

Security Framework for MPLS-TP

draft-mpls-tp-security-framework-01.txt

Editors:

Luyuan Fang

lufang@cisco.com

Ben Niven-Jenkins

ben@niven-jenkins.co.uk

Scott Mansfield

scott.mansfield@ericsson.com

July 26, 2011

81 IETF, Quebec, Canada

Contributing Co-authors

- Luyuan Fang lufang@cisco.com
- Ben Niven-Jenkins ben@niven-jenkins.co.uk
- Scott Mansfield scott.mansfield@ericsson.com
- Raymond Zhang raymond.zhang@bt.com
- Nabil Bitar nabil.bitar@verizon.com
- Masahiro Daikoku ms-daikoku@kddi.com
- Lai Wang Lai.wang@telenor.com
- Henry Yu henry.yu@twtelecom.com

Overview

- Content:
 - Identify and address MPLS-TP *specific* security issues.
 - Define MPLS-TP security reference models
 - Provide MPLS-TP security requirements
 - Identify MPLS-TP security threats
 - Provide MPLS-TP security threat mitigation recommendations
- Intended category: Informational
- Scope:
 - Focus on MPLS-TP specific security threats, e.g.
 - GAL/GAch for in-band OAM
 - NMS provisioning model
 - General attached applied in TP operations: DoS attack, ID/Label spoofing
 - Defer to existing RFCs for Internet Best Practice Guidelines, and MPLS/GMPLS Security Framework

Status and Next Steps

- Current status:
 - Accepted as MPLS WG document and issued 00 WG draft in Feb. 2011
 - Updated document with additional author Henry Yu, and minor updates, issued 01 draft May 2011
- Next Steps
 - Comments are welcome from WG
 - Issue new version and asking for WG last call