in RFC 792.

Table 16. Media Server Support for ICMP Destination Unreachable Codes

Destination Unreachable ICMP Code	Support	
	Receive	Transmit
Net Unreachable	Supported	Not Supported
Host Unreachable	Supported	Not Supported
Protocol Unreachable	Supported	Not Supported
Port Unreachable	Supported	Supported
Fragmentation Needed and DF Set	Supported	Not Supported
Source Route Failed	Supported	Not Supported

When the Media Server receives an ICMP Destination Unreachable message for ICMPv6, a Packet Too Big message, it executes a backoff procedure, to allow for the possibility that the UDP port is slow to initialize, or that a router is temporarily unavailable, but will soon recover. This is based on the received message, which indicates that the port does not exist, is no longer reachable, or that it is larger than the MTU for the path. The Media Server stops sending media for an interval, which lengthens with each subsequent received message. The RTP stream is stopped permanently after the nth backoff where n is the configured number of retries.

Other types of ICMP messages can be received during backoff periods. For example, when roundtrip delays are larger than the packetization interval or when video sent in bursts causes a burst of returned ICMP messages.

RTP Stream Timeout

The MSML interface can detect and report the loss of incoming RTP packets on a port. When the RTP stream timeout feature is enabled for a port, the Media Server monitors the received RTP packets. If no packets are received within the configured timeout period, the Media Server sends an MSML event.

The timeout period for a port can be changed mid-call. This can be done before or after the expiration of a previously set period.

NAT Traversal of RTP Packets

Network Address Translation (NAT) maps an entire subnet network (the private subnet) on to a second subnet (the public subnet) that has fewer IP addresses than the private subnet. NAT translates the IP addresses and port numbers of packets that pass through it by mapping the private local addresses and port numbers to a smaller range of IP addresses and port numbers on the public subnet.

Because the local IP address and port number negotiated by an end terminal located on the private network are only valid behind the NAT, they cannot be used by the Media Server to send RTP packets to the end terminal. To allow a device on the public network to determine the equivalent public destination address and port number of the private device, one solution is to inspect the source address and port number on incoming RTP packets after they are translated by the NAT. This solution is called symmetric RTP.

If symmetric RTP is enabled in the management interface, the Media Server uses the source address and port number of incoming RTP packets as the destination for outgoing RTP packets. If symmetric RTP is disabled, the Media Server uses the address and port number as negotiated through SDP as the destination for outgoing RTP packets.

For symmetric RTP to work, the end terminal must be configured to send RTP traffic. The end terminal does not receive any RTP packets from the Media Server until it has sent at least one RTP packet and the packet passes successfully through the network to the Media Server. If the end terminal is configured for receive-only operation, or if its RTP packets are suppressed due to silence suppression, the Media Server does not send any RTP packets.

To avoid delays in sending to terminals that are not located behind a NAT and with symmetric RTP enabled, the Media Server starts sending to the address and port as negotiated through SDP. If the end terminal is not located behind a NAT, the source address of the incoming RTP packets matches the SDP information and no change takes place. If the end terminal is located behind a NAT, the Media Server initially sends to the wrong destination. These packets may be simply ignored by the network or they may attract ICMP Destination Unreachable messages, in which case the Media Server begins its normal ICMP back-off procedure. The arrival of the first incoming RTP packet with a source IP address that does not match the one negotiated by SDP causes the Media Server to start sending to the new address.

Interactive Connectivity Establishment

The Interactive Connectivity Establishment (ICE) functionality interworks with different end-points as a solution for the Network Address Translator (NAT) traversal issues for Voice over IP (VoIP) applications. The presence of NAT in a VoIP network creates an issue in communication between the endpoints. The NATs assign private IP addresses to their endpoints behind the NAT and provide private-public address mapping when the endpoints communicate outside the NAT.

The ICE technique in NAT traversal for UDP-based multimedia sessions are established with the offer/answer model. ICE solves NAT issues for the media streams. ICE uses the Session Traversal Utilities for NAT (STUN) protocol and its extension, Traversal Using Relay NAT (TURN) protocol, and can be used by any protocol utilizing the offer/answer model. For example, SIP.

STUN. STUN protocol enables a device to discover its public IP address.

TURN. TURN protocol enables a server to relay data packets between the devices.

The Media Server supports ICE Lite, Full ICE, and Trickle ICE to communicate its public IP address and connect to other devices.

NOTE: The Media Server supports ICE on the **MSML** and **sip:conf** service context.

Full ICE

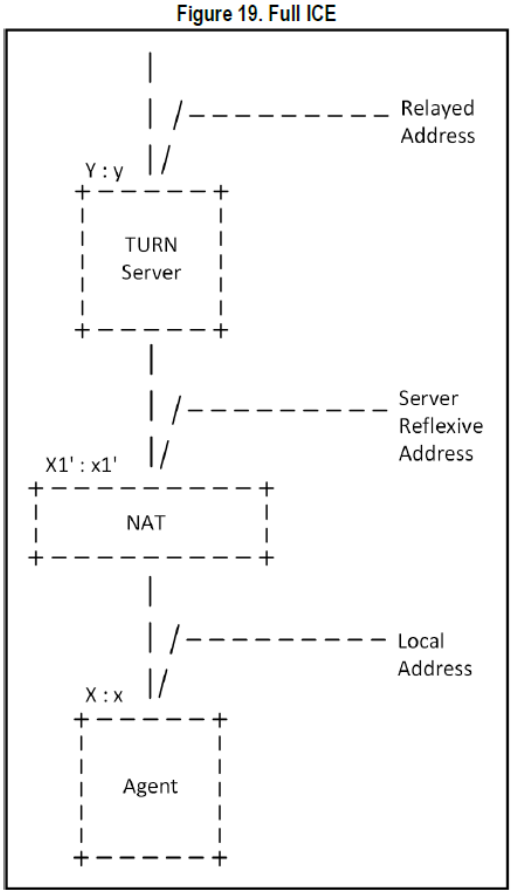
Full ICE is a full implementation of ICE. The Full ICE implementation in Media Server adheres to the following ICE processing phases in a sequential manner.

- **Gathering the candidate addresses.** The endpoints supporting the ICE determine whether they are behind the NATs or not. The endpoint sends the STUN binding request and the STUN server replies with the IP address. If the endpoint is behind the NAT, the address is visible to the STUN server, which is different than the endpoints local host address. If the TURN server is present, both the endpoints can communicate using the TURN server.

  There are three types of candidates.

  - **Host Candidate.** A candidate is obtained by binding to a specific port from an IP address on the host.
  - **Server Reflexive Candidate.** A candidate whose IP address and port are binding allocated by a NAT for an agent when it sends a packet through the NAT to a server.

Figure 19. Full ICE



- **Sorting of the candidates.** After the agent has gathered its candidates, it assigns each candidate with a priority value and sorts the candidates from high priority to low priority. The priority algorithms are designed to prefer direct routes over indirect routes, which has multiple media relays and NATs.
- **Offering and answering.** After the ICE candidates are gathered and sorted, the calling