

Internet Engineering Task Force  
Internet-Draft  
Intended status: Informational  
Expires: September 15, 2011

W. Wang  
Zhejiang Gongshang University  
K. Ogawa  
NTT Corporation  
E. Haleplidis  
University of Patras  
M. Gao  
Hangzhou BAUD Networks  
J. Hadi Salim  
Mojatatu Networks  
March 14, 2011

**Interoperability Report for Forwarding and Control Element Separation  
(ForCES)  
draft-ietf-forces-interop-01**

**Abstract**

This document captures test results from the second Forwarding and control Element Separation (ForCES) interop testing which took place on March 24-25, 2011 at the Internet Technology Lab (ITL) of Zhejiang Gongshang University in China.

**Status of this Memo**

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on September 15, 2011.

**Copyright Notice**

Copyright (c) 2011 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents

(<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

<u><a href="#">1.</a></u>	<u><a href="#">Introduction . . . . .</a></u>	<u><a href="#">4</a></u>
<u><a href="#">1.1.</a></u>	<u><a href="#">ForCES Protocol . . . . .</a></u>	<u><a href="#">4</a></u>
<u><a href="#">1.2.</a></u>	<u><a href="#">ForCES Model . . . . .</a></u>	<u><a href="#">4</a></u>
<u><a href="#">1.3.</a></u>	<u><a href="#">Transport Mapping Layer . . . . .</a></u>	<u><a href="#">4</a></u>
<u><a href="#">1.4.</a></u>	<u><a href="#">CE HA . . . . .</a></u>	<u><a href="#">5</a></u>
<u><a href="#">2.</a></u>	<u><a href="#">Terminology and Conventions . . . . .</a></u>	<u><a href="#">6</a></u>
<u><a href="#">2.1.</a></u>	<u><a href="#">Requirements Language . . . . .</a></u>	<u><a href="#">6</a></u>
<u><a href="#">2.2.</a></u>	<u><a href="#">Definitions . . . . .</a></u>	<u><a href="#">6</a></u>
<u><a href="#">3.</a></u>	<u><a href="#">Overview . . . . .</a></u>	<u><a href="#">8</a></u>
<u><a href="#">3.1.</a></u>	<u><a href="#">Date, Location, and Participants . . . . .</a></u>	<u><a href="#">8</a></u>
<u><a href="#">3.2.</a></u>	<u><a href="#">Testbed Configuration . . . . .</a></u>	<u><a href="#">8</a></u>
<u><a href="#">3.2.1.</a></u>	<u><a href="#">Access . . . . .</a></u>	<u><a href="#">8</a></u>
<u><a href="#">3.2.2.</a></u>	<u><a href="#">Local Configuration . . . . .</a></u>	<u><a href="#">9</a></u>
<u><a href="#">3.2.3.</a></u>	<u><a href="#">Distributed Configuration . . . . .</a></u>	<u><a href="#">10</a></u>
<u><a href="#">4.</a></u>	<u><a href="#">Scenarios . . . . .</a></u>	<u><a href="#">12</a></u>
<u><a href="#">4.1.</a></u>	<u><a href="#">Scenario 1 - LFB Operation . . . . .</a></u>	<u><a href="#">12</a></u>
<u><a href="#">4.1.1.</a></u>	<u><a href="#">Connection Diagram . . . . .</a></u>	<u><a href="#">12</a></u>
<u><a href="#">4.1.2.</a></u>	<u><a href="#">Design Considerations . . . . .</a></u>	<u><a href="#">12</a></u>
<u><a href="#">4.1.3.</a></u>	<u><a href="#">Testing Proccess . . . . .</a></u>	<u><a href="#">12</a></u>
<u><a href="#">4.2.</a></u>	<u><a href="#">Scenario 2 - TML with IPSec . . . . .</a></u>	<u><a href="#">12</a></u>
<u><a href="#">4.2.1.</a></u>	<u><a href="#">Connection Diagram . . . . .</a></u>	<u><a href="#">13</a></u>
<u><a href="#">4.2.2.</a></u>	<u><a href="#">Design Considerations . . . . .</a></u>	<u><a href="#">13</a></u>
<u><a href="#">4.2.3.</a></u>	<u><a href="#">Testing Proccess . . . . .</a></u>	<u><a href="#">14</a></u>
<u><a href="#">4.3.</a></u>	<u><a href="#">Scenario 3 - CE High Availability . . . . .</a></u>	<u><a href="#">14</a></u>
<u><a href="#">4.3.1.</a></u>	<u><a href="#">Connection Diagram . . . . .</a></u>	<u><a href="#">14</a></u>
<u><a href="#">4.3.2.</a></u>	<u><a href="#">Design Considerations . . . . .</a></u>	<u><a href="#">14</a></u>
<u><a href="#">4.3.3.</a></u>	<u><a href="#">Testing Proccess . . . . .</a></u>	<u><a href="#">15</a></u>
<u><a href="#">4.4.</a></u>	<u><a href="#">Scenario 4 - Packet forwarding . . . . .</a></u>	<u><a href="#">16</a></u>
<u><a href="#">4.4.1.</a></u>	<u><a href="#">Connection Diagram . . . . .</a></u>	<u><a href="#">16</a></u>
<u><a href="#">4.4.2.</a></u>	<u><a href="#">Design Considerations . . . . .</a></u>	<u><a href="#">17</a></u>
<u><a href="#">4.4.3.</a></u>	<u><a href="#">Testing Proccess . . . . .</a></u>	<u><a href="#">17</a></u>
<u><a href="#">5.</a></u>	<u><a href="#">Test Results . . . . .</a></u>	<u><a href="#">19</a></u>
<u><a href="#">5.1.</a></u>	<u><a href="#">LFB Operation Test . . . . .</a></u>	<u><a href="#">19</a></u>
<u><a href="#">5.2.</a></u>	<u><a href="#">TML with IPSec Test . . . . .</a></u>	<u><a href="#">24</a></u>
<u><a href="#">5.3.</a></u>	<u><a href="#">CE High Availability Test . . . . .</a></u>	<u><a href="#">25</a></u>
<u><a href="#">5.4.</a></u>	<u><a href="#">Packet Forwarding Test . . . . .</a></u>	<u><a href="#">26</a></u>
<u><a href="#">6.</a></u>	<u><a href="#">Discussions . . . . .</a></u>	<u><a href="#">29</a></u>



<a href="#">6.1.</a>	On Data Encapsulation Format . . . . .	<a href="#">29</a>
<a href="#">7.</a>	Contributors . . . . .	<a href="#">32</a>
<a href="#">8.</a>	Acknowledgements . . . . .	<a href="#">33</a>
<a href="#">9.</a>	IANA Considerations . . . . .	<a href="#">34</a>
<a href="#">10.</a>	Security Considerations . . . . .	<a href="#">35</a>
<a href="#">11.</a>	References . . . . .	<a href="#">36</a>
<a href="#">11.1.</a>	Normative References . . . . .	<a href="#">36</a>
<a href="#">11.2.</a>	Informative References . . . . .	<a href="#">36</a>
	Authors' Addresses . . . . .	<a href="#">37</a>

## **1. Introduction**

This document captures the results of the second interoperability test of the Forwarding and control Element Separation (ForCES) Framework which took place March 24-25, 2011 in the Internet Technology Lab (ITL) of Zhejiang Gongshang University in China. The tests involved several documents namely: ForCES protocol [[RFC5810](#)], ForCES FE model [[RFC5812](#)], ForCES TML [[RFC5811](#)], ForCES LFB Library [FORCES-LFBLIB] and ForCES CE HA specification[FORCES-CEHA]. Three independent ForCES implementations participated in the test.

Scenarios of ForCES LFB Operation, TML with IPSec, CE High Availability, and Packet Forwarding are constructed. Series of testing items for every scenario are carried out and interoperability results are achieved. Extended Wireshark and extended tcpdump are used to verify the results.

The first interop test held in July 2008 at the University of Patras, Greece, focussed on validating the basic semantics of the protocol and model[RFC6053].

### **1.1. ForCES Protocol**

The ForCES protocol works in a master-slave mode in which FEs are slaves and CEs are masters. The protocol includes commands for transport of Logical Function Block (LFB) configuration information, association setup, status, and event notifications, etc. The reader is encouraged to read FE-protocol [[RFC5810](#)] for further information.

### **1.2. ForCES Model**

The FE-MODEL [[RFC5811](#)] presents a formal way to define FE Logical Function Blocks (LFBs) using XML. LFB configuration components, capabilities, and associated events are defined when the LFB is formally created. The LFBs within the FE are accordingly controlled in a standardized way by the ForCES protocol.

### **1.3. Transport Mapping Layer**

The TML transports the PL messages. The TML is where the issues of how to achieve transport level reliability, congestion control, multicast, ordering, etc. are handled. It is expected that more than one TML will be standardized. The various possible TMLs could vary their implementations based on the capabilities of underlying media and transport. However, since each TML is standardized, interoperability is guaranteed as long as both endpoints support the same TML. All ForCES Protocol Layer implementations MUST be portable across all TMLs. Although more than one TML may be standardized for



the ForCES Protocol, for the purposes of the interoperability test, the mandated MUST IMPLEMENT SCTP TML [[RFC5811](#)] will be used.

#### [1.4.](#) CE HA

## **2. Terminology and Conventions**

### **2.1. Requirements Language**

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [[RFC2119](#)].

### **2.2. Definitions**

This document follows the terminology defined by ForCES related documents, including [RFC3654](#), [RFC3746](#), [RFC5810](#), [RFC5811](#), [RFC5812](#), [RFC5812](#). Some definitions are repeated below for clarity.

Control Element (CE) - A logical entity that implements the ForCES protocol and uses it to instruct one or more FEs on how to process packets. CEs handle functionality such as the execution of control and signaling protocols.

Forwarding Element (FE) - A logical entity that implements the ForCES protocol. FEs use the underlying hardware to provide per-packet processing and handling as directed/controlled by one or more CEs via the ForCES protocol.

LFB (Logical Functional Block) - The basic building block that is operated on by the ForCES protocol. The LFB is a well defined, logically separable functional block that resides in an FE and is controlled by the CE via the ForCES protocol. The LFB may reside at the FE's datapath and process packets or may be purely an FE control or configuration entity that is operated on by the CE. Note that the LFB is a functionally accurate abstraction of the FE's processing capabilities, but not a hardware-accurate representation of the FE implementation.

LFB Class and LFB Instance - LFBs are categorized by LFB Classes. An LFB Instance represents an LFB Class (or Type) existence. There may be multiple instances of the same LFB Class (or Type) in an FE. An LFB Class is represented by an LFB Class ID, and an LFB Instance is represented by an LFB Instance ID. As a result, an LFB Class ID associated with an LFB Instance ID uniquely specifies an LFB existence.

LFB Metadata - Metadata is used to communicate per-packet state from one LFB to another, but is not sent across the network. The FE model defines how such metadata is identified, produced, and consumed by the LFBs. It defines the functionality but not how metadata is encoded within an implementation.





LFB Components - Operational parameters of the LFBs that must be visible to the CEs are conceptualized in the FE model as the LFB components. The LFB components include, for example, flags, single-parameter arguments, complex arguments, and tables that the CE can read and/or write via the ForCES protocol (see below).

ForCES Protocol - While there may be multiple protocols used within the overall ForCES architecture, the term "ForCES protocol" and "protocol" refer to the "Fp" reference points in the ForCES framework in [[RFC3746](#)]. This protocol does not apply to CE-to-CE communication, FE-to-FE communication, or to communication between FE and CE managers. Basically, the ForCES protocol works in a master-slave mode in which FEs are slaves and CEs are masters.

ForCES Protocol Transport Mapping Layer (ForCES TML) - A layer in ForCES protocol architecture that uses the capabilities of existing transport protocols to specifically address protocol message transportation issues, such as how the protocol messages are mapped to different transport media (like TCP, IP, ATM, Ethernet, etc.), and how to achieve and implement reliability, multicast, ordering, etc. The ForCES TML specifications are detailed in separate ForCES documents, one for each TML.



### **3. Overview**

#### **3.1. Date, Location, and Participants**

The ForCES interoperability test meeting was held by IETF ForCES working group on March 24-25, 2011, and was chaired by Jamal Hadi Salim, the current ForCES working group co-chair. Three independent ForCES implementations participated in the test:

- \* Zhejiang Gongshang University/Hangzhou BAUD Networks, China. This implementation is referred to as "China" or in some cases "C" in the document for the sake of brevity.
- \* NTT Corporation, Japan. This implementation is referred to as "Japan" or in some cases "J" in the document for the sake of brevity.
- \* The University of Patras, Greece. This implementation is referred to as "Greece" or in some cases "G" in the document for the sake of brevity.

During the interoperability test, protocol analyzers Wireshark and tcpdump were used to verify the validity of ForCES protocol messages and in some cases semantics.

Some issues related to interoperability among implementations were discovered. Most of the issues were solved on site during the test. The most contentious issue found was on the format of encapsulation for protocol TLV (Refer to [Section 6](#)).

Some errata related to ForCES document were found by the interoperability test. The errata will be reported to related IETF RFCs.

At times, interoperability testing was exercised between 2 instead of all three representative implementations due to the third one lacking a specific feature; however, in ensuing discussions, all implementors mentioned they will be implementing any missing features in the future.

#### **3.2. Testbed Configuration**

##### **3.2.1. Access**

Japan and China physically attended on site at the Internet Technology Lab (ITL) of Zhejiang Gongshang University in China. The University of Patras implementation joined remotely from Greece. The chair, Jamal Hadi Salim, joined remotely from Canada by using the teamviewer tool [ref XXX]. The approach is as shown in figure 1. In the figure, FE/CE refers to FE or CE that the implementor may act alternatively.



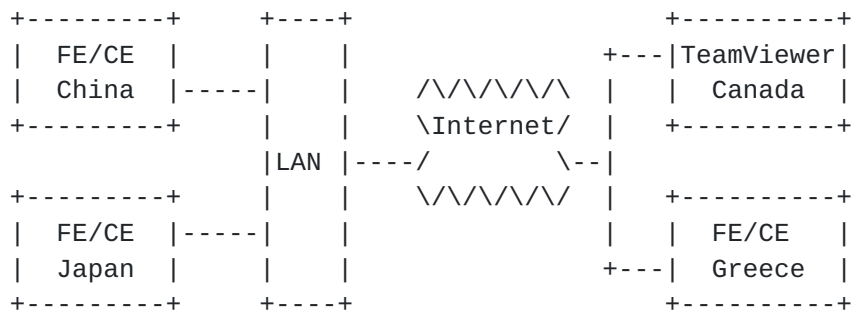


Figure 1: The Approach for all Participants

For interoperability test items, all CEs and FEs SHALL implement IPSEC security in the TML. For security, firewalls MUST be used that will allow only the specific IPs and the SCTP ports defined in the ForCES SCTP-TML [[RFC5811](#)].

### 3.2.2. Local Configuration

Hardwares and softwares including CEs and FEs from China and Japan implementations that were located within the ITL Lab of Zhejiang Gongshang University, were connected together using ethernet switches. The configuration can be seen in figure 2.



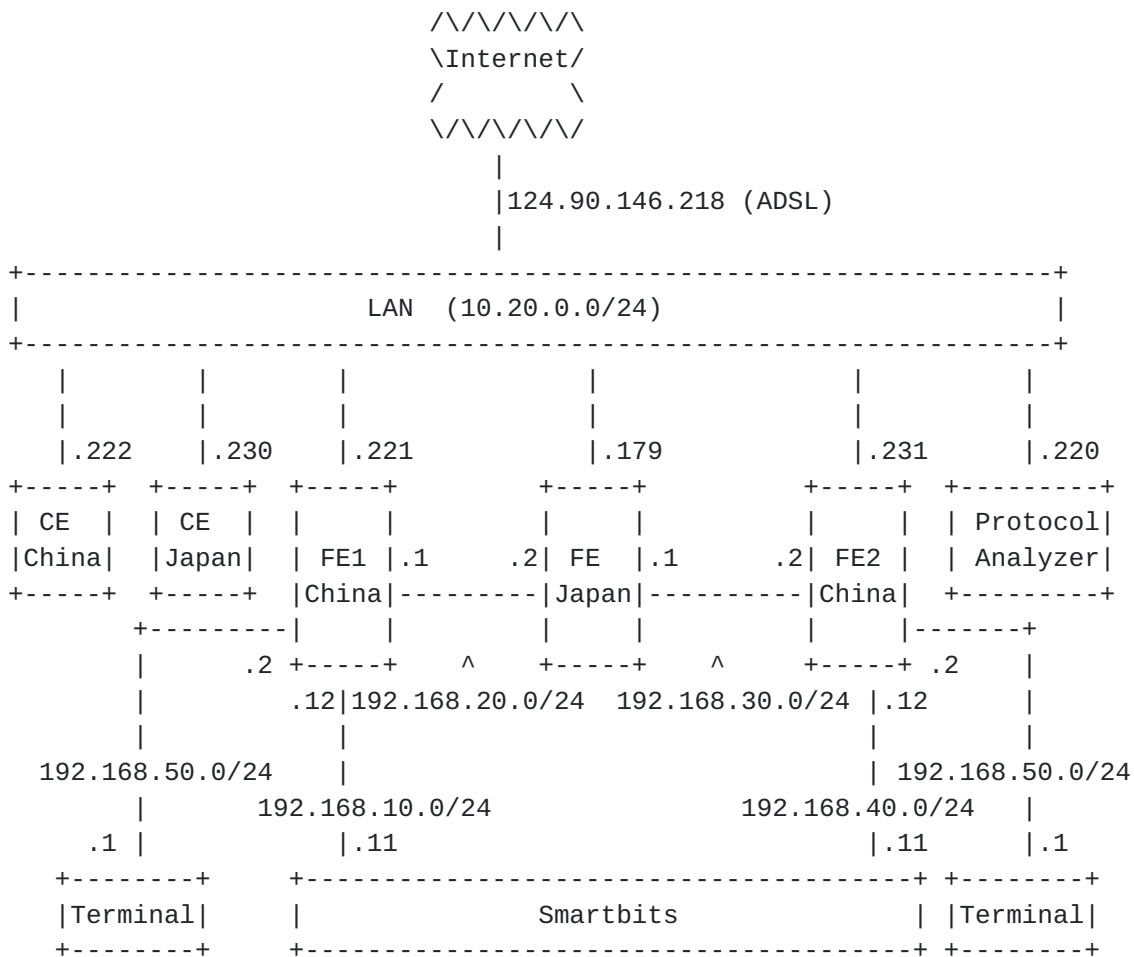


Figure 2: Testbed Configuration Located in ITL Lab,China

### 3.2.3. Distributed Configuration

Hardware/Software (CE and FE) of Greece that were located within the University of Patras premises, were connected together using LAN as shown in figure 3.





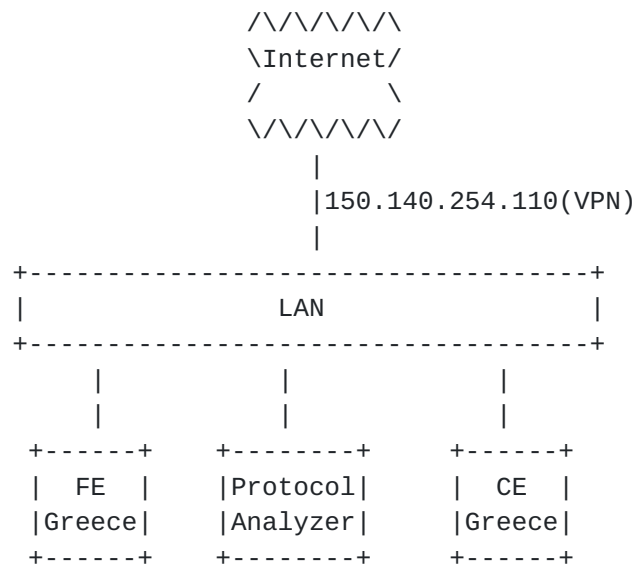


Figure 3: Testbed Configuration Located in the University of Patras, Greece

Above configurations can satisfy requirements of all scenarios that are mentioned in this document.



## 4. Scenarios

### 4.1. Scenario 1 - LFB Operation

#### 4.1.1. Connection Diagram

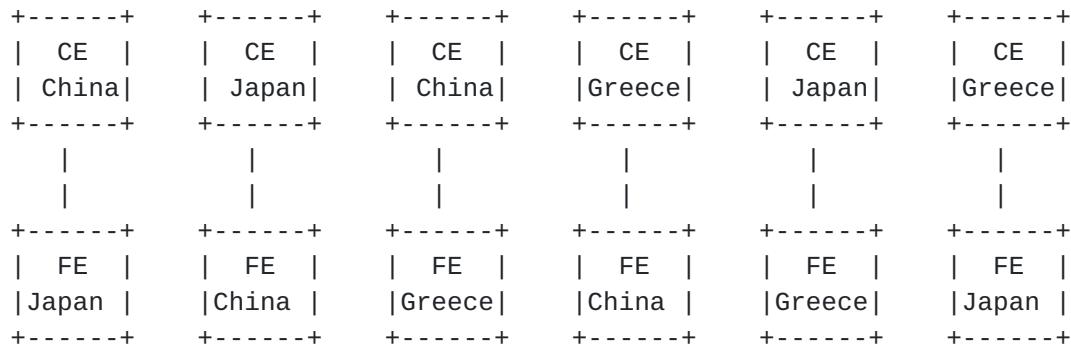


Figure 4: Scenario for LFB Operation

#### 4.1.2. Design Considerations

Firstly, the scenario of LFB Operation shown in Figure 4 is designed to verify all kinds of messages which are defined in [RFC 5810](#). Different implementor may have different choices on implementing [RFC 5810](#) using cases in the protocol messages. However as long as it complies with the [RFC 5810](#), the interoperating peer must have the ability to decode and handle it. Specially, what we want to verify the most is the format of encapsulation for PATH-DATA with nested PATH-DATAs, and the operation(SET, GET, DEL) of array, as well as array with nested array. (This case can be seen in ARP LFB's component of PortV4AddrInfoTable).

Second, the scenario is designed to verify the definition of ForCES LFB Library[I-D.ietf-forces-lfb-lib]. Successful test under this scenario means all the implementors have followed the instruction given by the ForCES LFB Library document.

#### 4.1.3. Testing Process

In order to make interoperability more credible, the three implementors carried out the test in an alternative way acting as a CE or an FE, as shown in figure 4, combined with 6 cases for this Scenario.

### 4.2. Scenario 2 - TML with IPSec



#### 4.2.1. Connection Diagram

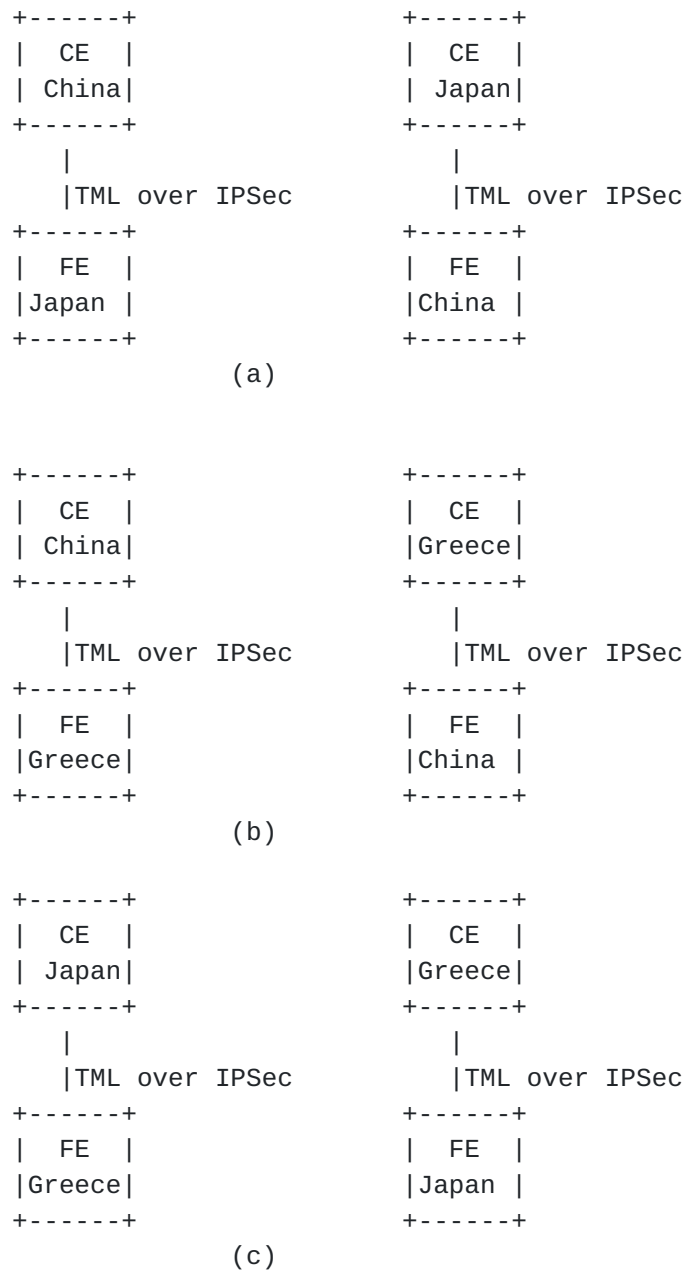


Figure 5: Scenario for LFB Operation with TML over IPsec

#### 4.2.2. Design Considerations

This scenario is designed to implement the requirement that stated in the section "7. Security Considerations" in [RFC 5811](#). For this reason, we designed the scenario to make TML run over IPsec channel that was pre-established. In this scenario, all operations for Scenario 1 were just repeated. In this way, we try to verify whether



all interactions between CE and FE can be done correctly under an IPSec enviroment.

#### 4.2.3. Testing Proccess

In this scenario, ForCES TML was run over IPSec channel. All the implementors joined in this interoperability used the same third-party tool software 'racoon' to establish IPSec channel. By this tool, China and Japan had a successful test, and the following items have been realized:

- o Internet Key Exchange (IKE) with certificates for endpoint authentication.
- o Transport Mode Encapsulating Security Payload (ESP). HMAC-SHA1-96 [RFC2404] for message integrity protection.

### 4.3. Scenario 3 - CE High Availability

#### 4.3.1. Connection Diagram

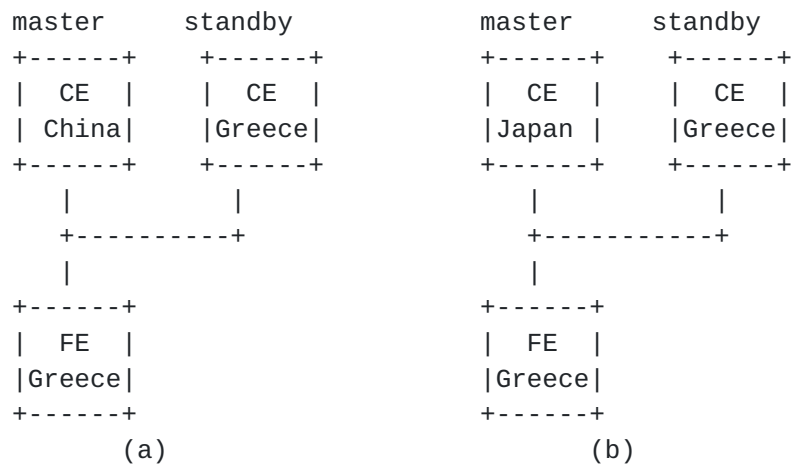


Figure 6: Scenario for CE High Availability

#### 4.3.2. Design Considerations

CE High Availability (CEHA) was also tested in this interoperability test based on the CEHA document [I-D.[draft-ietf-forces-ceha](#)].

The design of the setup and the scenario for the CEHA are as simple as possible to focus mostly on the mechanics of the CEHA, which are:

- o Associating with more than one CEs.





- o Switching to backup CE on master CE fail.

#### **4.3.3. Testing Process**

In this scenario one FE would be connected and associated with a master CE and a backup CE. In the pre-association phase, the FE would be configured to have China's or Japan's CE as master CE and Greece's CE as standby CE. The CEFailoverPolicy component of the FE Protocol Object LFB that specifies whether the FE is in High Availability mode (value 2 or 3) would either be set in the pre-association phase or in post-association phase by the master CE.

Once the FE is associated with the master CE it will move to the post-association phase. Then when the CEFailoverPolicy value is set to 2 or 3, then it will then attempt to connect and associate with the standby CE.

When the master CE is considered disconnected, either by TearDown, Loss of Heartbeats or Disconnected, FE would assume that the standby CE is now the master CE. FE will then send an Event Notification, Primary CE Down, to all associated CEs, only the standby CE in this case with the value of the new master CEID. The standby CE will then respond by setting with a configuration message the CEID of the FE Protocol Object with it's own ID, the same value, to confirm that the CE considers itself as the master as well.

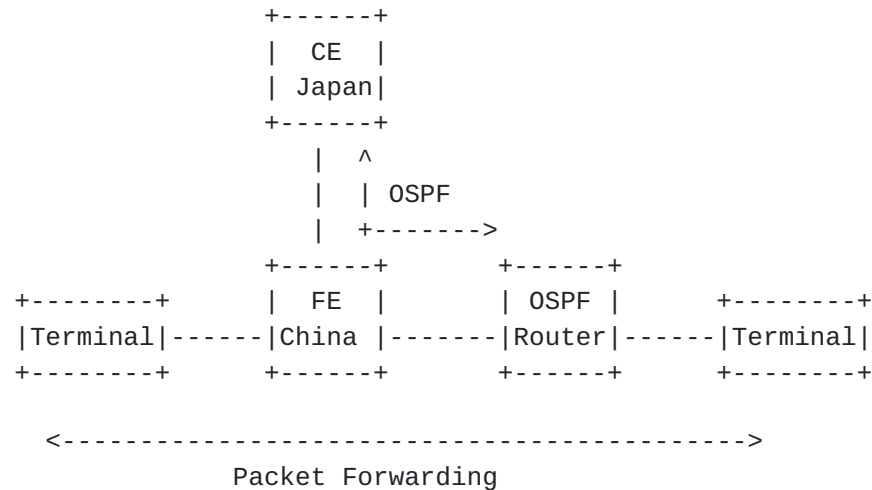
The steps of the CEHA scenario were the following:

1. In the pre-association phase, setup of FE with master CE and backup CE
2. FE connecting and associating with master CE.
3. When CEFailoverPolicy is set to 2 or 3, the FE will connect and associate with backup CE.
4. Once the master CE is considered disconnected then the FE chooses the first Associated backup CE.
5. It sends an Event Notification specifying that the master CE is down and who is now the master CE.
6. The new master CE sends a SET Configuration message to the FE setting the CEID value to who is now the new master CE completing the switch.

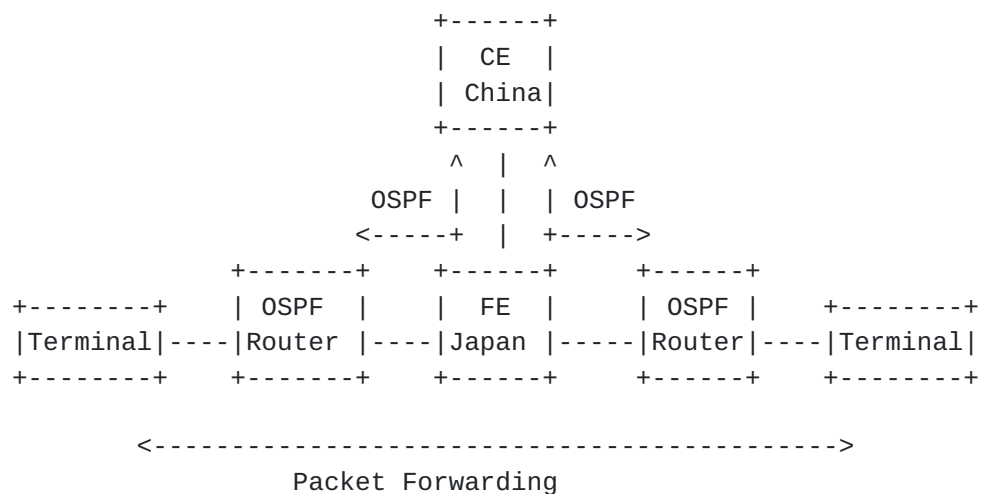


#### 4.4. Scenario 4 - Packet forwarding

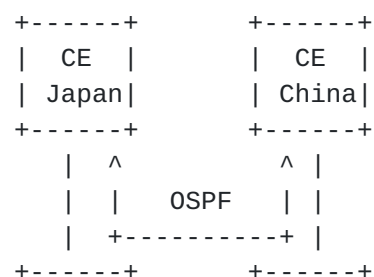
##### 4.4.1. Connection Diagram



(a)



(b)





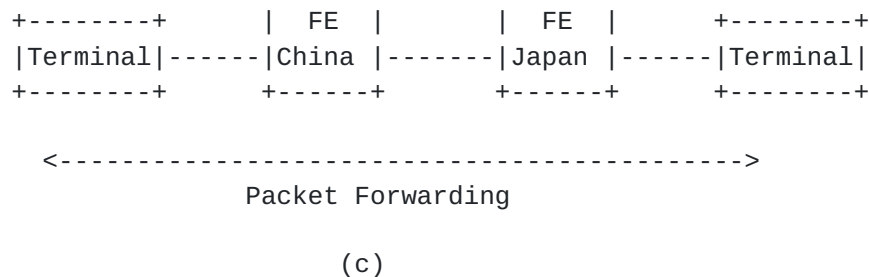


Figure 7: Scenario for IP Packet forwarding

#### 4.4.2. Design Considerations

This Scenario is used to verify some LFBs such as RedirectIn, RedirectOut, IPv4NextHop, IPv4UcastLPM defined by ForCES LFB library[I-D.ietf-forces-lfb-lib]. Cases of (a) and (b) in Figure 7 both need a RedirectIn LFB to send CE generated OSPF packets to FE by packet redirect messages. The OSPF packets are further sent to an outside OSPF Router by the FE via forwarding LFBs like IPv4NextHop, IPv4UcastLPM. A RedirectOut LFB in the FE sends OSPF packets received from the outside OSPF Router to CE by packet redirect messages also. In this process, meta-data that are included in packet redirect messages as defined by ForCES LFB library document should be coded and decoded by either CE or FE.

If above test process can be done, then this whole NE including FE and CE actually work like an OSPF router which exchanges OSPF protocol information with other OSPF routers. By running OSPF protocol, the CE can generate new routes and be loaded to FE. In the process, IPv4NextHop and Ipv4UcastLPM LFBs must be working to support operations.

By sending packet to the destination through the FE, FE should forward packet according to the route generated by OSPF. so, the data path in FE can be tested and LFBs such as EtherPHYCop, EtherMacIn, IPv4Classifier, IPv4Validator, EtherEncasulator, EtherMacOut also be verified.

#### 4.4.3. Testing Process

First, Boot terminals and routers, and set IP addresses of their interfaces.

Second, Boot CE and FE.

Third, Establish association between CE and FE, and set IP addresses of FE\_\_s interfaces.



Fifth, Start OSPF among CE and routers, and set FIB on FE.

Sixth, Send packets between terminals.



## 5. Test Results

### 5.1. LFB Operation Test

For the convinience sake, as mentioned earlier, abbreviations of 'C' means implementation from China, 'J' Japan implementaion, and 'G' Greece implemenation. Testing results of this scenario are listed in the following figure.

Test #	CE	FE(s)	Oper	LFB	Component/ Capability	Result	Comment
1	C	J				Success	As for the
	J	C				Success	format of
	C	G				Success	encapsulation
	G	C	GET	FEObject	LFBTopology	Success	on array,
	J	G				Success	only the case
	G	J				Success	of FULLDATA-
							-in-FULLDATA
2	C	J				Success	is supported
	J	C				Success	for everyone.
	C	G				Success	However more
	G	C	GET	FEObject	LFBSelector	Success	types such as
	J	G			s	Success	SPARSEDATA
	G	J				Success	should be
							supported
3	C	J				Success	in the
	J	C				Success	future.
	C	G				Success	
	G	C	GET	EtherPHYCop	PHYPortID	Success	
	J	G				Success	
	G	J				Success	
4	C	J				Success	
	J	C				Success	
	C	G				Success	
	G	C	GET	EtherPHYCop	AdminStatus	Success	
	J	G				Success	
	G	J				Success	
5	C	J				Success	
	J	C				Success	
	C	G				Success	
	G	C	GET	EtherPHYCop	OperStatus	Success	
	J	G				Success	
	G	J				Success	As for the
							format of



6	C	J				Success	PATH-DATA,
	J	C				Success	J use the
	C	G				Success	case of
	G	C	GET	EtherPHYCop	AdminLink	Success	PATH-DATA in
	J	G			Speed	Success	PATH-DATA,C
	G	J				Success	uses
							only one
7	C	J				Success	PATH-DATA with
	J	C				Success	mutiple IDs.
	C	G				Success	G uses ...
	G	C	GET	EtherPHYCop	OperLink	Success	
	J	G			Speed	Success	
	G	J				Success	
8	C	J				Success	
	J	C				Success	
	C	G				Success	
	G	C	GET	EtherPHYCop	AdminDuplex	Success	
	J	G			Speed	Success	
	G	J				Success	
							The side of
9	C	J				Success	C thinks that
	J	C				Success	CE SHOULD get
	C	G				Success	LFB instance
	G	C	GET	EtherPHYCop	OperDuplex	Success	data
	J	G			Speed	Success	according to
	G	J				Success	LFBSelectors.
10	C	J				Success	
	J	C				Success	
	C	G				Success	
	G	C	GET	EtherPHYCop	Carrier	Success	
	J	G			Status	Success	
	G	J				Success	
11	C	J				Success	
	J	C				Success	
	C	G				Success	
	G	C	GET	EtherMACIn	AdminStatus	Success	
	J	G				Success	
	G	J				Success	
12	C	J				Success	
	J	C				Success	
	C	G				Success	
	G	C	GET	EtherMACIn	LocalMac	Success	
	J	G			Addresses	Success	
	G	J				Success	



13	C	J					Success	
	J	C					Success	
	C	G					Success	
	G	C	GET	EtherMACIn	L2Bridging	Success		
	J	G			PathEnable	Success		
	G	J				Success		
14	C	J					Success	
	J	C					Success	
	C	G					Success	
	G	C	GET	EtherMACIn	Promiscuous	Success		
	J	G			Mode	Success		
	G	J				Success		
15	C	J					Success	
	J	C					Success	
	C	G					Success	
	G	C	GET	EtherMACIn	TxFlow	Success		
	J	G			Control	Success		
	G	J				Success		
16	C	J					Success	
	J	C					Success	
	C	G					Success	
	G	C	GET	EtherMACIn	RxFlow	Success		
	J	G			Control	Success		
	G	J				Success		
17	C	J					Success	
	J	C					Success	
	C	G					Success	
	G	C	GET	EtherMACIn	MACInStats	Success		
	J	G				Success		
	G	J				Success		
18	C	J					Success	
	J	C					Success	
	C	G					Success	
	G	C	GET	EtherMACOut	AdminStatus	Success		
	J	G				Success		
	G	J				Success		
19	C	J					Success	
	J	C					Success	
	C	G					Success	
	G	C	GET	EtherMACOut	MTU	Success		
	J	G				Success		



	G	J				Success	
20	C	J				Success	
	J	C				Success	
	C	G				Success	
	G	C	GET	EtherMACOut	TxFlow Control	Success	
	J	G				Success	
	G	J				Success	
21	C	J				Success	
	J	C				Success	
	C	G				Success	
	G	C	GET	EtherMACOut	TxFlow Control	Success	
	J	G				Success	
	G	J				Success	
22	C	J				Success	
	J	C				Success	
	C	G				Success	
	G	C	GET	EtherMACOut	MACOutStats	Success	
	J	G				Success	
	G	J				Success	
23	C	J				Success	
	J	C				Success	
	C	G				Success	
	G	C	GET	ARP	PortV4Addr InfoTable	Success	
	J	G				Success	
	G	J				Success	
24	C	J				Success	
	J	C				Success	
	C	G				Success	
	G	C	SET	ARP	PortV4Addr InfoTable	Success	
	J	G				Success	
	G	J				Success	
25	C	J				Success	C's misunder-
	J	C				Success	standing of
	C	G				Success	the PATHDATA
	G	C	DEL	ARP	PortV4Addr InfoTable	Success	in DEL
	J	G				Success	Operation.
	G	J				Success	Later C fixed
							the problem
26	C	J				Success	and make it
	J	C				Success	successful
	C	G				Success	in testing
	G	C	SET	EtherMACIn	LocalMAC	Success	with J.





	J	G			Addresses	Success	
	G	J				Success	
27	C	J				Success	
	J	C				Success	
	C	G				Success	
	G	C	SET	EtherMACIn	MTU	Success	
	J	G				Success	
	G	J				Success	
28	C	J				Success	By setting
	J	C				Success	new reachable
	C	G				Success	network, route
	G	C	SET	IPv4NextHop	IPv4NextHop	Success	entry can be
	J	G			Table	Success	added into
	G	J				Success	system.
29	C	J				Success	
	J	C				Success	
	C	G				Success	
	G	C	SET	IPv4Ucast	IPv4Prefix	Success	
	J	G		LPM	Table	Success	
	G	J				Success	
30	C	J				Success	
	J	C				Success	Corresponding
	C	G				Success	nexthop entry
	G	C	DEL	IPv4NextHop	IPv4NextHop	Success	MUST delete
	J	G			Table	Success	before prefix
	G	J				Success	entry.
31	C	J				Success	
	J	C				Success	
	C	G				Success	
	G	C	DEL	IPv4Ucast	IPv4Prefix	Success	
	J	G		LPM	Table	Success	
	G	J				Success	
32	C	J				Success	
	J	C				Success	
	C	G				Success	
	G	C	SET	EtherPHYCop	AdminStatus	Success	
	J	G				Success	
	G	J				Success	
33	C	J				Success	
	J	C				Success	
	C	G				Success	



	G	C	SET	Ether	VlanInput	Success
	J	G		Classifier	Table	Success
	G	J				Success
34	C	J				Success
	J	C				Success
	C	G				Success
	G	C	DEL	Ether	VlanInput	Success
	J	G		Classifier	Table	Success
	G	J				Success
35	C	J				Success
	J	C				Success
	C	G				Success
	G	C	SET	Ether	VlanOutput	Success
	J	G		Encapsulato	Table	Success
	G	J		r		Success
36	C	J				Success
	J	C				Success
	C	G				Success
	G	C	DEL	Ether	VlanOutput	Success
	J	G		Encapsulato	Table	Success
	G	J		r		Success
+-----+-----+-----+-----+-----+-----+-----+						

## 5.2. TML with IPSec Test

In this scenario, ForCES TML will run over IPSec channel. All the implementors who joined this interoperability test use the same third-party tool software 'racoon' to establish IPSec channel. To be mentioned is that we have not repeat all the operations listed in Scenario 1, only some typical operations have been done.

Although some problems still remains in the connection with Greece, the TML with IPSec test is considered as success. The goal was to verify whether the interaction between CE and FE can be done normally under such IPSec environment. Since Japan's and China's implementation worked it is assumed that Greece's would as well, as the problem was on the setup and configuration of the IPSec connection and not on the ForCES protocol perse.

During the test following results as shown in figure occurred.



Test #	CE	FE(s)	Oper	LFB	Component/ Capability	Result	Comment
1	C	J				Success	For unkown
	J	C				Success	error in
	C	G				Failure	configuration
	G	C	GET	FEObject	LFBTopology	Failure	with racoon,
	J	G				Failure	Greece still
	G	J				Failure	need some
							time to fix
2	C	J				Success	the issue.
	J	C				Success	So, this
	C	G				Failure	scenario only
	G	C	GET	FEObject	LFBSelector	Failure	took place
	J	G			s	Failure	between C and
	G	J				Failure	J.
3	C	J				Success	
	J	C				Success	
	C	G				Failure	
	G	C	SET	Ether	VlanInput	Failure	
	J	G		Classifier	Table	Failure	
	G	J				Failure	
4	C	J				Success	
	J	C				Success	
	C	G				Failure	
	G	C	DEL	Ether	VlanInput	Failure	
	J	G		Classifier	Table	Failure	
	G	J				Failure	

### 5.3. CE High Availability Test

In this scenario one FE will connect and associate with a master CE and a backup CE. When the master CE is considered disconnected the FE would attempt to find another associated CE to become the master CE.

The CEHA scenario as is described in Scenario 3 was completed successfully for both setups.

Due to a bug in the FE, a possible issue was caught. The bug in the FE introduced a delay in message handling of 1 second. The master CE was sending Heartbeats at a rate of one in 500milliseconds (2 per second). As heartbeats are of very low priority, the FE was working fine with associated only with the master CE. However when the FE



attempted to associate with the backup CE the following issue occurred.

The FE was checking first for messages from all priorities from the master CE and if the master CE hasn't sent any messages then it would check the backup CE. So, when the FE was ordered to begin associating with the backup CE, it sent the Association setup message, the backup CE received it, responded back with an Association Setup result, but the FE never processed managed to process it.

While the bug was fixed and the CEHA scenario was completed successfully, the issue still remains. This is actually an implementation issue of how the FE prioritizes incoming messages from multiple CEs. The recommended approach is the following:

- o The FE SHOULD receive and handle messages first from the master CE on all priority channels to maintain proper functionality and then receive and handle messages from the backup CEs.
- o Only when the FE is attempting to associate with the backup CEs, then the FE SHOULD receive and handle messages per priority channel from all CEs. When all backup CEs are associated with or deemed unreachable, then the FE SHOULD return to receiving and handling messages first from the master CE.

#### **5.4. Packet Forwarding Test**

The Scenario of packet forwarding is the most complex one because it need the Scenario 1 must be completed. In this scenario testing, the pattern of J-CE C-FE was carried out. Smartbits's 2 testing ports connect to FE's 2 data-forwarding ports, meanwhile smartbits simulate ospf router and try to exchange the OSPF hello packet and LSA packet with CE, because CE also has an OSPF process in it so that the whole NE including FE and CE looks like an OSPF router.

In this scenario, RedirectIn, RedirectOut, IPv4NextHop, IPv4UcastLPM LFB should join the data path. First, it must be sure that IPv4NextHop and IPv4UcastLPM can work normally so that route entry can be added to FE. Second, RedirectIn and RedirectOut LFB MUST work, only that can FE redirect out OSPF hello and LSA packets to CE received from smartBits, FE redirect in OSPF hello and LSA packets to smartBits received from CE's OSPF process.

During the test, results as shown in the following figure are recorded.

+----+----+----+-----+-----+-----+-----+-----+





Test #	CE	FE(s)	Item	LFB	Result	Comment
1	J	C	IPv4NextHopTable SET	IPv4NextHop	Success	Multicast route is added by
2	J	C	IPv4PrefixTable SET	IPv4Ucast LPM	Success	manual, this problem still need to be fixed in the
3	J	C	Redirect ospf packet from CE to SmartBits	RedirectIn	Success	future.
4	J	C	Redirect ospf packet from SmartBits to CE	RedirectOut	Success	As for redirect message, ospf hello packet in 2- direction can
5	J	C	Metadata in redirect message	RedirectOut RedirectIn	Success	be watched by wireshark. however ospf packet
6	J	C	OSPF neighborhood discovery	RedirectOut RedirectIn	Success	received from CE have an error with checksum, so
7	J	C	OSPF DD exchange	RedirectIn IPv4NextHop IPv4Ucast LPM	Success	smartBits will drop it with no neighborhood discovered.
8	J	C	OSPF LSA exchange	RedirectOut RedirectIn IPv4NextHop IPv4Ucast LPM	Success	
9	J	C	Data Forwarding	RedirectOut RedirectIn IPv4NextHop IPv4Ucast LPM	Success	
10	C	J	IPv4NextHopTable SET	IPv4NextHop	Success	
11	C	J	IPv4PrefixTable SET	IPv4Ucast LPM	Success	



12	C	J	Redirect ospf packet from CE to other OSPF router	RedirectIn	Success	
12	C	J	Redirect ospf packet from other OSPF router to CE	RedirectOut	Success	
13	C	J	Metadata in redirect message	RedirectOut RedirectIn	Success	
14	C	J	OSPF neiborhood discovery	RedirectOut RedirectIn	Success	
15	C	J	OSPF DD exchange	RedirectOut RedirectIn IPv4NextHop IPv4Ucast LPM	Failure	FE connected by 2 OSPF router, only 1 OSPF can be discovered by CE, so DD exchanging stopped.
16	C	J	OSPF LSA exchange	RedirectOut RedirectIn IPv4NextHop IPv4Ucast LPM	Failure	
17	J	C	Data Forwarding	RedirectOut RedirectIn IPv4NextHop IPv4Ucast LPM	TBD	



## 6. Discussions

### 6.1. On Data Encapsulation Format

In the first day of the test, it was found that the LFB inter-operations about tables all failed. The reason is found to be the different ForCES protocol data encapsulation method among different implementations. The encapsulation issues are detailed as below:

Assuming that an LFB has two components, one a struct with ID 1 and an array with ID 2 with two components of u32 both per row.

```
struct1: type struct, ID=1
  components are:
  a, type u32, ID=1
  b, type u32, ID=2
```

```
table1: type array, ID=2
  components for each row are (a struct of):
  x, type u32, ID=1
  y, type u32, ID=2
```

#### 1. On response of PATH-DATA format

When a CE sends a config/query ForCES protocol message to an FE from a different implementor, the CE probably receives response from the FE with different PATH-DATA encapsulation format. For example, if a CE sends a query message with a path of 1 to a third party FE to manipulate struct 1 as defined above, the FE is probable to generate response with two different PATH-DATA encapsulation format: one is the value with FULL/SPARSE-DATA and the other is the value with many parallel PATH-DATA TLV and nested PATH-DATA TLV, as below:

format 1:

```
  OPER = GET-RESPONSE-TLV
  PATH-DATA-TLV:
    IDs=1
    FULLDATA-TLV containing valueof(a),valueof(b)
```

format 2:

```
  OPER = GET-RESPONSS-TLV
  PATH-DATA-TLV:
    IDs=1
    PATH-DATA-TLV:
      IDs=1
      FULLDATA-TLV containing valueof(a)
    PATH-DATA-TLV:
      IDs=2
      FULLDATA-TLV containing valueof(b)
```



The interoperability test shows that an ForCES element (CE or FE) sender is free to choose whatever data structure that IETF ForCES documents define and best suits the element, while an 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. While in the case an ForCES element is free to choose any legitimate data structure as a response, it is preferred the ForCES element responds in the same format that the request was made, as it is most probably the data structure is the request sender looks forward to receive.

## 2. On operation to array

An array operation may also have several different data encapsulation formats. For instance, if a CE sends a config message to table 1 with a path of (2.1), which refers to component with ID=2, which is an array, and the second ID is the row, so row 1, it may be encapsulated with three formats as below:

format 1:

```
OPER = SET-TLV
  PATH-DATA-TLV:
    IDs=2.1
    FULLDATA-TLV containing valueof(x),valueof(y)
```

format 2:

```
OPER = SET-TLV
  PATH-DATA-TLV:
    IDs=2.1
    PATH-DATA-TLV:
      IDs=1
      FULLDATA-TLV containing valueof(x)
    PATH-DATA-TLV
      IDs=2
      FULLDATA-TLV containing valueof(y)
```

Moreover, if CE is targeting the whole array, for example if the array is empty and CE wants to add the first row to the table, it could also adopt another format:

format 3:

```
OPER = SET-TLV
  PATH-DATA-TLV:
    IDs=2
    FULLDATA-TLV containing rowindex=1,valueof(x),valueof(y)
```

The interoperability test experience shows that format 1 and format 3, which take full advantage of multiple data elements description in





one TLV of FULLDATA-TLV, get more efficiency, although format 2 can also get the same operating goal.

## **7. Contributors**

Contributors who have made major contributions to the interoperability test are as below:

Hirofumi Yamazaki  
NTT Corporation  
Tokyo  
Japan  
Email: yamazaki.horofumi@lab.ntt.co.jp

Rong Jin  
Zhejiang Gongshang University  
Hangzhou  
P.R.China  
Email: jinrong@zjgsu.edu.cn

Yuta Watanabe  
NTT Corporation  
Tokyo  
Japan  
Email: yuta.watanabe@ntt-at.co.jp

Xiaochun Wu  
Zhejiang Gongshang University  
Hangzhou  
P.R.China  
Email: spring-403@zjgsu.edu.cn



## **8. Acknowledgements**

The authors would also like thank the following test participants:

Chuanhuang Li, Hangzhou BAUD Networks  
Ligang Dong, Zhejiang Gongshang University  
Jingjing Zhou, Zhejiang Gongshang University  
Liaoyuan Ke, Hangzhou BAUD Networks  
Kelei Jin, Hangzhou BAUD Networks

## **9. IANA Considerations**

This memo includes no request to IANA.

## **10. Security Considerations**

TBD

## **11. References**

### **11.1. Normative References**

- [I-D.ietf-forces-ceha]  
Ogawa, K., Wang, W., Haleplidis, E., and J. Salim, "ForCES Intra-NE High Availability", [draft-ietf-forces-ceha-01](#) (work in progress), February 2011.
- [I-D.ietf-forces-lfb-lib]  
Wang, W., Haleplidis, E., Ogawa, K., Li, C., and J. Halpern, "ForCES Logical Function Block (LFB) Library", [draft-ietf-forces-lfb-lib-03](#) (work in progress), December 2010.
- [RFC3654] Khosravi, H. and T. Anderson, "Requirements for Separation of IP Control and Forwarding", [RFC 3654](#), November 2003.
- [RFC3746] Yang, L., Dantu, R., Anderson, T., and R. Gopal, "Forwarding and Control Element Separation (ForCES) Framework", [RFC 3746](#), April 2004.
- [RFC5810] Doria, A., Hadi Salim, J., Haas, R., Khosravi, H., Wang, W., Dong, L., Gopal, R., and J. Halpern, "Forwarding and Control Element Separation (ForCES) Protocol Specification", [RFC 5810](#), March 2010.
- [RFC5811] Hadi Salim, J. and K. Ogawa, "SCTP-Based Transport Mapping Layer (TML) for the Forwarding and Control Element Separation (ForCES) Protocol", [RFC 5811](#), March 2010.
- [RFC5812] Halpern, J. and J. Hadi Salim, "Forwarding and Control Element Separation (ForCES) Forwarding Element Model", [RFC 5812](#), March 2010.
- [RFC5813] Haas, R., "Forwarding and Control Element Separation (ForCES) MIB", [RFC 5813](#), March 2010.
- [RFC6053] Haleplidis, E., Ogawa, K., Wang, W., and J. Hadi Salim, "Implementation Report for Forwarding and Control Element Separation (ForCES)", [RFC 6053](#), November 2010.

### **11.2. Informative References**

- [RFC2629] Rose, M., "Writing I-Ds and RFCs using XML", [RFC 2629](#), June 1999.





Authors' Addresses

Weiming Wang  
Zhejiang Gongshang University  
18 Xuezheng Str., Xiasha University Town  
Hangzhou, 310018  
P.R.China

Phone: +86-571-28877721  
Email: wmwang@zjgsu.edu.cn

Kentaro Ogawa  
NTT Corporation  
Tokyo,  
Japan

Email: ogawa.kentaro@lab.ntt.co.jp

Evangelos Haleplidis  
University of Patras  
Patras,  
Greece

Email: ehalep@ece.upatras.gr

Ming Gao  
Hangzhou BAUD Networks  
408 Wen-San Road  
Hangzhou, 310012  
P.R.China

Phone: +86-571-28877751  
Email: gmyyqno1@pop.zjgsu.edu.cn

Jamal Hadi Salim  
Mojatatu Networks  
Ottawa  
Canada

Email: hadi@mojatatu.com

