In-band SA establishment for DHCPv6

Vishnu Ram

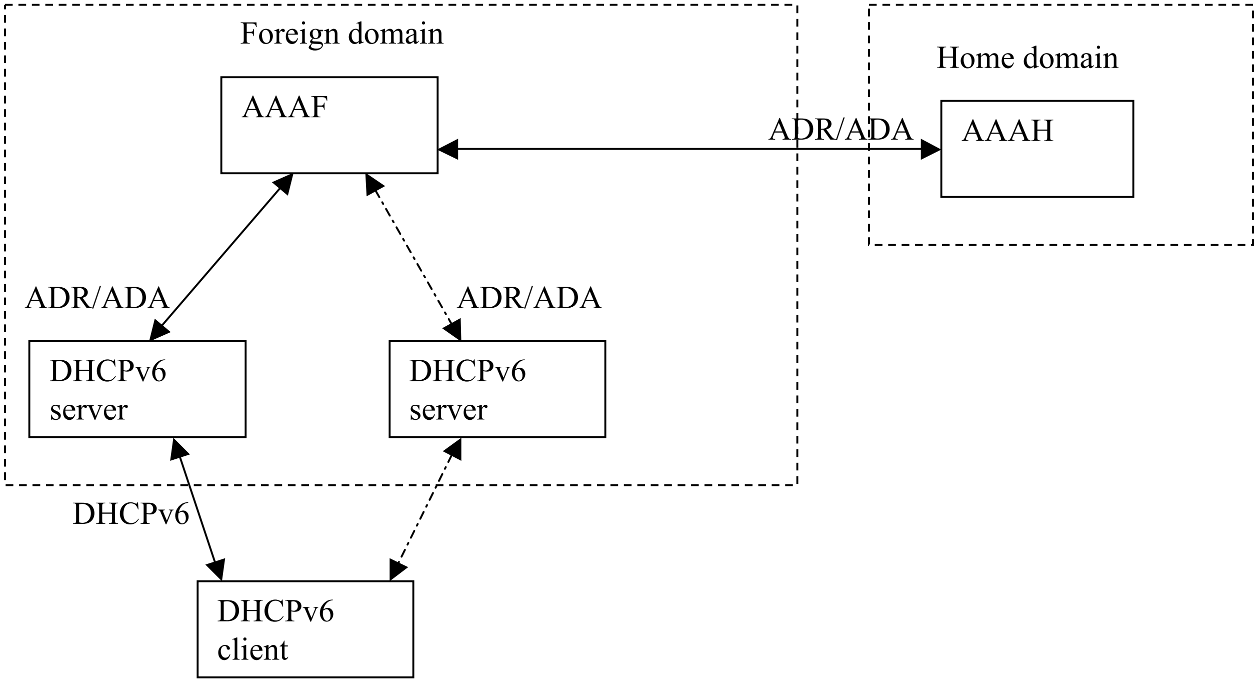
Motorola

vishnu@motorola.com

Background

- RFC3315 introduces authentication extensions for DHCPv6 which can be used for authenticating and authorizing DHCP messages
- It assumes the presence of a pre-configured shared key between DHCP server and DHCP client.
- Problem statement
  - The mechanism described in RFC3315 does not address inter-domain authentication.
  - It is not scalable since the shared key is transferred out-of-band.
  - There is no current mechanism to transfer the DHCP keys in band from home domain.
  - There is no current mechanism to transfer the configuration parameters from the home domain (eg: MIPv6 bootstrapping params).

Network Architecture



The above figure explains the network architecture for the DHCP security. The changes required to support the dynamic SA establishment using AAA are:

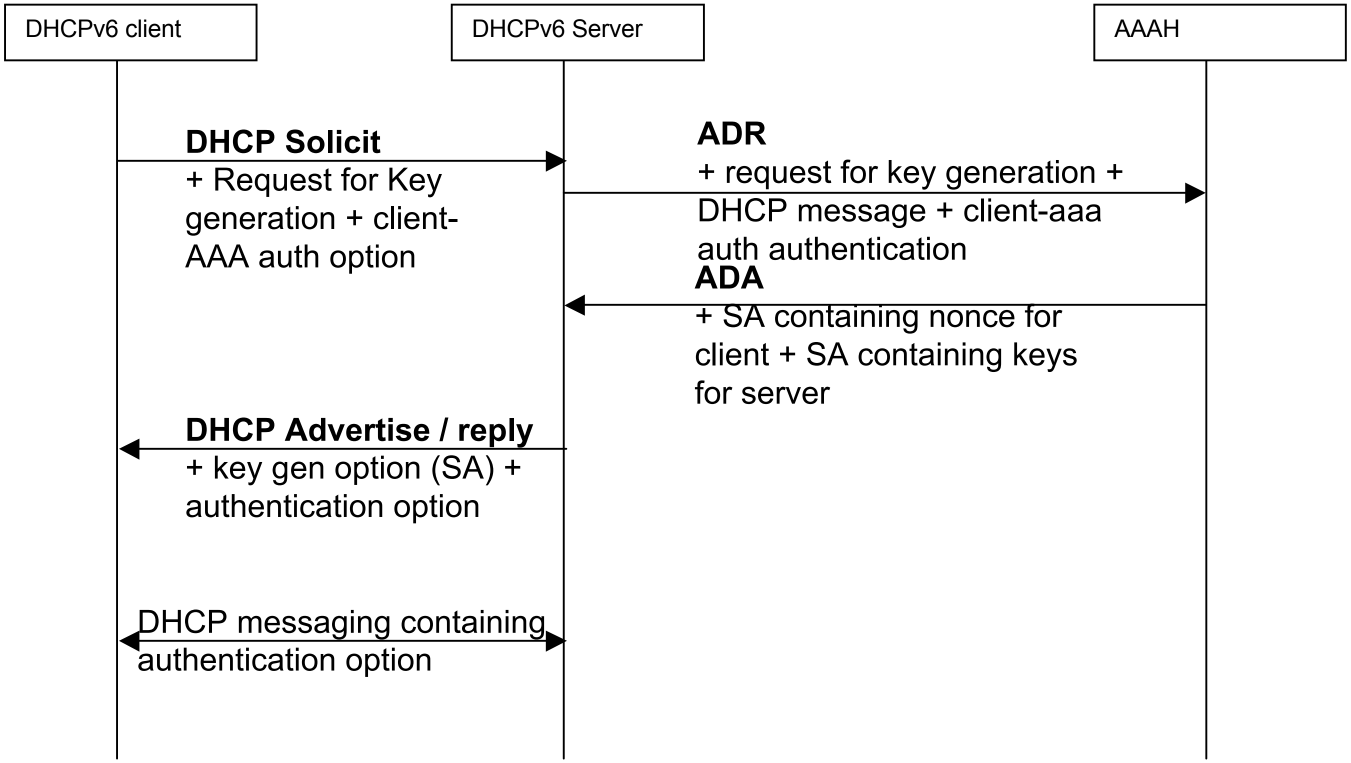
•The DHCPv6 would require options to carry the keying information from DHCPv6 server received from AAAH.

•The AAA interface between the DHCPv6 server and the AAAH to authenticate the client and also to transfer keys between AAAH and DHCPv6 server

•DHCPv6 client would require a security association with the AAAH. This SA is used to authenticate the client and to derive the DHCP keys.

•AAAF acts as a relay (Diameter app id 0xffffffff).

Initial key establishment (stateful autoconfiguration)



DHCPv6 client

DHCPv6 Server

AAAH

DHCP Solicit
+ Request for Key generation + client-AAA auth option

ADR
+ request for key generation + DHCP message + client-aaa auth authentication

ADA
+ SA containing nonce for client + SA containing keys for server

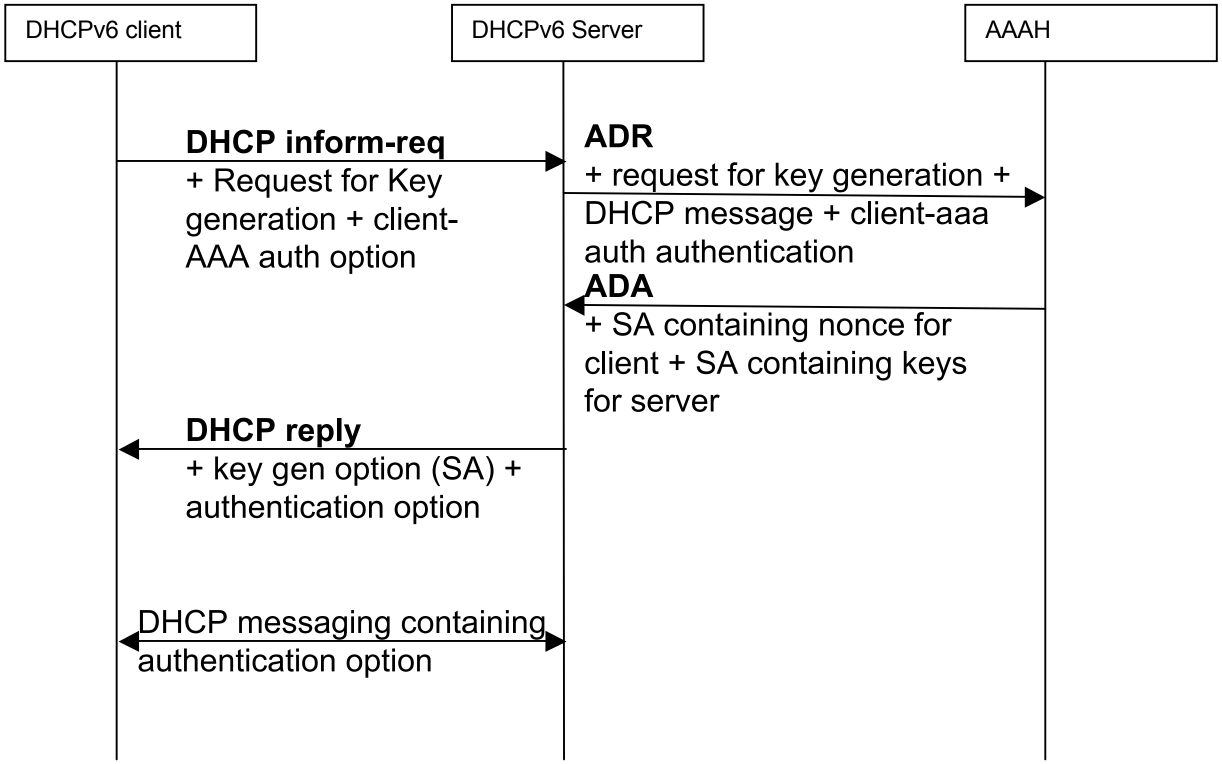
DHCP Advertise / reply
+ key gen option (SA) + authentication option

DHCP messaging containing authentication option

Initial key establishment (stateful autoconfiguration)

- When DHCP client sends DHCP Solicit it includes the request for key generation and the client – AAA authentication option.
- The DHCP server encapsulates the DHCP message by marking the authentication information field as zero, the client-AAA auth option and a request for generation of keys in the AAA-DHCP Request (ADR) message.
- The AAA server authenticates the user and message using the client-AAA authentication option by computing the HMAC over the DHCP message. The AAA is agnostic of the DHCP message format.
- If authentic, the AAA sends the SA including nonce (to be used by client) and SA including keys (to be used by server) in the AAA-DHCP Answer (ADA) message.
- The DHCP Server saves the SA (including keys) and sends the SA (including the nonce) to the client in the DHCP Advertise message.
- The DHCP Advertise message is protected using the authentication option constructed from the SA which was setup.
- From this point on, the DHCP Server and DHCP Client exchange messages which include the authentication option constructed from the SA which was setup.

Initial key establishment (stateless autoconfiguration)



DHCPv6 client

DHCPv6 Server

AAAH

DHCP inform-req
+ Request for Key generation + client-AAA auth option

ADR
+ request for key generation + DHCP message + client-aaa auth authentication

ADA
+ SA containing nonce for client + SA containing keys for server

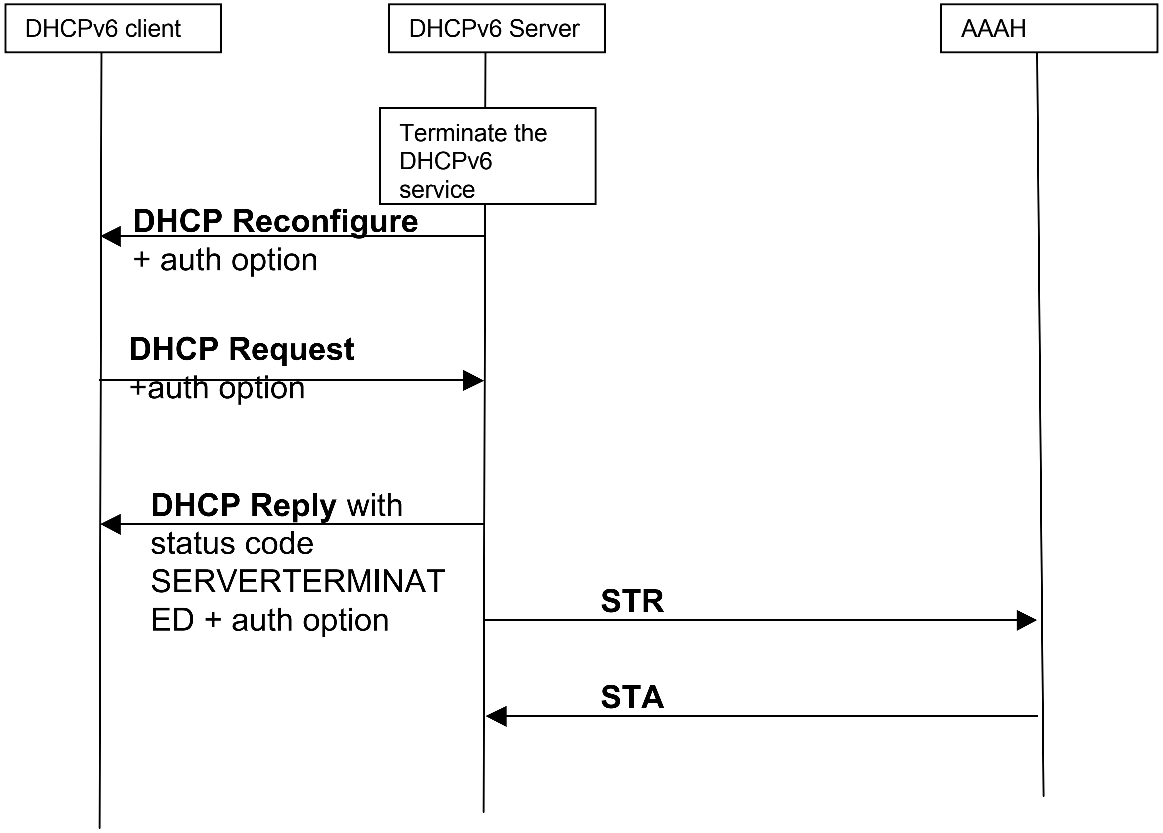
DHCP reply
+ key gen option (SA) + authentication option

DHCP messaging containing authentication option

Initial key establishment (stateless auto-configuration) contd

- When the DHCP client sends DHCP information request, it also includes the request for key generation and the client – AAA authentication option.
- The DHCP server encapsulates the DHCP message by marking the authentication information field as zero, the client-AAA auth option and a request for generation of keys in the AAA-DHCP Request (ADR) message.
- The AAA server authenticates the user and message using the client-AAA authentication option by computing the HMAC over the DHCP message. The AAA is agnostic of the DHCP message format.
- If authentic, the AAA sends the SA including nonce (to be used by client) and SA including keys (to be used by server) in the AAA-DHCP Answer (ADA) message.
- The DHCP Server saves the SA including keys and sends the SA (including the nonce) to the client in the DHCP Reply message.
- The DHCP Reply message is protected using the authentication option constructed from the SA which was setup.
- From this point on, the DHCP Server and DHCP Client exchange messages which include the authentication option constructed from the SA which was setup.

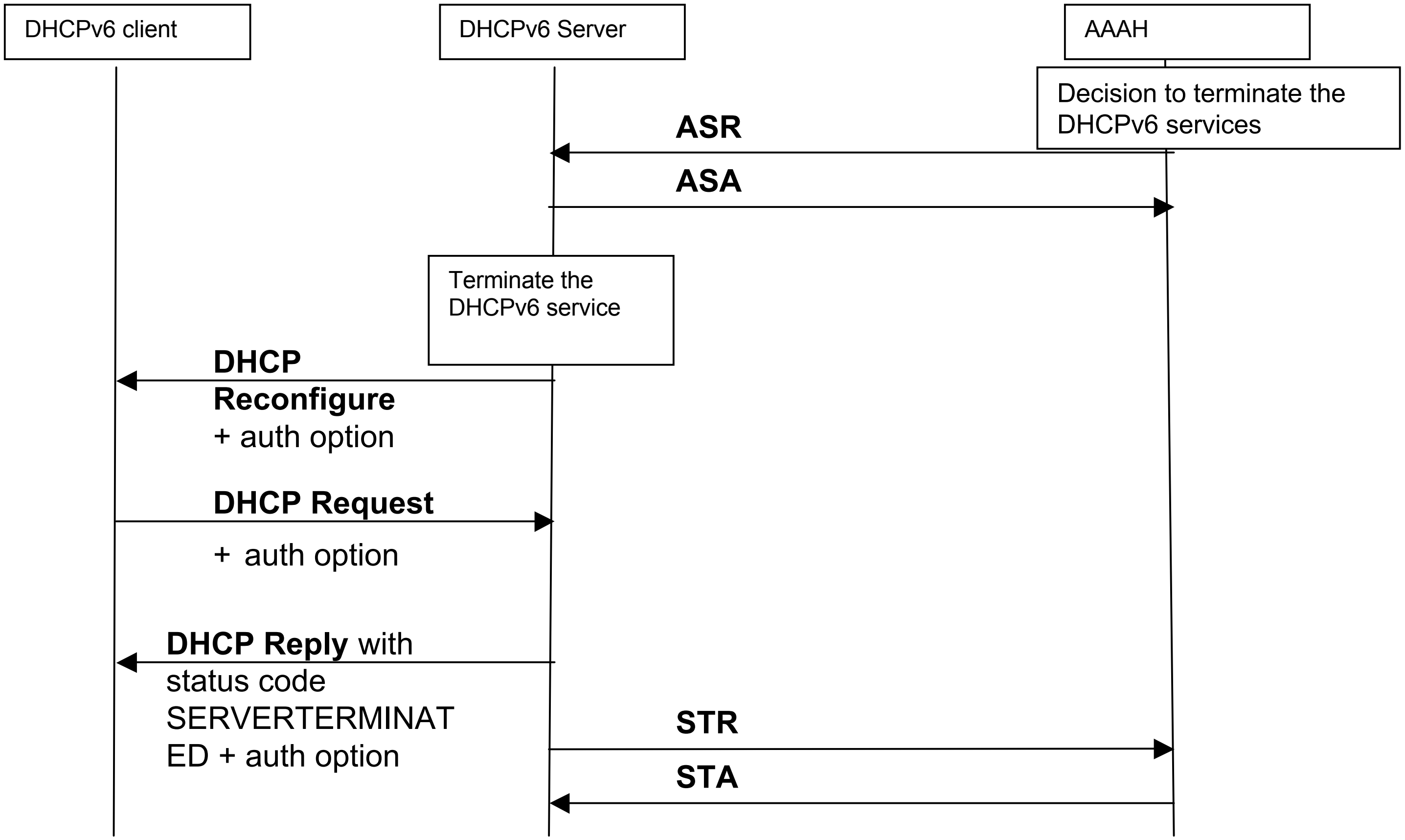
DHCP server initiated termination


DHCPv6 client
DHCPv6 Server
AAAH
Terminate the DHCPv6 service
DHCP Reconfigure + auth option
DHCP Request +auth option
DHCP Reply with status code SERVERTERMINATED + auth option
STR
STA

DHCP server initiated termination

- The DHCP server decides to terminate the DHCP service given to client. This can be a policy or admin decision.
- The server terminates the DHCP service by sending DHCP Reconfigure message to client.
- Client sends the DHCP Request and in response the server sends the DHCP Reply (with status code SERVERTERMINATED).
- DHCP Server sends Session Termination Request (STR) to AAAH.
- AAAH responds with STA which confirms the session clean up at the AAAH.

AAA initiated termination of DHCP service



DHCPv6 client

DHCPv6 Server

AAAH

Decision to terminate the DHCPv6 services

ASR

ASA

Terminate the DHCPv6 service

DHCP Reconfigure + auth option

DHCP Request

+ auth option

DHCP Reply with status code SERVERTERMINATED + auth option

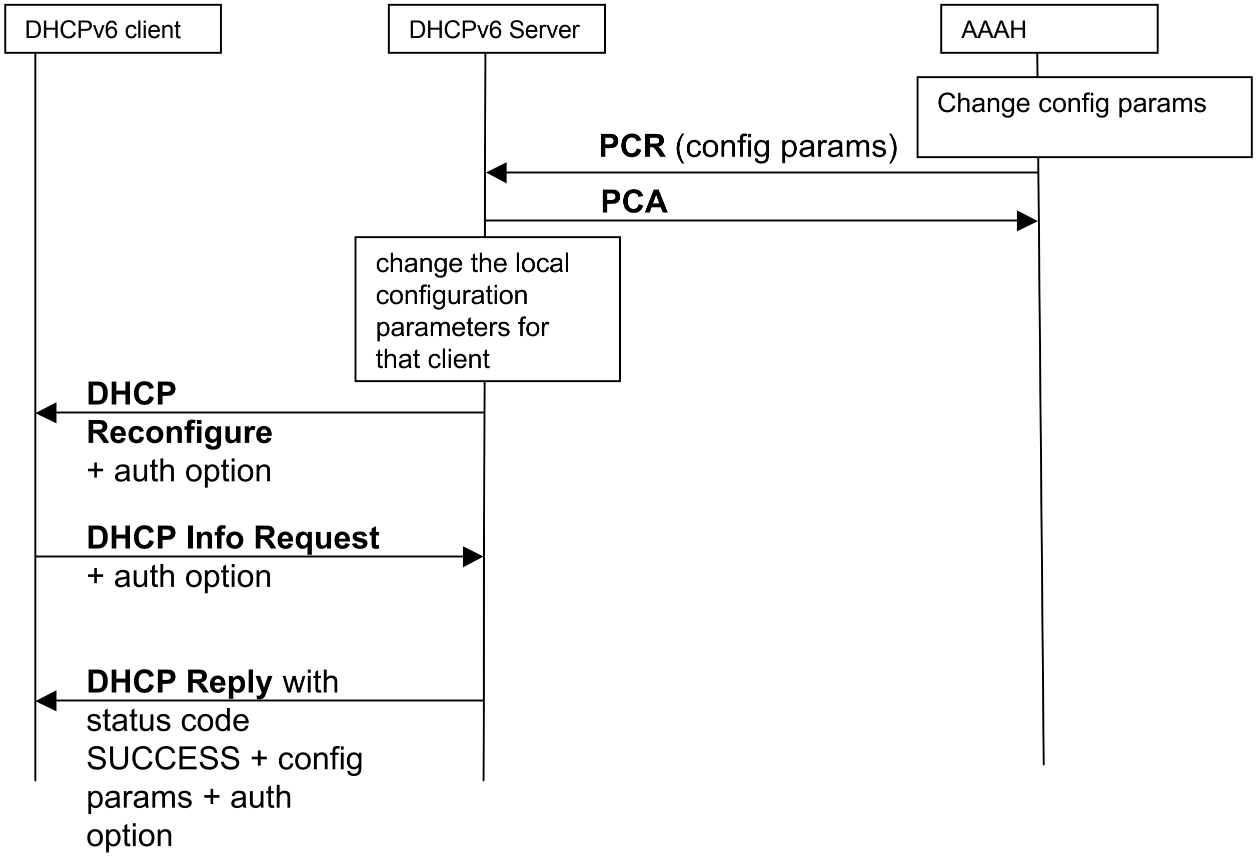
STR

STA

AAAH initiated termination

- When AAAH decides to terminate the DHCP service, it sends the Abort Session Request (ASR) to the DHCP server.
- DHCP Server sends Abort Session Answer (ASA) to confirm that it can terminate the DHCPv6 service given to client.
- The DHCP server terminates the DHCP service by sending DHCP Reconfigure message to client.
- Client sends the DHCP Request and in response the server sends the DHCP Reply (with status code SERVERTERMINATED).
- DHCP Server sends Session Termination Request (STR) to AAAH.
- AAAH responds with STA which confirms the session clean up at the AAAH.

AAAH initiated configuration update



DHCPv6 client

DHCPv6 Server

AAAH

Change config params

PCR (config params)

PCA

change the local configuration parameters for that client

DHCP Reconfigure + auth option

DHCP Info Request + auth option

DHCP Reply with status code SUCCESS + config params + auth option

AAAH initiated Configuration update

- The configuration information at the AAAH has changed and AAAH wants to update the client.
- The AAAH sends the Push Config Request (PCR) to the DHCP server with the new config params and the DHCP server sends Push Config Answer (PCA) in response to PCR.
- The DHCP Server sends DHCP Reconfigure to the client.
- Client sends the DHCP Info request and in response the server sends the changed configuration parameters in the DHCP Reply.
- These DHCP messages use the auth option for security.

Related IPR disclosures

- Title: METHOD FOR AUTHENTICATING A MOBILE NODE IN A COMMUNICATION NETWORK
- Applicants: VISHNU RAM O. V, VIHANG G. GANGARAM KAMBLE, SAUMYA G. UPADHYAYA

Related drafts

- draft-ram-dhc-dhcpv6-aakey-00.txt
- draft-ram-dhc-dhcpv6-diam-app-00.txt