draft-petithuguenin-p2psip-reload-one-to-many-00

Marc Petit-Huguenin
2013/03/11

Anycast in RELOAD

- As agreed, all the Broadcast, Multicast and Anycast stuff -in base was moved to this draft.

- The problem was that running a long-term connection on an Anycast address is not a good idea.

- As discussed, a RELOAD node sends a STUN Binding request to the IP/port in the configuration file, and receives a 300 Redirect with a Unicast IP address/port, that can be used to join the bootstrap node.

Security issue

- It is relatively easy to redirect the client to the wrong IP address, which is why this kind of mechanism generally requires some form of authentication, so the client knows that the answer is from the real server.

- The client will anyway quickly discover that the IP address does not use a correct certificate, so perhaps this attack is harmless.

Long-Term STUN Authentication

- One solution is to use the long-term authentication mechanism of STUN, using the same username and password that was used to acquire the RELOAD certificate. The client checks the MESSAGE-INTEGRITY in the STUN response to verify that the server really knows the password.

- This requires to distribute and synchronize the usernames/passwords on servers in different data centers.

DTLS

- Another solution may be to use the fact that the bootstrap servers are contacted after a certificate is retrieved from the enrollment server to establish a DTLS association with the Anycast address, using this newly acquired certificate, and then send the STUN Binding over it.
- But DTLS was never defined as transport for STUN (or TURN), so that requires an additional document.

Next

- WG item?

- Test server will be available if consensus found here.