Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: September 8, 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 7, 2011

Interoperability Report for Forwarding and Control Element Separation (ForCES) draft-ietf-forces-interop-00

Abstract

This document captures test results from the second Forwarding and control Element Separation (ForCES) interop testing which took place 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 8, 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

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 [ ] and ForCES CE HA specification[]. 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 of RFC3654, RFC3746, RFC5810,RFC5811,RFC5812,RFC5812. The 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 reffered to as "China" in the document for the sake of brevity.
* NTT Corporation, Japan. This implementation is referred to as "Japan" in the document for the sake of brevity.
* The University of Patras, Greece. This implementation is referred to as "Greece" 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). 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 the following figure.

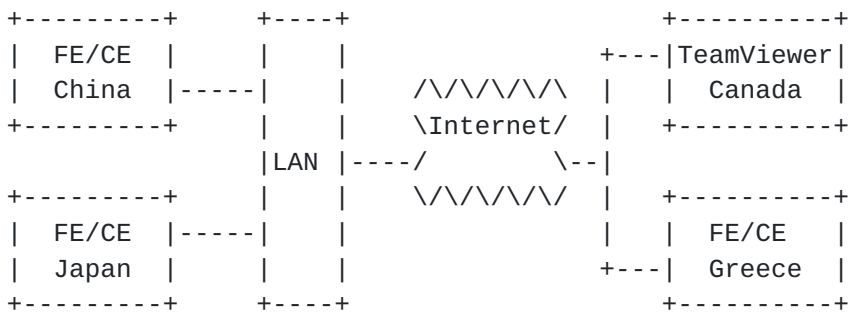

Figure 1: The Approach for all Participants

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

Hardware/Software (CEs and FEs) of China and Japan that were located within the ITL Lab of Zhejiang Gongshang University, were connected together using ethernet switches.The detailed configuration can be seen in the following figure.

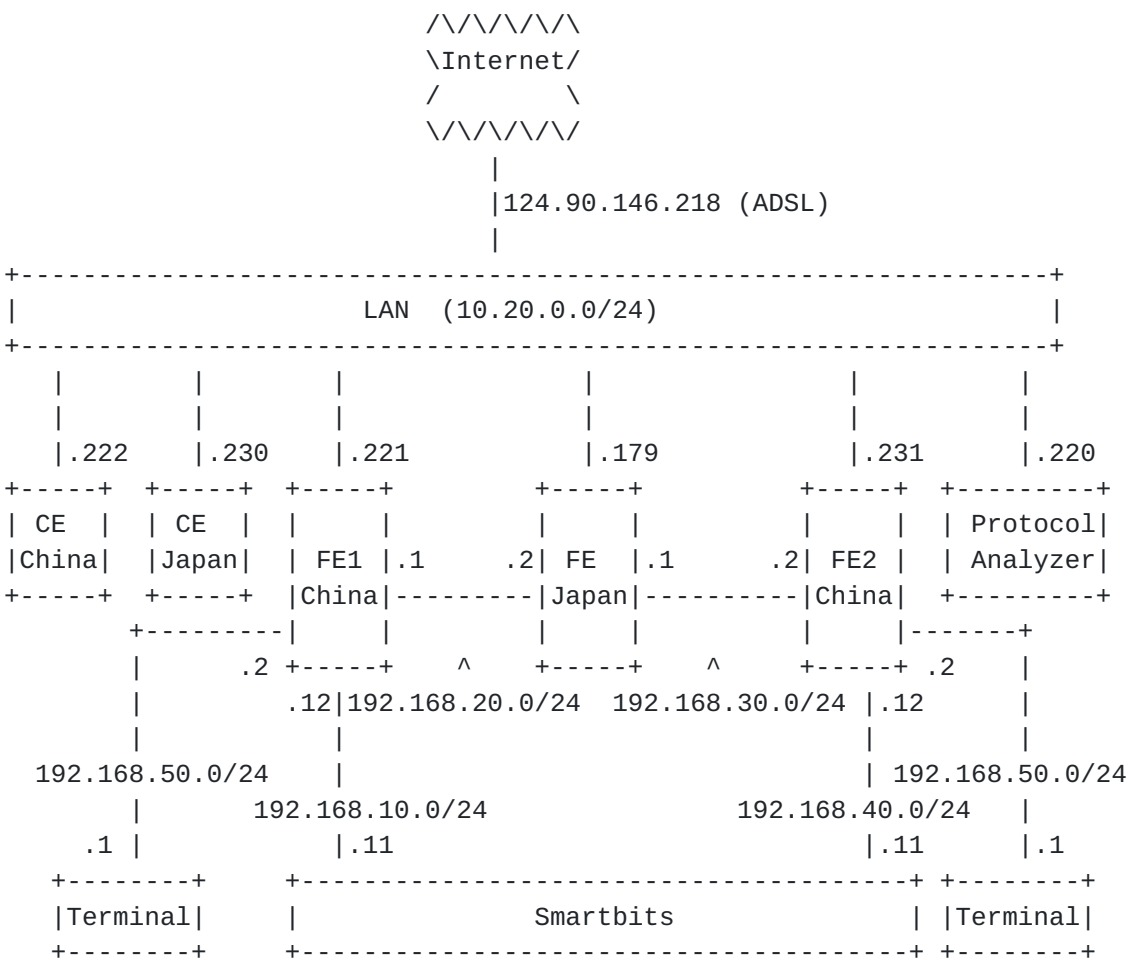

Figure 2: Testbed Configuration Located in ITL Lab,China

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 the following figure.

Such configuation can satisfy all scenarios that are mentioned in this document. Specially for the scenario of CE High Availability,in which CE of Greece will be the backup one.

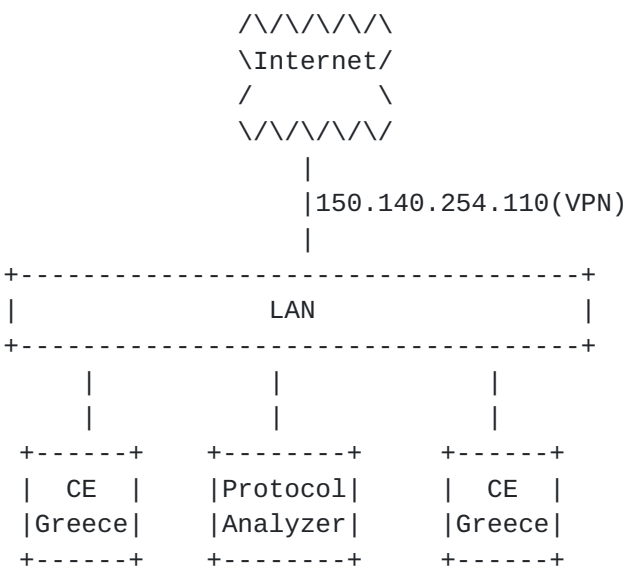

Figure 3: Testbed Configuration Located in the University of Patras,Greece

4. Scenarios

4.1. Scenario 1 - LFB Operation

4.1.1. Connection Diagram

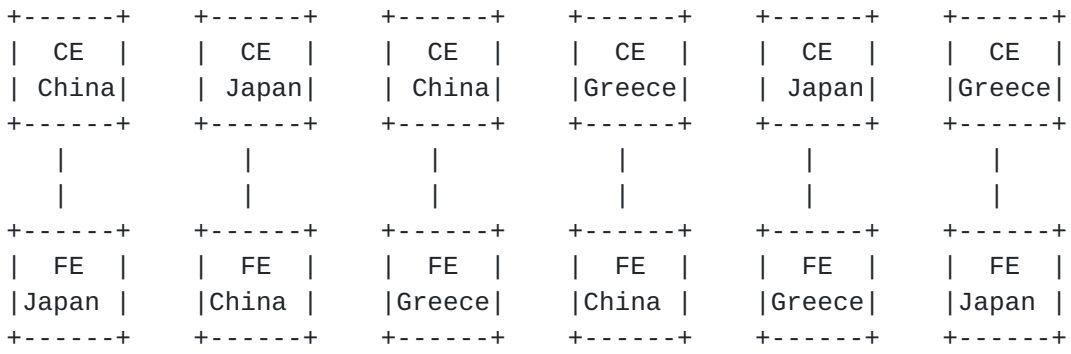

Figure 4: Scenario for LFB Operation

4.1.2. Design Considerations

First, 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 implemeting 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 th most is the format of encasulation for PATHDATA with nested PATHDATA 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 Lib[ ]. A succeeded operation in this scenario means all the meeting joining implementor follow the instruction given by the ForCES LFB Lib.

4.1.3. Testing Proccess

In order to make interoperability more credible,these three implementors carry out the test alternately. As shown in figure 4, every side's CE or FE must connect with the other two sides's FE or CE. So that, we shall have 6 cases in this Scenario.

4.2. Scenario 2 - TML with IPSec

4.2.1. Connection Diagram

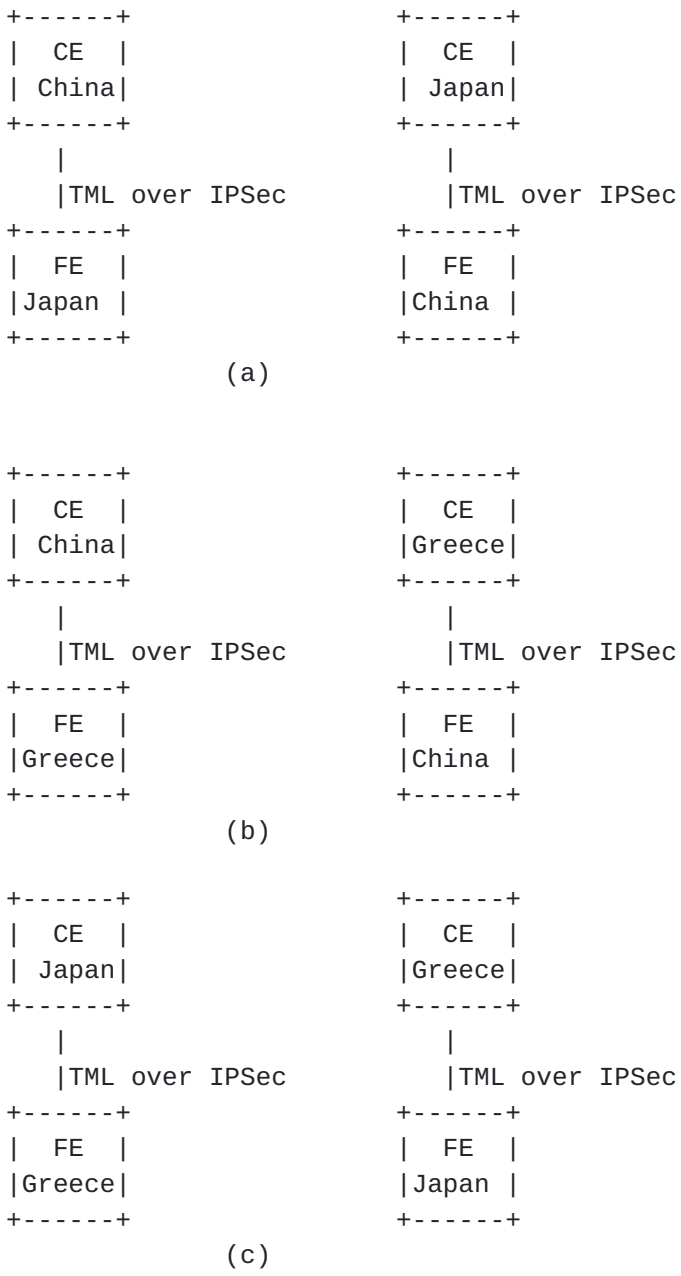

Figure 5: Scenario for LFB Operation with TML over IPSec

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 design the scenario to make TML to run over the IPSec channel that is pre-established. In this scenario all operations for Scenario 1 will be repeated. In this way, we try to verify whether

the interaction between CE and FE can be done normally under such IPSec enviroment.

4.2.3. Testing Proccess

In this scenario, ForCES TML will run over IPSec channel. All the implementors who joined in this interoperability testing use 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:

- Internet Key Exchange (IKE) with certificates for endpoint authentication.
- 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

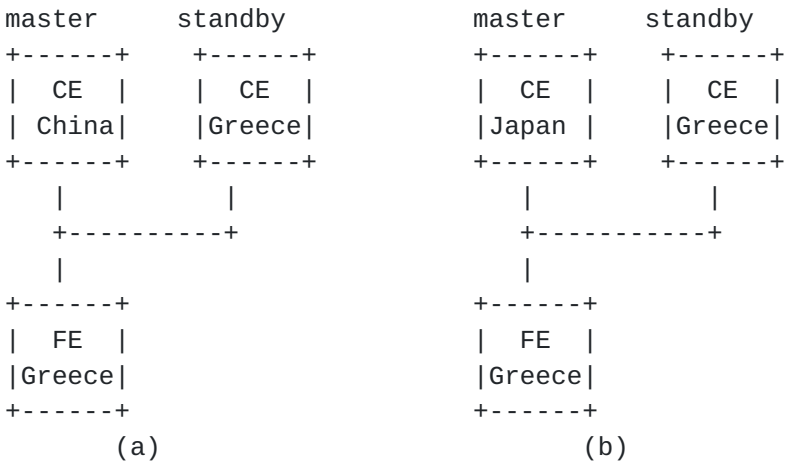

Figure 6: Scenario for CE High Availability

4.3.2. Design Considerations

CE High Availability was also tested in this interoperability test based on the the CEHA draft [draft-ietf-forces-ceha-01].

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.

4.3.3. Testing Proccess

In this scenario one FE would be connected with two CEs. In pre-association setup, the FE would be configured to have CE1 as master CE and CE2 as standby CE and CEFailoverPolicy to High Availability (2 or 3). The FE once associated with the master CE it would then attempt to connect and associate with the standby CE.

When 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.

4.4. Scenario 4 - Packet forwarding

4.4.1. Connection Diagram

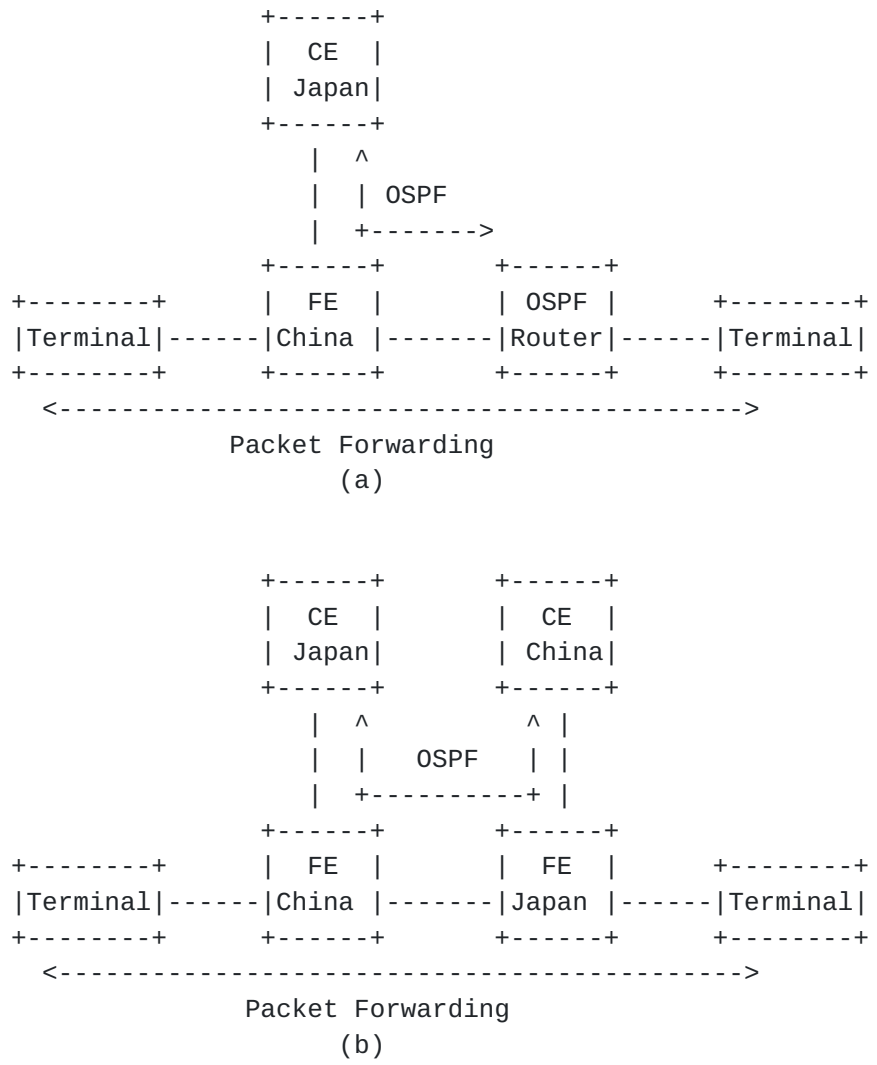

Figure 7: Scenario for IP Packet forwarding

4.4.2. Design Considerations

This Scenario can be used to verify some LFBs such as RedirectIn, RedirectOut, IPv4NextHop, IPv4UcastLPM.Cases of (a) and (b) in Figure 7 both need RedirectIn LFB send CE's OSPF packet to FE futher to the outside OSPF Router as Packet Redirect Message, RedirectOut LFB send OSPF packet received from the outside OSPF Router to CE as well as Packet Redirect Message.In such procedure, META DATA that included in Packet Redirect Message should be coded and decoded for both CE and FE.

If the above can be done with no issue, then the whole NE including FE and CE will work like an OSPF router exchanging OSPF protocol

information with other OSPF router. As for CE, after finishing OSPF exchanging, some routes maybe generated by OSPF and need to be added to FE. So, IPv4NextHop and Ipv4UcastLPM must be working to support such operation.

By sending packet to the destination through the FE, FE should forward packet according to the route generate 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 Proccess

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 of stating,abbreviation is used here.So 'C' means China ,'J' - Japan,'G'Greece and all testing results of this scenario are listed in the following figure as well.(Note: other Scenarios will follow the definition)

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

6	C	J				Success	PATHDATA,	
	J	C				Success	J use the	
	C	G				TBD	case of	
	G	C	GET	EtherPHYCop	AdminLink	Success	PATHDATA in	
	J	G			Speed	Success	PATHDATA,C	
	G	J				Success	uses	
							only one	
7	C	J				Success	PATHDATA with	
	J	C				Success	mutiple IDs.	
	C	G				TBD	G uses ...	
	G	C	GET	EtherPHYCop	OperLink	Success		
	J	G			Speed	Success		
	G	J				Success		
8	C	J				Success		
	J	C				Success		
	C	G				TBD		
	G	C	GET	EtherPHYCop	AdminDuplex	Success		
	J	G			Speed	Success		
	G	J				Success		
							The side of	
9	C	J				Success	C think that	
	J	C				Success	CE SHOULD get	
	C	G				TBD	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				TBD		
	G	C	GET	EtherPHYCop	Carrier	Success		
	J	G			Status	Success		
	G	J				Success		
11	C	J				Success		
	J	C				Success		
	C	G				TBD		
	G	C	GET	EtherMACIn	AdminStatus	Success		
	J	G				Success		
	G	J				Success		
12	C	J				Success		
	J	C				Success		
	C	G				TBD		
	G	C	GET	EtherMACIn	LocalMac	Success		
	J	G			Addresses	Success		
	G	J				Success		

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

	G	J					Success		
20	C	J					Success		
	J	C					Success		
	C	G					TBD		
	G	C	GET	EtherMACOut		TxFlow	Success		
	J	G				Control	Success		
	G	J					Success		
21	C	J					Success		
	J	C					Success		
	C	G					TBD		
	G	C	GET	EtherMACOut		TxFlow	Success		
	J	G				Control	Success		
	G	J					Success		
22	C	J					Success		
	J	C					Success		
	C	G					TBD		
	G	C	GET	EtherMACOut		MACOutStats	Success		
	J	G					Success		
	G	J					Success		
23	C	J					Success		
	J	C					Success		
	C	G					TBD		
	G	C	GET	ARP		PortV4Addr	Success		
	J	G				InfoTable	Success		
	G	J					Success		
24	C	J					Success		
	J	C					Success		
	C	G					TBD		
	G	C	SET	ARP		PortV4Addr	TBD		
	J	G				InfoTable	Success		
	G	J					Success		
25	C	J					Success	C's misunder-	
	J	C					Success	standing of	
	C	G					TBD	the PATHDATA	
	G	C	DEL	ARP		PortV4Addr	Failure	in DEL	
	J	G				InfoTable	Success	Operation.	
	G	J					Success	Later C fixed	
								the problem	
26	C	J					Success	and make it	
	J	C					Success	successful	
	C	G					TBD	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				TBD		
	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				TBD	network,Route	
	G	C	SET	IPv4NextHop	IPv4NextHop	TBD	entry can be	
	J	G			Table	Success	add into	
	G	J				Success	system.	
29	C	J				Success		
	J	C				Success		
	C	G				TBD		
	G	C	SET	IPv4Ucast	IPv4Prefix	TBD		
	J	G		LPM	Table	Success		
	G	J				Success		
30	C	J				Success		
	J	C				Success	Corresponding	
	C	G				TBD	nexthop entry	
	G	C	DEL	IPv4NextHop	IPv4NextHop	TBD	MUST delete	
	J	G			Table	Success	before prefix	
	G	J				Success	entry.	
31	C	J				Success		
	J	C				Success		
	C	G				TBD		
	G	C	DEL	IPv4Ucast	IPv4Prefix	TBD		
	J	G		LPM	Table	Success		
	G	J				Success		
32	C	J				Success		
	J	C				Success		
	C	G				TBD		
	G	C	SET	EtherPHYCop	AdminStatus	Success		
	J	G				Success		
	G	J				Success		
33	C	J				Success		
	J	C				Success		
	C	G				TBD		

	G	C	SET	Ether	VlanInput	Success		
	J	G		Classifier	Table	Success		
	G	J				Success		
34	C	J				Success		
	J	C				Success		
	C	G				TBD		
	G	C	DEL	Ether	VlanInput	Failure		
	J	G		Classifier	Table	Success		
	G	J				Success		
35	C	J				Success		
	J	C				Success		
	C	G				TBD		
	G	C	SET	Ether	VlanOutput	Success		
	J	G		Encapsulato	Table	Success		
	G	J		r		Success		
36	C	J				Success		
	J	C				Success		
	C	G				TBD		
	G	C	DEL	Ether	VlanOutput	Failure		
	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. During the test following results as shown in figure occured.

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

5.3. CE High Availability Test

In this scenario one FE would be connected with two CEs. In pre-association setup, the FE would be configured to have CE1 as master CE and CE2 as standby CE and CEFailoverPolicy to High Availability (2 or 3). The FE once associated with the master CE it would then attempt to connect and associate with the standby CE.

When 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.

5.4. Packet Forwarding Test

The Scenario of packet forwading 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 sured 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	Muticast route is added by manual,this problem still need to be fixed in the future.
2	J	C	IPv4PrefixTable SET	IPv4Ucast LPM	success	
3	J	C	Redirect ospf packet from CE to SmartBits	RedirectIn	failure	
4	J	C	Redirect ospf packet from SmartBits to CE	RedirectOut	success	As for redirect message, ospf hello packet in 2 direction can be wathed by wireshark. however ospf packet received from CE have an error with checksum,so smartBits will drop it with no neighborhood discovered.
5	J	C	Metadata in redirect message	RedirectOut RedirectIn	success	
6	J	C	OSPF neiborhood discovery	RedirectOut RedirectIn	failure	
6	J	C	OSPF LSA exchange	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:

1. On response of PATH-DATA format When a CE sends a config/query ForCES protocol message to an FE with a different implementor, the CE is probable to receive response from the FE with different PATH-DATA encaplation format. For example, if a CE sends a query message with a path (1.1.1) to a third party FE, the FE is probable to generate response with two different PATH-DATA encaplation format: the value with FULL/SPARSE-DATA, and the format of many parallel PATHDATA TLV and nested PATHDATA TLV, as below:

```
format 1:
    GET-RESPONSE:
     PATH DATA (id:1.2)
         FULL DATA(a,b)

format 2:
    GET-RESPONSE:
     PATH DATA
         PATH DATA
            FULL DATA
         PATH DATA
            FULL DATA
   ......
```

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) MUST be prepared to accept and process information (requests and responses) that use any legitimate structure defined by IETF ForCES documents.

2. On operation to array

An array operation may also have several different data encaplation formats. For example, a component of array with two elements (a and b) in one entry, CE may encapsulate a SET message in two format:

```
format 1:
    SET:
      PATH DATA (id:1.2)
          FULL DATA(a,b)
format 2:
    SET:
    PATH DATA
      PATH DATA (id:1)
         FULL DATA (a)
      PATH DATA (id:2)
         FULL DATA (b)
```

Via the interoperability test experience, this document recommends that format 1 be used for all array data format encapsulations. It is purely because format 1 can achieve the best efficiency.

6.2. On ...

TBD

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 Unviersity
Liaoyuan Ke, Hangzhou BAUD Networks
Kelei Jin,Hangzhou BAUD Networks

9. IANA Considerations

(TBD)

10. Security Considerations

TBD

11. References

11.1. Normative References

[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