LDP Hello Cryptographic Authentication

draft-zheng-mpls-ldp-hello-crypto-auth-02

Vero Zheng (verozheng@huawei.com)
Mach Chen (mach@huawei.com)
Manav Bhatia (manav.bhatia@alcatel-lucent.com)

Karp WG, IETF 81, Quebec City, 27 July 2011

Problem Statement

- **draft-ietf-karp-routing-tcp-analysis-00.txt**
- **Current State**
  - Established LDP session could be tore 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
- **Optimal State**
  - Should be able to determine the authenticity of the neighbors sending the Hello message
- **Gap Analysis**
  - Spoofing attacks can be solved by being able to authenticate the Hello messages,

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**
  - NIST Secure Hash Standard family of algorithms used
  - 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

- **A 64-bit strictly increasing sequence number used**
  - To guard against replay attacks
  - MUST be incremented for every LDP packet sent
- **Hash computing mistake fixed**
  - IP header excluded when computing hash
- **Auth Type field removed-considered redundant**
  - Auth Key ID identifies the algorithm and the secret key used

Next Steps

- **Continue to gather feedback from the list**
  - Need more feedback from security experts
- **Request adoption in MPLS WG**

Thank you