IPv6 READY Phase-2

Network Mobility (NEMO)

Interoperability Test Specification

Technical Document

Version 1.1.0

IPv6 Forum *http://www.ipv6forum.org*
IPv6 Ready Logo Committee *http://www.ipv6ready.org*

Modification Record

Version 1.1.0 May 16, 2008
- Major Revision Up
  Cover the RFC4877
  (add the "Fine-Grain Selectors" as Advenced Function)

Version 1.0.1 July 27, 2007

- Modify title, footer.
  Title:
  "IPv6 Ready Logo Phase 2" -> "IPv6 READY Phase-2"
  Title, footer:
  "Interoperability Test Scenario"
  -> "Interoperability Test Specification"
- Modify copyright.
- Editorial fix
  "Network Topology map" -> "Topology Map"
  "packet log" -> "Packet Capture File"

Version 1.0.0 January 22, 2007

- First Release

Acknowledgements

IPv6 Forum would like to acknowledge the efforts of the following organizations in the development of this test specification.

Principal Authors:

- IPv6 Promotion Council, Certification Working Group, Mobile IPv6 Sub Working Group

Commentators:

- TTA/IT Testing Laboratories

Introduction

The IPv6 forum plays a major role to bring together industrial parties to develop and deploy the next generation of IP protocols. Contrary to IPv4, which started with a small closed group of implementers, the universality of IPv6 leads to a huge number of implementations. Interoperability has always been considered a critical feature in the Internet community.
Due to the large number of IPv6 implementations, providing the market with a strong signal proving the level of interoperability across various products is important. To avoid confusion in the mind of customers, a unique global logo program needs to be defined. The IPv6 logo will give confidence to users that IPv6 is currently operational, which will also be a clear indication that the technology will still be used in the future. To summarize, this logo program will contribute to the feeling that IPv6 is available and ready to be used.

The IPv6 Logo Program consists of three phases:

Phase 1:
In the first stage, the Logo will indicate that the product includes IPv6 mandatory core protocols and can interoperate with other IPv6 implementations.

Phase 2:
The "IPv6 ready" step implies proper care, technical consensus, and clearly written technical references. The IPv6 Ready Logo will indicate that a product has successfully satisfied strong requirements stated by the IPv6 Logo Committee (v6LC).

To avoid confusion, the "IPv6 Ready" logo will be generic. The v6LC will define the test profiles with associated requirements for specific functionalities.

Phase 3:
Same as Phase 2 with IPsec mandated.

Table of Contents

[I] Interoperability Test Scenarios for Network Mobility

Modification Record..2

Acknowledgements...3

Introduction..4

Table of Contents..5

1. Overview..7

2. Interoperability test scenario for IPv6 Ready Logo Phase 2 program..............................9

2.1 Phase 2 certification and support function...9

2.2 Architecture of Interoperability test scenario 17

2.3 Interoperability test scenario for IPv6 Ready Logo Phase 2 program 19

2.4 Examples of "Interoperability test scenario for IPv6 Ready Logo Phase 2 program" 23

2.5 Test conditions of "Interoperability test scenario for IPv6 Ready Logo Phase 2 program"...23

2.6 Compatible conditions for acquisition of Phase 2 Logo..24

2.7 Submission for acquisition of Phase 2 Logo 30

2.7.1 Required data 30

2.7.2 Test Result Table..31

2.7.3 Data file name syntax 32

2.7.4 Data Archive..32

3. Test Procedure for Interoperability test scenario for IPv6 Ready Logo Phase 2............34

3.1. Test Settings 34

3.1.1 Topology 34

3.1.2 Initial test conditions 37

3.2. Test Procedure 38

3.2.1 Procedure..38

3.2.2 Procedure of verifying test scenario 47

3.3 Sequence of Interoperability Test Scenario 48

4. Configuration of various lifetimes and IPsec 50

4.1. Configurations of various lifetimes..50

4.2. IPsec configurations...50

4.3. Manual IPsec SA configurations 51

4.3.1. BU/BA [Transport Mode] for manual IPsec SA 52

4.3.2. MPS/MPA [Transport Mode] for manual IPsec SA 55

4.3.3. Payload [Tunnel Mode] for manual IPsec SA 57

4.4. Manual IPsec SA configurations with Fine-Grain Selectors 63

4.4.1. BU/BA [Transport Mode] for manual IPsec SA (Fine-Grain Selectors) 63

4.4.2. MPS/MPA [Transport Mode] for manual IPsec SA (Fine-Grain Selectors) 67

AUTHOR'S LIST 71

1. Overview

This document describes test scenarios to verify the interoperability between different implementations of Network Mobility, in the form of Home Agents (HAs) and Mobile Routers (MRs).

- Interoperability test scenario for IPv6 Ready Logo Phase 2 program

  "Interoperability test scenario for IPv6 Ready Logo Phase 2 program" includes all the test elements needed for acquisition of IPv6 Ready Phase 2 program Logo. In particular, the test scenario covers all the Priority A1 and the Priority A2 functions defined in "IPv6 Ready Logo Phase 2 Policy for NEMO" document. In this test scenario, each Advanced Function can be selectively tested according to the implementation situation of Priority A2.

  Details of Priority A2 and the selection of the corresponding test elements in the test scenario are described in Section 2.

In the following, Basic Functions are called "Priority A1" and Advanced Functions are called "Priority A2".

Acronyms

CN -	Correspondent Node
HA -	Home Agent
MR -	Mobile Router
VMN -	Visited Mobile Node
LFN -	Local Fixed Node
FL -	Foreign Link
HL -	Home Link
HoA -	Home Address
CoA -	Care-of Address
BCE -	Binding Cache Entry
BLE -	Binding Update List Entry
BU -	Binding Update
BA -	Binding Acknowledgement
DHAAD -	Dynamic Home Agent Address Discovery

HAAD -	Home Agent Address Discovery
MPS -	Mobile Prefix Solicitation
MPA -	Mobile Prefix Advertisement
MPD -	Mobile Prefix Discovery
De-Reg -	De-Registration
Re-Reg -	Re-Registration
HNP -	Home Network Prefix
HoA (from HNP) -	Home Address derived from Home Network Prefix.
HoA (from MNP) -	Home Address derived from Mobile Network Prefix.

Reference standards

This documentation covers functions specified in the IETF RFC and Network Mobility Test Profile listed below.

(1) RFC3963: Network Mobility (NEMO) Basic Support Protocol

(2) RFC3775: Mobility Support in IPv6

(3) RFC3776: Using IPsec to Protect Mobile IPv6 Signaling
Between Mobile Nodes and Home Agents

(4) RFC4877 Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture
(http://www.ietf.org/rfc/rfc4877.txt)

(5) Guidelines for Implementation (http://www.ipv6ready.org/about_phase2_test.html/)

(6) IPv6 Ready Logo Phase 2 Policy for NEMO
(http://www.ipv6ready.org/about_phase2_test.html)

2. Interoperability test scenario for IPv6 Ready Logo Phase 2 program

2.1 Phase 2 certification and support function

For equipment used in Network Mobility (HA, MR) to acquire a Phase 2 Logo based on "IPv6 Ready Logo Phase 2 Policy for NEMO", all Priority A1 functions must be supported from the viewpoint of interoperability. Furthermore, each Priority A2 may be selectively supported. In the case where equipment used in Network Mobility with Priority A2 is certificated, the support status of Priority A2 should be clarified and tested properly.

The List of the Priority A1 and the Priority A2 functions defined in "IPv6 Ready Logo Phase 2 Policy for NEMO" is shown in Table 2-1-2.

According to the support status of the Priority A2 functions shown in Table 2-1-2, the "Interoperability test scenario for IPv6 Ready Logo Phase 2 program" is to be configured as follows.

<1> Test elements for all Priority A1 functions are included.
<2> Test elements for the Priority A2 functions should be executed selectively according to the support status of the target equipment.

IPv6 READY Logo Phase 2 NEMO is currently based on NEMO Extended Home Network Model, in which additional prefixes are used, contiguous to the Home Link Prefix inherited from MIPv6. In addition, IPv6 READY Logo Phase 2 NEMO supports Home Address of Mobile Router derived from the prefix on the Home Link, as shown in Table 2-1-1. Home Address of Mobile Router derived from one of its Mobile Network Prefix is currently out of scope.

Table 2-1-1. The coverage of IPv6 READY Logo Phase 2 NEMO

Home Network Model	HoA(from HNP) [Home Address derived from Home Network Prefix]	HoA(from MNP) [Home Address derived from Mobile Network Prefix]
NEMO Extended Home Network	Target	N/A
NEMO Aggregated Home Network	N/A	N/A

Although NEMO may extend the concept of Home so that it is not only a flat subnet composed of Home Addresses but an aggregation that is itself subnetted in mobile and Home Networks, IPv6 READY Logo Phase 2 NEMO currently assumes Extended Home Network Model as a basic home network model supposed by RFC3963.

Table 2-1-2. HA and MR Priority A1 and Priority A2 functions

Function	HA	MR
Mobile network prefix registration	A1 *1	A1 *2 A2 *3
BU/BA (IPsec ESP)	A1	A1
encapsulation/decapsulation	A1	A1
Movement detection	-	A1
CoA formation		
visiting of FL		
DHAAD	A2	A2
MPD	A2	A2
Real HL	A2	A2
Fine-Grain Selectors	A2	A2

*1:

- must support both Implicit and Explicit modes

*2:

- must support either Implicit or Explicit modes

*3:

- must support both Implicit and Explicit modes

The test priority of each node becomes as shown in Table 2-1-3.

Table 2-1-3. Combination of mobile network prefixes registration

	Test Priority A1 (Basic)	Test Priority A2 (Advanced)
HA	Both of { - explicit mode - implicit mode}	
MR	One of { - explict mode - implicit mode}	Both of {- explicit mode - implicit mode}

The relationships between each Priority A1/Priority A2 function and the corresponding function item number defined in “Guidelines for Implementation” are shown in Table 2-2.

Table 2-2. Requirements and References

Target	Reference RFC (responding to Implementation Guideline)	Function		Section number in RFC	Function number in Implementation Guideline
HA	RFC3963	Basic Functions	Requirements for IPv6 Home Agents	6	1
			Mobile network prefix registration	6.1.1	3
				6.1.2	4-6,8
				6.2	15-22
				6.7	40-42
				9	25
			BU/BA	6	2
				6.2	9-14
				6.6	33-39
			Encapsulation/ decapsulatation / forwarding	6.4	27-28
				6.5	29-32
				9	24
		Advanced Functions	DHAAD	7	1
				7.1	2-3

				7.2	4-8
			Dynamic routing protocol	6.1.2	7
				6.3	26
				8	12-13, 17-18, 20-21
			Advertising reachability	6.3	23-25
			IPsec	9	22, 27
			Real HL	7.3	9-10
	RFC3775	Requirements for IPv6 Home Agents	Requirements	8.4	1
			Home Registration	8.4	2
			Encapsulation/ decapsulatation / forwarding	8.4	3-5
			Mobility Header	8.4	6
			BU/BA	8.4	7
			Home agent information option	8.4	8
			Mobile prefix advertisement	8.4	9
			IPsec ESP	8.4	10
			Multicast	8.4	11
			Stateful address autoconfiguration	8.4	12
		Basic Functions	Home Registration	10.1	1, 3
				10.3.1	1- 10, 18- 21, 23- 24, 26, 29- 30, 36- 38
			BU/BA (IPsec ESP)	4.1	1, 3 - 4
				4.2	11- 13, 19- 20
				4.3	22- 24
			Encapsulation/	10.4.1	1

			decapsulatation		10.4.2	17- 20
					10.4.5	40, 42
		Advanced Functions	DHAAD		10.5.1	1- 16
			MPD		10.6.2	2- 4, 8, 10- 13
					10.6.3	22- 28
					4.1	7- 8
					4.2	11- 13, 19
					4.3	22- 24
			Real HL		10.1	2, 4, 6- 10
					10.3.1	13- 17
					10.3.2	40- 43, 45- 50
					10.4.1	2- 11, 13- 16
					10.4.2	22- 24
					4.2	16- 18
	RFC4877	Advanced Function	Fine-Grain Selectors		4	5-7, 23-24, 40
MR	RFC3963	Basic Functions	Mobile router operation (including requirements for IPv6 Mobile Nodes)		5	1-4
					9	28
			Home Registration		5.1	5-7
				BU/BA including error proccessing	5.2	9-10, 13, 15-16
					5.3	18-21
					5.4	22-23
				Implicit mode	5.2	11
					5.4.1	24-27
				Explicit mode	5.2	12, 17
					5.4.2	28-36
					5.8	54
				Supporting both modes	5.2	14
					5.4	34

			Encapsulation/ decapsulatation / forwarding	5.5	37-38
				9	23
		Advanced Function	DHAAD	5.1	8
				5.3	20
				7	1
				7.1-7.2	2-5, 7
			Neighbor Discovery	5.6	40-45
				7.3	9-10
			Dynamic routing protocol	8	11, 14-16, 19
				9	26
			Multicast	5.7	46-47
			Real HL	5.6	40-41
				5.7	46
				5.8	48-54
			IPsec	9	27
	RFC3775	Requirements for IPv6 Mobile Nodes	Requirements	8.5	1
			Home Registration	8.5	2
			Home address option IPsec	8.5	3
			Encapsulation/ decapsulatation / forwarding	8.5	4-5
			Binding Error	8.5	6

			ICMP	8.5	7
			Movement detection Returning home	8.5	8
			Mobility Header	8.5	9
			RR	8.5	10
			BU/BA	8.5	11-13
			Mobile prefix advertisement	8.5	14
			DHAAD	8.5	15
			Route optimization	8.5	16
			Multicast	8.5	17
			Stateful address autoconfiguration	8.5	18
		Basic Function	Home Registration	11.1	2- 5, 8- 10
				11.7.1	1- 8, 13, 18- 21
				11.7.3	54- 59, 61- 62
			BU/BA (IPsec ESP)	11.7.3	51
				4.1	1, 3- 4
				4.2	11- 13, 19
				4.3	20- 22, 26, 32
			Encapsulation / decapsulation	11.3.1	4, 14- 16
			Movement detection, CoA formation, visiting of FL	11.5.1	2, 4- 7
				11.5.2	13
		Advanced Function	DHAAD	11.4.1	1- 5, 7- 11
			MPD	11.4.2	12- 26
				11.7.3	60
				4.1	7- 8
				4.2	11- 13, 19
				4.3	20- 22
				4.4	32
			Real HL	11.3.1	8

				11.5.4	32- 49
				4.2	16- 18
	RFC4877	Advanced Function	Fine-Grain Selectors	4	5-7, 23-24, 40

2.2 Architecture of Interoperability test scenario

The outline of the “Interoperability test scenario for IPv6 Ready Logo Phase 2 program” is as follows.

<1> First, one superset scenario, see Table 2-3, that covers all the Priority A1 and Priority A2 functions is developed.

<2> Moreover, the scenario can be reconstructed by combining only Priority A2 test elements that the target equipment supports.

<3> Verifying the functions in this document by checking the corresponding sequences below with the interoperability test scenarios should be possible.

<4> Intermediate checkpoints between major functions are set to confirm the progress of the testing.

*If you select the “Fine-Grain Selectors” of A2, you MUST execute the procedure with each IPsec configurations (Section 4.3 and Section 4.4).

Regarding point <1> above, considering implementer’s convenience and efficiency of the testing, the superset of the interoperability test scenarios that covers all the Priority A1 and Priority A2 functions is developed to execute all the required tests. This superset of the interoperability test scenarios can be built by combining every test element corresponding to each Functional Unit[1].

As for point <2> above, the Priority A2 Functional Units that are not supported by the target equipment used in Network Mobility (HA and MR) can be skipped and only the Functional Units of the supported Priority A2 functions can be executed in the test scenario. This architecture enables the test scenario to be applied to various implementation situations. Examples are shown in Figures 2-1 and 2-2.

In “Interoperability test scenario for IPv6 Ready Logo Phase 2 program”, when Functional Unit (No. 1 A2-1, Figure 2-1) is added to verify Priority A2 functions (e.g. DHAAD) the state immediately before and the state immediately after the state of the added Functional Unit are the same. The added Functional Unit (No. 1 A2-1, Figure 2-1) is connected with Functional Unit (No. 0 A1-1, Figure 2-1) before it and Functional Unit (No. 2 A1-1, Figure 2-1) just after it. When the states of the preceding and following Functional Units are the same as the added

[1] Functional Unit: A minimum set of sequences and procedures needed for verifying a specific function included in "Interoperability test scenarios for IPv6-Ready Logo Phase 2 program."

Functional Unit between them, they are smoothly connected. Therefore, the "Interoperability test scenario for IPv6 Ready Logo Phase 2 program" has a construction by which an implementer can verify all Priority A1 and Priority A2 functions in an arbitrary combination.

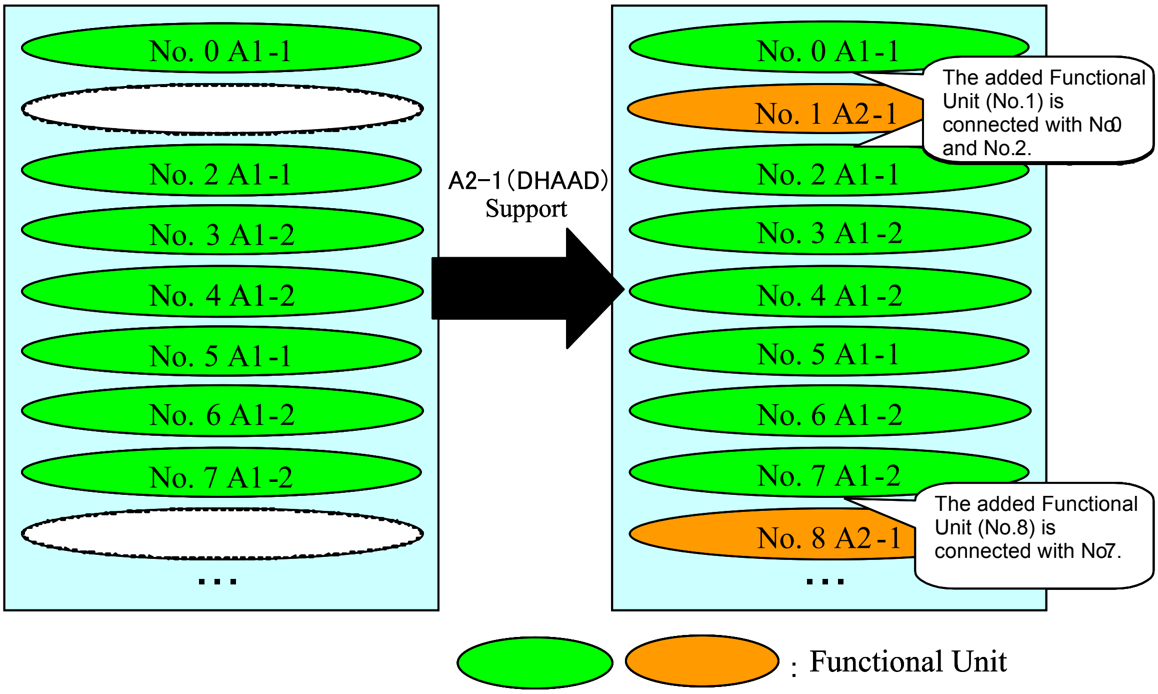


Figure 2-1. Scenario Architecture (1)

In point <3>, the "Interoperability test scenario for IPv6 Ready Logo Phase 2 program" consists of sequences of normal operation of equipment used in Network Mobility (HA and MR), and each Functional Unit in the interoperability test scenarios is executed not only for verifying its function, but for verifying the function of the Functional Unit before it. This architecture of interoperability test scenarios is depicted in Figure 2-2 in more detail.
(Figure 2-2 corresponds to sequence No. 1 to No.8 of Section 3.3.)

For example, Functional Unit (No. 3 A1-1, Figure 2-2) is executed not only for verifying its function but also for verifying the function of Functional Unit (No. 1 A2-1, Figure 2-2) and Functional Unit (No. 2 A2-2, Figure 2-2). Therefore, checking that sequences in packet capture files collected during the test are the same as sequences in "Interoperability test scenarios for IPv6 Ready Logo Phase 2 program" becomes the check of each function.

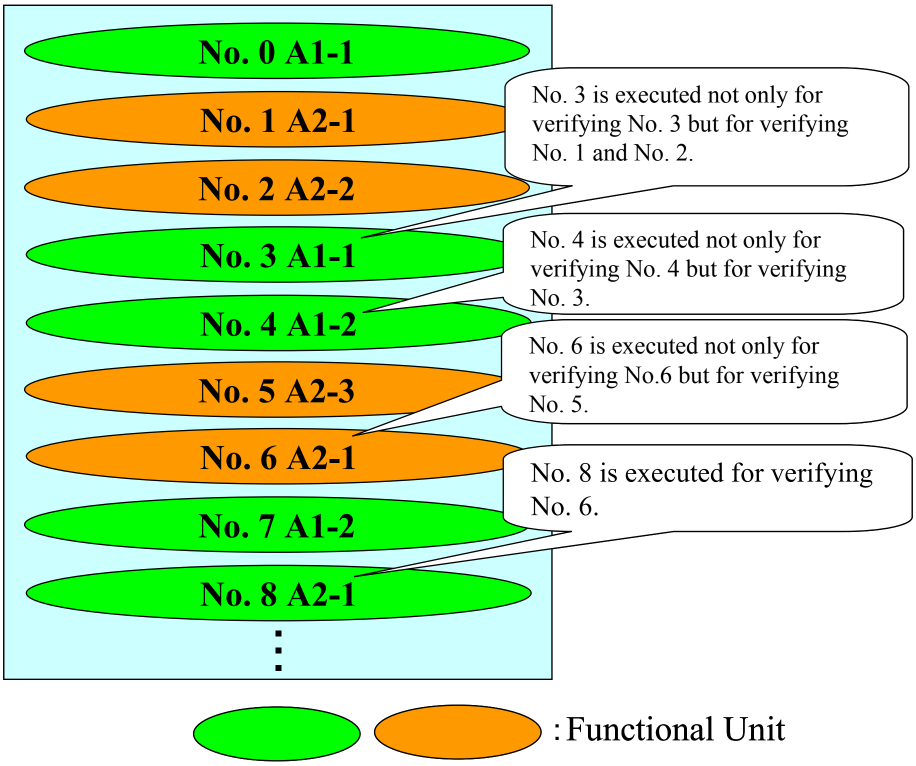

No. 0 A1-1
No. 1 A2-1
No. 2 A2-2
No. 3 A1-1
No. 4 A1-2
No. 5 A2-3
No. 6 A2-1
No. 7 A1-2
No. 8 A2-1
No. 3 is executed not only for verifying No. 3 but for verifying No. 1 and No. 2.
No. 4 is executed not only for verifying No. 4 but for verifying No. 3.
No. 6 is executed not only for verifying No.6 but for verifying No. 5.
No. 8 is executed for verifying No. 6.
: Functional Unit

Figure 2-2. Scenario Architecture (2)

In point <4>, the checkpoints that can be grouped as a Functional check unit are set in the interoperability test scenarios so that an implementer can verify the status of the test process. The contents of the check are described in the test procedure document (see Section 3). If the target Network Mobility equipment (HA and MR) has the function to display the state of the equipment, the function can be used with the methods in the test procedure document to execute tests more efficiently and accurately.

For example, in Table 2-3, verifying functions of the Functional Units from No. 0 to No. 8 is completed by Unit No. 8, and the Functional Units from No. 0 to No. 8 are grouped as a Functional check unit. Besides this example, there are some Functional Sets[2] grouped as a Functional check unit, and they are surrounded by thick lines in Table 2-3.

2.3 Interoperability test scenario for IPv6 Ready Logo Phase 2

[2] Functional Set: A checkpoint that can be grouped as a Functional check unit in "Interoperability test scenarios for IPv6-Ready Logo Phase 2 program."

program

The “Interoperability test scenario for IPv6 Ready Logo Phase 2 program” was developed from the viewpoint of the Phase 2 certification, as shown in Table 2-3. The selection method of the “Interoperability test scenario for IPv6 Ready Logo Phase 2 program” is explained in Table 2-3.

All Priority A1 functions are indispensable for Network Mobility IPv6 equipment (HA, and MR) to acquire a Phase 2 Logo, so all Functional Units for verifying Priority A1 (the column of Required Functions in Table 2-3 is "A1") must be included in the “Interoperability test scenario for IPv6 Ready Logo Phase 2 program”. When an MR is a candidate for Phase 2 certification, the Functional Units of No. 3, 5, 8, 9, 10, 11 and 12 in Table 2-3 must be included in the “Interoperability test scenario for IPv6 Ready Logo Phase 2 program” In the case of an HA, No. 0, 1, 2, 3, 5, 7, 8, 9, 10, 11, 12, 15, 18, 24 and 25 must be included.

Furthermore, when an HA or an MR acquires a Phase 2 Logo on the condition of supporting only Priority A2 functions represented by A2-a without supporting other Priority A2 functions represented by A2-b, the interoperability test scenarios, which include all Functional Units for verifying A2-a (the columns of Required Functions in Table 2-3 are "A1" or "A1 and A2-a"), are selected, and the interoperability test scenarios, which include Functional Units for verifying A2-b (the columns of Required Functions in Table 2-3 are "A1 and A2-b" or "A1, A2-a and A2-b"), are not selected.

Furthermore, when an HA or an MR acquires a Phase 2 Logo on the condition of supporting A2-a and A2-b, the interoperability test scenarios, which include all the Functional Units for verifying A2-a and A2-b (the columns of Required Functions in Table 2-3 are "A1" or "A1 and A2-a" or "A1 and A2-b" or "A1, A2-a and A2-b"), are selected.

The column of “Verify other functional unit” in Table 2-3 shows the numbers for Functional Units that can be checked according to the result of the verification of the preceding Functional Unit.

HA0 or HA1 is an HA that is a test object, and MR0 or MR1 is an MR that is a test object.

Table 2-3. Interoperability test scenario

Functional Set	No	Functional Unit	Required Functions		Verify other Functional Unit
			MR0	HA0	
Home Registration from FL (MR1)	0	Boot up MR, under FL	(A1) *		
	1	BU/BA (Initial Registration)	(A1) *		
	2	ICMP echo request (CN->LFN) ICMP echo reply (LFN->CN)	(A1) *		No.1
Home Registration from FL (MR0)	3	Boot up MR under FL	A1		
	4	DHAAD	A1 and DHAAD	A1 and DHAAD	
	5	BU/BA (Initial Registration)	A1		No. 4
Home Registration from FL with MPD (MR0)	6	MPS/MPA	A1 and MPD	A1 and MPD	
Moving from FL to FL (mobile network) (MR1) (Composition of Nested NEMO)	7	BU/BA (Moving) MR1	-	A1	
	8	ICMP echo request (CN->LFN) ICMP echo reply (LFN->CN)	A1		No. 5 and 7
Home Re-Registration from FL (MR0)	9	BU/BA (Re-Reg)	A1		
	10	ICMP echo request (CN->LFN) ICMP echo reply (LFN->CN)	A1		No. 9
Moving from FL to FL (MR0)	11	BU/BA (Moving)	A1		

	12	ICMP echo request (CN->LFN) ICMP echo reply (LFN->CN)	A1		No. 11
Returning Home (MR0)	13	BU/BA (Moving and De-Reg)	A1 and Real HL	A1 and Real HL	
	14	ICMP echo request (CN->LFN) ICMP echo reply (LFN->CN)	A1 and Real HL	A1 and Real HL	No. 13
Boot up under HL (MR0)	15	BU/BA（Moving）MR1	-	A1	
	16	Shutdown MR under HL	A1 and Real HL	A1and Real HL	
	17	Boot up MR under HL	A1 and Real HL	A1and Real HL	
	18	BU/BA（Moving）MR1	-	A1	
	19	ICMP echo request (CN->LFN) ICMP echo reply (LFN->CN)	A1 and Real HL	A1 and Real HL	No. 16
Moving from HL to FL (MR0)	20	Moving	A1 and Real HL	A1 and Real HL	
	21	DHAAD	A1, Real HL and DHAAD	A1, Real HL and DHAAD	
	22	BU/BA (Moving)	A1 and Real HL	A1 and Real HL	No. 19
	23	ICMP echo request (CN->LFN) ICMP echo reply (LFN->CN)	A1 and Real HL	A1 and Real HL	
Moving from FL (mobile network) to FL (MR1) (Release of nested	24	BU/BA (Moving)	-	A1	

NEMO)	25	ICMP echo request (CN->LFN) ICMP echo reply (LFN->CN)	-	A1	No. 22

*required procedures for executing “Interoperability test scenario for IPv6 Ready Logo Phase 2 program”

2.4 Examples of “Interoperability test scenario for IPv6 Ready Logo Phase 2 program”

Examples of “Interoperability test scenario for IPv6 Ready Logo Phase 2 program” are shown below.

1) Test scenario that includes A1 Architecture of MR (blue in Table 2-3)

MR supports all the Priority A1 functions in Table 2-1-2.

-> A operator chooses Functional Units, "A1", in "Required Function" in Table 2-3 (No. 3, 5,8,9,10,11 and 12).

2) Test scenario that includes A1 Architecture of HA (blue + green in Table 2-3)

HA supports all the Priority A1 functions in Table 2-1-2.

-> A operator chooses Functional Units, "A1", in "Required Function" in Table 2-3 (No. 0, 1, 2, 3,5,7,8,9,10,11,12,15,18,24 and 25).

3) Test scenario that includes A1 Architecture of HA/MR and DHAAD

HA supports all the Priority A1, DHAAD

MR supports all the Priority A1, DHAAD

->A operator chooses Functional Units, "A1", "A1 and DHAAD" in "Required Function" in Table 2-3

(No. 0, 1, 2, 3, 4, 5, 7, 8, 9, 10, 11, 12, 15, 18, 21, 24 and 25).

2.5 Test conditions of “Interoperability test scenario for IPv6 Ready Logo Phase 2 program”

The test network topologies and the test procedures of “Interoperability test scenario for IPv6 Ready Logo Phase 2 program” are described in Section 3. The test procedures correspond with Table 2-3. Configuration information, such as IPsec used in “Interoperability test scenario for IPv6 Ready Logo Phase 2 program" is described in Section 4. The detailed sequences of "Interoperability test scenario for IPv6 Ready Logo Phase 2 program" are described in Section 3.3. The detailed sequences also correspond with Table 2-3.

For Phase 2 certification, packet capture files collected during the test must be submitted, and command logs (e.g. ping) collected during the test must be submitted in addition to packet capture files.

2.6 Compatible conditions for acquisition of Phase 2 Logo

Network Mobility equipment (HA and MR) must execute the "Interoperability test scenario for IPv6 Ready Logo Phase 2 program" with two or more different types (different vendors) of equipment according to the combination of each test in Table 2-4 to acquire the IPv6 Ready Logo Phase 2 program Logo.

In a nested Network Mobility, there could be two cases for network mobility equipment to bind to HA. One is where all equipment binds to the same HA, and another is where all equipment binds to different HAs.
In the case of binding to the same HA, for MR, there does NOT need to be any consideration about which HA the MR binds to. However, in the case of binding to a different HA, we should consider a function such as double tunneling packets. Therefore, we assumed that the "same HA" situation includes the functions of "different HA", and the "Interoperability test scenario for IPv6 Ready Logo Phase 2 program" includes the nested situation with the same HA.

HA must execute the "Interoperability test scenario for IPv6 Ready Logo Phase 2 program" at four times with two types (different vendors) of equipment (MR) to acquire the IPv6 Ready Logo, HA Basic (A1). Two combinations of Binding mode and Home Address (Explicit x HoA (from HNP), Implicit x HoA (from HNP), must be executed in the "Interoperability test scenario for IPv6 Ready Logo Phase 2 program" with two types (different vendors) equipment (MR).

If you support Fine-Grain Selectors, you execute the same interoperability test again using Fine-Grain Selectors. Then you may select either Explicit mode or Implicit mode, because Fine-Grain Selectors are an independent function. Therefore, both HA and MR examinations increase two times when they support "Fine-Grain Selectors". At least, HA need six times examinations, and MR need four times examinations for BASIC tests and for "Fine-Grain

Selectors" tests, and need six times examinations for ADVANCED tests and for "Fine-Grain Selectors" tests.

Table 2-4 HA Basic (A1): case1 - four target vendors (MR)

	binding mode		MR(Vendor)
Test No.	Explicit	Implicit	
1	O		MR_Vendor_A
2	O		MR_Vendor_B
3		O	MR_Vendor_C
4		O	MR_Vendor_D
target vendors	MR_A, MR_B	MR_C, MR_D	

Table 2-5 HA Basic (A1): case2 - two target vendors (MR)

	binding mode		MR(Vendor)
Test No.	Explicit	Implicit	
1	O		MR_Vendor_A
2	O		MR_Vendor_B
3		O	MR_Vendor_A
4		O	MR_Vendor_B
target vendors	MR_A, MR_B	MR_A, MR_B	

MR must execute the “Interoperability test scenario for IPv6 Ready Logo Phase 2 program” at least two times with two types (different vendors) of equipment (HA) to acquire the IPv6 Ready Logo, MR Basic (A1). One combination of Binding mode and Home Address from (Explicit x HoA (from HNP), Explicit x HoA (from HNP)) must be executed in the “Interoperability test scenario for IPv6 Ready Logo Phase 2 program” with two types (different vendors) equipment (HA).

Table 2-6 MR Basic (A1) Explicit x HoA (from HNP)

	binding mode	HA(Vendor)
Test No.	Explicit	
1		HA_Vendor_A
2		HA_Vendor_B
target vendors	HA_A, HA_B	

MR must execute the “Interoperability test scenario for IPv6 Ready Logo Phase 2 program” at least four times with two types (different vendors) of equipment (MR) to acquire the IPv6 Ready Logo, MR Advanced (A2). Two combination of Binding mode and HoA formation (Explicit x HoA (from HNP), Implict x HoA (from HNP)) must be executed in the

“Interoperability test scenario for IPv6 Ready Logo Phase 2 program” with two types (different vendors) of equipment (HA).

Table 2-7 MR Advanced (A2): case 1 - four target vendors (HA)

	binding mode		HA(Vendor)
Test No.	Explicit	Implicit	
1	O		HA_Vendor_A
2	O		HA_Vendor_B
3		O	HA_Vendor_C
4		O	HA_Vendor_D
target vendors	HA_A, HA_B	HA_C, HA_D	

Table 2-8 MR Advanced (A2): case 2 - two target vendors (HA)

	binding mode		HA(Vendor)
Test No.	Explicit	Implicit	
1	O		HA_Vendor_A
2	O		HA_Vendor_B
3		O	HA_Vendor_A
4		O	HA_Vendor_B
target vendors	HA_A, HA_B	HA_A, HA_B	

If you support Fine-Grain Selectors, HA or MR must execute the “Interoperability test scenario for IPv6 Ready Logo Phase 2 program” add two times as shown below:

Table 2-9 HA Basic (A1) with Fine-Grain Selectors (A2): two target vendors (MR)

	binding mode		Fine-Grain Selectors	MR(Vendor)
Test No.	Explicit	Implicit		
1	O			MR_Vendor_A
2	O			MR_Vendor_B
3		O		MR_Vendor_A
4		O		MR_Vendor_B
5	O (explicit or implicit)		O	MR_Vendor_A
6	O (explicit or implicit)		O	MR_Vendor_B
target vendors	MR_A, MR_B	MR_A, MR_B	MR_A, MR_B	

In the case of four vendors, add two times as the same.

Table 2-10 MR Basic (A1) with Fine-Grain Selectors (A2) Explicit x HoA (from HNP)

	binding mode	Fine-Grain Selectors	HA(Vendor)
Test No.	Explicit		
1	O		HA_Vendor_A
2	O		HA_Vendor_B
3	O	O	HA_Vendor_A
4	O	O	HA_Vendor_B
target vendors	HA_A, HA_B	HA_A, HA_B	

Table 2-11 MR Advanced (A2) with Fine-Grain Selectors (A2): two target vendors (HA)

	binding mode		Fine-Grain Selectors	HA(Vendor)
Test No.	Explicit	Implicit		
1	O			HA_Vendor_A
2	O			HA_Vendor_B
3		O		HA_Vendor_A
4		O		HA_Vendor_B
5	O (explicit or implicit)		O	HA_Vendor_A
6	O (explicit or implicit)		O	HA_Vendor_B
target vendors	HA_A, HA_B	HA_A, HA_B	HA_A, HA_B	

In the case of four vendors, add two times as the same.

An example in the case of making a logo application by HA and MR is shown below.

1) In the case where an HA is a candidate for Phase 2 certification

When an HA is a candidate for Phase 2 certification, the “Interoperability test scenario for IPv6 Ready Logo Phase 2 program” must be executed with two or more MRs. An example of the minimum numbers of combinations is shown below.

<a composition of binding mode in Table 2.1.3>

Example: pattern 1 (Explicit x HoA (from HNP))

Test 1:

(CN0)---HA0*---MR0_a---MR1_b---(LFN0)

Test 2:

(CN0)---HA0*---MR0_b---MR1_a---(LFN0)

<Another composition of binding mode in Table 2.1.3>

Example: pattern 3 (Implicit x HoA (from HNP))

Test 3:

(CN0)---HA0*---MR0_c (MR0_a) ---MR1_d (MR1_b) ---(LFN0)

Test 4:

(CN0)---HA0*---MR0_d (MR0_b) ---MR1_c (MR1_a)---(LFN0)

At least, we need to combine Tests 1, 2, 3, and 4,
so that HoA (from HNP) and Explicit/Implicit can be selected.
HA0* is a candidate for Phase 2 certification.
MR0_a and MR0_b are different implementations (different vendors).
MR1_a and MR1_b are different implementations (different vendors).
MR0_c and MR0_d are different implementations (different vendors).
MR1_c and MR1_d are different implementations (different vendors).
CN0 and LFN0 are a reference for Phase 2 certification.

2) In the case where an MR is a candidate for Phase 2 certification

When an MR is a candidate for Phase 2 certification, the "Interoperability test scenario for IPv6 Ready Logo Phase 2 program" must be executed with two or more different HAs. An example of the minimum number of combinations is shown below.

Case of Priority A1 (Basic)

<A composition of binding mode in Table 2.1.3>

Example: pattern 1 (Explicit x HoA (from HNP))

Test 1:

(CN0)---HA0_a---MR0*---(MR1)---(LFN0)

Test 2:

(CN0)---HA0_b---MR0*---(MR1)---(LFN0)

MR0* is a candidate for Phase 2 certification.
HA0_a and HA0_b are different implementations (different vendors).
MR1, CN0, and LFN0 are a reference for Phase 2 certification.

Case of Priority A2 (Advanced)

<A composition of binding mode in Table 2.1.3>

Example: pattern 1 (Explicit x HoA (from HNP))

Test 1:

(CN0)---HA0_a---MR0*---(MR1)---(LFN0)

Test 2:

(CN0)---HA0_b---MR0*---(MR1)---(LFN0)

<Another composition of binding mode in Table 2.1.3>

Example: pattern 3 (Implicit x HoA (from HNP))

Test 3:

(CN0)---HA0_c (HA0_a) ---MR0*---(MR1)---(LFN0)

Test 4:

(CN0)---HA0_d (HA0_b) ---MR0*---(MR1)---(LFN0)

At least, we need to combine Tests 1, 2, 3, and 4,
so that all modes of HoA (from HNP) and Explicit/Implicit can be selected.

MR0* is a candidate for Phase 2 certification.
HA0_a and HA0_b are different implementations from different vendors.
HA0_c and HA0_d are different implementations from different vendors.
MR1, CN0, and LFN0 are references for Phase 2 certification.

2.7 Submission for acquisition of Phase 2 Logo

Submissions for acquisition of Phase 2 Logo are listed

2.7.1 Required data

Configuration and information of each node, Packet Capture File, Command Log, and Topology Map for **each** session is required for Phase 2 certification.

- **Configuration and information of each node** (node address, link, IPsec, and algorithm)

Link

Link[No.]	Link0	Link1	Link2
Network Address / Prefix			
	Link4	Link5	

Example

Link0
3ffe:0501:ffff:0100::/64

Router

Router[No.]	R0		R1	
Location - Link[No.]	Link0	Link1	Link1	Link2
Global Address (IPv6 Address)				
Link Local Address				
MAC address (Ether address)				

Example

R0
Home-Link0
3ffe:0501:ffff: 0100::1
fe80::1
00:11:11: 11:cn:01

Home Agent

Node[No.]		HA0
Company -HA- number		
Global Address (IPv6 Address)		
Link Local Address (IPv6 Address)		
MAC address (Ether address)		
binding mode	Explicit	
	Implicit	
Advance functions	DHAAD	
	MPD	
	RHL	
IPsec SA	BU/BA	
	MPD	
	Payload	
Encryption algorithms		3DES-CBC
Authentication algorithms		HMAC-SHA1

Example

HA0
CCC-HA-01
3ffe:0501:ffff: 0100::1
3ffe:0501:ffff: 0100:0211:11ff: fe11:ha01
00:11:11: 11:ha:01
X
-
X
X
-
X
X
X
3DES-CBC
HMAC-SHA1

*IPsec SA:the case where IPsec SA of transport mode is divided by BU/BA and MPD, and the case where it is made one are permitted.

Mobile Router

Node[No.]		MR0	MR1
Company -MN- number			
Addresses on the Home Link	Global Address (IPv6 Address)		
	Link Local Address (IPv6 Address)		
	MAC address (Ether address)		
Addresses on the Mobile Network	Global Address (IPv6 Address)		
	Link Local Address (IPv6 Address)		
	MAC address (Ether address)		
Care-of Address (FL1)			
Care-of Address (FL2)			
Care-of Address (FL4)			
binding mode	Explicit		
	Implicit		
Advance functions	DHAAD		
	MPD		
	RHL		
IPsecSA	BU/BA		
	MPD		
	Payload		
Encryption algorithm		3DES-CBC	3DES-CBC
Authentication algorithm		HMAC-SHA1	HMAC-SHA1

Example

MR1
EEE-MN-01
3ffe:0501:ffff: 0100::1
3ffe:0501:ffff: 0100:0211:1111: 1111:mn01
00:11:11: 11:mn:01
3ffe:0501:ffff: 0100::1
3ffe:0501:ffff: 0100:0211:1111: 1111:mn01
00:11:11: 11:mn:01
3ffe:0501:ffff: 0101::(Interface id)
3ffe:0501:ffff: 0102::(Interface id)
3ffe:0501:ffff: 0103::(Interface id)
X
-
X
X
-
X
X
X
3DES-CBC, NULL
HAMC-SHA1

Local Fixed Node

Node[No.]	LFN0
Company -LFN- number	
Global Address (IPv6 Address)	
Link Local Address (IPv6 Address)	
MAC address (Ether address)	

Correspondent Node

Node[No.]	CN0
Company -CN- number	
Global Address (IPv6 Address)	
Link Local Address (IPv6 Address)	
MAC address (Ether address)	

Example

CN0
AAA-CN-01
3ffe:0501:ffff: 0100::1
3ffe:0501:ffff: 0101:0211:11ff:
00:11:11: 11:cn:01

- **Packet Capture File** (e.g., tcpdump(pcap))

  Save the packet capture files on each link (including mobile link).

- **Command log**

  Save the command logs on each node (e.g., ping6, ifconfig, ipconfig /all)

- **Topology Map** （see Section 3.1.1）

2.7.2 Test Result Table

Select a candidate node from the following cases and complete each table.

1) In the case where an **HA** is a candidate for Phase 2 certification

binding mode*1		[ ] Explicit
		[ ] Implicit
Target node		MR0
HA0	PASS	🟩
Reference node		MR1, CN0, LFN0

Note)

*1: Please refer to Table 2.1.3, and select the combination

2) In the case where an **MR** is a candidate for Phase 2 certifications

binding mode*1		[ ] Explicit
		[ ] Implicit
Target node		HA0
MR0	PASS	🟩
Reference node		MR1, CN0, LFN0

Note)

*1: Please refer to Table 2.1.3, and select the combination

2.7.3 Data file name syntax

Use the following syntax, and name submitted files. A) and B) for **each** session are required for Phase 2 certification.

A) Required data (in Section 2.7.3)

Syntax: <Vendor-Node>.info

(e.g., vendor1-MR.info)

Syntax: packet_<link No>.dump

(e.g., packet_link1.dump)

Syntax: command.log

<Procedure No.>-<Vendor-Node (| _<Vendor-Node>) >-<command>.result

(e.g., 4_vendor2-MR_address.result
4_vendor3-CN_vendor4-MR_echo.result)

Syntax: topology.map

B) Test Result Table (in Section 2.7.4)

Syntax: result.tbl

2.7.4 Data Archive

Organize your data according to the following directory structure.

```
$Your_Device_ver/Interoperability/result.tbl

$Your_Device_ver/Interoperability/test1/<Vendor-Node>.info
$Your_Device_ver/Interoperability/test1/packet_<link No>.dump
$Your_Device_ver/Interoperability/test1/<procedure No.>-<Vendor-Node> ( |
 -<Vendor-Node>) -<command>.result
$Your_Device_ver/Interoperability/test1/topology.map

$Your_Device_ver/Interoperability/test2/<Vendor-Node>.info
$Your_Device_ver/Interoperability/test2/packet_<link No>.dump
$Your_Device_ver/Interoperability/test2/<procedure No.>-<Vendor-Node> ( |
 -<Vendor-Node>) -<command>.result
$Your_Device_ver/Interoperability/test2/topology.map

$Your_Device_ver/Interoperability/test3/<Vendor-Node>.info
$Your_Device_ver/Interoperability/test3/packet_<link No>.dump
```

$Your_Device_ver/Interoperability/test3/<procedure No.>-<Vendor-Node> (| -<Vendor-Node>) -<command>.result
$Your_Device_ver/Interoperability/test3/topology.map

$Your_Device_ver/Interoperability/test4/<Vendor-Node>.info
$Your_Device_ver/Interoperability/test4/packet_<link No>.dump
$Your_Device_ver/Interoperability/test4/<procedure No.>-<Vendor-Node> (| -<Vendor-Node>) -<command>.result
$Your_Device_ver/Interoperability/test4/topology.map

(If you select the "Fine-grain Selectors", add your data as following directory structure.)
$Your_Device_ver/Interoperability/test5/<Vendor-Node>.info
$Your_Device_ver/Interoperability/test5/packet_<link No>.dump
$Your_Device_ver/Interoperability/test5/<procedure No.>-<Vendor-Node> (| -<Vendor-Node>) -<command>.result
$Your_Device_ver/Interoperability/test5/topology.map

$Your_Device_ver/Interoperability/test6/<Vendor-Node>.info
$Your_Device_ver/Interoperability/test6/packet_<link No>.dump
$Your_Device_ver/Interoperability/test6/<procedure No.>-<Vendor-Node> (| -<Vendor-Node>) -<command>.result
$Your_Device_ver/Interoperability/test6/topology.map

Put first interoperability data file in "Interoperability/test1/" directory.
Put second interoperability data file in "Interoperability/test2/" directory.
Put third interoperability data file in "Interoperability/test3/" directory.
Put fourth interoperability data file in "Interoperability/test4/" directory.
Put fifth interoperability data file in "Interoperability/test5/" directory.
Put sixth interoperability data file in "Interoperability/test6/" directory.
Make a tar.gz archive file, and submit the archived file.

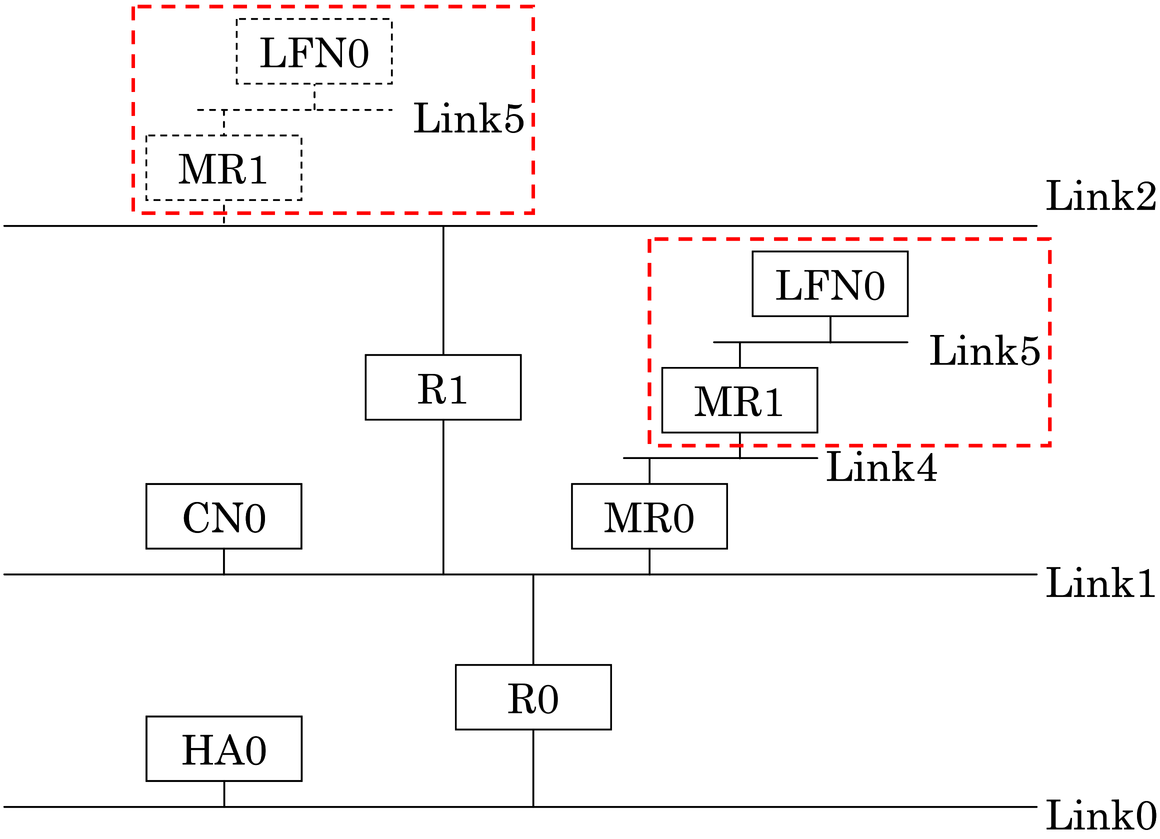
3. Test Procedure for Interoperability test scenario for IPv6 Ready Logo Phase 2

3.1. Test Settings

3.1.1 Topology

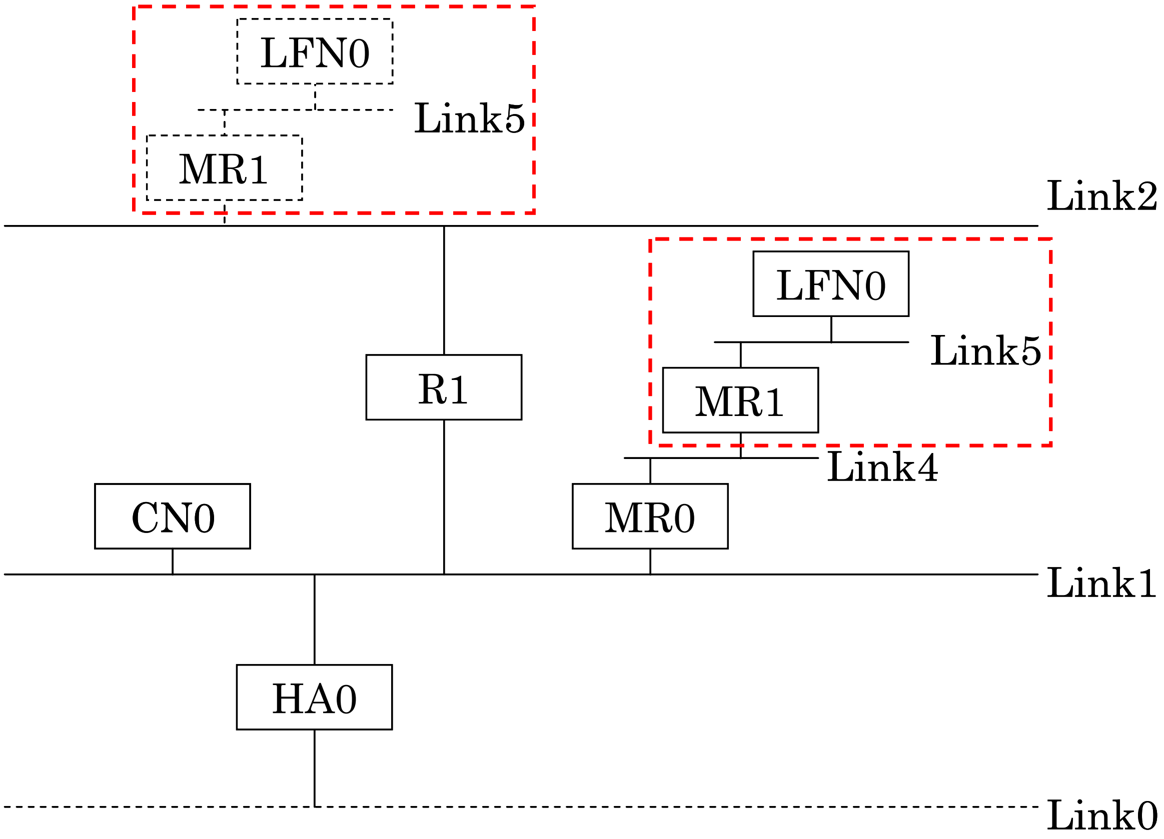
The topologies used in this scenario are shown below. HA and MR are connected as follows. There are two cases of Real Home Link, the setting in which HAs have a physical home link, and of Virtual Home Link, the setting in which HAs do not have a physical home link. An example of the topology of a Real Home Link is shown in Section 3.1.1.1, and an example of the topology of a Virtual Home Link is shown in Section 3.1.1.2.

3.1.1.1 Real Home Link



* The number of routers is not limited. The number of routers can be changed according to the number of interfaces of routers.

3.1.1.2 Virtual Home Link



* The number of routers is not limited. The number of routers can be changed according to the number of interfaces of routers.

<<Link Information>>

- Link0

  3ffe:501:ffff:100::/64 (home link for MR0)

- Link1

  3ffe:501:ffff:101::/64 (foreign link for MR0)

- Link2

  3ffe:501:ffff:102::/64 (foreign link for MR0)

- Link4 (nemo link)

  3ffe:501:ffff:104::/64 (nemo link for MR1)

- Link5 (nested nemo link)

  3ffe:501:ffff:105::/64 (nemo link for LFN0)

<<Node Information>>

- HA0

  3ffe:501:ffff:100::200 (Real Home Link)

  3ffe:501:ffff:101::1   (Virtual Home Link)

- MR0(Link0, HL)

  Home address formation:

    HoA (from HNP) 3ffe:501:ffff:100::(Interface ID) or 3ffe:501:ffff:100::400

- MR0(Link1, FL)

  3ffe:501:ffff:101::(Interface ID) (Care-of address)

- MR0(Link2, FL)

  3ffe:501:ffff:102::(Interface ID) (Care-of address)

- MR1(Link0, HL)

  Home address formation:

    HoA (from HNP) 3ffe:501:ffff:100::(Interface ID) or 3ffe:501:ffff:100::500

- MR1(Link2, FL)

  3ffe:501:ffff:102::(Interface ID) Care-of address

- MR1(Link4, FL(nested NEMO Link))

  3ffe:501:ffff:104::(Interface ID) Care-of address

- R0(Link0)

  3ffe:501:ffff:100::1

- R0(Link1)

  3ffe:501:ffff:101::1

- R1(Link1)

  3ffe:501:ffff:101::2

- R1(Link2)

  3ffe:501:ffff:102::2

- CN0(Link1)

  3ffe:501:ffff:101::100

- LFN0(Link5)

  3ffe:501:ffff:105::(Interface ID)

3.1.2 Initial test conditions

To execute this scenario, the following initial conditions should be satisfied.

(a) HA0

- Does not have BCE for MR0 and MR1.
- The following setting should be configured.
  - o IPsec: Refer to Section 4(manual configuration)
  - o MNP: Refer to Table 2-1-2

(b) MR0

- Does not have BLE for HA0.
- The following settings should be configured.
  - o HoA: (manual configuration or stateless address autoconfiguration)
  - o HA Address: (manual configuration or DHAAD)
  - o CoA: (stateless address autoconfiguration)
  - o IPsec: Refer to Section 4 (manual configuration)
  - o MNP: Refer to Table 2-1-2

(c) MR1

- Does not have BLE for HA0.
- The following settings should be configured.
  - o HoA: (manual configuration or stateless address autoconfiguration)
  - o HA Address: (manual configuration or DHAAD)
  - o CoA: (stateless address autoconfiguration)
  - o IPsec: Refer to Section 4(manual configuration)
  - o MNP: Refer to Table 2-1-2

(d) R0

- Setting static route from CN0 to HA0.

(e) R1

- Setting static route from CN0 to HA0.

(f) CN0

- none

(g) LFN0

- none

3.2. Test Procedure

3.2.1 Procedure

The procedure executed in this scenario is stated as follows. The procedure can be used in cases of Real Home Link and Virtual Home Link.

When a Phase 2 Logo applicant is an HA, the procedure for HA0 is performed.

When a Phase 2 Logo applicant is an MR, the procedure for MR0 is performed.

<<Initialization>>

No. 0 Boot up MR1 under Foreign Link

1 Connect CN0 to Link1.

2 Boot up CN0 under Link1.

=> Save the address information about CN0. (For example, 'ifconfig' Command.)
This file is named '0_ <Vendor>-CN _address.result'.

3 Connect HA0 to Link0.

4 Boot up HA0 under Link0.

=> Save the address information about HA0. (For example, 'ifconfig' Command.)
This file is named '0_<Vendor>-HA_address.result'.

5 Connect MR1 to Link2 (FL).

6 Boot up MR1 at Link2 (FL).

7 Connect LFN0 at Link5.

8 Boot up LFN0 at Link5.

No. 1 (MR1) BU/BA (Initial Registration)

1 Transmit a BU from MR1 (Link2, FL) to HA0.

2 Observe a BA from HA0 to MR1 (Link2, FL).

=> Save the address information about MR1 for checking HoA and CoA of MR1.
(For example, 'ifconfig' Command.)
This file is named '1_<Vendor>-MR1_address.result'.

=> Save the address information about LFN0. (For example, 'ifconfig' Command.)
This file is named '1_<Vendor>-LFN_address.result'.

*Verify the other functional unit as follows.

** If the equipment state can be displayed, the generated BCE and BLE may be verified depending on the capability of the equipment function.　(For example, use a status display command.)

No. 2 (CN0) ICMP echo request (CN->LFN) + ICMP echo reply (LFN->CN)

1 Transmit an ICMPv6 echo request from CN0 to LFN0 (Link5).

=> Save the command log of CN0 for ICMPv6 echo. (For example, 'ping6' Command.)

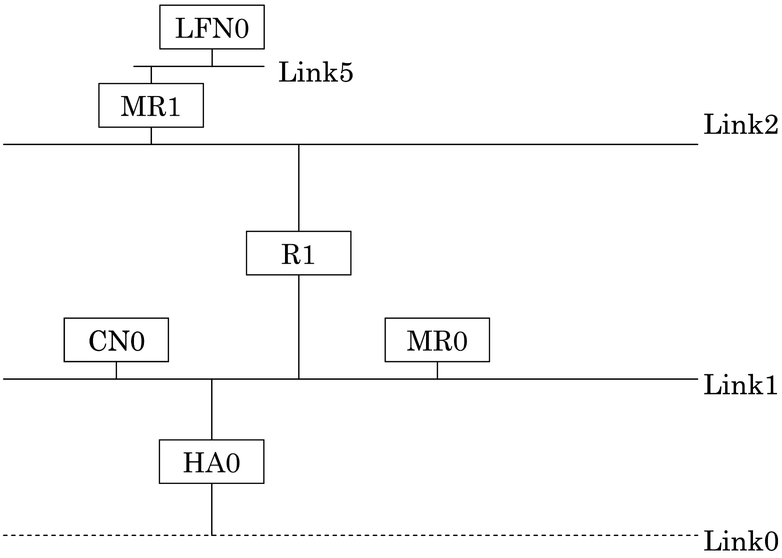
This file is named '2_<Vendor>-CN _<Vendor>-LFN_echo.result'.

2 Observe an ICMPv6 echo reply from LFN0 (Link5) to CN0.

(LFN0 sends ICMPv6 echo reply to CN0 via the HA0.)

<<Procedure>>

No. 3 Boot up MR0 at Foreign Link



1 Connect MR0 to Link1 (FL).

2 Boot up MR0 at Link1 (FL).

=> Save the address information about MR0. (For example, 'ifconfig' Command.)

This file is named '3_ <Vendor>-MR0 _address.result'.

No. 4 (MR0) DHAAD

1 Transmit an HAAD request from MR0 (Link1, FL) to HA0.

2 Observe an HAAD reply from HA0 to MR0 (Link1, FL).

No. 5 (MR0) BU/BA (Initial Registration)

1 Transmit a BU from MR0 (Link1, FL) to HA0.

2 Observe a BA from HA0 to MR0 (Link1, FL).

=> Save the address information about MR0 for checking HoA and CoA of MR0.

(For example, 'ifconfig' Command.)

This file is named '5_<Vendor>-MR0_address.result'.

*Verify the other functional unit as follows.

a. If the DHAAD function is selected, verify that the destination address of BU is the HA address acquired with DHAAD executed in procedure No. 4.

** If the equipment state can be displayed, the generated BCE and BLE may be verified depending on the capability of the equipment function. . (For example, use a status display command.)

No. 6 (MR0) MPS/MPA

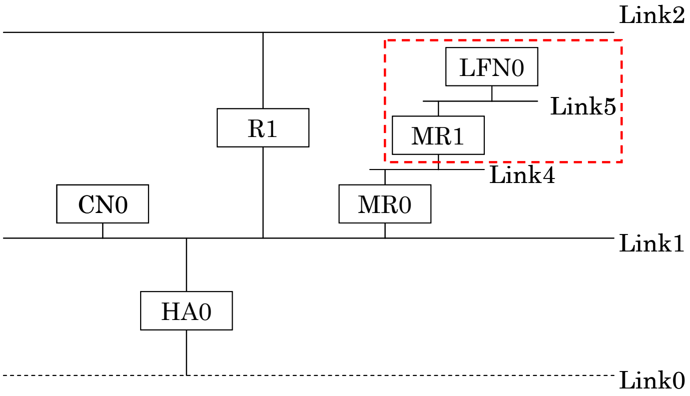
1 Transmit an MPS from MR0 (Link1, FL) to HA0.

2 Observe an MPA from HA0 to MR0 (Link1, FL).

***The transmission of MPS/MPA can be performed at any time after procedure No. 5.

No. 7 (MR1) BU/BA (Moving)

*Formation of nested NEMO [MR0(Link1)---MR1(Link4)---LFN0(Link5)]



1 Remove MR1 from Link2 (FL).

2 Connect MR1 to Link4 (FL).

3 Observe a BU from MR1 (Link4, FL) to HA0.

4 Observe a BA from HA0 to MR1 (Link4, FL).

=> Save the address information about MR1 for checking new CoA of MR1.

(For example, 'ifconfig' Command.)

This file is named '7_<Vendor>-MR1_address.result'.

** If the equipment state can be displayed, the generated BCE and BLE may be verified depending on the capability of the equipment function. .. (For example, use a status display command.)

No. 8 (CN0) ICMP echo request (CN->LFN) + ICMP echo reply (LFN->CN)

1 Transmit an ICMPv6 echo request from CN0 to LFN0 (Link5).

=> Save the command log on CN0 for ICMPv6 echo. (For example, 'ping6' Command.)

This file is named '8_<Vendor>-CN _<Vendor>-LFN_echo.result'.

2 Observe an ICMPv6 echo reply from LFN0 (Link5) to CN0.

(LFN0 sends ICMPv6 echo reply to CN0 via the HA0.)

No. 9 (MR0) BU/BA (Re-Reg)

1 MR0 (Link1, FL) stays on the same link and waits.

2 Observe a BU (Re-Reg) to refresh the lifetime from MR0 (Link1, FL) to HA0 before the lifetime of the binding generated in procedure No. 5 expires.

** If the equipment state can be displayed, the generated BCE and BLE may be verified depending on the capability of the equipment function.

(For example, use a status display command.)

No. 10 (CN0) ICMP echo request (CN->LFN) + ICMP echo reply (LFN->CN)

1 Transmit an ICMPv6 echo request from CN0 to LFN0 (Link5).

=> Save the command log on CN0 for ICMPv6 echo. (For example, 'ping6' Command.)

This file is named '10_<Vendor>-CN_<Vendor>-LFN_echo.result'.

2 Observe an ICMPv6 echo reply from LFN0 (Link5) to CN0.

(LFN0 sends ICMPv6 echo reply to CN0 via the HA.)

No. 11 (MR0) BU/BA (Moving)

1 Remove MR0 from Link1 (FL).

2 Connect MR0 to Link2 (FL).

3 Observe a BU from MR0 (Link2, FL) to HA0.

4 Observe a BA from HA0 to MR0 (Link2, FL).

=> Save the address information about MR0 for checking new CoA of MR0.

(For example, 'ifconfig' Command.)

This file is named '11_<Vendor>-MR0_address.result'.

** If the equipment state can be displayed, the generated BCE and BLE may be verified depending on the capability of the equipment function. .. (For example, use a status display command.)

No. 12 (CN0) ICMP echo request (CN->LFN) + ICMP echo reply (LFN->CN)

1 Transmit an ICMPv6 echo request from CN0 to LFN0 (Link5).

=> Save the command log on CN0 for ICMPv6 echo. (For example, 'ping6' Command.)
This file is named '12_<Vendor>-CN_<Vendor>-LFN_echo.result'.

2 Observe an ICMPv6 echo reply from LFN0 (Link5) to CN0.
(LFN0 sends ICMPv6 echo reply to CN0 via the HA.)

No. 13 (MR0) BU/BA (Moving + De-Reg)

1 Remove MR0 from Link1 (FL) or Link2 (FL).
2 Connect MR0 to Link0 (HL).
3 Observe a BU from MR0 (Link0, HL) to HA0.
4 Observe a BA from HA0 to MR0 (Link0, HL).

=> Save the address information about MR0 for checking address of MR0.
(For example, 'ifconfig' Command.)
This file is named '13_<Vendor>-MR0_address.result'.

** If the equipment state can be displayed, the deleted BCE and BLE may be verified depending on the capability of the equipment function.

No. 14 (CN0) ICMP echo request (CN->LFN) + ICMP echo reply (LFN->CN)

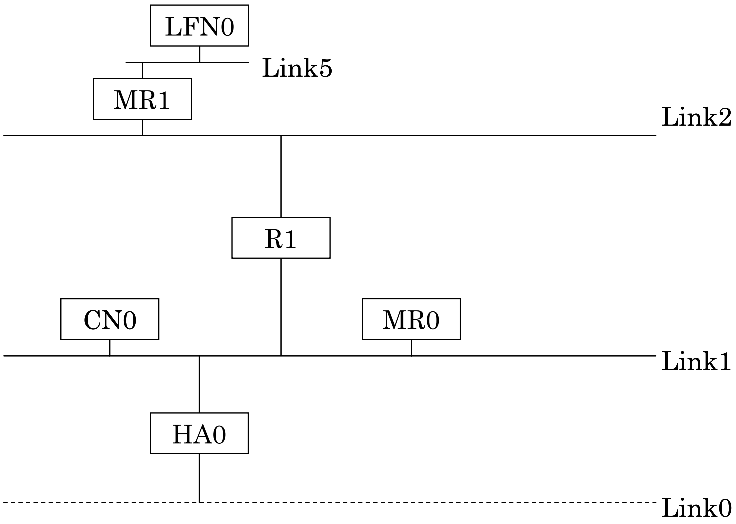
1 Transmit an ICMPv6 echo request from CN0 to LFN0 (Link5).

=> Save the command log on CN0 for ICMPv6 echo. (For example, 'ping6' Command.)
This file is named '14_<Vendor>-CN_<Vendor>-LFN_echo.result'.

2 Observe an ICMPv6 echo reply from LFN0 (Link5) to CN0.
(MR0 is on its home link, so it forwards an ICMPv6 request/reply without encapsulation.)

No. 15 (MR1) BU/BA (Moving)

*Release from formation of nested NEMO



1 Remove MR1 from Link4 (FL).

2 Connect MR1 to Link2 (FL).

3 Observe a BU from MR1 (Link2, FL) to HA0.

4 Observe a BA from HA0 to MR1 (Link2, FL).

=> Save the address information about MR1 for checking new CoA of MR1.

(For example, 'ifconfig' Command.)

This file is named '15_<Vendor>-MR1_address.result'.

** If the equipment state can be displayed, the generated BCE and BLE may be verified depending on the capability of the equipment function. .. (For example, use a status display command.)

No. 16 Shutdown MR0 on Home Link

1 Shutdown MR0 (Link0, HL).

No. 17 Boot up MR0 on Home Link

1 Boot up MR0 (Link0, HL).

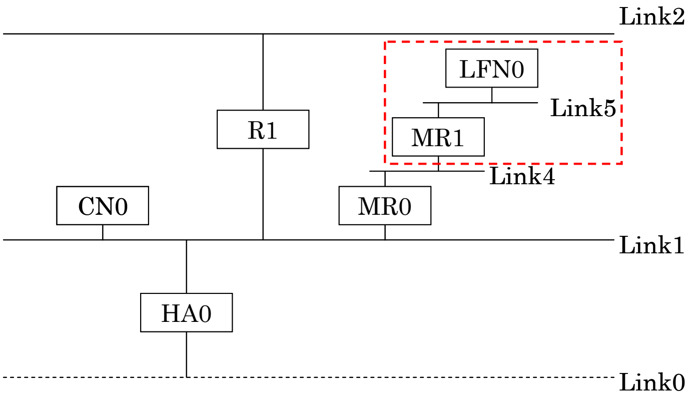
=> Save the address information about MR0 for checking address.

(For example, 'ifconfig' Command.)

This file is named '17_<Vendor>-MR0_address.result'.

No. 18 (MR1) BU/BA (Moving)

*Formation of nested NEMO [MR0(Link1)---MR1(Link4)---LFN0(Link5)]



1 Remove MR1 from Link2 (FL).

2 Connect MR1 to Link4 (FL).

3 Observe a BU from MR1 (Link4, FL) to HA0.

4 Observe a BA from HA0 to MR1 (Link4, FL).

=> Save the address information about MR1 for checking new CoA of MR1.

(For example, 'ifconfig' Command.)

This file is named '18_<Vendor>-MR1_address.result'.

** If the equipment state can be displayed, the generated BCE and BLE may be verified depending on the capability of the equipment function. .. (For example, use a status display command.)

No. 19 (CN0) ICMP echo request (CN->LFN) + ICMP echo reply (LFN->CN)

1 Transmit an ICMPv6 echo request from CN0 to LFN0 (Link5).

=> Save the command log on CN0 for ICMPv6 echo. (For example, 'ping6' Command.)

This file is named '19_<Vendor>-CN_<Vendor>-LFN_echo.result'.

2 Observe an ICMPv6 echo reply from LFN0 (Link5) to CN0.

(LFN0 sends ICMPv6 echo reply directly to CN0, not via the HA.)

No. 20 (MR0) Moving

1 Remove MR0 from Link0 (HL).

2 Connect MR0 to Link1 (FL).

No. 21 (MR0) DHAAD

1 Transmit an HAAD request from MR0 (Link1, FL) to HA0.

2 Observe an HAAD reply from HA0 to MR0 (Link1, FL).

No. 22 (MR0) BU/BA (Moving)

1 Observe a BU from MR0 (Link1, FL) to HA0.

2 Observe a BA from HA0 to MR0 (Link1, FL).

=> Save the address information about MR0 for checking new CoA of MR0.
(For example, 'ifconfig' Command.)
This file is named '22_<Vendor>-MR0_address.result'.

*Verify the other functional unit as follows.

a. If the DHAAD function is selected, verify that destination address of BU is the HA address acquired with DHAAD executed in procedure No. 21.

**If the equipment state can be displayed, the generated BCE and BLE may be verified depending on the capability of the equipment function. . (For example, use a status display command.)

No. 23 (CN0) ICMP echo request (CN->LFN) + ICMP echo reply (LFN->CN)

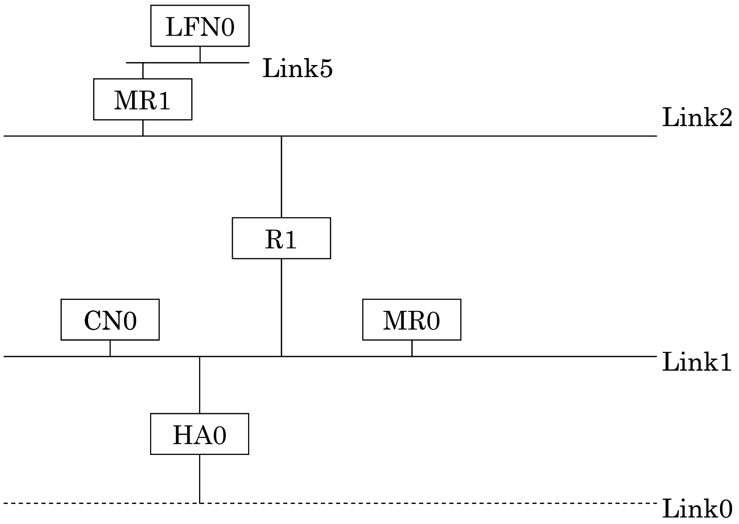
1 Transmit an ICMPv6 echo request from CN0 to LFN0 (Link5).

=> Save the command log on CN0 for ICMPv6 echo. (For example, 'ping6' Command.)
This file is named '23_<Vendor>-CN_<Vendor>-LFN_echo.result'.

2 Observe an ICMPv6 echo reply from LFN0 (Link5) to CN0.
(LFN0 sends ICMPv6 echo reply to CN0 via the HA.)

No. 24 (MR1) BU/BA (Moving)

*Release from formation of nested NEMO



1 Remove MR1 from Link4 (FL).

2 Connect MR1 to Link2 (FL).

3 Observe a BU from MR1 (Link2, FL) to HA0.

4 Observe a BA from HA0 to MR1 (Link2, FL).

=> Save the address information about MR1 for checking new CoA of MR1.

(For example, 'ifconfig' Command.)

This file is named '24_<Vendor>-MR1_address.result'.

** If the equipment state can be displayed, the generated BCE and BLE may be verified depending on the capability of the equipment function. .. (For example, use a status display command.)

No. 25 (CN0) ICMP echo request (CN->LFN) + ICMP echo reply (LFN->CN)

1 Transmit an ICMPv6 echo request from CN0 to LFN0 (Link5).

=> Save the command log on CN0 for ICMPv6 echo. (For example, 'ping6' Command.)

This file is named '25_<Vendor>-CN _<Vendor>-LFN_echo.result'.

2 Observe an ICMPv6 echo reply from LFN0 (Link5) to CN0.

(LFN0 sends ICMPv6 echo reply to CN0 via the HA0.)

3.2.2 Procedure of verifying test scenario

Network Mobility sequence under the actual execution of this scenario is described in Section 3.3.

Check that sequences in the log are the same as that in Section 3.3.

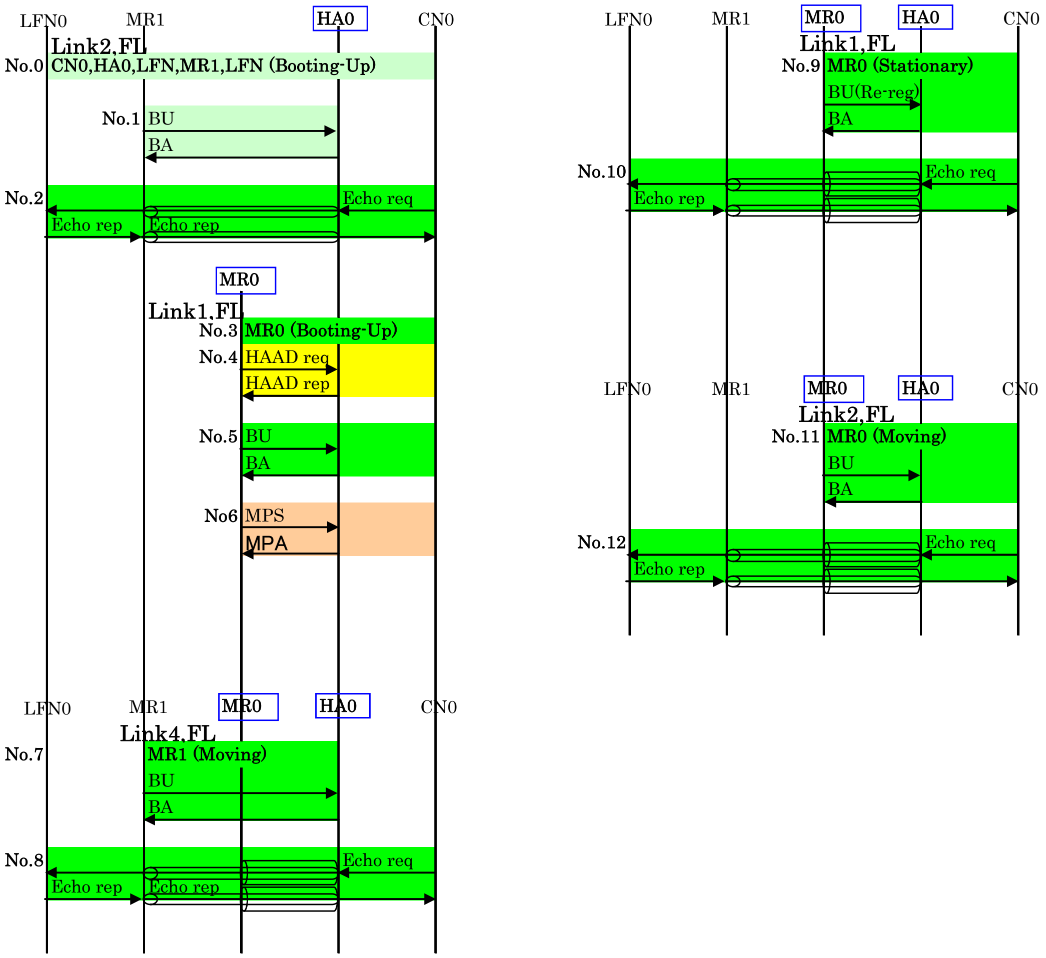
The check should be executed at either stage 'A' or 'B'.

A. Under each procedure of Section 3.2.1

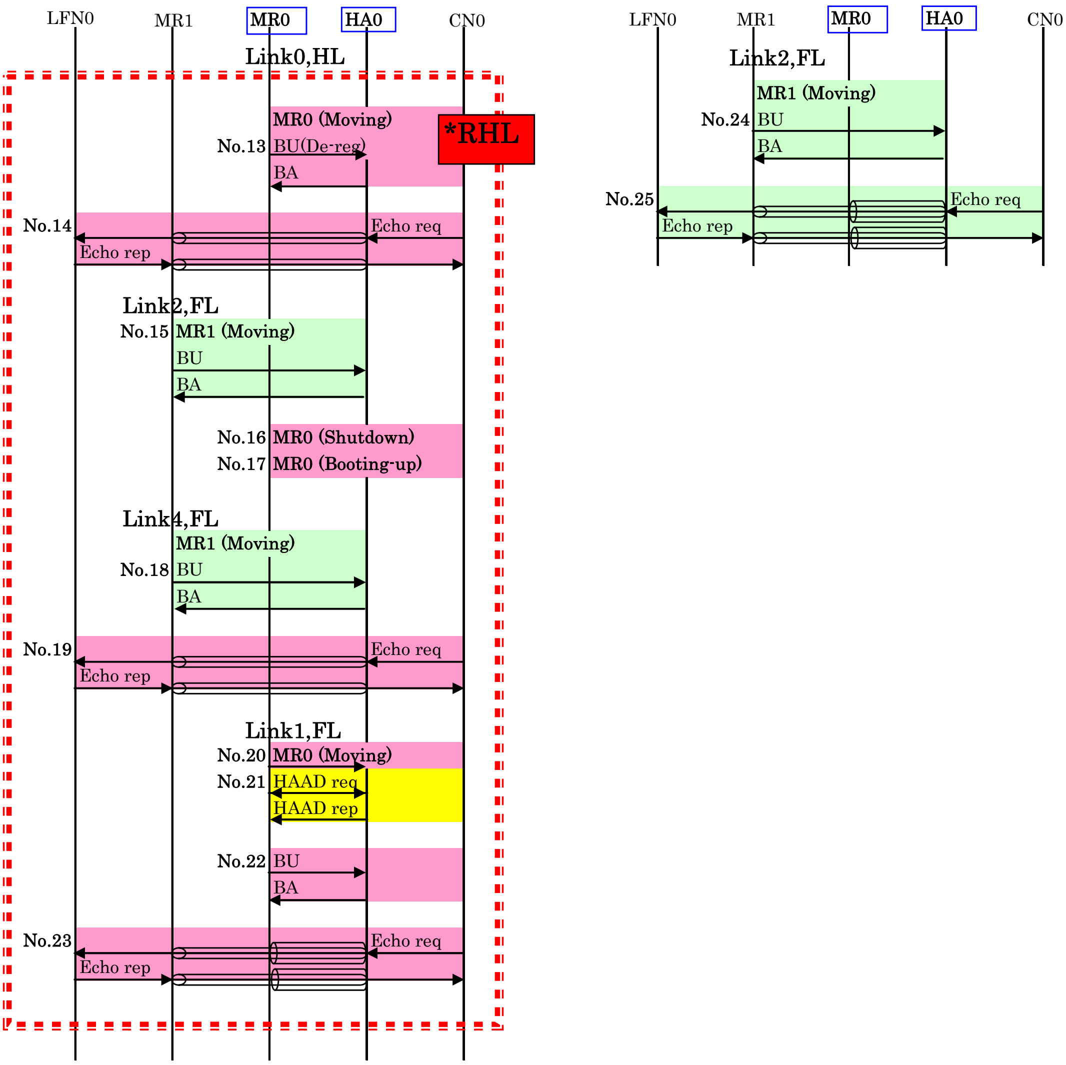
B. After executing test scenario

3.3 Sequence of Interoperability Test Scenario

Sequence of Interoperability Test Scenario (1/2)



Sequence of Interoperability Test Scenario (2/2)



4. Configuration of various lifetimes and IPsec

4.1. Configurations of various lifetimes

To execute this scenario, various lifetimes are set as follows.

Binding Cache

- Home Registration: 420 seconds

4.2. IPsec configurations

IPsec configurations are set as described in Section 4.3 to use manual configurations of IPsec SA in testing.

In case of executing "Fine-Grain Selectors" mode, see Section 4.4.

4.3. Manual IPsec SA configurations

SPD and SAD entries to protect BU/BA, MPS/MPA, and Payload packets between HA and MR are described below.

According to RFC3963, in the case where IPsec SAs for transport mode are divided by BU/BA and MPD, and the case where two IPsec SAs are grouped as one are permitted.

However, considering the interoperability in the case of executing the “Interoperability test scenario for IPv6 Ready Logo Phase 2 program”, IPsec SAs must be separated according to BU/BA and MPD.

In the case of executing “Interoperability test scenarios for implementers”, IPsec SAs may be grouped as one.

Moreover, when IPsec SAs for transport mode are grouped as one, IPsec SA configurations for BU/BA are used (see Section 4.3.1). ("Any" is set as Transport Layer Protocol.) When IPsec SAs for tunnel mode are grouped as one, IPsec SA configurations for Payload are used (see Section 4.3.4). ("Any" is set as Transport Layer Protocol.)

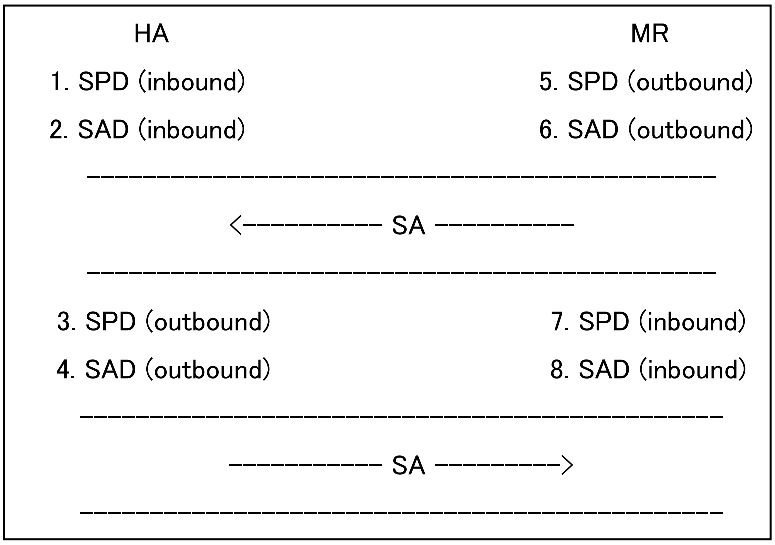


Figure 4.1 Manual IPsec SA configurations between HA and MR

4.3.1. BU/BA [Transport Mode] for manual IPsec SA

<SPD for HA (inbound) and MR (outbound) (refer to 1 and 5 in Figure 4.1)>

Source Address	MR Home Address
Destination Address	HA Address
IPsec Protocol	ESP
Transport Layer Protocol	MH(*)
IPsec protocol mode	transport mode

<SPD for HA (outbound) and MR (inbound) (refer to 3 and 7 in Figure 4.1)>

Source Address	HA Address
Destination Address	MR Home Address
IPsec Protocol	ESP
Transport Layer Protocol	MH(*)
IPsec protocol mode	transport mode

(*)In case of executing "Fine-Grain Selectors" mode, see Section 4.4.1.

<SA1 for HA 0 (inbound) and MR0 (outbound) (refer to 2 and 6 in Figure 4.1)>

	MR0	HA0
Source Address	MR Home Address	MR Home Address
Destination Address	HA Address	HA Address
IPsec Protocol	ESP	ESP
SPI	0x111	0x111
Authentication algorithm	HMAC-SHA1-96	HMAC-SHA1-96
Authentication keys	V6LC-111--1234567890	V6LC-111--1234567890
Encryption algorithm	3DES-CBC	3DES-CBC
Encryption keys	V6LC-111--12345678901234	V6LC-111--12345678901234

<SA1 for HA 0 (inbound) and MR1 (outbound) (refer to 2 and 6 in Figure 4.1)>

	MR1	HA0
Source Address	MR Home Address	MR Home Address
Destination Address	HA Address	HA Address
IPsec Protocol	ESP	ESP
SPI	0x121	0x121
Authentication algorithm	HMAC-SHA1-96	HMAC-SHA1-96
Authentication keys	V6LC-121--1234567890	V6LC-121--1234567890
Encryption algorithm	3DES-CBC	3DES-CBC
Encryption keys	V6LC-121--12345678901234	V6LC-121--12345678901234

<SA2 for HA 0 (outbound) and MR0 (inbound) (refer to 4 and 8 in Figure 4.1)>

	MR0	HA0
Source Address	HA Address	HA Address
Destination Address	MR Home Address	MR Home Address
IPsec Protocol	ESP	ESP
SPI	0x112	0x112
Authentication algorithm	HMAC-SHA1-96	HMAC-SHA1-96
Authentication keys	V6LC-112--1234567890	V6LC-112--1234567890
Encryption algorithm	3DES-CBC	3DES-CBC
Encryption keys	V6LC-112--12345678901234	V6LC-112--12345678901234

<SA2 for HA 0 (outbound) and MR1 (inbound) (refer to 4 and 8 in Figure 4.1)>

	MR1	HA0
Source Address	HA Address	HA Address
Destination Address	MR Home Address	MR Home Address
IPsec Protocol	ESP	ESP
SPI	0x122	0x122
Authentication algorithm	HMAC-SHA1-96	HMAC-SHA1-96
Authentication keys	V6LC-122--1234567890	V6LC-122--1234567890
Encryption algorithm	3DES-CBC	3DES-CBC
Encryption keys	V6LC-122--12345678901234	V6LC-122--12345678901234

** HMAC-SHA1-96 and 3DES-CBC must be selected as Authentication algorithm and Encryption algorithm in "Interoperability test scenario for IPv6 Ready Logo Phase 2 program"

4.3.2. MPS/MPA [Transport Mode] for manual IPsec SA

<SPD for HA (inbound) and MR (outbound) (refer to 1 and 5 in Figure 4.1)>

Source Address	MR Home Address
Destination Address	HA Address
IPsec Protocol	ESP
Transport Layer Protocol	ICMPv6 (*)(**)
IPsec protocol mode	transport mode

<SPD for HA (outbound) and MR (inbound) (refer to 3 and 7 in Figure 4.1)>

Source Address	HA Address
Destination Address	MR Home Address
IPsec Protocol	ESP
Transport Layer Protocol	ICMPv6 (*)(**)
IPsec protocol mode	transport mode

(*)In the case of executing "Interoperability test scenario for IPv6 Ready Logo Phase 2 program", "ICMPv6" is set as the Transport Layer Protocol of an IPsec selector. If the ICMPv6 message type is supported, "Any" is set as the ICMPv6 message type.

(**)In case of executing "Fine-Grain Selectors" mode, see Section 4.4.2.

<SA5 for HA0 (inbound) and MR0 (outbound) (refer to 2 and 6 in Figure 4.1)>

	MR0	HA0
Source Address	MR Home Address	MR Home Address
Destination Address	HA Address	HA Address
IPsec Protocol	ESP	ESP
SPI	0x115	0x115
Authentication algorithm	HMAC-SHA1-96	HMAC-SHA1-96
Authentication keys	V6LC-115--1234567890	V6LC-115--1234567890
Encryption algorithm	3DES-CBC	3DES-CBC
Encryption keys	V6LC-115--12345678901234	V6LC-115--12345678901234

<SA5 for HA0 (inbound) and MR1 (outbound) (refer to 2 and 6 in Figure 4.1)>

	MR1	HA0
Source Address	MR Home Address	MR Home Address
Destination Address	HA Address	HA Address
IPsec Protocol	ESP	ESP
SPI	0x125	0x125
Authentication algorithm	HMAC-SHA1-96	HMAC-SHA1-96
Authentication keys	V6LC-125--1234567890	V6LC-125--1234567890
Encryption algorithm	3DES-CBC	3DES-CBC
Encryption keys	V6LC-125--12345678901234	V6LC-125--12345678901234

<SA6 for HA0 (outbound) and MR0 (inbound) (refer to 4 and 8 in Figure 4.1)>

	MR0	HA0
Source Address	HA Address	HA Address
Destination Address	MR Home Address	MR Home Address
IPsec Protocol	ESP	ESP
SPI	0x116	0x116
Authentication algorithm	HMAC-SHA1-96	HMAC-SHA1-96
Authentication keys	V6LC-116--1234567890	V6LC-116--1234567890
Encryption algorithm	3DES-CBC	3DES-CBC
Encryption keys	V6LC-116--12345678901234	V6LC-116--12345678901234

<SA6 for HA0 (outbound) and MR1 (inbound) (refer to 4 and 8 in Figure 4.1)>

	MR1	HA0
Source Address	HA Address	HA Address
Destination Address	MR Home Address	MR Home Address

IPsec Protocol	ESP	ESP
SPI	0x126	0x126
Authentication algorithm	HMAC-SHA1-96	HMAC-SHA1-96
Authentication keys	V6LC-126--1234567890	V6LC-126--1234567890
Encryption algorithm	3DES-CBC	3DES-CBC
Encryption keys	V6LC-126--12345678901234	V6LC-126--12345678901234

** HMAC-SHA1-96 and 3DES-CBC must be selected as Authentication algorithm and Encryption algorithm in "Interoperability test scenario for IPv6 Ready Logo Phase 2 program"

4.3.3. Payload [Tunnel Mode] for manual IPsec SA

This configuration is for development. It is not used in "Interoperability test scenario for IPv6 Ready Logo Phase 2 program"

SA9 and SA10 are NOT described in RFC3963 and RFC3776 for payload packet.

<SPD for HA (inbound) and MR (outbound) (refer to 1 and 5 in Figure 4.1)>

Source Address	MR Home Address
Destination Address	Any
IPsec Protocol	ESP
Transport Layer Protocol	Any
IPsec protocol mode	Transport mode

<SPD for HA (outbound) and MR (inbound) (refer to 3 and 7 in Figure 4.1)>

Source Address	MR Home Address
Destination Address	Any
IPsec Protocol	ESP
Transport Layer Protocol	Any
IPsec protocol mode	Transport mode

<SA7 for HA 0 (inbound) and MR0 (outbound) (refer to 2 and 6 in Figure 4.1)>

	MR0	HA0

Outer Source Address	MR Care of Address	MR Care of Address
Outer Destination Address	HA Address	HA Address
Inner Source Address	MR Home Address	MR Home Address
Inner Destination Address	Any	Any
IPsec Protocol	ESP	ESP
SPI	0x117	0x117
Authentication algorithm	HMAC-SHA1-96	HMAC-SHA1-96
Authentication keys	V6LC-117--1234567890	V6LC-117--1234567890
Encryption algorithm	3DES-CBC	3DES-CBC
Encryption keys	V6LC-117--12345678901234	V6LC-117--12345678901234

<SA7 for HA 0 (inbound) and MR1 (outbound) (refer to 2 and 6 in Figure 4.1)>

	MR1	HA0
Outer Source Address	MR Care of Address	MR Care of Address
Outer Destination Address	HA Address	HA Address
Inner Source Address	MR Home Address	MR Home Address
Inner Destination Address	Any	Any
IPsec Protocol	ESP	ESP
SPI	0x127	0x127
Authentication algorithm	HMAC-SHA1-96	HMAC-SHA1-96
Authentication keys	V6LC-127--1234567890	V6LC-127--1234567890
Encryption algorithm	3DES-CBC	3DES-CBC

Encryption keys	V6LC-127--12345678901 234	V6LC-127--12345678901 234

<SA8 for HA 0 (outbound) and MR0 (inbound) (refer to 4 and 8 in Figure 4.1)>

	MR0	HA0
Outer Source Address	HA Address	HA Address
Outer Destination Address	MR Care of Address	MR Care of Address
Inner Source Address	Any	Any
Inner Destination Address	MR Home Address	MR Home Address
IPsec Protocol	ESP	ESP
SPI	0x118	0x118
Authentication algorithm	HMAC-SHA1-96	HMAC-SHA1-96
Authentication keys	V6LC-118--1234567890	V6LC-118--1234567890
Encryption algorithm	3DES-CBC	3DES-CBC
Encryption keys	V6LC-118--12345678901 234	V6LC-118--12345678901 234

<SA8 for HA 0 (outbound) and MR1 (inbound) (refer to 4 and 8 in Figure 4.1)>

	MR1	HA0
Outer Source Address	HA Address	HA Address
Outer Destination Address	MR Care of Address	MR Care of Address
Inner Source Address	Any	Any
Inner Destination Address	MR Home Address	MR Home Address
IPsec Protocol	ESP	ESP
SPI	0x128	0x128

Authentication algorithm	HMAC-SHA1-96	HMAC-SHA1-96
Authentication keys	V6LC-128--1234567890	V6LC-128--1234567890
Encryption algorithm	3DES-CBC	3DES-CBC
Encryption keys	V6LC-128--12345678901 234	V6LC-128--12345678901 234

<SA9 for HA 0 (inbound) and MR0 (outbound) (refer to 2 and 6 in Figure 4.1)>

	MR0	HA0
Outer Source Address	MR Care of Address	MR Care of Address
Outer Destination Address	HA Address	HA Address
Inner Source Address	MNP	MNP
Inner Destination Address	Any	Any
IPsec Protocol	ESP	ESP
SPI	0x119	0x119
Authentication algorithm	HMAC-SHA1-96	HMAC-SHA1-96
Authentication keys	V6LC-119--1234567890	V6LC-119--1234567890
Encryption algorithm	3DES-CBC	3DES-CBC
Encryption keys	V6LC-119—1234567890 1234	V6LC-119--12345678901 234

<SA9 for HA 0 (inbound) and MR1 (outbound) (refer to 2 and 6 in Figure 4.1)>

	MR1	HA0
Outer Source Address	MR Care of Address	MR Care of Address
Outer Destination Address	HA Address	HA Address
Inner Source	MNP	MNP

Address		
Inner Destination Address	Any	Any
IPsec Protocol	ESP	ESP
SPI	0x129	0x129
Authentication algorithm	HMAC-SHA1-96	HMAC-SHA1-96
Authentication keys	V6LC-129--1234567890	V6LC-129--1234567890
Encryption algorithm	3DES-CBC	3DES-CBC
Encryption keys	V6LC-129--12345678901234	V6LC-129--12345678901234

<SA10 for HA 0 (outbound) and MR0 (inbound) (refer to 4 and 8 in Figure 4.1)>

	MR0	HA0
Outer Source Address	HA Address	HA Address
Outer Destination Address	MR Care of Address	MR Care of Address
Inner Source Address	Any	Any
Inner Destination Address	MNP	MNP
IPsec Protocol	ESP	ESP
SPI	0x11A	0x11A
Authentication algorithm	HMAC-SHA1-96	HMAC-SHA1-96
Authentication keys	V6LC-11A-1234567890	V6LC-11A-1234567890
Encryption algorithm	3DES-CBC	3DES-CBC
Encryption keys	V6LC-11A-12345678901234	V6LC-11A-12345678901234

<SA10 for HA 0 (outbound) and MR1 (inbound) (refer to 4 and 8 in Figure 4.1)>

	MR1	HA0

Outer Source Address	HA Address	HA Address
Outer Destination Address	MR Care of Address	MR Care of Address
Inner Source Address	Any	Any
Inner Destination Address	MNP	MNP
IPsec Protocol	ESP	ESP
SPI	0x12A	0x12A
Authentication algorithm	HMAC-SHA1-96	HMAC-SHA1-96
Authentication keys	V6LC-12A-1234567890	V6LC-12A-1234567890
Encryption algorithm	3DES-CBC	3DES-CBC
Encryption keys	V6LC-12A-12345678901234	V6LC-12A-12345678901234

Reference: Method of calculating SPI, Authentication keys, and Encryption keys for Manual IPsec SA between HA and MR

- Method of calculating SPI

SPI = (HA-No+1) * 0x100 + (MR-No+1) * 0x10 + SA-No

Example:

1) [HA-No=0] : [MR-No=0] : [SA-No=1]

0x100 + 0x10 + 0x1 = 0x111

2) [HA-No=1] : [MR-No=1] : [SA-No=4]

0x200 + 0x20 + 0x4 = 0x224

- Method of selecting authentication keys

Relationship between Algorithm and Key is shown below.

Algorithm	Key (<SPI> is SPI number(HEX))
HMAC-SHA1	V6LC-<SPI>--1234567890
HMAC-MD5	V6LC-<SPI>--123456

NULL	(none)

Example:

1) [HA-No=0] : [MR-No=1] : [SA-No=1] (HMAC-SHA1)

0x100 + 0x20 + 0x1 = 0x121

Key = 'V6LC-121--1234567890'

- Method of selecting Encryption keys

Relationship between Algorithm and Key is shown below.

Algorithm	Key (<SPI> is the base on HEX)
3DES-CBC	V6LC-<SPI>--12345678901234
DES-CBC	V6LC-<SPI>
NULL	(none)

Example:

1) [HA-No=1] : [MR-No=1] : [SA-No=1] (3DES-CBC)

0x200 + 0x20 + 0x1 = 0x221

Key = 'V6LC-221--12345678901234'

4.4. Manual IPsec SA configurations with Fine-Grain Selectors

4.4.1. BU/BA [Transport Mode] for manual IPsec SA (Fine-Grain Selectors)

<SPD for HA (inbound) and MR (outbound) (refer to 1 and 5 in Figure 4.1)>

Source Address	MR Home Address
Destination Address	HA Address
IPsec Protocol	ESP
Transport Layer Protocol	MH
Message Type	BU
IPsec protocol mode	transport mode

<SPD for HA (outbound) and MR (inbound) (refer to 3 and 7 in Figure 4.1)>

Source Address	HA Address
Destination Address	MR Home Address
IPsec Protocol	ESP

Transport Layer Protocol	MH
Message Type	BA
IPsec protocol mode	transport mode

<SA1 for HA 0 (inbound) and MR0 (outbound) (refer to 2 and 6 in Figure 4.1)>

	MR0	HA0
Source Address	MR Home Address	MR Home Address
Destination Address	HA Address	HA Address
IPsec Protocol	ESP	ESP
SPI	0x111	0x111
Authentication algorithm	HMAC-SHA1-96	HMAC-SHA1-96
Authentication keys	V6LC-111--1234567890	V6LC-111--1234567890
Encryption algorithm	3DES-CBC	3DES-CBC
Encryption keys	V6LC-111--12345678901234	V6LC-111--12345678901234

<SA1 for HA 0 (inbound) and MR1 (outbound) (refer to 2 and 6 in Figure 4.1)>

	MR1	HA0
Source Address	MR Home Address	MR Home Address
Destination Address	HA Address	HA Address
IPsec Protocol	ESP	ESP
SPI	0x121	0x121
Authentication algorithm	HMAC-SHA1-96	HMAC-SHA1-96
Authentication keys	V6LC-121--1234567890	V6LC-121--1234567890
Encryption algorithm	3DES-CBC	3DES-CBC
Encryption keys	V6LC-121--12345678901234	V6LC-121--12345678901234

<SA2 for HA 0 (outbound) and MR0 (inbound) (refer to 4 and 8 in Figure 4.1)>

	MR0	HA0
Source Address	HA Address	HA Address
Destination Address	MR Home Address	MR Home Address
IPsec Protocol	ESP	ESP
SPI	0x112	0x112
Authentication algorithm	HMAC-SHA1-96	HMAC-SHA1-96
Authentication keys	V6LC-112--1234567890	V6LC-112--1234567890
Encryption algorithm	3DES-CBC	3DES-CBC
Encryption keys	V6LC-112--12345678901234	V6LC-112--12345678901234

<SA2 for HA 0 (outbound) and MR1 (inbound) (refer to 4 and 8 in Figure 4.1)>

	MR1	HA0
Source Address	HA Address	HA Address
Destination Address	MR Home Address	MR Home Address
IPsec Protocol	ESP	ESP
SPI	0x122	0x122
Authentication algorithm	HMAC-SHA1-96	HMAC-SHA1-96
Authentication keys	V6LC-122--1234567890	V6LC-122--1234567890
Encryption algorithm	3DES-CBC	3DES-CBC
Encryption keys	V6LC-122--12345678901234	V6LC-122--12345678901234

** HMAC-SHA1-96 and 3DES-CBC must be selected as Authentication algorithm and Encryption algorithm in "Interoperability test scenario for IPv6 Ready Logo Phase 2 program"

4.4.2. MPS/MPA [Transport Mode] for manual IPsec SA (Fine-Grain Selectors)

<SPD for HA (inbound) and MR (outbound) (refer to 1 and 5 in Figure 4.1)>

Source Address	MR Home Address
Destination Address	HA Address
IPsec Protocol	ESP
Transport Layer Protocol	ICMPv6
Message Type	MPS
IPsec protocol mode	transport mode

<SPD for HA (outbound) and MR (inbound) (refer to 3 and 7 in Figure 4.1)>

Source Address	HA Address
Destination Address	MR Home Address
IPsec Protocol	ESP
Transport Layer Protocol	ICMPv6
Message Type	MPA
IPsec protocol mode	transport mode

<SA5 for HA0 (inbound) and MR0 (outbound) (refer to 2 and 6 in Figure 4.1)>

	MR0	HA0
Source Address	MR Home Address	MR Home Address
Destination Address	HA Address	HA Address
IPsec Protocol	ESP	ESP
SPI	0x115	0x115
Authentication algorithm	HMAC-SHA1-96	HMAC-SHA1-96
Authentication keys	V6LC-115--1234567890	V6LC-115--1234567890
Encryption algorithm	3DES-CBC	3DES-CBC
Encryption keys	V6LC-115--12345678901234	V6LC-115--12345678901234

<SA5 for HA0 (inbound) and MR1 (outbound) (refer to 2 and 6 in Figure 4.1)>

	MR1	HA0
Source Address	MR Home Address	MR Home Address
Destination Address	HA Address	HA Address
IPsec Protocol	ESP	ESP
SPI	0x125	0x125
Authentication algorithm	HMAC-SHA1-96	HMAC-SHA1-96
Authentication keys	V6LC-125--1234567890	V6LC-125--1234567890
Encryption algorithm	3DES-CBC	3DES-CBC
Encryption keys	V6LC-125--12345678901234	V6LC-125--12345678901234

<SA6 for HA0 (outbound) and MR0 (inbound) (refer to 4 and 8 in Figure 4.1)>

	MR0	HA0
Source Address	HA Address	HA Address
Destination Address	MR Home Address	MR Home Address
IPsec Protocol	ESP	ESP
SPI	0x116	0x116
Authentication algorithm	HMAC-SHA1-96	HMAC-SHA1-96
Authentication keys	V6LC-116--1234567890	V6LC-116--1234567890
Encryption algorithm	3DES-CBC	3DES-CBC
Encryption keys	V6LC-116--12345678901234	V6LC-116--12345678901234

<SA6 for HA0 (outbound) and MR1 (inbound) (refer to 4 and 8 in Figure 4.1)>

	MR1	HA0
Source Address	HA Address	HA Address
Destination Address	MR Home Address	MR Home Address
IPsec Protocol	ESP	ESP
SPI	0x126	0x126
Authentication algorithm	HMAC-SHA1-96	HMAC-SHA1-96
Authentication keys	V6LC-126--1234567890	V6LC-126--1234567890
Encryption algorithm	3DES-CBC	3DES-CBC
Encryption keys	V6LC-126--12345678901234	V6LC-126--12345678901234

** HMAC-SHA1-96 and 3DES-CBC must be selected as Authentication algorithm and Encryption algorithm in “Interoperability test scenario for IPv6 Ready Logo Phase 2 program”

****

This documentation is produced by Mobile IPv6 SWG members of Certification WG in the IPv6 Promotion Council.
The SWG members currently include Nippon Telegraph and Telephone Corporation (NTT), Yokogawa Electric Corporation, YASKAWA INFORMATION SYSTEMS Corporation, and NTT Advanced Technology Corporation (NTT-AT).

AUTHOR'S LIST

Tadashi Ito (NTT)

Hiroyuki Ohnishi (NTT)

Takaaki Moriya (NTT)

Harutaka Ueno (NTT)

Hiroshi Miyata (Yokogawa Electric Corporation)

Yukiyo Akisada (Yokogawa Electric Corporation)

Kaoru Inoue (YASKAWA INFORMATION SYSTEMS Corporation)

Mitsuharu Okumura (YASKAWA INFORMATION SYSTEMS Corporation)

Kiyoaki Kawaguchi (YASKAWA INFORMATION SYSTEMS Corporation)

Minako Araki (YASKAWA INFORMATION SYSTEMS Corporation)

Kouichiro Ohgushi (YASKAWA INFORMATION SYSTEMS Corporation)

Shiho Homan (YASKAWA INFORMATION SYSTEMS Corporation)

Aya Ogasawara (YASKAWA INFORMATION SYSTEMS Corporation)

Yoshio Yoshida (NTT-AT)

Takaaki Matsuura (NTT-AT)

Taisuke Sako (NTT-AT)

Kenzo Kodama (NTT-AT)