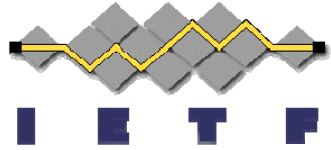


Forcerenew Nonce Authentication

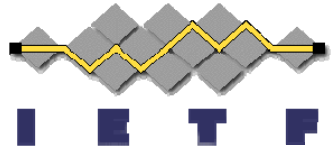
draft-ietf-dhc-forcerenew-nonce-01

D. Miles - Alcatel-Lucent
W. Dec - Cisco Systems
J. Bristow - Swisscom
R. Maglione - Telecom Italia



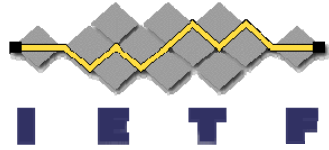
Problem Statement

- Forcerenew is used to set the DHCP client to the RENEW state and change host parameters
- Current forcerenew (RFC 3203) requires token authentication from DHCP server to client
- The authentication scheme specified in RFC 3118 uses shared secrets distributed out-of-band – not always practical to deploy in advance



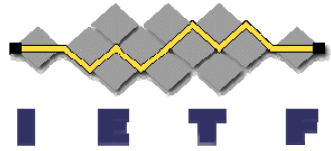
Proposal

- This draft defines a new scheme which use of Forcerenew Key Authentication to exchange a key between Server and client during initial DHCP exchange
- The key is used by the client to validate a server forcerenew message
- Mirrors the functionality in DHCPv6 (RFC 3315) – equivalent to the Reconfigure Key Authentication protocol



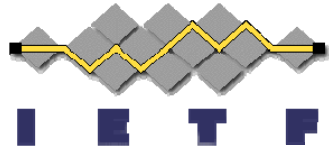
History

- Initial version presented in Dublin IETF-72
- Individual draft accepted as WG item in San Francisco IETF-74 (March 2009)
- Version -00 submitted in June 2009
- Version -00 declared by the chairs ready for WG last call during IETF-76 (November 2009)
- A follow up discussion happened on the list in February 2010



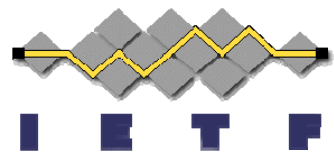
Main changes in - 01

- Clarified the scenario of applicability in the introduction:
 - This mechanism is intended to be used in Broadband Access Networks described in TR-101 document of the Broadband Forum

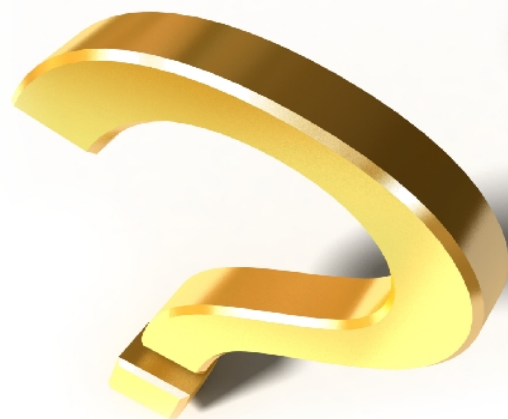


Next Step

- The authors believe the document is ready for WG Last Call



Questions?



Thanks!

IETF 80