

IPv6 support for WebRTC

IPv6 support for WebRTC is added since build [5.2.660](#). This led to some changes in configuration settings and connection establishing procedure.

Configuration

By default, IPv6 support is disabled. To enable this feature, the following should be done:

- in [flashphoner.properties](#) file set the external IPv6 server address and allow IPv6 candidates

```
ip_v6=2a03:b0c0:3:e0::42e:c002
ice_add_ipv6_candidate=true
```

- in [wcs-core.properties](#) file allow IPv6 stack

```
-Djava.net.preferIPv4Stack=false
```

The following settings can be used to set comma separated IPv4 and IPv6 interfaces to bind

- `hls.address`
- `http.address`
- `https.address`
- `rtmfp.address`
- `rtmp.address`
- `rtsp.address`
- `rtsp_client.address`
- `ws.address`
- `wss.address`

Connection establishing procedure

Connection establishing to exchange WebRTC media traffic now looks as follows:

1. Server waits for incoming Binding Request queries to IPv4 and IPv6 interfaces.

2. When a query with **USE-CANDIDATE** attribute is received, the candidate is marked as nominated to use, if **Binding Response** would be received

The screenshot shows a network traffic capture on UDP port 31010. Packet 101 is a Binding Request from 2a00:1fa0:4640:7dbd:9c2f:4227:7f3c:6c5d to 2a03:b0c0:31:e0:42e:c001. Packet 103 is a Binding Success Response from the same source to the same destination. The packet details for packet 103 show the following attributes:

- Message Type: 0x0001 (Binding Request)
- Message Length: 124
- Message Cookie: 2112a442
- Message Transaction ID: 4a38622f33577943959565a
- Attributes:
 - Attribute Type: USE-CANDIDATE (0x0025)
 - Attribute Length: 0
 - Attribute Type: PRIORITY (0x0024)
 - Attribute Length: 4
 - Priority: 1845584255
 - MESSAGE-INTEGRITY
 - FINGERPRINT

3. For every browser **Binding Request** server sends **Binding Response**

The screenshot shows a network traffic capture on UDP port 31010. Packet 101 is a Binding Request from 2a00:1fa0:4640:7dbd:9c2f:4227:7f3c:6c5d to 2a03:b0c0:31:e0:42e:c001. Packet 103 is a Binding Success Response from the same source to the same destination. The packet details for packet 103 show the following attributes:

- Message Type: 0x0001 (Binding Response)
- Message Length: 132
- Message Cookie: 2112a442
- Message Transaction ID: 4a38622f33577943959565a
- Attributes:
 - Attribute Type: XOR-MAPPED-ADDRESS (0x0020)
 - Attribute Length: 20
 - Reserved: 00
 - Protocol Family: IPv6 (0x02)
 - Port (XOR-d): fe7a
 - Port: 57192
 - IP (XOR-d): 0012b2bc701f92af703b6446653a07
 - IP: 2a00:1fa0:4640:7dbd:9c2f:4227:7f3c:6c5d
 - USERNAME: 44e81b0/80c5/11ea/b076/d3886f5540f6aqt0e64e6nuk:KD0K
 - SOFTWARE
 - MESSAGE-INTEGRITY
 - FINGERPRINT

4. At the same time, server sends **Binding Request** to browser. Requests will be repeated if necessary with the following period (1500 ms by default)

stun_freshness_period=1500

The screenshot shows a network traffic capture on UDP port 31010. Packet 101 is a Binding Request from 2a00:1fa0:4640:7dbd:9c2f:4227:7f3c:6c5d to 2a03:b0c0:31:e0:42e:c001. Packet 103 is a Binding Success Response from the same source to the same destination. The packet details for packet 103 show the following attributes:

- Message Type: 0x0001 (Binding Request)
- Message Length: 128
- Message Cookie: 2112a442
- Message Transaction ID: 3b60e38871091959736216d
- Attributes:
 - Attribute Type: USERNAME (0x0006)
 - Attribute Length: 55
 - Username: KD0K:44e81b0/80c5/11ea/b076/d3886f5540f6aqt0e64e6nuk
 - Padding: 1
 - ICE-CONTROLLED
 - PRIORITY
 - Attribute Type: PRIORITY (0x0024)
 - Attribute Length: 4
 - Priority: 2113939711
 - SOFTWARE
 - MESSAGE-INTEGRITY
 - FINGERPRINT

5. When **Bindind Response** is received from the first candidate, the timeout is started to wait for another candidates as set in the following parameter (1000 ms by default)

```
stun_wait_candidate_timeout=1000
```

6. When timeout is finished, server sends DTLS **Client Hello** to the priority candidate

The image shows a Wireshark network capture of a STUN-RTCPeerConnection handshake. The capture is filtered for 'udp.port == 51910'. The packet list shows a sequence of STUN messages: Binding Request, Binding Success Response, XOR-MAPPED-ADDRESS, and another Binding Success Response. This is followed by a DTLSv1.2 Client Hello message. The packet details for the Client Hello (packet 125) show: Content Type: Handshake (22), Version: DTLS 1.0 (0x0001), Epoch: 0, Sequence Number: 0, Length: 216. The handshake protocol details are also visible in the lower pane.

When establishing connection with Safari browser, IPv4 candidates are preferred unless some problem in STUN-DTLS procedure occur with such candidate. Therefore, in Safari IPv4 will be used if client has both IPv4 and IPv6 interfaces working and traffic between client and server is not blocked. In other browsers (see example pictures above) IPv6 candidates are preferred.

Known issues

1. WebRTC publishing/playback does not work in any browser on IPv6 only host

Symptoms

Stream publishing or playback fails with **Failed by ICE timeout** error

Solution

If a host has only IPv6 address (and localhost), ICE candidates exchange does not work, **RTCPeerConnection.onicecandidate** event is nor fired in most browsers. Use RTMP to publish and RTSP, RTMP, HLS to play.