LDP Hello Cryptographic Authentication

draft-zheng-mpls-ldp-hello-crypto-auth-01

Vero Zheng  (verozheng@huawei.com)
Mach Chen     (mach@huawei.com)

Karp WG, IETF 80, Prague, 1 April 2011
Problem Statement

- Established LDP session could be torn down by spoofed Hello
  - By specifying a smaller Hold Time or changing the Transport Address
  - Reported as real problem in operation networks
- RFC5036 does not provide any security mechanisms for use with Hello messages
  - The current TCP authentication mechanism can not help here
Draft Objective

- Secure the Hello message against spoofing attack
  - Introduces a new Cryptographic Authentication TLV
  - Used in LDP Hello message as an optional parameter
- Enhances the authentication mechanism for LDP
  - LSR can be configured to only accept Hello messages from specific peers when authentication is in use
- It’s Simple, its Backward Compatible and its Secure
Changes Since Last Version

- Protection to replay attack removed
- Cryptographic algorithms update
  - Keyed MD5 dropped—considered not strong enough
  - HMAC–SHA used instead
  - HMAC–SHA–256 is a MUST, SHOULD support HMAC–SHA–1 and MAY support either HMAC–SHA–384 or HMAC–SHA–512
Next Steps

- Continue to gather feedback from the list
- Where should we take this work?
- Need more feedback from security experts
Thank you