Interoperability Report for ForCES
(draft-ietf-forces-interop-01)

IETF 80 Meeting
March 27, 2011, Prague, Czech Republic

Kentaro Ogawa, ogawa.kentaro@lab.ntt.co.jp
Evangelos Haleplidis, ehalep@ece.upatras.gr
Weiming Wang, wmwang@zjgsu.edu.cn
Ming Gao, gmyyqno1@pop.zjgsu.edu.cn
Jamal Hadi Salim, hadi@mojatatu.com
Summary

• Location, Date and Participants
• Tested Material
• Testbed Configuration
  – Access
  – Local
  – Distributed
• Scenarios Tested
• Test Results
• Issues Found
Location, Date and Participants

• Location
  – Zhejiang Gongshang University – China
  – the Internet Technology Lab (ITL)

• Date
  – 24-25/2/ 2011

• Participants
  – Zhejiang Gongshang University/Hangzhou BAUD Networks, China
  – NTT Corporation, Japan
  – The University of Patras, Greece
Tested Material

- Protocol, RFC5810
- Model, RFC5812
- LFB Lib, draft-03
- CEHA, draft-01
Testbed Configuration-Access
Testbed Configuration-Distributed

CE-Greece

ForCEs Protocol Analyzer

Internet

FE-Greece

150.140.254.110 (VPN)
Scenario 1 - LFB Operation

-To verify that the interoperating peer complying with RFC 5810 can decode and handle messages defined in RFC 5810.

-To verify the definition of ForCES LFB Library.

-Three implementors carried out the test in an alternative way acting as a CE or an FE, combined with 6 cases for this scenario.
Scenario 2 - TML with IPSec

-To verify that the interoperating peer can make TML run over IPSec channel that was pre-established.

-The third party tool software 'racoon' was used to establish IPSec channel.

-Three implementors carried out the test in an alternative way acting as a CE or an FE, combined with 6 cases for this scenario.
Scenario 3 - CE High Availability

- To verify the CEHA mechanics based on the CEHA document.
- One FE connected and associated with a master and backup CE.
- When the master CE is considered disconnected, the FE attempts to find another associated CE to become the master CE.
Scenario 4 - Packet forwarding (1)

- To verify some LFBs related to the IPv4 forwarding, such as EtherPHYCop, EtherMacIn, EtherClassifier, IPv4Validator, EtherEncasulator, EtherMacOut, RedirectIn, RedirectOut, IPv4NextHop, IPv4UcastLPM.

- To confirm that whole NE including FE and CE actually work like an OSPF router which exchanges OSPF protocol information with other OSPF routers.
Scenario 4 - Packet forwarding (2)
Scenario 4 - Packet forwarding(3)

Packet Flow
Test Results - Scenario 1

- Tested operations related to the IPv4 forwarding.

- Queried and configured FEObject, EtherPHYCop, EtherMacIn, EtherMacOut, EtherClassifier, ARP, EtherEncasulator, IPv4NextHop, IPv4UcastLPM.

- Succeeded in all of 6 configuration patterns.
Test Results - Scenario 2

- Tested some typical operations in the operation list of scenario1 over IPSec channel.

- Succeeded in the local configuration with Chinese and Japanese implementation.

- Some problems still remains in the distributed configuration with Greece, on the setup of the IPSec connection but not on the ForCES protocol.
Test Results - Scenario 3

• Succeeded in both of 2 configuration patterns.

• Implementation issue of how the FE prioritizes incoming messages from multiple CEs was occurred.
Test Results - Scenario 4

• Succeeded in the pattern with Japanese CE and Chinese FE.

• Some problems still remains in the pattern with Chinese CE and Japan FE, on the OSPF process but not on the ForCES protocol.
Issues Found

• About the data encapsulation format, response of PATH-DATA format and operation to array.
  - ForCES element (CE or FE) sender is free to choose whatever data structure that IETF ForCES documents define and best suits the element.
  - ForCES element (CE or FE) is preferable to accept and process information (requests and responses) that use any legitimate structure defined by IETF ForCES documents.
  - It is preferred the ForCES element responds in the same format that the request was made.

• About the message handle prioritization in the FE.
Thanks!