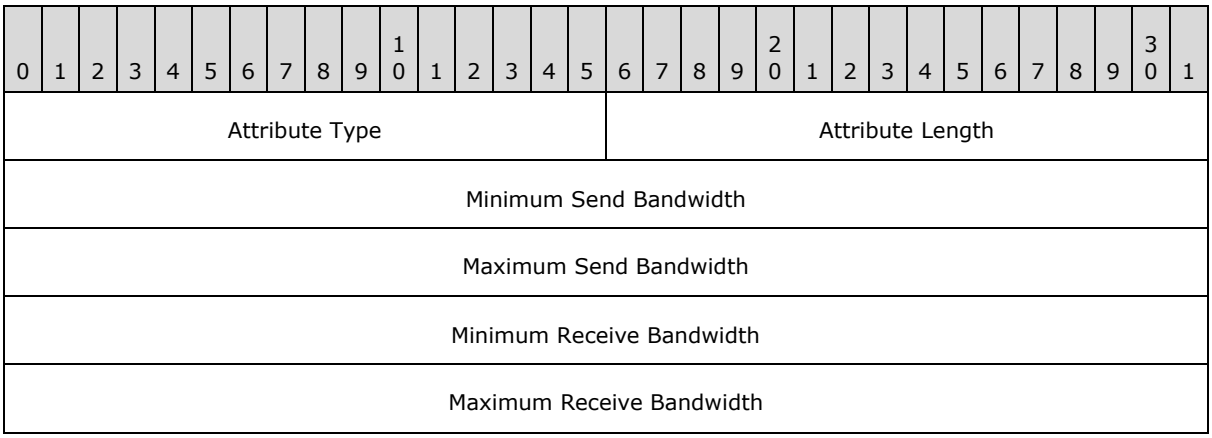
2.2.3 Bandwidth Reservation Amount

The **Bandwidth Reservation Amount** attribute is used by the client to indicate the amount of bandwidth that the **Bandwidth Admission Control Message** is requesting. This attribute MUST be included in all **Reservation Check** and **Reservation Commit** messages. It MUST be included in a **Reservation Update** message that requests a change in the bandwidth reservation amount.

When the client includes this attribute as part of a **Reservation Check** message, the bandwidth values MUST identify the bandwidth range (minimum and maximum) for the client's media stream.

When the client includes this attribute as part of a **Reservation Commit** message, the bandwidth values MUST be set to the bandwidth that the client expects to use for the media stream. The server (2) MUST commit the bandwidth reservation for the maximum amounts indicated in the attribute.

When the client includes this attribute as part of a **Reservation Update** message, the bandwidth values can be less than, greater than, or equal to the committed bandwidth reservation value. If the client is using a **Reservation Update** to ask for an increase in the bandwidth reservation, the server (2) could deny the increase. If the client sends a **Reservation Update** with the bandwidth values set to zero, the server (2) treats the message as a cancellation of the reservation and releases the bandwidth committed to the reservation. If the server (2) is not being used to relay the media stream and the reservation is released, the server (2) SHOULD disconnect the TURN session. When the server (2) includes this attribute in the response to a **Reservation Update**, the bandwidth values specify the amount of bandwidth that the server (2) has reserved for the client's media stream.



Attribute Type (2 bytes): Set to "0x8058".

Attribute Length (2 bytes): Length of the following fields. Set to "0x0010".

Minimum Send Bandwidth (4 bytes): The minimum bandwidth requirements, in kilobits per second, for the client's outbound media stream.

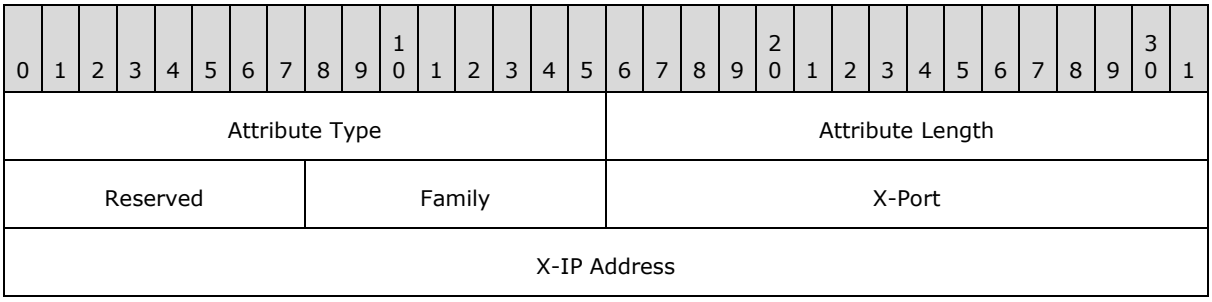
Maximum Send Bandwidth (4 bytes): The maximum bandwidth requirements, in kilobits per second, for the client's outbound media stream.

Minimum Receive Bandwidth (4 bytes): The minimum bandwidth requirements, in kilobits per second, for the client's inbound media stream.

Maximum Receive Bandwidth (4 bytes): The maximum bandwidth requirements, in kilobits per second, for the client's inbound media stream.

2.2.4 Remote Site Address

The **Remote Site Address** attribute contains the transport address that the remote client is using to contact its TURN server. This address maps the client into the bandwidth admission control network topology, and is used to identify the network site in which the remote client resides. There is an assumption that a client MUST be in a single network site. In other words, if the client has multiple IP addresses, only one address from the client is needed to identify the client's network site. This attribute MUST be included by the client in all **Reservation Check** and **Reservation Commit** request messages.



Attribute Type (2 bytes): Set to "0x8059".

Attribute Length (2 bytes): The attribute length is 8 bytes for an IPv4 address.

Reserved (1 byte): These bits MUST be set to "0" on send and ignored on receive.

Family (1 byte): The address family of the address. It MUST have the value "0x01: IPv4". If the value is anything other than 0x01 the attribute MUST be silently ignored.

X-Port (2 bytes): The port is a network byte ordered representation of the IP port. This value is created from the exclusive-or of the source port with the most significant 16 bits of the Transaction ID. If the port was 0x1122 (network byte order) and the most significant 16 bits of the Transaction ID was 0x4455 (network byte order), the resulting X-Port is "0x1122 ^ 0x4455 = 0x5577".

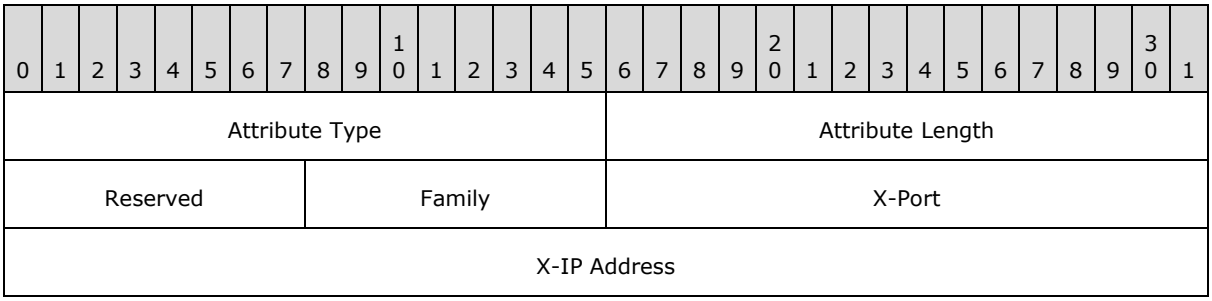
X-IP Address (4 bytes): The client's network byte ordered 32-bit IPv4 address. This value is created from the exclusive-or of the IP address with the most significant 32 bits of the Transaction ID. If the IPv4 address was 0x11223344 and the most significant 32 bits of the Transaction ID was 0xaabbccdd, the resulting X-Address is "0x11223344 ^ 0xaabbccdd = 0xbb99ff99".

2.2.5 Remote Relay Site Address

The **Remote Relay Site Address** attribute contains the IP address that the remote client received from an **Allocate Request** from its TURN server. This address maps the TURN server into the bandwidth admission control network topology, and is used to identify the network site that the TURN server is in.

If the remote client has allocated a transport address from its TURN server, it MUST include this attribute in the **Reservation Check**.

If the remote client uses the relay transport address for the media stream, this attribute MUST be included in the **Reservation Commit** request message. If the remote client does not use the relay transport address for the media stream, it MUST NOT include this attribute in the **Reservation Commit** request message.



Attribute Type (2 bytes): Set to "0x805A".

Attribute Length (2 bytes): The attribute length is 8 bytes for an IPv4 address.

Reserved (1 byte): These bits MUST be set to "0" on send and ignored on receive.

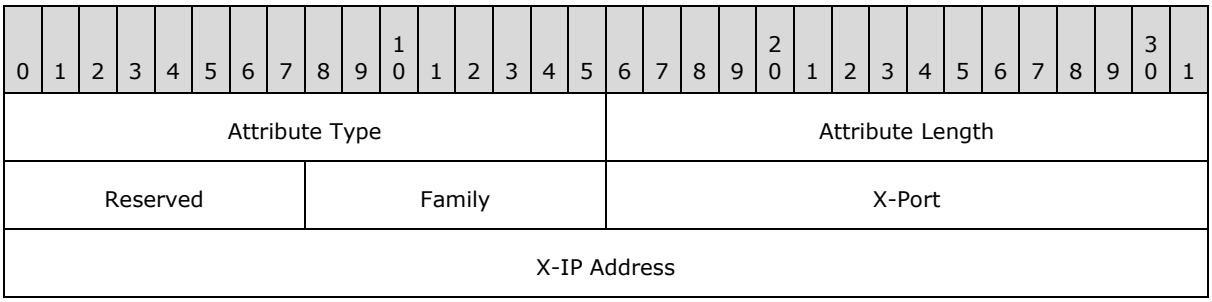
Family (1 byte): The address family of the address. It MUST have the value "0x01: IPv4". If the value is anything other than 0x01 the attribute MUST be silently ignored.

X-Port (2 bytes): A network byte ordered representation of the IP port. This value is created from the exclusive-or of the source port with the most significant 16 bits of the Transaction ID. If the port was 0x1122 (network byte order) and the most significant 16 bits of the Transaction ID was 0x4455 (network byte order), the resulting X-Port is "0x1122 ^ 0x4455 = 0x5577".

X-IP Address (4 bytes): The client's network byte ordered 32-bit IPv4 address. This value is created from the exclusive-or of the IP address with the most significant 32 bits of the Transaction ID. If the IPv4 address was 0x11223344 and the most significant 32 bits of the Transaction ID was 0xaabbccdd, the resulting X-Address is "0x11223344 ^ 0xaabbccdd = 0xbb99ff99".

2.2.6 Local Site Address

The **Local Site Address** attribute contains the IP address that the client is using to contact its TURN server. This address maps the client into the bandwidth admission control network topology, and is used to identify the network site that the client is in. There is an assumption that a client MUST be in a single network site. In other words, if the client has multiple IP addresses, only one address from the client is needed to identify the client's network site. This attribute MUST be included by the client in all **Reservation Check** and **Reservation Commit** request messages.



Attribute Type (2 bytes): Set to "0x805B".

Attribute Length (2 bytes): The attribute length is 8 bytes for an IPv4 address.

Reserved (1 byte): These bits MUST be set to "0" on send and ignored on receive.

Family (1 byte): The address family of the address. It MUST have the value "0x01: IPv4". If the value is anything other than 0x01 the attribute MUST be silently ignored.

X-Port (2 bytes): A network byte ordered representation of the IP port. This value is created from the exclusive-or of the source port with the most significant 16 bits of the Transaction ID. If the port was 0x1122 (network byte order) and the most significant 16 bits of the Transaction ID was 0x4455 (network byte order), the resulting X-Port is "0x1122 ^ 0x4455 = 0x5577".

X-IP Address (4 bytes): The client's network byte ordered 32-bit IPv4 address. This value is created from the exclusive-or of the IP address with the most significant 32 bits of the Transaction ID. If the IPv4 address was 0x11223344 and the most significant 32 bits of the Transaction ID was 0xaabbccdd, the resulting X-Address is "0x11223344 ^ 0xaabbccdd = 0xbb99ff99".

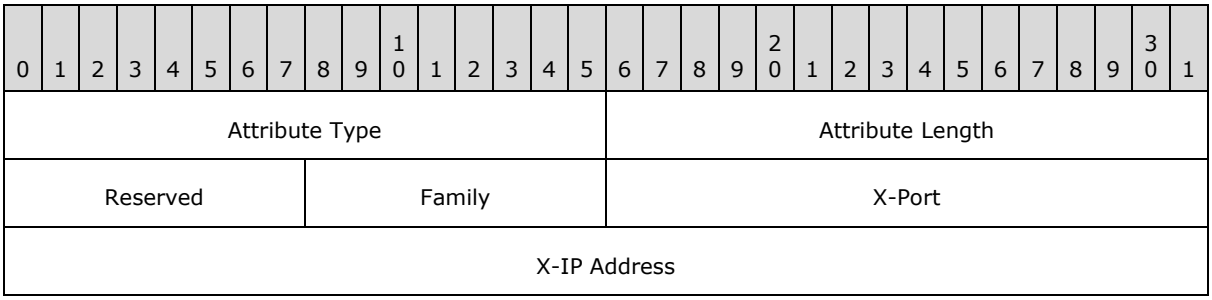
2.2.7 Local Relay Site Address

The **Local Relay Site Address** attribute contains the IP address that the local client received from its TURN server. This address maps the TURN server into the bandwidth admission control network topology, and is used to identify the network site that the TURN server is in.

If the local client has previously allocated a transport address from its TURN server, it MUST include this attribute in the **Reservation Check** message. If the local client is attempting to allocate a

transport address from its TURN server as part of the **Allocate Request** message carrying the **Reservation Check**, the client MUST NOT include this attribute.

If the local client uses the relay transport address for the media stream, this attribute MUST be included in the **Reservation Commit** request message. If the local client does not use the relay transport address for the media stream, it MUST NOT include this attribute in the **Reservation Commit** request message.



Attribute Type (2 bytes): Set to "0x805C".

Attribute Length (2 bytes): The attribute length is 8 bytes for an IPv4 address.

Reserved (1 byte): These bits MUST be set to "0" on send and ignored on receive.

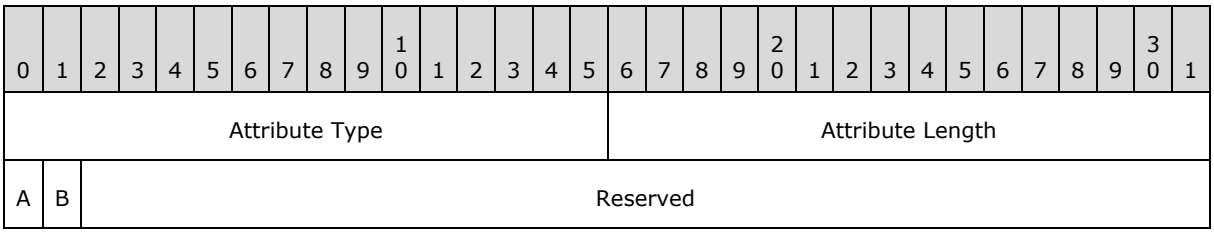
Family (1 byte): The address family of the address. It MUST have the value "0x01: IPv4". If the value is anything other than 0x01 the attribute MUST be silently ignored.

X-Port (2 bytes): A network byte ordered representation of the IP port. This value is created from the exclusive-or of the source port with the most significant 16 bits of the Transaction ID. If the port was 0x1122 (network byte order) and the most significant 16 bits of the Transaction ID was 0x4455 (network byte order), the resulting X-Port is "0x1122 ^ 0x4455 = 0x5577".

X-IP Address (4 bytes): The client's network byte ordered 32-bit IPv4 address. This value is created from the exclusive-or of the IP address with the most significant 32 bits of the Transaction ID. If the IPv4 address was 0x11223344 and the most significant 32 bits of the Transaction ID was 0xaabbccdd, the resulting X-Address is "0x11223344 ^ 0xaabbccdd = 0xbb99ff99".

2.2.8 Remote Site Address Response

The **Remote Site Address Response** attribute is sent by the server (2) in response to a **Reservation Check** request message that contained a **Remote Site Address** attribute. It indicates to the client the availability of the **Remote Site Address** as a viable transport address to be used for media connectivity.



Maximum Send Bandwidth
Maximum Receive Bandwidth

Attribute Type (2 bytes): Set to "0x805D".

Attribute Length (2 bytes): Set to "0x000C".

A - Valid (V) flag (1 bit): Identifies if the **Remote Site Address** is a valid transport address and should be included in the connectivity check as specified in section 3.2.5.1. If the network path between the **Remote Site Address** and **Local Site Address** passed the bandwidth admission policy check, the server (2) sets the flag (**V** = "1"). If the network path between the **Remote Site Address** and the **Local Site Address** failed the bandwidth admission policy check, the server (2) clears the flag (V = "0").

B - PSTN Failover (F) flag (1 bit): Used by the server (2) to inform the client of the option of failing over to **public switched telephone network (PSTN)** if the network path between the **Remote Site Address** and **Local Site Address** failed the bandwidth admission policy check. If the V flag is cleared (V = "0") and this flag is set (F = "1"), the client SHOULD attempt to re-route the call over the PSTN.

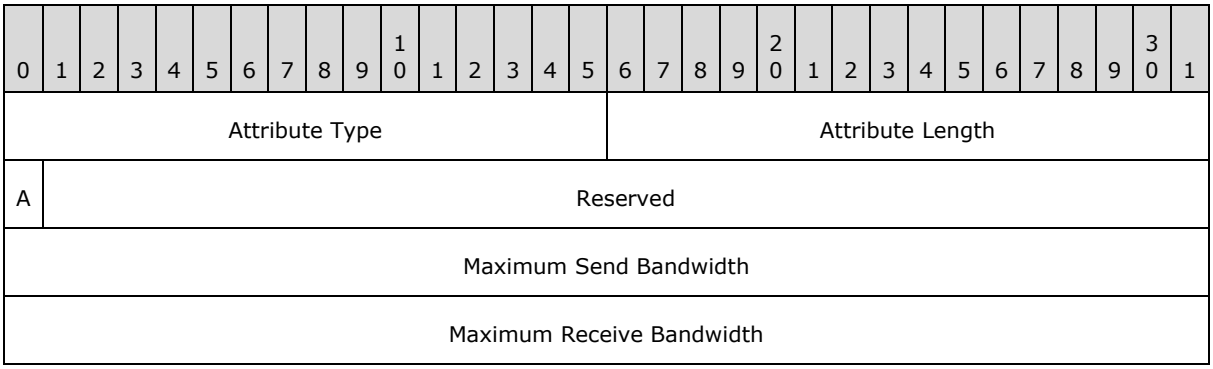
Reserved (30 bits): These bits MUST be set to "0" on send and ignored on receive.

Maximum Send Bandwidth (4 bytes): The maximum amount of bandwidth available for sending data from the **Remote Site Address**. This value is within the bandwidth range requested in the **Check Request** message. The server (2) sets this field to zero if the network path between the **Remote Site Address** and the **Local Site Address** fails the bandwidth admission policy check.

Maximum Receive Bandwidth (4 bytes): The maximum amount of bandwidth available for receiving data into the **Remote Site Address**. This value is within the bandwidth range requested in the **Check Request** message. The server (2) sets this field to zero if the network path between the **Remote Site Address** and the **Local Site Address** fails the bandwidth admission policy check.

2.2.9 Remote Relay Site Address Response

The **Remote Relay Site Address Response** attribute is sent by the server (2) in response to a **Reservation Check** request message that contained a **Remote Relay Site Address** attribute. It indicates to the client the availability of the **Remote Relay Site Address** as a viable transport address to be used for media connectivity.



Attribute Type (2 bytes): Set to "0x805E".

Attribute Length (2 bytes): Set to "0x000C".

A - Valid (V) flag (1 bit): Identifies if the **Remote Relay Site Address** is a valid transport address and should be included in the connectivity check as specified in section 3.2.5.1. If the network path between the **Remote Site Address** and **Remote Relay Site Address** passed the bandwidth admission policy check, the server (2) sets the flag (V = "1"). If the network path between the **Remote Site Address** and **Remote Relay Site Address** failed the bandwidth admission policy check, the server (2) clears the flag (V = "0").

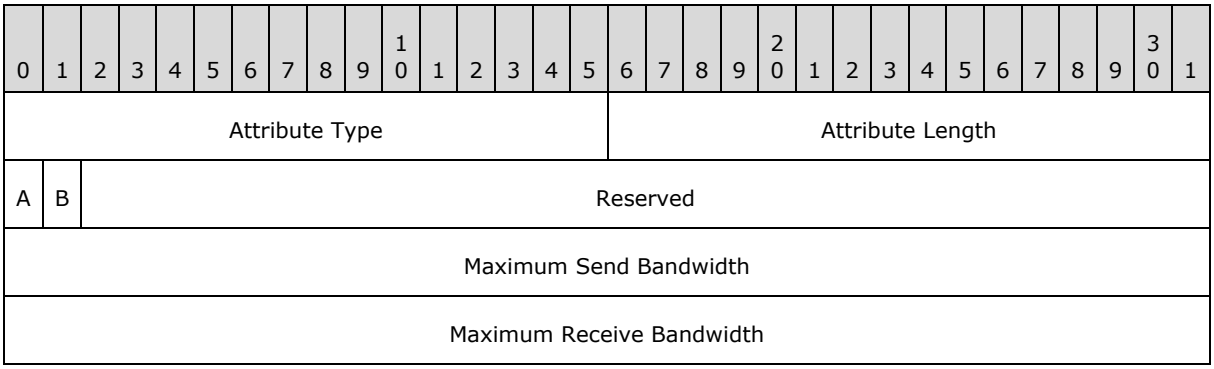
Reserved (31 bits): These bits MUST be set to "0" on send and ignored on receive.

Maximum Send Bandwidth (4 bytes): The maximum amount of bandwidth available for sending data from **Remote Relay Site Address**. This value is within the bandwidth range requested in the **Check Request** message. The server (2) sets this field to zero if the network path between the **Remote Site Address** and the **Remote Relay Site Address** fails the bandwidth admission policy check.

Maximum Receive Bandwidth (4 bytes): The maximum amount of bandwidth available for receiving data into the **Remote Relay Site Address**. This value is within the bandwidth range requested in the **Check Request** message. The server (2) sets this field to zero if the network path between the **Remote Site Address** and the **Remote Relay Site Address** fails the bandwidth admission policy check.

2.2.10 Local Site Address Response

The **Local Site Address Response** attribute is sent by the server (2) in response to a **Reservation Check** request message that contained a **Local Site Address** attribute. It is used to indicate to the client the availability of the **Local Site Address** as a viable transport address to be used for media connectivity.



Attribute Type (2 bytes): Set to "0x805F".

Attribute Length (2 bytes): Set to "0x000C".

A - Valid (V) flag (1 bit): Identifies if the **Local Site Address** is a valid transport address and should be included in the connectivity check as specified in section 3.2.5.1. If the network path between the **Remote Site Address** and **Local Site Address** passed the bandwidth admission policy check, the server (2) sets the flag (V = "1"). If the network path between the **Remote Site Address** and the **Local Site Address** failed the bandwidth admission policy check, the server (2) clears the flag (V = "0").

B - PSTN Failover (F) flag (1 bit): Used by the server (2) to inform the client of the option of failing over to PSTN if the network path between the **Local Site Address** and **Remote Site Address** failed the bandwidth admission policy check. If the **V** flag is cleared (V = "0") and this flag is set (F = "1"), the client SHOULD attempt to re-route the call over the PSTN.

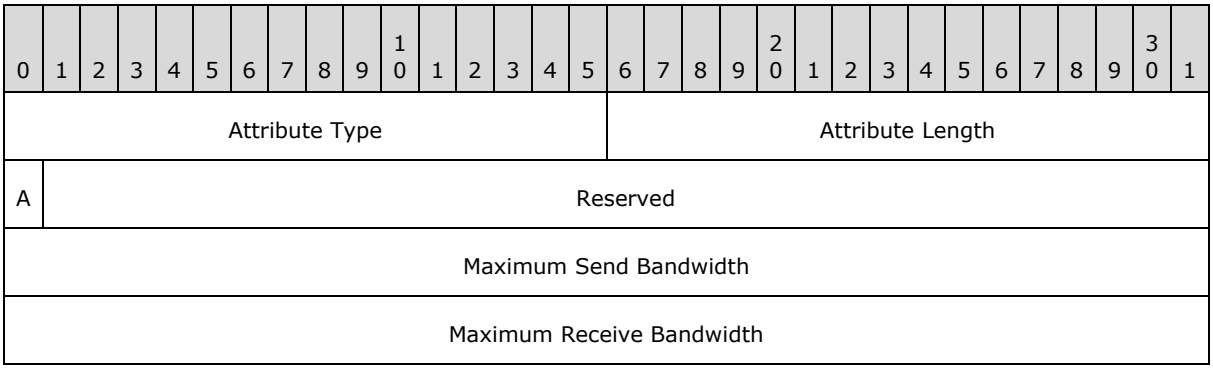
Reserved (30 bits): These bits MUST be set to "0" on send and ignored on receive.

Maximum Send Bandwidth (4 bytes): The maximum amount of bandwidth available for sending data from the **Local Site Address**. This value is within the bandwidth range requested in the **Check Request** message. The server (2) sets this field to zero if the network path between the **Remote Site Address** and the **Local Site Address** fails the bandwidth admission policy check.

Maximum Receive Bandwidth (4 bytes): The maximum amount of bandwidth available for receiving data into the **Local Site Address**. This value is within the bandwidth range requested in the **Check Request** message. The server (2) sets this field to zero if the network path between the **Remote Site Address** and the **Local Site Address** fails the bandwidth admission policy check.

2.2.11 Local Relay Site Address Response

The **Local Relay Site Address Response** attribute is sent by the server (2) in response to a **Reservation Check** request message that contained a **Local Relay Site Address** attribute. It indicates to the client the availability of the **Local Relay Site Address** as a viable transport address to be used for media connectivity.



Attribute Type (2 bytes): Set to "0x8060".

Attribute Length (2 bytes): Set to "0x000C".

A - Valid (V) flag (1 bit): Identifies if the **Local Relay Site Address** is a valid transport address and should be included in the connectivity check as specified in section 3.2.5.1. If the network path between the **Local Site Address** and **Local Relay Site Address** passed the bandwidth admission policy check, the server (2) sets the flag (V = "1"). If the network path between the **Local Site Address** and **Local Relay Site Address** failed the bandwidth admission policy check, the server (2) clears the flag (V = "0").

Reserved (31 bits): These bits MUST be set to "0" on send and ignored on receive.

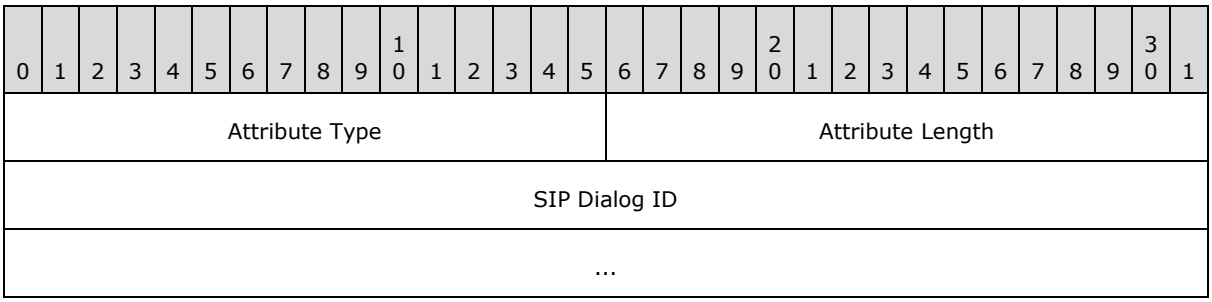
Maximum Send Bandwidth (4 bytes): The maximum amount of bandwidth available for sending data from **Local Relay Site Address**. This value is within the bandwidth range requested in the **Check Request** message. The server (2) sets this field to zero if the network

path between the **Local Site Address** and the **Local Relay Site Address** fails the bandwidth admission policy check.

Maximum Receive Bandwidth (4 bytes): The maximum amount of bandwidth available for receiving data into the **Local Relay Site Address**. This value is within the bandwidth range requested in the **Check Request** message. The server (2) sets this field to zero if the network path between the **Local Site Address** and the **Local Relay Site Address** fails the bandwidth admission policy check.

2.2.12 SIP Dialog Identifier

The **SIP Dialog Identifier** attribute is used by the client to identify the SIP **dialog** associated with the bandwidth reservation. Once the client knows the **SIP Dialog Identifier**, it MAY include this attribute in the **Bandwidth Admission Control Reservation Commit** message and any subsequent **Reservation Update** messages. The server (2) can use this attribute for logging purposes to map the media session to the signaling session.



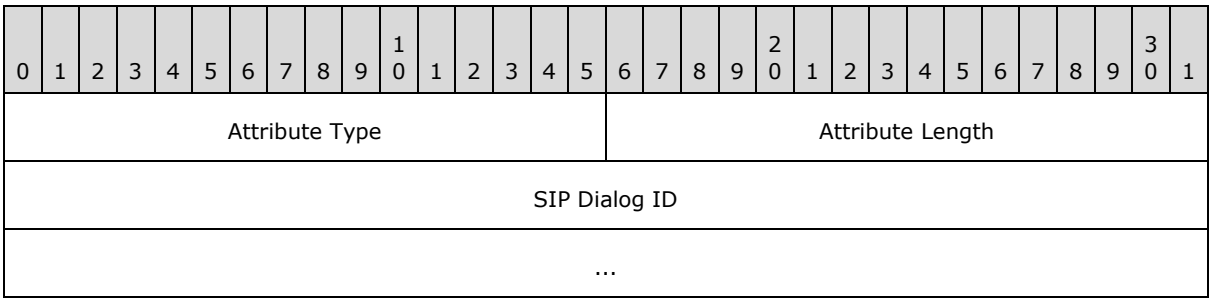
Attribute Type (2 bytes): Set to "0x8061".

Attribute Length (2 bytes): The length in bytes of the SIP **Dialog ID** field. The length of the **SIP Dialog ID** MUST NOT exceed 256 bytes.

SIP Dialog ID (variable): The SIP dialog identifier. The length of the **SIP Dialog ID** MUST NOT exceed 256 bytes.

2.2.13 SIP Call Identifier

The **SIP Call Identifier** attribute is used by the client to identify the SIP **call** associated with the bandwidth reservation. Once the client knows the **SIP Call Identifier**, it SHOULD include this attribute in the initial **Bandwidth Admission Control Reservation Check** message. The server (2) can use this attribute for logging purposes to map the media session to the signaling session.



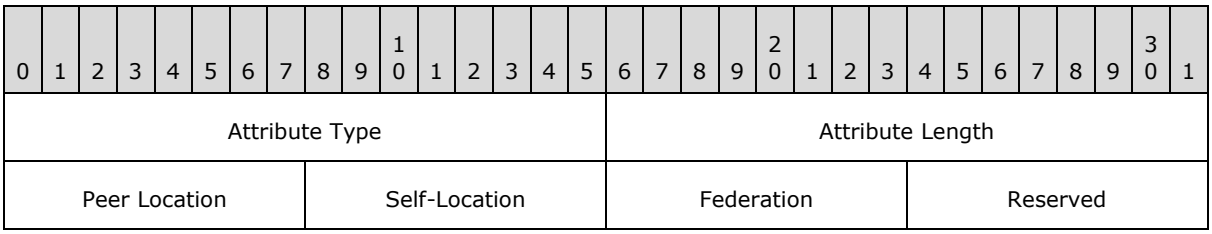
Attribute Type (2 bytes): Set to "0x8062".

Attribute Length (2 bytes): The length in bytes of the SIP **Call ID** field. The length of the **SIP Call ID** MUST NOT exceed 256 bytes.

SIP Call ID (variable): The SIP Call Identifier. The length of the **SIP Call ID** MUST NOT exceed 256 bytes.

2.2.14 Location Profile

The **Location Profile** is used by the client to indicate location information about the local client and the remote peer with which it is communicating. This attribute MUST be sent in all **Bandwidth Admission Control Reservation Check** and **Reservation Commit** messages.



Attribute Type (2 bytes): Set to "0x8068".

Attribute Length (2 bytes): The length, in bytes, of the following fields. Set to "0x0004".

Peer-Location (1 byte): This field identifies the location of the remote peer that the client is communicating with. It MUST have one of the following values:

- "0x00": Unknown – The location of the peer cannot be determined.
- "0x01": Internet – The peer is located on the public internet.
- "0x02": Intranet – The peer is located on a private intranet.

Self-Location (1 byte): This field identifies the location of the local client. It MUST have one of the following values:

- "0x00": Unknown – The location of the local client cannot be determined.
- "0x01": Internet – The local client is located on the public internet.
- "0x02": Intranet – The local client is located on a private intranet.

Federation (1 byte): This field identifies the **federation (2)** status of the peer that the client is communicating with. It MUST have one of the following values:

- "0x00": No Federation – The peer is located within the enterprise.
- "0x01": Enterprise Federation – The peer is located in a federated enterprise.
- "0x02": Public Cloud Federation – The peer is located in a federated public cloud.

Reserved (1 byte): These bits MUST be set to "0" on send and ignored on receive.

3 Protocol Details

3.1 Common Details

The procedures specified apply to both TCP and UDP transport protocols unless explicitly specified in the procedure.

All **Bandwidth Admission Control** messages MUST be included in properly formatted **Allocate Request** and **Allocate Response** message pairs, as specified in [MS-TURN] section 3.1.8 and [MS-TURN] section 3.1.10. The **Allocate Request** and **Allocate Response** messages MUST be part of an authenticated TURN session, as specified in [MS-TURN] section 3.1.12. **Bandwidth Admission Control** message attributes SHOULD be part of the first authenticated **Allocate Request** message.

3.1.1 Abstract Data Model

None.

3.1.2 Timers

None.

3.1.3 Initialization

None.

3.1.4 Higher-Layer Triggered Events

None.

3.1.5 Message Processing Events and Sequencing Rules

None.

3.1.6 Timer Events

None.

3.1.7 Other Local Events

None.

3.2 Client Details

3.2.1 Abstract Data Model

None.

3.2.2 Timers

This protocol adds one new timer to the timers specified in [MS-TURN] section 3.2.2.

Bandwidth Reservation Update Timer: This timer MUST be used by the client to keep an already committed bandwidth reservation active. The client MUST start the timer when it completes the **Allocate Request/Response** message transaction that carries a **Bandwidth Admission Control**

Reservation Commit message. The client MUST complete an **Allocate Request/Response** transaction carrying a **Bandwidth Admission Control Reservation Update** message, as specified in section 3.2.4.3, every 60 seconds.

3.2.3 Initialization

In addition to the initialization specified in [MS-TURN] section 3.2.3, the client MUST know the local transport address of the peer. If the peer has allocated a transport address from a TURN server, the client MUST know the allocated transport address of the peer. The client also MUST have successfully authenticated with the TURN server, as specified in [MS-TURN] section 3.1.12.

3.2.4 Higher-Layer Triggered Events

This section outlines the higher-layer events that trigger a client to start the various phases of bandwidth management.

3.2.4.1 Checking for Bandwidth Admission Control

Before a client begins connectivity checks with a peer, it MUST contact the server (2) to check for the availability of bandwidth between the client and peer network sites. This check is made by sending an authenticated **Allocate Request** message, as specified in [MS-TURN] section 3.1.12, to the server (2). The authenticated **Allocate Request** is constructed as follows:

- The request MUST include a **Bandwidth Admission Control Message** attribute with a message type of **Reservation Check**, as specified in section 2.2.1.
- The request MUST include a **Remote Site Address** attribute, as specified in section 2.2.4, containing the peer's local transport address.
- If the peer is using a TURN server and has an allocated transport address, the request MUST include a **Remote Relay Site Address** attribute, as specified in section 2.2.5, containing the transport address allocated by the TURN server.
- The request MUST include a **Local Site Address** attribute, as specified in section 2.2.6.
- The request MUST include a **Bandwidth Reservation Amount** attribute, as specified in section 2.2.3.
- The request SHOULD include a **MS-Service Quality** attribute, as specified in [MS-TURN] section 2.2.2.18. If this attribute is not present, the media stream is considered to be an audio stream.
- The request SHOULD include the **SIP Call Identifier** attribute, as specified in section 2.2.13.
- The request MUST include the **Location Profile** attribute, as specified in section 2.2.14.

3.2.4.2 Committing a Bandwidth Reservation

When a client and its peer complete connectivity checks and decide on a media connectivity path, the client MUST contact the server (2) to reserve the bandwidth against the network links between the network sites involved in the media path. This reservation is made by sending an authenticated **Allocate Request** message, as specified in [MS-TURN] section 3.1.12, to the server (2). The authenticated **Allocate Request** is constructed as follows:

- The request MUST include a **Bandwidth Admission Control Message** attribute with a message type of **Reservation Commit**, as specified in section 2.2.1.

- The request MUST include a **Remote Site Address** attribute, as specified in section 2.2.4.
- If the media connectivity path is using the remote TURN server, the request MUST include a **Remote Relay Site Address** attribute, as specified in section 2.2.5.
- The request MUST include a **Local Site Address** attribute as specified in section 2.2.6.
- If the media connectivity path is using the local TURN server, the request MUST include a **Local Relay Site Address** attribute, as specified in section 2.2.7.
- The request MUST include a **Bandwidth Reservation Amount** attribute, as specified in section 2.2.3.
- The request SHOULD include an **MS-Service Quality** attribute as specified in [MS-TURN] section 2.2.2.18. If this attribute is not present the media stream is considered to be an audio stream.
- The request SHOULD include the **SIP Dialog Identifier** attribute, as specified in section 2.2.12.
- The request MUST include the **Location Profile** attribute, as specified in section 2.2.14.

3.2.4.3 Updating a Bandwidth Reservation

After a client has committed a bandwidth reservation with the server (2), it might request changing the amount of bandwidth that it reserved. The client can attempt to increase or decrease the reservation. The client MUST notify the server (2) of this change request. This update is made by sending an authenticated **Allocate Request** message, as specified in [MS-TURN] section 3.1.12, to the server (2). The authenticated **Allocate Request** is constructed as follows:

- The request MUST include a **Bandwidth Admission Control Message** attribute with a message type of **Reservation Update,** as specified in section 2.2.1.
- The request MUST include a **Bandwidth Reservation ID** attribute, as specified in section 2.2.2.
- If the update is sent in response to an attempt to change, either increase or decrease, the amount of bandwidth currently committed to the reservation, the request MUST include a **Bandwidth Reservation Amount** attribute, as specified in section 2.2.3. If the update is sent in response to the **Bandwidth Reservation Update Timer** firing, the request can include a **Bandwidth Reservation Amount** attribute, as specified in section 2.2.3.
- The request SHOULD include the **SIP Dialog Identifier** attribute, as specified in section 2.2.12.

3.2.5 Message Processing Events and Sequencing Rules

When a client receives an **Allocate Response** message, it MUST follow the procedure specified in [MS-TURN] section 3.2.5.1, with the following exceptions:

- The response can contain a **Mapped Address** attribute, as specified in [MS-TURN] section 2.2.2.15.
- The response can contain a **Bandwidth Admission Control Message** attribute, as specified in section 2.2.1.

3.2.5.1 Receiving a Bandwidth Admission Control Check Response Message

When a client receives an **Allocate Response** message with a transaction identifier that matches the transaction identifier of an **Allocate Request** message that included a **Bandwidth Admission Control Reservation Check** message, it proceeds as follows:

- The response MUST contain a **Remote Site Address Response** attribute, as specified in section 2.2.8.
- If the original request message contained a **Remote Relay Site Address** attribute the response MUST contain a **Remote Relay Site Address Response** attribute, as specified in section 2.2.9.
- The response MUST contain a **Local Site Address Response** attribute, as specified in section 2.2.10.
- If the TURN server allocated a relay transport address on behalf of the client, the response MUST contain a **Local Relay Site Address Response** attribute, as specified in section 2.2.11.

If the response message is valid, the client MUST check the flags for each of the included site address response attributes. The server (2) marks the **Valid (V)** flag of each of the site address response attributes, based on the available bandwidth over three possible network paths:

- **Local Site Address** to the **Remote Site Address.**
- **Local Site Address** to the **Local Relay Site Address**, if present.
- **Remote Site Address** to the **Remote Relay Site Address**, if present.

The rules for checking the network paths are as follows:

- The network path between the **Local Site Address** and the **Remote Site Address** is only available if both the **Local Site Address Response** attribute and **Remote Site Address Response** attribute are flagged as valid (**V**="1"). If either of these attributes are marked as invalid (**V**="0"), the network path is not available because of bandwidth constraints.
- If either of **Local Site Address** or **Remote Site Address** attributes are marked as invalid (**V**="0") and the **PSTN Failover** flag is set (**F**="1") the bandwidth policy allows redirecting the connection over PSTN. The client SHOULD consider the network path to the PSTN gateway as a valid network path.
- If the **Local Relay Site Address Response** attribute is present and it is flagged as valid (**V**="1"), the **Local Site Address** – **Local Relay Site Address** network path is available. If the **Local Relay Site Address Response** attribute is not present or if it is flagged as invalid (**V**="0"), the **Local Site Address – Local Relay Site Address** network path is not available.
- If the **Remote Relay Site Address Response** attribute is present and it is flagged as valid (**V**="1"), the **Remote Site Address – Remote Relay Site Address** network path is available. If the **Remote Relay Site Address Response** attribute is not present or if it is flagged as invalid (**V**="0"), the **Remote Site Address – Remote Relay Site Address** network path is not available.

A full check failure occurs when there is no valid network path out of either the **Local Site Address** or the **Remote Site Address**. A partial connection failure occurs if any path out of either the **Local Site Address** or the **Remote Site Address** is not available. The client SHOULD use all valid network paths to explore connectivity options with the peer. The client MUST NOT use any network paths that are marked as invalid.

3.2.5.2 Receiving a Bandwidth Admission Control Commit Response Message

When a client receives an **Allocate Response** message with a transaction identifier that matches the transaction identifier of an **Allocate Request** message that included a **Bandwidth Admission Control Reservation Commit** message, it proceeds as follows:

- The response MUST contain a **Bandwidth Reservation Identifier** attribute, as specified in section 2.2.2.
- The response MUST contain a **Bandwidth Reservation Amount** attribute, as specified in section 2.2.3.

If the response is valid, the client SHOULD check the **Reservation ID** value. If the value is zero, the bandwidth reservation is not being tracked by the server (2). If the client is not using the TURN session for the media stream, it SHOULD disconnect the session. If the **Reservation ID** value is nonzero, it is used for all further messages dealing with the reservation.

3.2.5.3 Receiving a Bandwidth Admission Control Update Response Message

When a client receives an **Allocate Response** message with a transaction identifier that matches the transaction identifier of an **Allocate Request** message that included a **Bandwidth Admission Control Reservation Update** message it proceeds as follows:

- The response MUST contain a **Bandwidth Reservation Identifier** attribute, as specified in section 2.2.2.
- The response SHOULD include a **Bandwidth Reservation Amount** attribute as specified in section 2.2.3.

If the response is valid and a **Bandwidth Reservation Amount** attribute is present, the client MUST check the send and receive bandwidth values to verify the amount of bandwidth that the server (2) has reserved for the media session. If the response was the result of a request to increase the amount of bandwidth in the reservation, it is possible that the server (2) was not able to reserve the full amount of the request.

3.2.6 Timer Events

Bandwidth Reservation Update Timer Expiration: Upon expiry of the **Bandwidth Reservation Update** timer, the client MUST transmit a **Bandwidth Admission Control Reservation Update** message, as specified in section 3.2.4.3.

3.2.7 Other Local Events

None.

3.3 Server Details

3.3.1 Abstract Data Model

None.

3.3.2 Timers

This protocol adds one new timer to the timers specified in [MS-TURN] section 3.3.2.

Bandwidth Reservation Lifetime Timer: This timer MUST be used by the server (2) to time out a stale bandwidth reservation from a client. The server (2) MUST start the timer when it completes the **Allocate Request/Response** message transaction that carries a **Bandwidth Admission Control Reservation Commit** message. The server (2) MUST receive an **Allocate Request** message carrying a **Bandwidth Admission Control Reservation Update** message, as specified in

section 3.2.4.3, every 60 seconds. The server (2) MUST restart the timer when it receives a **Bandwidth Admission Control Reservation Update** message.

3.3.3 Initialization

In addition to the initialization requirements specified in [MS-TURN] section 3.3.3, the server (2) needs to be configured with appropriate network topology information. This information includes network subnets that are used to identify network sites, along with bandwidth policy for any network links used to connect the network sites.

3.3.4 Higher-Layer Triggered Events

None.

3.3.5 Message Processing Events and Sequencing Rules

When the server (2) receives an **Allocate Request** message, it MUST follow the procedure specified in [MS-TURN] section 3.3.5.1. The following sections specify additional procedures that the server (2) MUST follow when the **Allocate Request** message contains a **Bandwidth Admission Control Message** attribute, as specified in section 2.2.1.

3.3.5.1 Receiving a Bandwidth Admission Control Check Request Message

If the **Allocate Request** message contains a **Bandwidth Admission Control Message** attribute with a value of **Reservation Check**, the request is processed as follows:

- The request MUST include a **Bandwidth Reservation Amount** attribute, as specified in section 2.2.3. If this attribute is not included, the server (2) MUST continue to process the **Allocate Request** message as specified in [MS-TURN] section 3.3.5.1 and ignore the **Bandwidth Admission Control Message** action.
- The request MUST include a **Remote Site Address** attribute, as specified in section 2.2.4. If this attribute is not included, the server (2) MUST continue to process the **Allocate Request** message as specified in [MS-TURN] section 3.3.5.1 and ignore the **Bandwidth Admission Control Message** action.
- If the peer is using a TURN server and has an allocated transport address, the request MUST include a **Remote Relay Site Address** attribute, as specified in section 2.2.5, containing the transport address allocated by the TURN server.
- The request SHOULD include a **Local Site Address** attribute, as specified in section 2.2.6. If this attribute is not present, the server (2) MUST use the source transport address of the message to identify the requesting client's local site address.
- If the server (2) allocated a public transport address on behalf of the client as part of processing the **Allocate Request** message, the server (2) MUST use the allocated transport address to identify the requesting client's **Local Relay Site Address**.
- The request SHOULD include a **MS-Service Quality** attribute, as specified in [MS-TURN] section 2.2.2.18. If this attribute is not present, the server (2) SHOULD treat the **Reservation Check** as a check for an audio stream.
- The request SHOULD include the **SIP Call Identifier** attribute, as specified in section 2.2.13.
- The request MUST include the **Location Profile** attribute, as specified in section 2.2.14

If all of the required attributes are present and valid, the server (2) MUST use the bandwidth admission control network topology to map the site address attributes present in the request to network sites, and then map the network sites to the network paths connecting the sites. The server (2) MUST check the bandwidth request against the bandwidth policy for the network paths. There are three possible network paths that can be checked:

- The network path between the network sites mapped by the **Remote Site Address** and the **Remote Relay Site Address**.
- The network path between the network sites mapped by the **Local Site Address** and the **Local Relay Site Address**.
- The network path between the network sites mapped by the **Local Site Address** and the **Remote Site Address**.

Once the server (2) has finished checking the bandwidth policy for the available network paths, it MUST respond with an **Allocate Response** message:

- The response MUST be formed as specified in [MS-TURN] section 3.3.5.1.
- The response MUST include a **Bandwidth Admission Control Message** attribute with a value of **Reservation Check**, as specified in section 2.2.1.
- The response MUST include a **Remote Site Address Response** attribute, as specified in section 2.2.8. If the bandwidth policy passed for the network path between the network sites identified by the **Remote Site Address** and the **Local Site Address**, the attribute MUST have the **Valid** bit set (**V**="1") and the bandwidth values set to the amount of bandwidth the policy allowed. If the bandwidth policy failed, the attribute MUST have the **Valid** bit cleared (**V**="0") and the bandwidth values set to zero. If the bandwidth policy supports redirecting the connection to PSTN, the server (2) MUST set the **PSTN Failover** bit (**F**="1"), otherwise the **PSTN Failover** bit MUST be cleared (**F**="0").
- If a **Remote Relay Site Address** attribute was present in the request, the response MUST include a **Remote Relay Site Address Response** attribute, as specified in section 2.2.9. If the bandwidth policy passed for the network path between the network sites identified by the **Remote Site Address** and the **Remote Relay Site Address**, the attribute MUST have the **Valid** bit set (**V**="1") and the bandwidth values set to the amount of bandwidth the policy allowed. If the bandwidth policy failed, the attribute MUST have the **Valid** bit cleared (**V**="0") and the bandwidth values set to zero.
- If the server (2) allocated a public transport address on behalf of the client, the response MUST include a **Local Relay Site Address Response** attribute, as specified in section 2.2.11. If the bandwidth policy passed for the network path between the network sites identified by the **Local Site Address** and the **Local Site Relay Address**, the attribute MUST have the **Valid** bit set (**V**="1") and the bandwidth values set to the amount of bandwidth the policy allowed. If the bandwidth policy failed, the attribute MUST have the **Valid** bit cleared (**V**="0") and the bandwidth values set to zero.
- The response MUST include a **Local Site Address Response** attribute, as specified in section 2.2.10. If the bandwidth policy passed for the network path between the network sites identified by the **Remote Site Address** and the **Local Site Address**, the attribute MUST have the **Valid** bit set (**V**="1") and the bandwidth values set to the amount of bandwidth the policy allowed. If the bandwidth policy failed, the attribute MUST have the **Valid** bit cleared (**V**="0") and the bandwidth values set to zero. If the bandwidth policy supports redirecting the connection to PSTN, the server (2) MUST set the **PSTN Failover** bit (**F**="1"); otherwise the **PSTN Failover** bit MUST be cleared (**F**="0").

3.3.5.2 Receiving a Bandwidth Admission Control Commit Request Message

If the **Allocate Request** message contains a **Bandwidth Admission Control Message** attribute with a value of **Reservation Commit**, the request is processed as follows:

- The request MUST include a **Bandwidth Reservation Amount** attribute, as specified in section 2.2.3. If this attribute is not included, the server (2) MUST continue to process the **Allocate Request** message as specified in [MS-TURN] section 3.3.5.1 and ignore the **Bandwidth Admission Control Message** action.
- The request MUST include a **Remote Site Address** attribute, as specified in section 2.2.4. If this attribute is not included, the server (2) MUST continue to process the **Allocate Request** message as specified in [MS-TURN] section 3.3.5.1 and ignore the **Bandwidth Admission Control Message** action.
- If the media connectivity path is using the remote TURN server, the request MUST include a **Remote Relay Site Address** attribute, as specified in section 2.2.7.
- The request MUST include a **Local Site Address** attribute, as specified in section 2.2.6. If this attribute is not included, the server (2) MUST continue to process the **Allocate Request** message as specified in [MS-TURN] section 3.3.5.1 and ignore the **Bandwidth Admission Control Message** action.
- If the media connectivity path is using the local TURN server, the request MUST include a **Local Relay Site Address** attribute, as specified in section 2.2.7.
- The request SHOULD include a **MS-Service Quality** attribute, as specified in [MS-TURN] section 2.2.2.18. If this attribute is not present, the server (2) SHOULD treat the **Reservation Commit** as a commit for an audio stream.
- The request SHOULD include the **SIP Dialog Identifier** attribute, as specified in section 2.2.12.
- The request MUST include the **Location Profile** attribute, as specified in section 2.2.14.

If all of the required attributes are present and valid, the server (2) MUST use the bandwidth admission control network topology to map the site address attributes present in the request to network sites and then map the network sites to the network paths connecting the sites. The server (2) MUST commit the bandwidth amount against the bandwidth policy for the network paths involved. There are three possible network paths:

- The network path between the network sites mapped by the **Remote Site Address** and the **Remote Relay Site Address,** if the **Remote Relay Site Address** attribute is present.
- The network path between the network sites mapped by the **Local Site Address** and the **Local Relay Site Address**, if the **Local Relay Site Address** attribute is present.
- The network path between the network sites mapped by the **Local Site Address** and the **Remote Site Address**.

Once the server (2) has finished committing the bandwidth reservation against the bandwidth policies of the mapped network paths, it MUST respond with an **Allocate Response** message:

- The response MUST be formed as specified in [MS-TURN] section 3.2.5.1.
- The response MUST include a **Bandwidth Admission Control Message** attribute with a value of **Reservation Commit**, as specified in section 2.2.1.

- The response MUST include a **Bandwidth Reservation Identifier** attribute, as specified in section 2.2.2.
- The response MUST include a **Bandwidth Reservation Amount** attribute, as specified in section 2.2.3.

3.3.5.3 Receiving a Bandwidth Admission Control Update Request Message

If the **Allocate Request** message contains a **Bandwidth Admission Control Message** attribute with a value of **Reservation Update**, the request is processed as follows:

- The request MUST include a **Bandwidth Reservation Identifier** attribute, as specified in section 2.2.2. If the **Reservation ID** value does not match an active bandwidth reservation, the server (2) MUST continue to process the **Allocate Request** message as specified in [MS-TURN] section 3.3.5.1 and ignore the **Bandwidth Admission Control Message** action.
- The request SHOULD include a **Bandwidth Reservation Amount** attribute, as specified in section 2.2.3.
- The request SHOULD include the **SIP Dialog Identifier** attribute, as specified in section 2.2.12.

If all of the required attributes are present and valid, the server (2) MUST restart the **Bandwidth Reservation Lifetime** timer.

If the **Bandwidth Reservation Amount** attribute is present, the server (2) MUST check the bandwidth values against the bandwidth values that were previously committed for this reservation. If the values are lower than the committed values, the server (2) SHOULD update the reservation, returning unused bandwidth back to the bandwidth policies of the network paths involved in the reservation. If the values are higher than the committed values, the server (2) MUST re-check the network paths involved in the reservation for the availability of additional bandwidth. If bandwidth is available, the server (2) SHOULD reserve additional bandwidth for the reservation.

Once the server (2) has finished restarting the timer and updating the bandwidth reservation, it responds with an **Allocate Response** message specified as follows:

- The response MUST be formed as specified in [MS-TURN] section 3.3.5.1.
- The response MUST include a **Bandwidth Admission Control Message** attribute with a value of **Reservation Update**, as specified in section 2.2.1.
- The response MUST include a **Bandwidth Reservation Identifier** attribute, as specified in section 2.2.2.
- The response SHOULD include a **Bandwidth Reservation Amount** attribute, as specified in section 2.2.3.

3.3.6 Timer Events

Bandwidth Reservation Lifetime Timer Expiration: Upon expiration of the **Bandwidth Reservation Lifetime Timer**, the server (2) MUST release the bandwidth reserved by the client in its **Bandwidth Admission Control Reservation Commit** message. If the server (2) is not involved with relaying the media stream for the associated TURN client, it SHOULD disconnect the connection.

3.3.7 Other Local Events

None.

3.4 Proxy Details

None.

3.4.1 Abstract Data Model

None.

3.4.2 Timers

None.

3.4.3 Initialization

None.

3.4.4 Higher-Layer Triggered Events

None.

3.4.5 Message Processing Events and Sequencing Rules

None.

3.4.6 Timer Events

None.

3.4.7 Other Local Events

None.

4 Protocol Examples

In the following diagrams, two TURN clients implementing this protocol are communicating using SIP, as described in [RFC3261]. The clients require the establishment of a media flow between them, and request that media flow to be managed by the server (2). The client initiating the connection does an allocation of a public transport address from its TURN server, as described in [MS-TURN] section 3.2.4.1, which it includes in the **SDP** of the SIP **INVITE** sent to the peer, as described in [RFC4566]. The details of the **SIP message** exchange are not included in the example; only the basic message flow used to communicate the public transport addresses of the protocol client and peer to each other are included.

In the following diagram, TURN Client1 has a local transport address of 10.0.0.1:12345, which places it in network site1. TURN Client2 has a local transport address of 10.0.10.1:45678, which places it in network site2. The TURN server implementing this protocol extension has a local address of 10.0.0.2:3478 and a public transport address, from which it allocates relay transport addresses, of 192.0.2.20 The public transport address of the TURN server is configured so that it is associated with network site1. Both clients can route directly to the TURN server. There is a 1.54 Mb/s WAN link, Wan link1, that connects network site2 to network site1.

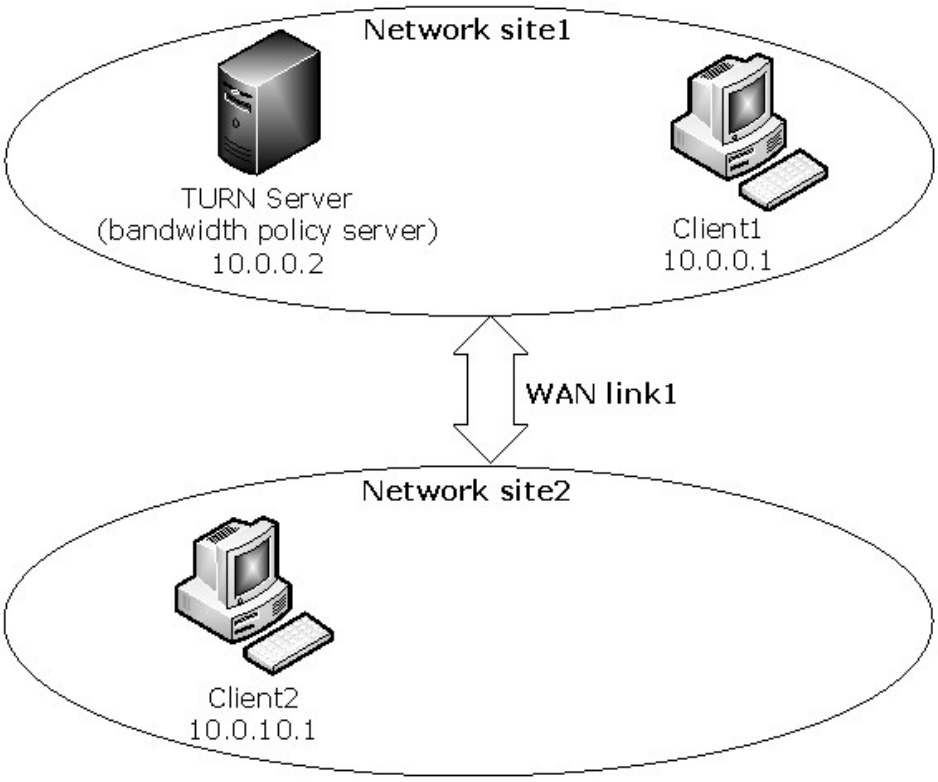


Figure 3: Two TURN clients connecting using SIP

The following diagram shows the bandwidth admission control message flow for the network deployment described in the preceding diagram where WAN Link1, between Network Site1 and Network Site2, has the full 1.54Mb/s of bandwidth available for use. TURN Client1 is attempting to make a voice call to TURN Client2 over WAN link1. The voice call requires between 64Kb/s and 128Kb/s of network bandwidth.

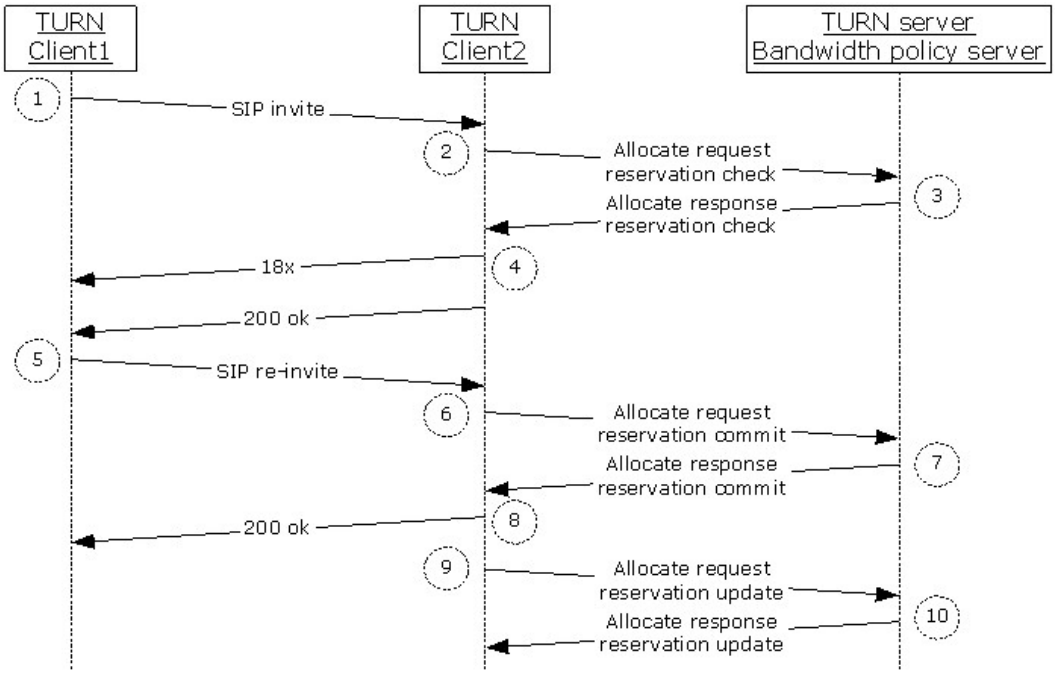


Figure 4: Bandwidth admission control message flow when sufficient bandwidth is available

1. Client1 allocates a public transport from the TURN server following the procedures described in [MS-TURN] section 3.2.4.1. Client1's relay transport address allocated by the TURN server is 192.0.2.20:55667. Client1 adds the relay transport address, along with its local transport address 10.0.0.1:12345, to the SDP of the SIP INVITE and sends the SIP INVITE to TURN Client2.

2. When Client2 receives the SIP INVITE from Client1, it knows both the local transport address and the relay transport address of Client1. Client2 can now do a bandwidth check with the TURN server to verify the availability of network bandwidth between itself and Client1. It follows the procedure specified in section 3.2.4.1 to check for bandwidth admission control. It uses the following attributes in the **Allocate Request** carrying the **Reservation Check** message:

    1. **Bandwidth Admission Control Message** attribute with a value of **Reservation Check**.

    2. A **Remote Site Address** attribute containing Client1's local transport address xor'd with the TURN message transaction identifier.

    3. A **Remote Relay Site Address** attribute containing Client1's relay transport address xor'd with the TURN message transaction identifier.

    4. A **Local Site Address** attribute containing Client2's local transport address xor'd with the TURN message transaction identifier.

    5. A **Bandwidth Reservation Amount** attribute with a value of 64 kilobytes for the minimum send/receive bandwidth and 128 kilobytes for the maximum send/receive bandwidth

    6. An **MS-Service Quality** attribute with a stream type of "Audio" and a service quality of "best effort delivery".

7. A **Location Profile** attribute with the **Peer-Location** set to "Intranet", the **Self-Location** set to "Intranet" and **Federation** set to "Not Federated".

3. When the server (2) receives the **Allocate Request** message containing the **Reservation Check**, it follows the procedure specified in section 3.3.5.1 to determine if there is bandwidth available between Client1 and Client2. In this case, Client1's local transport address maps to network site1, Client1's relay transport address maps to network site1, Client2's local transport address maps to network site2, and Client2's relay transport address maps to network site1.

    1. The server (2) checks the network path for each of the site addresses included in the **Reservation Check** request:

        1. The server (2) checks the path between the **Remote Site Address** and the **Remote Relay Site Address**. Because both of these addresses map into the same network site, there is no bandwidth management constraints on that path and it is considered a valid network path. The server (2) marks the **Remote Relay Site Address** as valid for the full bandwidth amount, which is 128 kilobytes.

        2. The server (2) checks the path between the **Local Site Address** and the **Local Relay Site Address**. In this case, the **Local Site Address** maps to network site2 but the **Local Relay Site Address** maps to network site1 and there is a bandwidth managed link, WAN link1, between these sites. The server (2) checks the amount of bandwidth requested in the **Bandwidth Reservation Amount** attribute against the amount of bandwidth currently available on WAN link1. Because this is the first call over this link there is still 1.54 megabytes available. The bandwidth amount being requested is 64 kilobytes-128 kilobytes, so the server (2) marks the **Local Relay Site Address** as valid for the full bandwidth amount, which is 128 kilobytes.

        3. The server (2) checks the path between the **Local Site Address** and the **Remote Site Address**. In this case, the **Local Site Address** maps to network site2 but the **Remote Site Address** maps to network site1 and there is a bandwidth managed link, WAN link1, between these sites. The server (2) checks the amount of bandwidth requested in the **Bandwidth Reservation Amount** attribute against the amount of bandwidth currently available on WAN link1. Because this is the first call over this link, there is still 1.54 megabytes available. The bandwidth amount being requested is 64 kilobytes-128 kilobytes, so the server (2) marks both the **Local Site Address** and **Remote Site Address** as valid for the full bandwidth amount, which is 128 kilobytes.

    2. The server (2) replies to Client2 with an **Allocate Response** message and includes the following attributes:

        1. A **Bandwidth Access Control Message** attribute with a value of "Reservation Check".

        2. A **Remote Site Address Response** attribute with the **Valid** flag set (**V**="1") and a value of 128 kilobytes for the bandwidth amount value.

        3. A **Remote Relay Site Address Response** attribute with a **Valid** flag set (**V**="1") and a value of 128 kilobytes for the bandwidth amount value.

        4. A **Local Site Address Response** attribute with the **Valid** flag set (**V**="1") and a value of 128 kilobytes for the bandwidth amount value.

        5. A **Local Relay Site Address Response** attribute with the **Valid** flag set (**V**="1") and a value of 128 kilobytes for the bandwidth amount values.

4. When Client2 receives the **Allocate Response** message with the **Reservation Check** results, it follows the procedure specified in section 3.2.5.1 to determine which transport addresses can be

used for the media stream. Because all network paths between both clients are marked as valid, it includes both its local and relay transport addresses in the SDP included in the SIP **200 OK** message sent to Client1. In parallel, Client2 begins to explore the connectivity paths with Client1's local and relay transport addresses.

5. When Client1 receives the SIP 200 OK response that includes Client2's transport addresses, it uses Client2's transport addresses advertised in the SDP of the SIP 200 OK message to begin checking connectivity. In this example, Client1 and Client2 find that the best connectivity option is over each client's local transport address. When Client1 finishes checking for connectivity, it sends a SIP re-INVITE to Client2 with SDP containing the local transport address.

6. When Client2 receives the SIP re-INVITE from Client1, it uses the transport addresses advertised in the SDP along with the local transport addresses that passed the connectivity check to identify the network path over which the media stream will flow. In this example, the network path is between the local transport address of each client. Client2 uses these two transport addresses to do a **Reservation Commit** with the server (2). It follows the procedure specified in section 3.2.4.2 to commit a bandwidth admission control reservation. It uses the following attributes in the **Allocate Request** carrying the **Reservation Commit** message:

    1. A **Bandwidth Admission Control Message** attribute with a value of **Reservation Commit**.

    2. A **Remote Site Address** attribute containing Client1's local transport address xor'd with the TURN message transaction identifier.

    3. A **Local Site Address** attribute containing Client2's local transport address xor'd with the TURN message transaction identifier.

    4. A **Bandwidth Reservation Amount** attribute with a value of 128 kilobytes for the minimum and maximum send/receive bandwidths.

    5. A **MS-Service Quality** attribute with a stream type of "Audio" and a service quality of "best effort delivery".

    6. A **Location Profile** attribute with the **Peer-Location** set to "Intranet", the **Self-Location** set to "Intranet" and **Federation** set to "Not Federated".

7. When the server (2) receives the **Allocate Request** message containing the **Reservation Commit**, it follows the procedure specified in section 3.2.5.2 to commit the bandwidth reservation against the bandwidth policy for the network path specified by the site address attributes. In this example, the network path between the two clients is identified by the **Local Site Address** attribute and the **Remote Site Address** attribute, which map to WAN Link1. The server (2) commits 128 kilobytes, the amount of bandwidth from the **Bandwidth Reservation Amount** attribute, against the bandwidth policy covering WAN Link1. This leaves 1.412 megabytes (1.54 megabytes –128 kilobytes = 1.412 megabytes) of bandwidth available on WAN Link1. Once the server (2) has finished committing the bandwidth reservation against the bandwidth policy, it replies to Client2 in an **Allocate Response** message containing the following attributes:

    1. A **Bandwidth Admission Control Message** attribute with a value of **Reservation Commit**.

    2. A **Bandwidth Reservation Identifier** containing the reservation identifier created when the reservation was committed.

    3. A **Bandwidth Reservation Amount** attribute containing 128 kilobytes for the minimum/maximum send/receive bandwidth values.

8. When Client2 receives the **Allocate Response** message with the **Reservation Commit** results, it follows the procedure specified in section 3.2.5.2 and stores the **Reservation ID** returned in the **Bandwidth Reservation Identifier** attribute. The **Reservation ID** is used in subsequent **Reservation Update** messages sent to the server (2).

9. When the **Reservation Update** timer fires on Client2, it refreshes the bandwidth reservation with the server (2). The refresh follows the procedure specified in section 3.2.4.3. It uses the following attributes in the **Allocate Request** carrying the **Reservation Update** message:

    1. A **Bandwidth Admission Control Message** attribute with a value of **Reservation Update.**

    2. A **Bandwidth Reservation Identifier** attribute with a **Reservation ID** value that matches the reservation id received in response to the original **Reservation Commit** message.

    3. A **Bandwidth Reservation Amount** attribute with the minimum/maximum send/receive bandwidth values set to 128 kilobytes, which is the amount of bandwidth reserved when the reservation was committed.

10. When the server (2) receives the **Allocate Request** message containing the **Reservation Update**, it follows the procedure specified in section 3.3.5.3 to refresh the reservation. When the server (2) has reset the **Bandwidth Reservation Lifetime** timer, it replies to Client2 with an **Allocate Response** message containing the following attributes:

    1. A **Bandwidth Admission Control Message** attribute with a value of **Reservation Update**.

    2. A **Bandwidth Reservation Identifier** containing the reservation identifier created when the reservation was committed.

    3. A **Bandwidth Reservation Amount** attribute with the minimum/maximum send/receive bandwidth values set to 128 kilobytes, which is the amount of bandwidth reserved when the reservation was committed.

The following diagram shows the bandwidth admission control message flow for the network deployment described in the previous diagram in the example where WAN Link1, between Network Site1 and Network Site2, has no bandwidth available for use. TURN Client1 is attempting to make a voice call to TURN Client2 over WAN link1. The voice call requires between 64 kilobytes and 128 kilobytes of network bandwidth.

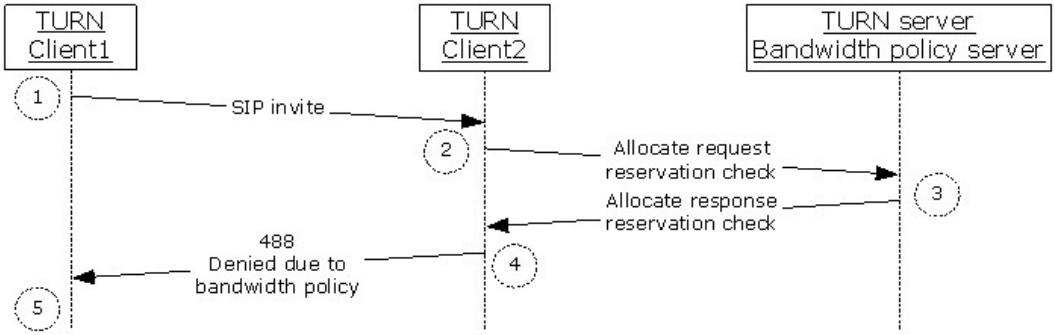


Figure 5: Bandwidth admission control message flow when insufficient bandwidth is available

1. Client1 allocates a public transport from the TURN server following the procedures specified in [MS-TURN] section 3.2.4.1. Client1's relay transport address, allocated by the TURN server, is 192.0.2.20:55667. Client1 adds the relay transport address, along with its local transport

address 10.0.0.1:12345, to the SDP of the SIP INVITE and sends the SIP INVITE to TURN Client2.

2. When Client2 receives the SIP INVITE from Client1, it knows both the local transport address and relay transport address of Client2. Client2 can now do a bandwidth check with the TURN server to verify the availability of network bandwidth between itself and Client1. It follows the procedure specified in section 3.2.4.1 to check for bandwidth admission control. It uses the following attributes in the **Allocate Request** carrying the **Reservation Check** message:

    1. A **Bandwidth Admission Control Message** attribute with a value of **Reservation Check**.

    2. A **Remote Site Address** attribute containing Client1's local transport address xor'd with the TURN message transaction identifier.

    3. A **Remote Relay Site Address** attribute containing Client1's relay transport address xor'd with the TURN message transaction identifier.

    4. A **Local Site Address** attribute containing Client2's local transport address xor'd with the TURN message transaction identifier.

    5. A **Bandwidth Reservation Amount** attribute with a value of 64Kb/s for the minimum send/receive bandwidth and 128Kb/s for the maximum send/receive bandwidth.

    6. A **MS-Service Quality** attribute with a stream type of Audio and a service quality of best effort delivery.

    7. A **Location Profile** attribute with the **Peer-Location** set to "Intranet", the **Self-Location** set to "Intranet" and **Federation** set to "Not Federated".

3. When the server (2) receives the **Allocate Request** message containing the **Reservation Check**, it follows the procedure specified in section 3.3.5.1 to determine if there is bandwidth available between Client1 and Client2. In this case, Client1's local transport address maps to network site1, Client1's relay transport address maps to network site1, Client2's local transport address maps to network site2, and Client2's relay transport address maps to network site1.

    1. The server (2) checks the network path for each of the site addresses included in the **Reservation Check** request:

        1. The server (2) checks the path between the **Remote Site Address** and the **Remote Relay Site Address**. Because both of these addresses map into the same network site, there is no bandwidth management constraints on that path and it is considered a valid network path. The server (2) marks the **Remote Relay Site Address** as valid for the full bandwidth amount, which is 128 kilobytes.

        2. The server (2) checks the path between the **Local Site Address** and the **Local Relay Site Address**. In this case, the **Local Site Address** maps to network site2 but the **Local Relay Site Address** maps to network site1 and there is a bandwidth managed link, WAN link1, between these sites. The server (2) checks the amount of bandwidth requested in the **Bandwidth Reservation Amount** attribute against the amount of bandwidth currently available on WAN link1. Because all of the 1.54 megabytes that were available have been consumed by other calls, no bandwidth is available for a new call. The server (2) marks the **Local Relay Site Address** as invalid and sets the bandwidth value to zero.

        3. The server (2) checks the path between the **Local Site Address** and the **Remote Site Address**. In this case, the **Local Site Address** maps to network site2 but the **Remote Site Address** maps to network site1 and there is a bandwidth managed link, WAN link1, between these sites. The server (2) checks the amount of bandwidth requested in the

Bandwidth Reservation Amount attribute against the amount of bandwidth currently available on WAN link1. Because all of the 1.54 megabytes that was available has been consumed by other calls, no bandwidth is available for a new call. The server (2) marks both the **Local Site Address** and **Remote Site Address** as invalid and sets the bandwidth values to zero.

2. The server (2) replies to Client2 with an **Allocate Response** message and includes the following attributes:

    1. A **Bandwidth Access Control Message** attribute with a value of **Reservation Check**.

    2. A **Remote Site Address Response** attribute with the **Valid** flag cleared (**V**="0") and a value of 0 kilobytes for the bandwidth amount values.

    3. A **Remote Relay Site Address Response** attribute with a **Valid** flag set (**V**="1") and a value of 128 kilobytes for the bandwidth amount values.

    4. A **Local Site Address Response** attribute with the **Valid** flag cleared (**V**="0") and a value of zero kilobytes for the bandwidth amount values.

    5. A **Local Relay Site Address Response** attribute with the **Valid** flag cleared (**V**="0") and a value of zero kilobytes for the bandwidth amount values.

4. When Client2 receives the **Allocate Response** message with the **Reservation Check** results, it follows the procedure specified in section 3.2.5.1 to determine which transport addresses can be used for the media stream. Because all network paths out of the local site are marked as invalid, Client2 is not able to check connectivity with Client1. Client2 sends a SIP 488 Call denied because of bandwidth policy failure response message to Client1.

5. When Client1 receives the SIP 488 response, it notifies the user of the connection failure, indicating that no bandwidth was available to make the call.

The following diagram shows the bandwidth admission control message flow for the network deployment described in the first figure in the example, titled Bandwidth admission control message flow when sufficient bandwidth is available, where WAN Link1, between Network Site1 and Network Site2, has no bandwidth available for use. Both Network Site1 and Network Site2 have PSTN gateway devices. TURN Client1 is attempting to make a voice call to TURN Client2 over WAN link1. The voice call requires between 64 kilobytes and 128 kilobytes of network bandwidth. Network Site1 is configured with a bandwidth policy that supports redirection of connections to PSTN if there is a bandwidth check failure.

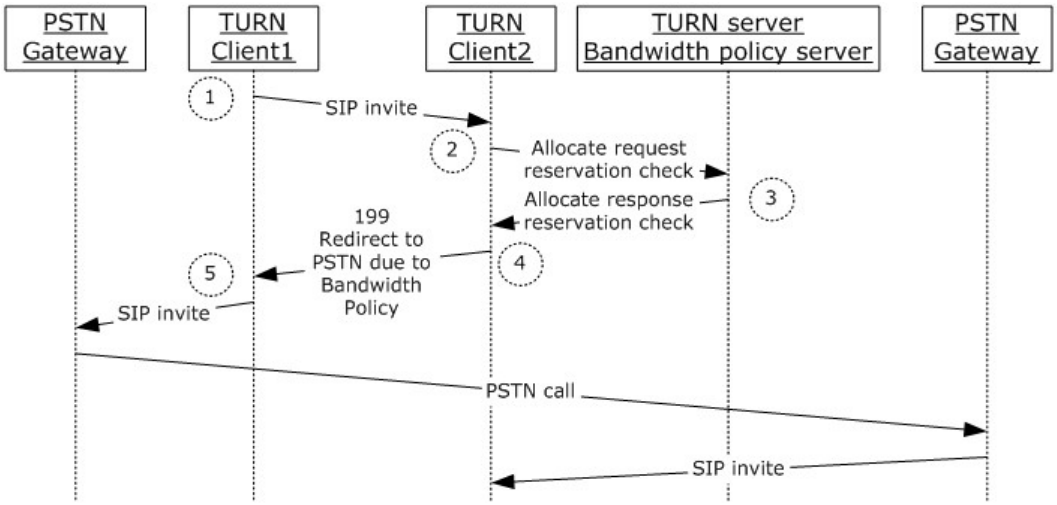


Figure 6: Bandwidth admission control message flow with PSTN Gateways

1. Client1 allocates a public transport from the TURN server following the procedures specified in [MS-TURN] section 3.2.4.1. Client1's relay transport address, allocated by the TURN server, is 192.0.2.20:55667. Client1 adds the relay transport address, along with its local transport address 10.0.0.1:12345, to the SDP of the SIP INVITE and sends the SIP INVITE to TURN Client2.

2. When Client2 receives the SIP INVITE from Client1, it knows both the local transport address and relay transport address of Client1. Client2 can now do a bandwidth check with the TURN server to verify the availability of network bandwidth between itself and Client1. It follows the procedure specified in section 3.2.4.1 to check for bandwidth admission control. It uses the following attributes in the **Allocate Request** carrying the **Reservation Check** message:

    1. A **Bandwidth Admission Control Message** attribute with a value of **Reservation Check**.

    2. A **Remote Site Address** attribute containing Client1's local transport address xor'd with the TURN message transaction identifier.

    3. A **Remote Relay Site Address** attribute containing Client1's relay transport address xor'd with the TURN message transaction identifier.

    4. A **Local Site Address** attribute containing Client2's local transport address xor'd with the TURN message transaction identifier.

    5. A **Bandwidth Reservation Amount** attribute with a value of 64 kilobytes for the minimum send/receive bandwidth and 128 kilobytes for the maximum send/receive bandwidth.

    6. A **MS-Service Quality** attribute with a stream type of "Audio" and a service quality of "best effort delivery".

    7. A **Location Profile** attribute with the **Peer-Location** set to "Intranet", the **Self-Location** set to "Intranet" and **Federation** set to "Not Federated".

3. When the server (2) receives the **Allocate Request** message containing the **Reservation Check**, it follows the procedure specified in section 3.3.5.1 to determine if there is bandwidth available between Client1 and Client2. In this case, Client1's local transport address maps to

network site1, Client1's relay transport address maps to network site1, Client2's local transport address maps to network site2, and Client2's relay transport address maps to network site1.

1. The server (2) checks the network path for each of the site addresses included in the **Reservation Check** request:

    1. The server (2) checks the path between the **Remote Site Address** and the **Remote Relay Site Address**. Because both of these addresses map into the same network site, there is no bandwidth management constraints on that path and it is considered a valid network path. The server (2) marks the **Remote Relay Site Address** as valid for the full bandwidth amount, which is 128 kilobytes.

    2. The server (2) checks the path between the **Local Site Address** and the **Local Relay Site Address**. In this case, the **Local Site Address** maps to network site2 but the **Local Relay Site Address** maps to network site1 and there is a bandwidth managed link, WAN link1, between these sites. The server (2) checks the amount of bandwidth requested in the **Bandwidth Reservation Amount** attribute against the amount of bandwidth currently available on WAN link1. Because all of the 1.54 megabytes that were available have been consumed by other calls, no bandwidth is available for a new call. The server (2) marks the **Local Relay Site Address** as invalid and sets the bandwidth value to zero.

    3. The server (2) checks the path between the **Local Site Address** and the **Remote Site Address**. In this case, the **Local Site Address** maps to network site2 but the **Remote Site Address** maps to network site1 and there is a bandwidth managed link, WAN link1, between these sites. The server (2) checks the amount of bandwidth requested in the **Bandwidth Reservation Amount** attribute against the amount of bandwidth currently available on WAN link1. Because all of the 1.54 megabytes that were available have been consumed by other calls, no bandwidth is available for a new call. The server (2) marks both the **Local Site Address** and **Remote Site Address** as invalid and sets the bandwidth values to zero. The server (2) checks the PSTN failover bandwidth policy for network site1 and finds that PSTN failover is supported, so it marks the **PSTN Failover** flag for the **Remote Site Address** as valid. The server (2) checks the PSTN failover bandwidth policy for network site2 and finds that PSTN failover is supported, so it marks the **PSTN Failover** flag for the **Local Site Address** as valid.

2. The server (2) replies to Client2 with an **Allocate Response** message and includes the following attributes:

    1. A **Bandwidth Access Control Message** attribute with a value of **Reservation Check**.

    2. A **Remote Site Address Response** attribute with the **Valid** flag cleared (**V**="0"), the **PSTN Failover** flag set (**F**="1") and a value of zero kilobytes for the bandwidth amount value.

    3. A **Remote Relay Site Address Response** attribute with a **Valid** flag set (**V**="1") and a value of 128 kilobytes for the bandwidth amount value.

    4. A **Local Site Address Response** attribute with the **Valid** flag cleared (**V**="0"), the **PSTN Failover** flag set (**F**="1") and a value of zero kilobytes for the bandwidth amount value.

    5. A **Local Relay Site Address Response** attribute with the **Valid** flag cleared (**V**="0") and a value of 0 kilobytes for the bandwidth amount values.

4. When Client2 receives the **Allocate Response** message with the **Reservation Check** results, it follows the procedure specified in section 3.2.5.1 to determine which transport addresses can be used for the media stream. Because all network paths out of the local site are marked as invalid, Client2 is not able to check connectivity with Client1. Because the **PSTN Failover** flag is set,

Client2 sends a SIP 199 Call redirected to PSTN because of bandwidth policy failure response message to Client1.

5. When Client1 receives the SIP 199 response redirecting it to attempt to use the PSTN gateway, it sends a SIP INVITE to a local PSTN gateway signaling it to use the PSTN to attempt to connect to Client2. The details of this signaling are omitted from this example. When Client2 receives the SIP INVITE from its local PSTN gateway device, it follows the example detailed in the diagram titled Bandwidth admission control message flow when sufficient bandwidth is available, and does a new **Reservation Check** and **Reservation Commit** for the media flow to the gateway.

5 Security

5.1 Security Considerations for Implementers

This protocol has the same security considerations described in [MS-TURN] section 5. Additional considerations and mitigations for this protocol are as follows.

A client requests the bandwidth amount to reserve for a media stream in a **Reservation Commit** or a **Reservation Update** message. This makes it possible for a malicious client to consume all of the available bandwidth for a bandwidth managed WAN link. It is recommended that a server (2) have a configurable parameter that specifies the maximum reservation bandwidth amount that a client can reserve in a single **Reservation Commit** or **Reservation Update** message.

5.2 Index of Security Parameters

6 Appendix A: Product Behavior

The information in this specification is applicable to the following Microsoft products or supplemental software. References to product versions include released service packs:

- Microsoft® Lync™ Server 2010
- Microsoft® Lync™ 2010

Exceptions, if any, are noted below. If a service pack or Quick Fix Engineering (QFE) number appears with the product version, behavior changed in that service pack or QFE. The new behavior also applies to subsequent service packs of the product unless otherwise specified. If a product edition appears with the product version, behavior is different in that product edition.

Unless otherwise specified, any statement of optional behavior in this specification that is prescribed using the terms SHOULD or SHOULD NOT implies product behavior in accordance with the SHOULD or SHOULD NOT prescription. Unless otherwise specified, the term MAY implies that the product does not follow the prescription.

7 Change Tracking

No table of changes is available. The document is either new or has had no changes since its last release.

8 Index

N

O

P

R

S

T

V