IETF91 RADEXT WG Meeting
11 Nov 2014, Honolulu, HI, USA

draft-ietf-radext-dynamic-discovery -12

Draft Status

- -11 entered PROTO Write-Up phase
- JK noted a number of issues on the draft
- Almost all very easy to fix, went into -12
- One issue needs tackling :
  certificate lifetime < DNS discovered timeout

What's the issue ?

- dynamic-discovery describes ways to get a server IP address, protocol, port and **validity period** of results for all your RADIUS/TLS and RADIUS/DTLS needs
- set of these servers is « the end »
- After that, actual TLS contact is made with servers from that list, in order of preference
- During TLS certificate exchange, the presented server certificate may have a shorter NotAfter than what DNS yielded
- So even though DNS might have said the TLS connection can stay up for n seconds, cert might suggest to kill the connection after m < n seconds
- It should be stated « somewhere » that the actual connection lifetime is also dependent on TLS NotAfter, not only DNS resolution results
- Where ?

Where ?

- dynamic-discovery is not talking about the actual TLS connection ; adding there would be unnatural
- RADIUS/TLS faces the NotAfter timeout problem in any case, even if no dynamic discovery is used
- So much more natural, but that's an issued RFC and issued RFCs never change :-)
- Suggestion : since folks indicated a preference to move RFC6614 from EXP to STD anyway, add small text regarding « caution, certificate expiry needs to be considered » while doing that move.
- See also our rechartering discussion

Next steps

- Settle this issue
- Next round of PROTO write-up, publication