LDP Hello Cryptographic Authentication

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

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

MPLS WG, IETF 80, Prague, 31 Mar 2011

Problem Statement

- 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

Transport Address
Reported as real problem in operation networks
The current TCP authentication mechanism can not help here
RFC5036 does not provide any security mechanisms for use with Hello messages
The current TCP authentication mechanism can not help here

Draft Objective

- 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

- It's Simple, its Backward Compatible and its Secure

Draft Status

- **Karp BGP/LDP/MSDP Design Team formed**
- **draft-mahesh-bgp-ldp-msdp-analysis-00 produced**

Changes Since Last Version

SHA-1 and MAY support either HMAC-SHA-384 or HMAC-SHA-512

- 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
  - **Present in Karp tomorrow**

Thank you