Experimental Mobile IPv6

Self Test Specification for Mobile Node with IKEv1

Technical Document Version 1.0.2

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



Modification Record

Version 1.0.2 November 1, 2007

Editorial

Title, footer, and copyright were fixed.

Version 1.0.1 July 18, 2006 Correction of cover and Acknowledgements.

Version 1.0.0 June 12, 2006



Acknowledgements

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

Principle Authors:

- IPv6 Promotion Council, Certification Working Group

Commentators:

- IRISA-INRIA



Introduction

The IPv6 forum plays a major role to bring together industrial actors, to develop and deploy the new 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 as a critical feature in the Internet community. Due to the large number of IPv6 implementations, it is important to provide the market a strong signal proving the level of interoperability across various products.

To avoid confusion in the mind of customers, a globally unique logo programme should be defined. The IPv6 logo will give confidence to users that IPv6 is currently operational. It will also be a clear indication that the technology will still be used in the future. To summarize, this logo programme will contribute to the feeling that IPv6 is available and ready to be used.

The IPv6 Logo Programme consists in three phases

Phase 1:

In a 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 a proper care, technical consensus and clear 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 logo "IPv6 Ready" 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.

This document is an experimental enhancing part of "Mobile IPv6" test specification.

"Mobile IPv6 with IKEv1" is experimental and IPv6 Ready Logo doesn't include IKEv1 right now. However, we have sorted out the documents about IKEv1 and we want to publish them here.



Table of Contents

[I] Experimental Mobile IPv6 Self Test Specification for Mobile Node w/ IKEv1

Modification Record	2
Acknowledgements	3
Introduction	4
Table of Contents	5
3 Common Setup	7
3.1 Common Setup-1 (Experimental enhancing part)	7
6. Test Specification: Mobile Node operation	8
6.13 IPsec SA	8
6.13.1 manual configuration	8
6.13.1.1 MN-1-1-2-1-001 - Use the manual configuration of security association between	า
MN and HA	8
6.13.2 auto configuration	11
6.13.2.1 Binding Updates and Acknowledgements	11
6.13.2.1.1 MN-1-2-1-1-001 - Sending BU (Establishing New SA1/SA2)	
6.13.2.1.2 MN-1-2-1-1-002 - Sending BU (Foreign -> Stay, ISAKMP SA expired, IPsed	Э
SA1/SA2 expired)	14
6.13.2.1.3 MN-1-2-1-1-004 - Sending BU (Foreign -> Stay, ISAKMP SA exist, IPsed	3
SA1/SA2 expired)	17
6.13.2.1.4 MN-1-2-1-1-012 - Sending BU (Foreign -> Foreign -> Stay, ISAKMP SA	4
discard, IPsec SA1/SA2 expired)	20
6.13.2.1.5 MN-1-2-1-1-014 - Sending BU (Foreign -> Foreign -> Stay, ISAKMP SA	4
update, IPsec SA1/SA2 expired)	23
6.13.2.1.6 MN-1-2-1-1-022 - Sending BU (Foreign -> Home -> Foreign, ISAKMP SA	4
expired, IPsec SA1/SA2 expired)	26
6.13.2.1.7 MN-1-2-1-1-024 - Sending BU (Foreign -> Home -> Foreign, ISAKMP SA	4
exist, IPsec SA1/SA2 expired)	29
6.13.2.1.8 MN-1-2-1-1-025 - Sending BU (Foreign -> Home -> Foreign, IPsec	3
SA1/SA2 exist)	32
6.13.2.2 Return Routability Signaling	35
6.13.2.2.1 MN-1-2-2-1-001 - Sending HoTI (Establishing New SA3/SA4)	35
6.13.2.2.2 MN-1-2-2-1-002 - Sending HoTI (Foreign -> Stay, ISAKMP SA expired	,
IPsec SA3/SA4 expired)	38
6.13.2.2.3 MN-1-2-2-1-004 - Sending HoTI (Foreign -> Foreign -> Stay, ISAKMP SA	4
discard, IPsec SA3/SA4 expired)	42
6.13.2.2.4 MN-1-2-2-1-006 - Sending HoTI (Foreign -> Foreign -> Stay, ISAKMP SA	4
update, IPsec SA3/SA4 expired)	
6.13.2.2.5 MN-1-2-2-1-018 - Sending HoTI (Security policy entries is inactive)	
6.13.2.2.6 MN-1-2-2-1-010 - Sending HoTI (Foreign -> home -> Foreign, ISAKMP SA	
expired, IPsec SA3/SA4 expired)	



6.13.2.2.7 MN-1-2-2-1-014 - Sending HoTI (Foreign -> home -> Foreign, ISAKMP SA	4
exist, IPsec SA3/SA4 expired)	61
6.13.2.3 Prefix Discovery	66
6.13.2.3.1 MN-1-2-3-1-001 - Sending MPS (Establishing New SA5/SA6)	66
6.13.2.3.2 MN-1-2-3-1-002 - Sending MPS (Foreign -> Stay, ISAKMP SA expired	,
IPsec SA5/SA6 expired)	69
6.13.2.3.3 MN-1-2-3-1-004 - Sending MPS (Foreign -> Foreign -> Stay, ISAKMP SA	4
discard, IPsec SA5/SA6 expired)	72
6.13.2.3.4 MN-1-2-3-1-006 - Sending MPS (Foreign -> Foreign -> Stay, ISAKMP SA	4
update, IPsec SA5/SA6 expired)	75
6.13.2.3.5 MN-1-2-3-1-010 - Sending MPS (Foreign -> Home -> Foreign, ISAKMP SA	4
expired, IPsec SA5/SA6 expired)	78
6.13.2.3.6 MN-1-2-3-1-014 - Sending MPS (Foreign -> Home -> Foreign, ISAKMP SA	4
exist, IPsec SA5/SA6 expired)	82
6.13.2.3.7 MN-1-2-3-1-017 - Sending MPS (Foreign -> Home -> Foreign, IPsec	3
SA5/SA6 exist)	86
ALITHOR'S LIST	20



3 Common Setup

3.1 Common Setup-1 (Experimental enhancing part)

- Set IKE configuration
 - > MN must be the initiator of the Security Association.
 - > MN should establish required IPsecSA as an initiator after ISAKMP SA establishment.



6. Test Specification: Mobile Node operation

There are experimental enhancing parts.

6.13 IPsec SA

6.13.1 manual configuration

6.13.1.1 MN-1-1-2-1-001 - Use the manual configuration of security association between MN and HA

[PURPOSE]

MN-1-1-2-1-001 - Use the manual configuration of security association between MN and HA

[CATEGORY]

HOST: ADVANCED FUNCTION (REAL HOME LINK)

[REQUIREMENT OF TEST]

Function of Real Home Link: YES

[TOPORGY]

Refer to 2.1.1.1 Common Topology-1

[TEST SETUP]

Refer to 3.1 Common Setup-1

[INITIALIZATION]

NONE

		5.4	50	0110
HA0	NUT0	R1	R2	CNO
				I
	>			1.Router Advertisement
	1			
	NUTX			I
				I
	<	-		2.Router Advertisement
				I
<-				3.Neighbor Solicitation(NUD)
				4.(no reply)
				I
<-				5.Binding Update
	>			6.Binding Acknowledgement



		1
NUTO	i	i
	İ	
>		7.Router Advertisement
		I
>		8.Neighbor Solicitation(NUD)
		9.(no reply)
		I
<		10.Binding Update
>		11.Binding Acknowledgement
<		12.Neighbor Advertisement
I I I I NUTX I		1
I MILLX I		.
I I I	l	1
i i i		
		 13.Router Advertisement
i i i		 14.Neighbor Solicitation(NUD)
		 14.Neighbor Solicitation(NUD) 15.(no reply)
		 14.Neighbor Solicitation(NUD)
		14.Neighbor Solicitation(NUD) 15.(no reply) 16.Binding Update (*1)
		14.Neighbor Solicitation(NUD) 15.(no reply) 16.Binding Update (*1)
		14.Neighbor Solicitation(NUD) 15.(no reply) 16.Binding Update (*1) 17.Binding Acknowledgement

- 1. Send Router Advertisement. (HA0 -> HA0_allnode_multi) (Refer to 5.2.2)
- 2. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)
- 3. Receive Neighbor Solicitation(NUD). (NUT0 -> HA0) (Refer to 5.3.3)
- 4. (no reply)
 - # Wait during a maximum of 3 seconds(RFC2461).
- 5. Receive Binding Update to HAO. (NUTX -> HAO) (Refer to 5.14.1)
- 6. Send Binding Acknowledgement. (HA0 -> NUTX) (Refer to 5.15.1)
- 7. Send Router Advertisement. (HA0 -> HA0_allnode_multi) (Refer to 5.2.2)
- 8. Receive Neighbor Solicitation(NUD). (NUTX -> R1) (Refer to 5.3.3)
- 9. (no reply)
 - # Wait during a maximum of 3 seconds(RFC2461).
- 10. Receive Binding Update to HA0. (NUT0 -> HA0) (Refer to 5.14.1)
- 11. Send Binding Acknowledgement. (HA0 -> NUT0) (Refer to 5.15.1)
- 12. Receive Neighbor Advertisement. (NUT0 -> NUT0_allnode_multi) (Refer to 5.4.1)
- 13. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)
- 14. Receive Neighbor Solicitation(NUD). (NUT0 -> HA0) (Refer to 5.3.3)
- 15. (no reply)



Wait during a maximum of 3 seconds(RFC2461).

16. Receive Binding Update to HAO. (NUTX -> HAO) (*1) (Refer to 5.14.1)

IPv6 Header	Source Address	MN care-of (global)	
	Destination Add	HA (global)	
Destination Option Header	Home Address	MN home (global)	
Encapsulating	Security Param	Any	
Security	Sequence	Any	
Payload	Initialization Ve	Any	
Mobility Header	MH Type		5
Mobility options	Alternate	Туре	3
•	Care-of Address	Option Length	16
		Address	MN care-of

17. Send Binding Acknowledgement. (HA0 -> NUTX) (Refer to 5.15.1)

IPv6 Header	Source Address	HA (global)
	Destination Address	MN care-of (global)
Type2 Routing Header	Home Address	MN (global)
Encapsulating	Security Parameter Index	Any
Security	Sequence	Any
Payload	Initialization Vector	Any
Mobility Header	MH Type	6

- 18. Send ICMP Echo Request. (HA0 -> NUTX with Type2 Routing Header) (Refer to 5.7.3)
- 19. Receive ICMP Echo Reply. (NUTX -> HA0 with Home Address Option) (*2) (Refer to 5.8.3)

[JUDGMENT]

(*1) PASS: HA0 receives Binding Update.

Then, check whether this packet fills all of the following.

- The ESP header is included.
- The Acknowledge(A) bit is set to ON.
- The Home Registration(H) bit is set to ON.
- The Alternate Care-of Address mobility option is included.
 - The Care-of Address field is set to the Care-of Address.
- (*2) PASS: HA0 receives ICMP Echo Reply with Home Address Option.

[REFERENCES]

RFC3775 Mobility Support in IPv6 See Section 11.7.1, 6.1.7

RFC3776 Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents

See Section 4.2



6.13.2 auto configuration

6.13.2.1 Binding Updates and Acknowledgements

6.13.2.1.1 MN-1-2-1-1-001 - Sending BU (Establishing New SA1/SA2)

[PURPOSE]

MN-1-2-1-1-001 - Sending BU (Establishing New SA1/SA2)

[CATEGORY]

HOST: ADVANCED FUNCTION (IKE)

[REQUIREMENT OF TEST]

Function of IKE: YES

[TOPORGY]

Refer to 2.1.1.1 Common Topology-1

[TEST SETUP]

Refer to 3.1 Common Setup-1

[INITIALIZATION]

• In the case of Real Home Link

HA0	NUT0	R1	R2	CNO
1	1	- 1	- 1	1
	>		- 1	1.Router Advertisement
				I
	NUTX			I
	- 1			I
	<			2.Router Advertisement
	1			I
<-				3.Neighbor Solicitation
	1			4.(no reply)
1	1			1

- 1. Send Router Advertisement. (HA0 -> HA0_allnode_multi) (Refer to 5.2.2)
- 2. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)
- 3. Receive Neighbor Solicitation. (NUT0 -> HA0) (Refer to 5.3.3)
- 4. (no reply)
- In the case of Virtual Home Link

HA0	NUTX	R1	R2	CNO
		1	- 1	



| | <---- | | 1.Router Advertisement

1. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)

[PROCEDURE]

HA0	NUTX	R1	R2	CNO
		- 1	- 1	1
	<			1.Router Advertisement
		- 1		1
<==	==>	- 1		a.IKE Phase1 (ISAKMP SA)
<==	==> ==>	- 1		b.IKE Phase2 (IPsec SA1/SA2)
	- 1	- 1		1
<		- 1		2.Binding Update (*1)
	>	- 1		3.Binding Acknowledgement
	- 1	- 1		1
	>	- 1	- 1	4.ICMP Echo Request
<				5.ICMP Echo Reply (*2)
	1			

- 1. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)
- a. IKE Phase1 (ISAKMP SA)
- b. IKE Phase2 (IPsec SA1/SA2)
- 2. Receive Binding Update. (NUTX -> HA0) (*1) (Refer to 5.14.1)

IPv6 Header	Source Address	MN care-of (global)	
	Destination Add	Iress	HA (global)
Destination Option Header	Home Address	MN home (global)	
Encapsulating	Security Param	Any	
Security	Sequence	Any	
Payload	Initialization Ve	Any	
Mobility Header	MH Type		5
Mobility options	Alternate	Туре	3
	Care-of Address	Option Length	16
A		Address	MN care-of

- 3. Send Binding Acknowledgement. (HA0 -> NUTX) (Refer to 5.15.1)
- 4. Send ICMP Echo Request. (HA0 -> NUTX with Type2 Routing Header) (Refer to 5.7.3)
- 5. Receive ICMP Echo Reply. (NUTX -> HA0 with Home Address Option) (*2) (Refer to 5.8.3)

[JUDGMENT]

(*1) PASS: HA0 receives Binding Update.

Then, check whether this packet fills all of the following,

- using new IPsec SA1.
- (*2) PASS: HA0 receives ICMP Echo Reply with Home Address Option.



[REFERENCES]

RFC3775 Mobility Support in IPv6 See Section 11.3.2

RFC3776 Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents

See Section 4.4



6.13.2.1.2 MN-1-2-1-1-002 - Sending BU (Foreign -> Stay, ISAKMP SA expired, IPsec SA1/SA2 expired)

[PURPOSE]

MN-1-2-1-1-002 - Sending BU (Foreign -> Stay, ISAKMP SA expired, IPsec SA1/SA2 expired)

[CATEGORY]

HOST: ADVANCED FUNCTION (IKE)

[REQUIREMENT OF TEST]

Function of IKE: YES

[TOPORGY]

Refer to 2.1.1.1 Common Topology-1

[TEST SETUP]

Refer to 3.1 Common Setup-1

[INITIALIZATION]

• In the case of Real Home Link

HA0	NUT0	R1	R2	CNO
				1
	>			1.Router Advertisement
				I
	NUTX			1
				1
	<			2.Router Advertisement
				1
<-				3.Neighbor Solicitation
				4.(no reply)
- 1				

- 1. Send Router Advertisement. (HA0 -> HA0_allnode_multi) (Refer to 5.2.2)
- 2. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)
- 3. Receive Neighbor Solicitation. (NUT0 -> HA0) (Refer to 5.3.3)
- 4. (no reply)
- In the case of Virtual Home Link

HA0	NUTX	R1	R2	CNO	
		1			
	<	-		1.Router Advertisemen	t
- 1	1	1	1		



1. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)

HAO	NUTX	R1	R2	CNO
1	1		1	
1	<		1	1.Router Advertisement
1		1	1	
<===	⇒		1	a.IKE Phase1 (ISAKMP SA)
<===	>		1	b.IKE Phase2 (IPsec SA1/SA2)
1	1		1	
<			1	2.Binding Update
	·>		1	3.Binding Acknowledgement
1	1		1	
1	1		1	:
1				I
1				c.(expire ISAKMP SA)
<===	=>			d1.IKE Phase1 (ISAKMP SA)
1				I
				:
				I
				e.(expire IPsec SA1/SA2)
<===	⇒			d2.IKE Phase1 (ISAKMP SA)
<===	⇒			f.IKE Phase2 (IPsec SA1/SA2) (*1)
<	·-		1	4.Binding Update (*2)
	·>			5.Binding Acknowledgement
1			1	1
	·>		1	6.ICMP Echo Request
<	·-		1	7.ICMP Echo Reply (*3)
1	1	1		

- 1. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)
- a. IKE Phase1 (ISAKMP SA)
- b. IKE Phase2 (IPsec SA1/SA2)
- 2. Receive Binding Update. (NUTX -> HA0) (Refer to 5.14.1)
- 3. Send Binding Acknowledgement. (HA0 -> NUTX) (Refer to 5.15.1)
- c. (expire ISAKMP SA)
- d1. IKE Phase1 (ISAKMP SA) or [d2]
- e. (expire IPsec SA1/SA2)
- d2. [d1] or IKE Phase1 (ISAKMP SA)
- f. IKE Phase2 (IPsec SA1/SA2) (*1)



4. Receive Binding Update. (NUTX -> HA0) (*2) (Refer to 5.14.1)

IPv6 Header	Source Address	5	MN care-of (global)	
	Destination Add	HA (global)		
Destination Option Header	Home Address		MN home (global)	
Encapsulating	Security Param	eter Index	Any	
Security	Sequence		Any	
Payload	Initialization Ve	ctor	Any	
Mobility Header	MH Type		5	
Mobility options	Mobility options Alternate		3	
	Care-of	Option Length	16	
	Address	Address	MN care-of	

- 5. Send Binding Acknowledgement. (HA0 -> NUTX) (Refer to 5.15.1)
- 6. Send ICMP Echo Request. (HA0 -> NUTX with Type2 Routing Header) (Refer to 5.7.3)
- 7. Receive ICMP Echo Reply. (NUTX -> HA0 with Home Address Option) (*3) (Refer to 5.8.3)

[JUDGMENT]

- (*1) PASS: IPsec SA1/SA2 is re-established after re-establishing ISAKMP SA.
- (*2) PASS: HA0 receives Binding Update.
 - Then, check whether this packet fills all of the following,
 - using new IPsec SA1.
- (*3) PASS: HA0 receives ICMP Echo Reply with Home Address Option.

[REFERENCES]

RFC3775 Mobility Support in IPv6 See Section 11.3.2



6.13.2.1.3 MN-1-2-1-1-004 - Sending BU (Foreign -> Stay, ISAKMP SA exist, IPsec SA1/SA2 expired)

[PURPOSE]

MN-1-2-1-1-004 - Sending BU (Foreign -> Stay, ISAKMP SA exist, IPsec SA1/SA2 expired)

[CATEGORY]

HOST: ADVANCED FUNCTION (IKE)

[REQUIREMENT OF TEST]

Function of IKE: YES

[TOPORGY]

Refer to 2.1.1.1 Common Topology-1

[TEST SETUP]

Refer to 3.1 Common Setup-1

[INITIALIZATION]

• In the case of Real Home Link

HA0	NUT0	R1	R2	CNO
-	1	- 1		1
	>	- 1		1.Router Advertisement
	1	- 1		I
	NUTX	- 1		I
	1	- 1		I
	<			2.Router Advertisement
	1	- 1		1
<-		- 1		3.Neighbor Solicitation
	1	- 1		4.(no reply)
-	1	-		1

- 1. Send Router Advertisement. (HA0 -> HA0_allnode_multi) (Refer to 5.2.2)
- 2. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)
- 3. Receive Neighbor Solicitation. (NUT0 -> HA0) (Refer to 5.3.3)
- 4. (no reply)
- In the case of Virtual Home Link

HA0	NUTX	R1	R2	CNO	
		1			
	<	-		1.Router Advertisemen	t
- 1	1	1	1		



1. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)

[PROCEDURE]

HA0	NUTX	R1	R2	CNO
	1			
	<-			1.Router Advertisement
	- 1			
<==	:=>			a.IKE Phase1 (ISAKMP SA)
<==	:=>			b.IKE Phase2 (IPsec SA1/SA2)
	1			
<				2.Binding Update
	->			3.Binding Acknowledgement
	1			
	- 1			:
	1			
	1			c.(expire IPsec SA1/SA2)
<==	:=>			d.IKE Phase2 (IPsec SA1/SA2) (*1)
1	- 1			
<				4.Binding Update (*2)
	->			5.Binding Acknowledgement
	- 1			
	->			6.ICMP Echo Request
<				7.ICMP Echo Reply (*3)
1	- 1		1	1

- 1. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)
- a. IKE Phase1 (ISAKMP SA)
- b. IKE Phase2 (IPsec SA1/SA2)
- 2. Receive Binding Update. (NUTX -> HA0) (Refer to 5.14.1)
- 3. Send Binding Acknowledgement. (HA0 -> NUTX) (Refer to 5.15.1)
- c. (expire IPsec SA1/SA2)
- d. IKE Phase2 (IPsec SA1/SA2) (*1)
- 4. Receive Binding Update. (NUTX -> HA0) (*2) (Refer to 5.14.1)

IPv6 Header	Source Address	MN care-of (global)	
	Destination Add	HA (global)	
Destination Option Header	Home Address		MN home (global)
Encapsulating	Security Param	eter Index	Any
Security	Sequence		Any
Payload	Initialization Ved	Any	
Mobility Header	MH Type		5
Mobility options	options Alternate Care-of Address	Туре	3
		Option Length	16
		Address	MN care-of

5. Send Binding Acknowledgement. (HA0 -> NUTX) (Refer to 5.15.1)



- 6. Send ICMP Echo Request. (HA0 -> NUTX with Type2 Routing Header) (Refer to 5.7.3)
- 7. Receive ICMP Echo Reply. (NUTX -> HA0 with Home Address Option) (*3) (Refer to 5.8.3)

[JUDGMENT]

- (*1) PASS: IPsec SA1/SA2 is re-established.
- (*2) PASS: HA0 receives Binding Update.
 - Then, check whether this packet fills all of the following,
 - using new IPsec SA1.
- $(\ensuremath{^*}3)$ PASS: HA0 receives ICMP Echo Reply with Home Address Option.

[REFERENCES]

RFC3775 Mobility Support in IPv6 See Section 11.3.2



6.13.2.1.4 MN-1-2-1-1-012 - Sending BU (Foreign -> Foreign -> Stay, ISAKMP SA discard, IPsec SA1/SA2 expired)

[PURPOSE]

MN-1-2-1-1-012 - Sending BU (Foreign -> Foreign -> Stay, ISAKMP SA discard, IPsec SA1/SA2 expired)

[CATEGORY]

HOST: ADVANCED FUNCTION (IKE)

[REQUIREMENT OF TEST]

Function of IKE: YES

[TOPORGY]

Refer to 2.1.1.1 Common Topology-1

[TEST SETUP]

Refer to 3.1 Common Setup-1

[INITIALIZATION]

• In the case of Real Home Link

HA0	NUTO	R1	R2	CNO
	1		- 1	1
	>			1.Router Advertisement
				I
	NUTX			I
				I
	<			2.Router Advertisement
				I
<-				3.Neighbor Solicitation
				4.(no reply)
- 1		- 1		

- 1. Send Router Advertisement. (HA0 -> HA0_allnode_multi) (Refer to 5.2.2)
- 2. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)
- 3. Receive Neighbor Solicitation. (NUT0 -> HA0) (Refer to 5.3.3)
- 4. (no reply)
- In the case of Virtual Home Link

HA0	NUTX	R1	R2	CNO
		1	- 1	I
	<		- 1	1.Router Advertisement
		1		1



1. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)

LDUK	_,				
HA0	NUT	ГХ	R1	R2	CNO
			1		
		<			1.Router Advertisement
				1	1
<=	==>			1	a.IKE Phase1 (ISAKMP SA)
<=	==>			1	b.IKE Phase2 (IPsec SA1/SA2)
				1	1
<-				1	2.Binding Update
	>			1	3.Binding Acknowledgement
1				1	1
-		<		1	4.Router Advertisement
1				1	1
<-				1	5.Binding Update
	>		Ì	Ì	6.Binding Acknowledgement
			1	1	ſ
İ			İ	İ	c.(discard ISAKMP SA)
<=	==>		İ	Ì	d1.IKE Phase1 (ISAKMP SA)
Ì			İ	Ì	Ì
İ			İ	İ	i:
i	İ	· 	İ	i	Ì
i			i	i	e.(expire IPsec SA1/SA2)
· <=	==>		İ	i	d2.IKE Phase1 (ISAKMP SA)
· <=	==>		İ	i	f.IKE Phase2 (IPsec SA1/SA2) (*1)
i			i	i	, , ,
<-			i	i	7.Binding Update (*2)
'	>	ļ	i	i	8.Binding Acknowledgement
i			i	i	
	>	' 	i	i	9.ICMP Echo Request
		 	İ	i	10.1CMP Echo Reply (*3)
'	'	 	İ	i	
ı	- 1	l	1	I	I

- 1. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)
- a. IKE Phase1 (ISAKMP SA)
- b. IKE Phase2 (IPsec SA1/SA2)
- 2. Receive Binding Update. (NUTX -> HA0) (Refer to 5.14.1)
- 3. Send Binding Acknowledgement. (HA0 -> NUTX) (Refer to 5.15.1)
- 4. Send Router Advertisement. (R2 -> R2_allnode_multi) (Refer to 5.2.1)
- 5. Receive Binding Update. (NUTY -> HA0) (Refer to 5.14.1) # (K)bit on/off



- 6. Send Binding Acknowledgement. (HA0 -> NUTY) (Refer to 5.15.1) # (K)bit off
- c. (discard ISAKMP SA)
- d1. IKE Phase1 (ISAKMP SA) or [d2]
- e. (expire IPsec SA1/SA2)
- d2. [d1] or IKE Phase1 (ISAKMP SA)
- f. IKE Phase2 (IPsec SA1/SA2) (*1)
- 7. Receive Binding Update. (NUTY -> HA0) (*2) (Refer to 5.14.1)

IPv6 Header	Source Address	MN care-of (global)				
	Destination Add	Iress	HA (global)			
Destination Option Header	Home Address		MN home (global)			
Encapsulating	Security Param	eter Index	Any			
Security	Sequence	Any				
Payload	Initialization Ve	Any				
Mobility Header	MH Type		5			
Mobility options	Alternate	Туре	3			
	Care-of	Option Length	16			
	Address	Address	MN care-of			

- 8. Send Binding Acknowledgement. (HA0 -> NUTY) (Refer to 5.15.1)
- 9. Send ICMP Echo Request. (HA0 -> NUTY with Type2 Routing Header) (Refer to 5.7.3)
- 10. Receive ICMP Echo Reply. (NUTY -> HA0 with Home Address Option) (Refer to 5.8.3)

[JUDGMENT]

- (*1) PASS: IPsec SA1/SA2 is re-established after re-establishing ISAKMP SA.
- (*2) PASS: HA0 receives Binding Update.

Then, check whether this packet fills all of the following,

- using new IPsec SA1.
- (*3) PASS: HA0 receives ICMP Echo Reply with Home Address Option.

[REFERENCES]

RFC3775 Mobility Support in IPv6 See Section 11.7.3



6.13.2.1.5 MN-1-2-1-1-014 - Sending BU (Foreign -> Foreign -> Stay, ISAKMP SA update, IPsec SA1/SA2 expired)

[PURPOSE]

MN-1-2-1-014 - Sending BU (Foreign -> Foreign -> Stay, ISAKMP SA update, IPsec SA1/SA2 expired)

[CATEGORY]

HOST: ADVANCED FUNCTION (IKE)

[REQUIREMENT OF TEST]

Function of IKE: YES

NUT sets (K) bit in BU which is transmitted to HA: YES

[TOPORGY]

Refer to 2.1.1.1 Common Topology-1

[TEST SETUP]

Refer to 3.1 Common Setup-1

[INITIALIZATION]

• In the case of Real Home Link

HA0	NUT0	R1	R2	CNO
-				1
-	>			1.Router Advertisement
				1
	NUTX			1
				1
	<-			2.Router Advertisement
				1
<				3.Neighbor Solicitation
				4.(no reply)
				1

- 1. Send Router Advertisement. (HA0 -> HA0_allnode_multi) (Refer to 5.2.2)
- 2. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)
- 3. Receive Neighbor Solicitation. (NUT0 -> HA0) (Refer to 5.3.3)
- 4. (no reply)
- In the case of Virtual Home Link

HA0	NUTX	R1	R2	CNO
		1		I
	<			1.Router Advertisement



1. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)

HA0	NUTX	R1	R2	CNO
			1	1
	<	1		1.Router Advertisement
<==	=>		1	a.IKE Phase1 (ISAKMP SA)
<==	=>		1	b.IKE Phase2 (IPsec SA1/SA2)
			1	1
'			1	2.Binding Update
	->		!	3.Binding Acknowledgement
l			1	
	<		1	4.Router Advertisement
			1	
•		1		5.Binding Update
	->		1	6.Binding Acknowledgement
		1	1	(undata ISAKMD SA)
1	 	1	1	c.(update ISAKMP SA)
l I	 	1	1	1
1	l I	l I	1	1 •
l I	l I	l I	l I	d.(expire IPsec SA1/SA2)
 <==	->	1	i I	e.IKE Phase2 (IPsec SA1/SA2) (*1)
\	I	1	i I	0.1112 1110302 (11300 0/11/0/12) (1)
<		 	i	7.Binding Update (*2)
•	->	' 	i	8.Binding Acknowledgement
İ	İ	1		
	->	i	i	9.ICMP Echo Request
· <		İ	i	10.ICMP Echo Reply (*3)
i	İ		İ	. , ,

- 1. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)
- a. IKE Phase1 (ISAKMP SA)
- b. IKE Phase2 (IPsec SA1/SA2)
- 2. Receive Binding Update. (NUTX -> HA0) (Refer to 5.14.1)
- 3. Send Binding Acknowledgement. (HA0 -> NUTX) (Refer to 5.15.1)
- 4. Send Router Advertisement. (R2 -> R2_allnode_multi) (Refer to 5.2.1)
- 5. Receive Binding Update. (NUTY -> HA0) (Refer to 5.14.1) # (K)bit on
- 6. Send Binding Acknowledgement. (HA0 -> NUTY) (Refer to 5.15.1)



(K)bit on

- c. (update ISAKMP SA)
- d. (expire IPsec SA1/SA2)
- e. IKE Phase2 (IPsec SA1/SA2) (*1)
- 7. Receive Binding Update. (NUTY -> HA0) (*2) (Refer to 5.14.1)

IPv6 Header	Source Address	5	MN care-of (global)
	Destination Add	dress	HA (global)
Destination Option Header	Home Address		MN home (global)
Encapsulating	Security Param	eter Index	Any
Security	ecurity Sequence		Any
Payload	Initialization Ve	ctor	Any
Mobility Header	MH Type		5
Mobility options	Alternate	Type	3
Care-of Address		Option Length	16
	Address	Address	MN care-of

- 8. Send Binding Acknowledgement. (HA0 -> NUTY) (Refer to 5.15.1)
- 9. Send ICMP Echo Request. (HA0 -> NUTY with Type2 Routing Header) (Refer to 5.7.3)
- 10. Receive ICMP Echo Reply. (NUTY -> HA0 with Home Address Option) (*3) (Refer to 5.8.3)

[JUDGMENT]

- (*1) PASS: IPsec SA1/SA2 is re-established without re-establishment of ISAKMP SA.
- (*2) PASS: HA0 receives Binding Update.
 - Then, check whether this packet fills all of the following,
 - using new IPsec SA1.
- (*3) PASS: HA0 receives ICMP Echo Reply with Home Address Option.

[REFERENCES]

RFC3775 Mobility Support in IPv6 See Section 11.7.1, 11.7.3



6.13.2.1.6 MN-1-2-1-1-022 - Sending BU (Foreign -> Home -> Foreign, ISAKMP SA expired, IPsec SA1/SA2 expired)

[PURPOSE]

MN-1-2-1-1-022 - Sending BU (Foreign -> Home -> Foreign, ISAKMP SA expired, IPsec SA1/SA2 expired)

[CATEGORY]

HOST: ADVANCED FUNCTION (IKE)

[REQUIREMENT OF TEST]

Function of IKE: YES

Function of Real Home Link: YES

[TOPORGY]

Refer to 2.1.1.1 Common Topology-1

[TEST SETUP]

Refer to 3.1 Common Setup-1

[INITIALIZATION]

HA0	NUT0	R1	R2	CNO
-		- 1	1	I
	>			1.Router Advertisement
				I
	NUTX		- 1	I
			1	I
	<			2.Router Advertisement
			1	I
<-			1	3.Neighbor Solicitation
		- 1	1	4.(no reply)
		- 1	1	I

- 1. Send Router Advertisement. (HA0 -> HA0_allnode_multi) (Refer to 5.2.2)
- 2. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)
- 3. Receive Neighbor Solicitation. (NUT0 -> HA0) (Refer to 5.3.3)
- 4. (no reply)

HA0	NUTX	R1	R2	CNO
		1		I
	<			1.Router Advertisement
				1
<=	==>	- 1		a.IKE Phase1 (ISAKMP SA)
<=	==>	1		b.IKE Phase2 (IPsec SA1/SA2)



	 2.Binding Update 3.Binding Acknowledgement
NUTO	
	 4.Router Advertisement
	5.Binding Update 6.Binding Acknowledgement
	7.Neighbor Advertisement
	 c.(expire ISAKMP SA)
	 d.(expire IPsec SA1/SA2)
NUTX	
	 8.Router Advertisement
	e.IKE Phase1 (ISAKMP SA) f.IKE Phase2 (IPsec SA1/SA2) (*1)
	 9.Binding Update (*2) 10.Binding Acknowledgement
	 11.ICMP Echo Request 12.ICMP Echo Reply (*3)

- 1. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)
- a. IKE Phase1 (ISAKMP SA)
- b. IKE Phase2 (IPsec SA1/SA2)
- 2. Receive Binding Update. (NUTX -> HA0) (Refer to 5.14.1)
- 3. Send Binding Acknowledgement. (HA0 -> NUTX) (Refer to 5.15.1)
- 4. Send Router Advertisement. (HA0 -> HA0_allnode_multi) (Refer to 5.2.2)
- 5. Receive Binding Update. (NUT0 -> HA0) (Refer to 5.14.1)
- 6. Send Binding Acknowledgement. (HA0 -> NUT0) (Refer to 5.15.1)



- 7. Receive Neighbor Advertisement. (NUT0(Unspecified) -> HA0_allnode_multi) (Refer to 5.4.1)
- c. (expire ISAKMP SA)
- d. (expire IPsec SA1/SA2)
- 8. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)
- e. IKE Phase1 (ISAKMP SA)
- f. IKE Phase2 (IPsec SA1/SA2) (*1)
- 9. Receive Binding Update. (NUTX -> HA0) (*2) (Refer to 5.14.1)

IPv6 Header	Source Address	5	MN care-of (global)
	dress	HA (global)	
Destination Option Header	Home Address		MN home (global)
Encapsulating	Security Param	eter Index	Any
Security	Sequence	Any	
Payload	Initialization Ve	Any	
Mobility Header	MH Type		5
Mobility options	Alternate	Туре	3
	Care-of	Option Length	16
Address	Address	Address	MN care-of

- 10. Send Binding Acknowledgement. (HA0 -> NUTX) (Refer to 5.15.1)
- 11. Send ICMP Echo Request. (HA0 -> NUTX with Type2 Routing Header) (Refer to 5.7.3)
- 12. Receive ICMP Echo Reply. (NUTX -> HA0 with Home Address Option) (*3) (Refer to 5.8.3)

[JUDGMENT]

- (*1) PASS: IPsec SA1/SA2 is re-established after re-establishing ISAKMP SA.
- (*2) PASS: HA0 receives Binding Update.
 - Then, check whether this packet fills all of the following,
 - using new IPsec SA1.
- (*3) PASS: HA0 receives ICMP Echo Reply with Home Address Option.

[REFERENCES]

RFC3776 Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents

See Section 4.2



6.13.2.1.7 MN-1-2-1-1-024 - Sending BU (Foreign -> Home -> Foreign, ISAKMP SA exist, IPsec SA1/SA2 expired)

[PURPOSE]

MN-1-2-1-1-024 - Sending BU (Foreign -> Home -> Foreign, ISAKMP SA exist, IPsec SA1/SA2 expired)

[CATEGORY]

HOST: ADVANCED FUNCTION (IKE)

[REQUIREMENT OF TEST]

Function of IKE: YES

Function of Real Home Link: YES

[TOPORGY]

Refer to 2.1.1.1 Common Topology-1

[TEST SETUP]

Refer to 3.1 Common Setup-1

[INITIALIZATION]

HA0	NUT0	R1	R2	CNO
1	1	1		I
	>			1.Router Advertisement
				I
	NUTX			I
				I
	<			2.Router Advertisement
		- 1		I
<-		- 1		3.Neighbor Solicitation
				4.(no reply)
		- 1		I

- 1. Send Router Advertisement. (HA0 -> HA0_allnode_multi) (Refer to 5.2.2)
- 2. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)
- 3. Receive Neighbor Solicitation. (NUT0 -> HA0) (Refer to 5.3.3)
- 4. (no reply)

HA0	NUTX	R1	R2	CNO
			1	I
	<		- 1	1.Router Advertisement
				I
<=	==>			a.IKE Phase1 (ISAKMP SA)
<=	==>		- 1	b.IKE Phase2 (IPsec SA1/SA2)



	 	 2.Binding Update 3.Binding Acknowledgement
I I I NUTO		1
		4.Router Advertisement
		5.Binding Update 6.Binding Acknowledgement
		 7.Neighbor Advertisement
		 :
	İ	c.(expire ISAKMP SA)
NUTX		
		8.Router Advertisement
		d.IKE Phase1 (ISAKMP SA) e.IKE Phase2 (IPsec SA1/SA2) (*1)
	 	 9.Binding Update (*2) 10.Binding Acknowledgement
	 	 11.ICMP Echo Request 12.ICMP Echo Reply (*3)

- 1. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)
- a. IKE Phase1 (ISAKMP SA)
- b. IKE Phase2 (IPsec SA1/SA2)
- 2. Receive Binding Update. (NUTX -> HA0) (Refer to 5.14.1)
- 3. Send Binding Acknowledgement. (HA0 -> NUTX) (Refer to 5.15.1)
- 4. Send Router Advertisement. (HA0 -> HA0_allnode_multi) (Refer to 5.2.2)
- 5. Receive Binding Update. (NUT0 -> HA0) (Refer to 5.14.1)
- 6. Send Binding Acknowledgement. (HA0 -> NUT0) (Refer to 5.15.1)
- 7. Receive Neighbor Advertisement. (NUT0(Unspecified) -> HA0_allnode_multi) (Refer to 5.4.1)
- c. (expire ISAKMP SA)



- 8. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)
- d. IKE Phase1 (ISAKMP SA)
- e IKE Phase2 (IPsec SA1/SA2) (*1)
- 9. Receive Binding Update. (NUTX -> HA0) (*2) (Refer to 5.14.1)

IPv6 Header	Source Address	5	MN care-of (global)
	Destination Add	dress	HA (global)
Destination Option Header	Home Address		MN home (global)
Encapsulating	Security Param	eter Index	Any
Security	Sequence		Any
Payload	Initialization Ve	ctor	Any
Mobility Header	MH Type		5
Mobility options	Alternate	Туре	3
	Care-of	Option Length	16
Address	Address	Address	MN care-of

- 10. Send Binding Acknowledgement. (HA0 -> NUTX) (Refer to 5.15.1)
- 11. Send ICMP Echo Request. (HA0 -> NUTX with Type2 Routing Header) (Refer to 5.7.3)
- 12. Receive ICMP Echo Reply. (NUTX -> HA0 with Home Address Option) (*3) (Refer to 5.8.3)

[JUDGMENT]

- (*1) PASS: IPsec SA1/SA2 is re-established.
- (*2) PASS: HA0 receives Binding Update.
 - Then, check whether this packet fills all of the following,
 - using new IPsec SA1.
- (*3) PASS: HA0 receives ICMP Echo Reply with Home Address Option.

[REFERENCES]

RFC3776 Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents

See Section 4.2



6.13.2.1.8 MN-1-2-1-1-025 - Sending BU (Foreign -> Home -> Foreign, IPsec SA1/SA2 exist)

[PURPOSE]

MN-1-2-1-1-025 - Sending BU (Foreign -> Home -> Foreign, IPsec SA1/SA2 exist)

[CATEGORY]

HOST: ADVANCED FUNCTION (IKE)

[REQUIREMENT OF TEST]

Function of IKE: YES

Function of Real Home Link: YES

[TOPORGY]

Refer to 2.1.1.1 Common Topology-1

[TEST SETUP]

Refer to 3.1 Common Setup-1

[INITIALIZATION]

HA0	NUT0	R1	R2	CNO
1				1
	>			1.Router Advertisement
				1
	NUTX			1
				1
	<			2.Router Advertisement
				1
<-				3.Neighbor Solicitation
				4.(no reply)
1				1

- 1. Send Router Advertisement. (HA0 -> HA0_allnode_multi) (Refer to 5.2.2)
- 2. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)
- 3. Receive Neighbor Solicitation. (NUT0 -> HA0) (Refer to 5.3.3)
- 4. (no reply)

HA0	NUTX	R1	R2	CNO
-			- 1	1
	<		- 1	1.Router Advertisement
			1	1
<=	==>		- 1	a.IKE Phase1 (ISAKMP SA)
<=	==>		- 1	b.IKE Phase2 (IPsec SA1/SA2)
			- 1	1
<-			1	2.Binding Update



>		1	3.Binding Acknowledgement
	1		I
NUTO	1		I
1			I
>			4.Router Advertisement
	1		I
<	1		5.Binding Update
>	1		6.Binding Acknowledgement
1			I
<			7.Neighbor Advertisement
			1
NUTX	1		I
	1		I
<	-		8.Router Advertisement
1			I
<			9.Binding Update (*1)
>	1		10.Binding Acknowledgement
1	1		I
>			11.ICMP Echo Request
<	1		12.ICMP Echo Reply (*2)
1			I

- 1. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)
- a. IKE Phase1 (ISAKMP SA)
- b. IKE Phase2 (IPsec SA1/SA2)
- 2. Receive Binding Update. (NUTX -> HA0) (Refer to 5.14.1)
- 3. Send Binding Acknowledgement. (HA0 -> NUTX) (Refer to 5.15.1)
- 4. Send Router Advertisement. (HA0 -> HA0_allnode_multi) (Refer to 5.2.2)
- 5. Receive Binding Update. (NUT0 -> HA0) (Refer to 5.14.1)
- 6. Send Binding Acknowledgement. (HA0 -> NUT0) (Refer to 5.15.1)
- 7. Receive Neighbor Advertisement. (NUT0(Unspecified) -> HA0_allnode_multi) (Refer to 5.4.1)
- 8. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)
- 9. Receive Binding Update. (NUTX -> HA0) (*1) (Refer to 5.14.1)

Source Address	(global)	
Destination Add	HA (global)	
Home Address		MN home (global)
Security Param	eter Index	Any
Sequence		Any
Initialization Ve	ctor	Any
MH Type		5
Alternate Care-of Address	Туре	3
	Option Length	16
	Address	MN care-of
	Destination Add Home Address Security Param Sequence Initialization Ve MH Type Alternate Care-of	Security Parameter Index Sequence Initialization Vector MH Type Alternate Care-of Option Length

- 10. Send Binding Acknowledgement. (HA0 -> NUTX) (Refer to 5.15.1)
- 11. Send ICMP Echo Request. (HA0 -> NUTX with Type2 Routing Header)



(Refer to 5.7.3)

12. Receive ICMP Echo Reply. (NUTX -> HA0 with Home Address Option) (*2) (Refer to 5.8.3)

[JUDGMENT]

(*1) PASS: HA0 receives Binding Update.

Then, check whether this packet fills all of the following,

- using old IPsec SA1.

(*2) PASS: HA0 receives ICMP Echo Reply with Home Address Option.

[REFERENCES]

RFC3776 Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents

See Section 4.2



6.13.2.2 Return Routability Signaling

6.13.2.2.1 MN-1-2-2-1-001 - Sending HoTI (Establishing New SA3/SA4)

[PURPOSE]

MN-1-2-2-1-001 - Sending HoTI (Establishing New SA3/SA4)

[CATEGORY]

HOST: ADVANCED FUNCTION (IKE (AND RETURN ROUTABILITY))

[REQUIREMENT OF TEST]

Function of IKE: YES

Function of Return Routability: YES

[TOPORGY]

Refer to 2.1.1.1 Common Topology-1

[TEST SETUP]

Refer to 3.1 Common Setup-1

[INITIALIZATION]

• In the case of Real Home Link

HAO	NUTO	R1	R2	CNO
	1			I
	>			1.Router Advertisement
	1			I
	NUTX			I
				I
	<	-		2.Router Advertisement
				I
<-				3.Neighbor Solicitation
				4.(no reply)
	1			1

- 1. Send Router Advertisement. (HA0 -> HA0_allnode_multi) (Refer to 5.2.2)
- 2. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)
- 3. Receive Neighbor Solicitation. (NUT0 -> HA0) (Refer to 5.3.3)
- 4. (no reply)
- In the case of Virtual Home Link

HA0	NUTX	R1	R2	CNO
		1		I
	<		1	1.Router Advertisement



1. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)

HAO NUT	ГХ І	R1 F	R2	CNO
		l		I
	<			1.Router Advertisement
				I
<===>				a.IKE Phase1 (ISAKMP SA)
<===>				b.IKE Phase2 (IPsec SA1/SA2)
				I
<				2.Binding Update
>				3.Binding Acknowledgement
		l	l	
<===>				c.IKE Phase2 (IPsec SA3/SA4)
<===>				d.IKE Phase2 (IPsec SA7/SA8)
				(It is if required)
====>	<			4.ICMP Echo Request
		 	l	5 Home Test Init (*1)
<====				1
	l			
				7.Care-of Test
====>	<			8.Home test
		l	l	
<====				9.ICMP Echo Reply
			>	10.Binding Update (*2)
			>	11.ICMP Echo Reply
			l	

- 1. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)
- a. IKE Phase1 (ISAKMP SA)
- b. IKE Phase2 (IPsec SA1/SA2)
- 2. Receive Binding Update. (NUTX -> HA0) (Refer to 5.14.1)
- 3. Send Binding Acknowledgement. (HA0 -> NUTX) (Refer to 5.15.1)
- c. IKE Phase2 (IPsec SA3/SA4)
- d. IKE Phase2 (IPsec SA7/SA8)
- 4. Send ICMP Echo Request. (out: HA0 -> NUTX, in: CN0 -> NUT0) (Refer to 5.7.2)
- 5. Receive Home Test Init. (out: NUTX -> HA0, in: NUT0 -> CN0) (*1) (Refer to 5.10.2)



- 6. Receive Care-of Test Init. (NUTX -> CN0) (Refer to 5.11.1)
- 7. Send Care-of Test. (CN0 -> NUTX) (Refer to 5.13.1)
- 8. Send Home Test. (out: HA0 -> NUTX, in: CN0 -> NUT0) (Refer to 5.12.2)
- 9. Receive ICMP Echo Reply or [11]. (out: NUTX -> HA0, in: NUT0 -> CN0) (Refer to 5.8.2)
- 10. Receive Binding Update. (NUTX -> CN0) (*2) (Refer to 5.14.3)

		, , , , , , , , , , , , , , , , , , , ,	(
IPv6 Header	Source Address	MN care-of	
	Destination Add	CN (global)	
Destination Option Header	Home Address		MN home (global)
Mobility Header	MH Type		5
Mobility options	Nonce	Option Type	4
	Indices	Option Length	4
		Home Nonce Index	Any
		Care-of Nonce Index	Any
	Binding	Option Type	5
	Authorization	Option Length	12
	Data	Authenticator	Anv

11. [9] or Receive ICMP Echo Reply. (NUTX -> CN0 with Home Address Option) (Refer to 5.8.3)

[JUDGMENT]

(*1) PASS: CN0 receives Home Test Init.

Then, check whether this packet fills all of the following,

- using new IPsec SA3.

(*2) PASS: CN0 receives Binding Update.

[REFERENCES]

RFC3775 Mobility Support in IPv6 See Section 11.3.2



6.13.2.2.2 MN-1-2-2-1-002 - Sending HoTI (Foreign -> Stay, ISAKMP SA expired, IPsec SA3/SA4 expired)

[PURPOSE]

MN-1-2-2-1-002 - Sending HoTI (Foreign -> Stay, ISAKMP SA expired, IPsec SA3/SA4 expired)

[CATEGORY]

HOST: ADVANCED FUNCTION (IKE (AND RETURN ROUTABILITY))

[REQUIREMENT OF TEST]

Function of IKE: YES

Function of Return Routability: YES

[TOPORGY]

Refer to 2.1.1.1 Common Topology-1

[TEST SETUP]

Refer to 3.1 Common Setup-1

[INITIALIZATION]

HAO	NUT0	R1	R2	CNO
		1		1
	>	- 1		1.Router Advertisement
		1		I
	NUTX	- 1		I
		- 1		I
	<			2.Router Advertisement
				1
<-		- 1		3.Neighbor Solicitation
		- 1		4.(no reply)
		- 1		I

- 1. Send Router Advertisement. (HA0 -> HA0_allnode_multi) (Refer to 5.2.2)
- 2. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)
- 3. Receive Neighbor Solicitation. (NUT0 -> HA0) (Refer to 5.3.3)
- 4. (no reply)
- In the case of Virtual Home Link

HA0	NUTX	R1	R2	CNO
		1		I
	<			1.Router Advertisement



1. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)

HA0	NU	ГХ Г	R1	R2	CNO
 		 < 	 	 	 1.Router Advertisement
	==>		 	 	a.IKE Phase1 (ISAKMP SA) b.IKE Phase2 (IPsec SA1/SA2)
	>		 	 	2.Binding Update 3.Binding Acknowledgement
-	==>		 	 	c.IKE Phase2 (IPsec SA3/SA4) d.IKE Phase2 (IPsec SA7/SA8) (It is if required)
==	==>	 <	 	 	 - 4.ICMP Echo Request
 <= 				>	> 5.Home Test Init > 6.Care-of Test Init
==	==>	•	 		- 7.Care-of Test - 8.Home test
 <= 	===			>	 > 9.ICMP Echo Reply > 10.Binding Update > 11.ICMP Echo Reply
	==>	 	 	 	e.(expire ISAKMP SA) f1.IKE Phase1 (ISAKMP SA)
 		 	 	 	 :
	==>	 	 	 	g.(expire IPsec SA3/SA4) f2.IKE Phase1 (ISAKMP SA) h.IKE Phase2 (IPsec SA3/SA4) (*1)
 ==	==>	 < 	 	 	 - 12.ICMP Echo Request
 <=	===	 	I 	 >	> 13.Home Test Init (*2)



	>	14.Care-of Test Init
	<	15.Care-of Test
====>	<	16.Home test
<====	>	17.ICMP Echo Reply
	>	18.Binding Update (*3)
	>	19.ICMP Echo Reply

- 1. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)
- a. IKE Phase1 (ISAKMP SA)
- b. IKE Phase2 (IPsec SA1/SA2)
- 2. Receive Binding Update. (NUTX -> HA0) (Refer to 5.14.1)
- 3. Send Binding Acknowledgement. (HA0 -> NUTX) (Refer to 5.15.1)
- c. IKE Phase2 (IPsec SA3/SA4)
- d. IKE Phase2 (IPsec SA7/SA8)
- 4. Send ICMP Echo Request. (out: HA0 -> NUTX, in: CN0 -> NUT0) (Refer to 5.7.2)
- 5. Receive Home Test Init. (out: NUTX -> HA0, in: NUT0 -> CN0) (Refer to 5.10.2)
- 6. Receive Care-of Test Init. (NUTX -> CN0) (Refer to 5.11.1)
- 7. Send Care-of Test. (CN0 -> NUTX) (Refer to 5.13.1)
- 8. Send Home Test. (out: HAO -> NUTX, in: CNO -> NUTO) (Refer to 5.12.2)
- 9. Receive ICMP Echo Reply or [11]. (out: NUTX -> HA0, in: NUT0 -> CN0) (Refer to 5.8.2)
- 10. Receive Binding Update. (NUTX -> CN0) (Refer to 5.14.3)
- 11. [9] or Receive ICMP Echo Reply. (NUTX -> CN0 with Home Address Option) (Refer to 5.8.3)
- e. (expire ISAKMP SA)
- f1. IKE Phase1 (ISAKMP SA) or [f2]
- g. (expire IPsec SA3/SA4)
- f2.[f1] or IKE Phase1 (ISAKMP SA)
- h. IKE Phase2 (IPsec SA3/SA4) (*1)
- 12. Send ICMP Echo Request. (out: HA0 -> NUTX, in: CN0 -> NUT0) (Refer to 5.7.2)
- 13. Receive Home Test Init. (out: NUTX -> HA0, in: NUT0 -> CN0) (*2) (Refer to 5.10.2)

IPv6 Header	Source Address	MN Care-of (global)
	Destination Address	(global) HA
		(global)
Encapsulating	Security Parameters Index	Any
Security	Sequence Number	Any
Payload	Initialization Vector	Any
IPv6 Header	Source Address	MN home



		(global)
	Destination Address	CN (global)
Mobility Header	MH Type	1

- 14. Receive Care-of Test Init. (NUTX -> CN0) (Refer to 5.11.1)
- 15. Send Care-of Test. (CN0 -> NUTX) (Refer to 5.13.1)
- 16. Send Home Test. (out: HA0 -> NUTX, in: CN0 -> NUT0) (Refer to 5.12.2)
- 17. Receive ICMP Echo Reply or [19]. (out: NUTX -> HA0, in: NUT0 -> CN0) (Refer to 5.8.2)
- 18. Receive Binding Update. (NUTX -> CN0) (*3) (Refer to 5.14.3)

IPv6 Header	Source Address	MN care-of	
	Destination Add	Iress	CN
			(global)
Destination	Home Address		MN home
Option Header		(global)	
Mobility Header	MH Type		5
Mobility options	Nonce	Option Type	4
	Indices	Option Length	4
		Home Nonce Index	Any
		Care-of Nonce Index	Any
	Binding	Option Type	5
	Authorization		12
	Data	Authenticator	Any

19. [17] or Receive ICMP Echo Reply. (NUTX -> CN0 with Home Address Option) (Refer to 5.8.3)

[JUDGMENT]

(*1) PASS: CN0 receives Home Test Init.

Then, check whether this packet fills all of the following,

- using new IPsec SA3.

(*2) PASS: CN0 receives Binding Update.

[REFERENCES]

RFC3775 Mobility Support in IPv6 See Section 11.3.2



6.13.2.2.3 MN-1-2-2-1-004 - Sending HoTI (Foreign -> Foreign -> Stay, ISAKMP SA discard, IPsec SA3/SA4 expired)

[PURPOSE]

MN-1-2-2-1-004 - Sending HoTI (Foreign -> Foreign -> Stay, ISAKMP SA discard, IPsec SA3/SA4 expired)

[CATEGORY]

HOST: ADVANCED FUNCTION (IKE (AND RETURN ROUTABILITY))

[REQUIREMENT OF TEST]

Function of IKE: YES

Function of Return Routability: YES

[TOPORGY]

Refer to 2.1.1.1 Common Topology-1

[TEST SETUP]

Refer to 3.1 Common Setup-1

[INITIALIZATION]

HAO	NUT0	R1	R2	CNO
		1		1
	>	- 1		1.Router Advertisement
		1		I
	NUTX	- 1		I
		- 1		I
	<			2.Router Advertisement
				I
<-		- 1		3.Neighbor Solicitation
		- 1		4.(no reply)
		- 1		I

- 1. Send Router Advertisement. (HA0 -> HA0_allnode_multi) (Refer to 5.2.2)
- 2. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)
- 3. Receive Neighbor Solicitation. (NUT0 -> HA0) (Refer to 5.3.3)
- 4. (no reply)
- In the case of Virtual Home Link

HA0	NUTX	R1	R2	CNO
		1		I
	<			1.Router Advertisement



1. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)

HAO NU	TX R1	R2	CNO
			 1.Router Advertisement
 <===> <===>	: :		a.IKE Phase1 (ISAKMP SA) b.IKE Phase2 (IPsec SA1/SA2)
<>	: :		2.Binding Update 3.Binding Acknowledgement
 <===> <===>	: :		c.IKE Phase2 (IPsec SA3/SA4) d.IKE Phase2 (IPsec SA7/SA8) (It is if required)
====>		 	 4.ICMP Echo Request
1	 <		7.Care-of Test
	 	 	8.Home test > 9.ICMP Echo Reply > 10.Binding Update > 11.ICMP Echo Reply
l l NU	TY		
			 12.Router Advertisement
<			13.Binding Update 14.Binding Acknowledgement
	 		e.(discard ISAKMP SA) f1.IKE Phase1 (ISAKMP SA)
 <==== 	'	 	 > 15.Home Test Init > 16.Care-of Test Init
 ====> 	< < 	 	17.Care-of Test 18.Home test
•			-



	>	19.Binding Update
		:
		g.(expire IPsec SA3/SA4)
<===>		f2.IKE Phase1 (ISAKMP SA)
<===>		h.IKE Phase2 (IPsec SA3/SA4) (*1)
====>	<	20.ICMP Echo Request
<====	>	21.Home Test Init
	>	22.Care-of Test Init
	<	23.Care-of Test
====>	<	24.Home test
		1
<====	>	25.ICMP Echo Reply
	>	26.Binding Update (*3)
	>	27.ICMP Echo Reply

- 1. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)
- a. IKE Phase1 (ISAKMP SA)
- b. IKE Phase2 (IPsec SA1/SA2)
- 2. Receive Binding Update. (NUTX -> HA0) (Refer to 5.14.1)
- 3. Send Binding Acknowledgement. (HA0 -> NUTX) (Refer to 5.15.1)
- c. IKE Phase2 (IPsec SA3/SA4)
- d. IKE Phase2 (IPsec SA7/SA8)
- 4. Send ICMP Echo Request. (out: HA0 -> NUTX, in: CN0 -> NUT0) (Refer to 5.7.2)
- 5. Receive Home Test Init. (out: NUTX -> HA0, in: NUT0 -> CN0) (Refer to 5.10.2)
- 6. Receive Care-of Test Init. (NUTX -> CN0) (Refer to 5.11.1)
- 7. Send Care-of Test. (CN0 -> NUTX) (Refer to 5.13.1)
- 8. Send Home Test. (out: HA0 -> NUTX, in: CN0 -> NUT0) (Refer to 5.12.2)
- 9. Receive ICMP Echo Reply or [11]. (out: NUTX -> HA0, in: NUT0 -> CN0) (Refer to 5.8.2)
- 10. Receive Binding Update. (NUTX -> CN0) (Refer to 5.14.3)
- 11. [9] or Receive ICMP Echo Reply. (NUTX -> CN0 with Home Address Option) (Refer to 5.8.3)
- 12. Send Router Advertisement. (R2 -> R2_allnode_multi) (Refer to 5.2.1)
- 13. Receive Binding Update. (NUTY -> HA0) (Refer to 5.14.1) # (K)bit on/off



- 14. Send Binding Acknowledgement. (HA0 -> NUTY) (Refer to 5.15.1) # (K)bit off
- e. (discard ISAKMP SA)
- f1. IKE Phase1 (ISAKMP SA) or [f2]
- 15. Receive Home Test Init. (out: NUTY -> HA0, in: NUT0 -> CN0) (Refer to 5.10.2)
- 16. Receive Care-of Test Init. (NUTY -> CN0) (Refer to 5.11.1)
- 17. Send Care-of Test. (CN0 -> NUTY) (Refer to 5.13.1)
- 18. Send Home Test. (out: HA0 -> NUTY, in: CN0 -> NUT0) (Refer to 5.12.2)
- 19. Receive Binding Update. (NUTY -> CN0) (Refer to 5.14.3)
- g. (expire IPsec SA3/SA4)
- f2. [f1] or IKE Phase1 (ISAKMP SA)
- h. IKE Phase2 (IPsec SA3/SA4) (*1)
- 20. Send ICMP Echo Request. (out: HAO -> NUTY, in: CNO -> NUTO) (Refer to 5.7.2)
- 21. Receive Home Test Init. (out: NUTY -> HA0, in: NUT0 -> CN0) (*2) (Refer to 5.10.2)

IPv6 Header	Source Address	MN Care-of (global)
	Destination Address	HA (global)
Encapsulating	Security Parameters Index	Any
Security	Sequence Number	Any
Payload	Initialization Vector	Any
IPv6 Header	Source Address	MN home (global)
	Destination Address	CN (global)
Mobility Header MH Type		1

- 22. Receive Care-of Test Init. (NUTY -> CN0) (Refer to 5.11.1)
- 23. Send Care-of Test. (CN0 -> NUTY) (Refer to 5.13.1)
- 24. Send Home Test. (out: HA0 -> NUTY, in: CN0 -> NUT0) (Refer to 5.12.2)
- 25. Receive ICMP Echo Reply or [27]. (out: NUTY -> HA0, in: NUT0 -> CN0) (Refer to 5.8.2)
- 26. Receive Binding Update. (NUTY -> CN0) (*3) (Refer to 5.14.3)

IPv6 Header	Source Address	MN care-of	
	Destination Add	dress	CN
			(global)
Destination	Home Address		MN home
Option Header		(global)	
Mobility Header	MH Type	5	
Mobility options	Nonce	Option Type	4
	Indices	Option Length	4
		Home Nonce Index	Any
		Care-of Nonce Index	Any
	Binding	Option Type	5
	Authorization	Option Length	12
	Data	Authenticator	Any

27. [25] or Receive ICMP Echo Reply. (NUTY -> CN0 with Home Address Option) (Refer to 5.8.3)

[JUDGMENT]

- (*1) PASS: IPsec SA3/SA4 is re-established after re-establishing ISAKMP SA.
- (*2) PASS: CN0 receives Home Test Init.

Then, check whether this packet fills all of the following,



- using new IPsec SA3. (*3) PASS: CN0 receives Binding Update.

[REFERENCES]

RFC3775 Mobility Support in IPv6 See Section 11.7.3



6.13.2.2.4 MN-1-2-2-1-006 - Sending HoTI (Foreign -> Foreign -> Stay, ISAKMP SA update, IPsec SA3/SA4 expired)

[PURPOSE]

MN-1-2-2-1-006 - Sending HoTI (Foreign -> Foreign -> Stay, ISAKMP SA update, IPsec SA3/SA4 expired)

[CATEGORY]

HOST: ADVANCED FUNCTION (IKE (AND RETURN ROUTABILITY))

[REQUIREMENT OF TEST]

Function of IKE: YES

Function of Return Routability: YES

NUT sets (K) bit in BU which is transmitted to HA: YES

[TOPORGY]

Refer to 2.1.1.1 Common Topology-1

[TEST SETUP]

Refer to 3.1 Common Setup-1

[INITIALIZATION]

HA0	NUT0	R1	R2	CNO
				1
	>			1.Router Advertisement
				I
	NUTX			I
				1
	<	-		2.Router Advertisement
				1
<-				3.Neighbor Solicitation
				4.(no reply)
				I

- 1. Send Router Advertisement. (HA0 -> HA0_allnode_multi) (Refer to 5.2.2)
- 2. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)
- 3. Receive Neighbor Solicitation. (NUT0 -> HA0) (Refer to 5.3.3)
- 4. (no reply)
- In the case of Virtual Home Link

HA0	NUTX	R1	R2	CNO
		1	- 1	



| | <---- | | | 1.Router Advertisement

1. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)

HAO N	JTX R1	R2	CNO
			 1.Router Advertisement
 <===> <===>		 	a.IKE Phase1 (ISAKMP SA) b.IKE Phase2 (IPsec SA1/SA2)
<>		 	2.Binding Update 3.Binding Acknowledgement
			c.IKE Phase2 (IPsec SA3/SA4) d.IKE Phase2 (IPsec SA7/SA8) (It is if required)
====>			4.ICMP Echo Request
			5.Home Test Init 6.Care-of Test Init
 ====>	<		7.Care-of Test
		>	 9.ICMP Echo Reply 10.Binding Update 11.ICMP Echo Reply
 N	 JTY	 	
			 12.Router Advertisement
<>			13.Binding Update 14.Binding Acknowledgement
 		 	 e.(update ISAKMP SA)
 <==== 	•	 >	 15.Home Test Init 16.Care-of Test Init
 ====>	<	 	17.Care-of Test 18.Home test
I	1 I	I	1



	>	19.Binding Update
		1
		:
		f.(expire IPsec SA3/SA4)
<===>		g.IKE Phase2 (IPsec SA3/SA4) (*1)
====>	<	20.ICMP Echo Request
<====	>	21.Home Test Init (*2)
	>	22.Care-of Test Init
	<	23.Care-of Test
====>	<	24.Home test
<====	>	25.ICMP Echo Reply
	>	26.Binding Update (*3)
	>	27.ICMP Echo Reply

- 1. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)
- a. IKE Phase1 (ISAKMP SA)
- b. IKE Phase2 (IPsec SA1/SA2)
- 2. Receive Binding Update. (NUTX -> HA0) (Refer to 5.14.1)
- 3. Send Binding Acknowledgement. (HA0 -> NUTX) (Refer to 5.15.1)
- c. IKE Phase2 (IPsec SA3/SA4)
- d. IKE Phase2 (IPsec SA7/SA8)
- 4. Send ICMP Echo Request. (out: HA0 -> NUTX, in: CN0 -> NUT0) (Refer to 5.7.2)
- 5. Receive Home Test Init. (out: NUTX -> HA0, in: NUT0 -> CN0) (Refer to 5.10.2)
- 6. Receive Care-of Test Init. (NUTX -> CN0) (Refer to 5.11.1)
- 7. Send Care-of Test. (CN0 -> NUTX) (Refer to 5.13.1)
- 8. Send Home Test. (out: HA0 -> NUTX, in: CN0 -> NUT0) (Refer to 5.12.2)
- 9. Receive ICMP Echo Reply or [11]. (out: NUTX -> HA0, in: NUT0 -> CN0) (Refer to 5.8.2)
- 10. Receive Binding Update. (NUTX -> CN0) (Refer to 5.14.3)
- 11. [9] or Receive ICMP Echo Reply. (NUTX -> CN0 with Home Address Option) (Refer to 5.8.3)
- 12. Send Router Advertisement. (R2 -> R2_allnode_multi) (Refer to 5.2.1)
- 13. Receive Binding Update. (NUTY -> HA0) (Refer to 5.14.1) # (K)bit on
- 14. Send Binding Acknowledgement. (HA0 -> NUTY) (Refer to 5.15.1)



(K)bit on

- e. (update ISAKMP SA)
- 15. Receive Home Test Init. (out: NUTY -> HA0, in: NUT0 -> CN0) (Refer to 5.10.2)
- 16. Receive Care-of Test Init. (NUTY -> CN0) (Refer to 5.11.1)
- 17. Send Care-of Test. (CN0 -> NUTY) (Refer to 5.13.1)
- 18. Send Home Test. (out: HA0 -> NUTY, in: CN0 -> NUT0) (Refer to 5.12.2)
- 19. Receive Binding Update. (NUTY -> CN0) (Refer to 5.14.3)
- f. (expire IPsec SA3/SA4)
- g. IKE Phase2 (IPsec SA3/SA4) (*1)
- 20. Send ICMP Echo Request. (out: HAO -> NUTY, in: CNO -> NUTO) (Refer to 5.7.2)
- 21. Receive Home Test Init. (out: NUTY -> HA0, in: NUT0 -> CN0) (*2) (Refer to 5.10.2)

IPv6 Header	Source Address	MN Care-of (global)
	Destination Address	HA (global)
Encapsulating	Security Parameters Index	Any
Security	Sequence Number	Any
Payload	Initialization Vector	Any
IPv6 Header	Source Address	MN home (global)
	Destination Address	CN (global)
Mobility Header	MH Type	1

- 22. Receive Care-of Test Init. (NUTY -> CN0) (Refer to 5.11.1)
- 23. Send Care-of Test. (CN0 -> NUTY) (Refer to 5.13.1)
- 24. Send Home Test. (out: HA0 -> NUTY, in: CN0 -> NUT0) (Refer to 5.12.2)
- 25. Receive ICMP Echo Reply or [27]. (out: NUTY -> HA0, in: NUT0 -> CN0) (Refer to 5.8.2)
- 26. Receive Binding Update. (NUTY -> CN0) (*3) (Refer to 5.14.3)

IPv6 Header	Source Address	MN care-of	
	Destination Add	CN (global)	
Destination Option Header	Home Address	MN home (global)	
Mobility Header	MH Type		5
Mobility options	Nonce	Option Type	4
	Indices	Option Length	4
		Home Nonce Index	Any
		Care-of Nonce Index	Any
	Binding Opt		5
	Authorization	Option Length	12
	Data	Authenticator	Anv

27. [25] or Receive ICMP Echo Reply. (NUTY -> CN0 with Home Address Option) (Refer to 5.8.3)

[JUDGMENT]

- (*1) PASS: IPsec SA3/SA4 is re-established without re-establishment of ISAKMP SA.
- (*2) PASS: CN0 receives Home Test Init.

Then, check whether this packet fills all of the following,

- using new IPsec SA3.
- (*3) PASS: CN0 receives Binding Update.



[REFERENCES]

RFC3775 Mobility Support in IPv6 See Section 11.7.1, 11.7.3



6.13.2.2.5 MN-1-2-2-1-018 - Sending HoTI (Security policy entries is inactive)

[PURPOSE]

MN-1-2-2-1-018 - Sending HoTI (Security policy entries is inactive)

[CATEGORY]

HOST: ADVANCED FUNCTION (IKE (AND RETURN ROUTABILITY))

[REQUIREMENT OF TEST]

Function of IKE: YES

Function of Real Home Link: YES Function of Return Routability: YES

[TOPORGY]

Refer to 2.1.1.1 Common Topology-1

[TEST SETUP]

Refer to 3.1 Common Setup-1

[INITIALIZATION]

HA0	NUT0	R1	R2	CNO
		1		1
	>			1.Router Advertisement
-				I
	NUTX			I
				I
	<			2.Router Advertisement
				I
<-				3.Neighbor Solicitation
				4.(no reply)
				1

- 1. Send Router Advertisement. (HA0 -> HA0_allnode_multi) (Refer to 5.2.2)
- 2. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)
- 3. Receive Neighbor Solicitation. (NUT0 -> HA0) (Refer to 5.3.3)
- 4. (no reply)
- In the case of Virtual Home Link

HA0	NUTX	R1	R2	CNO	
				1	
	<			1.Router /	Advertisement
		1			



1. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)

[PROCEDURE]			
HA0	NUTX	R1	R2 C1	NO
		 	 	 1.Router Advertisement
 <=== <===	•	 	 	a.IKE Phase1 (ISAKMP SA) b.IKE Phase2 (IPsec SA1/SA2)
 < 		 	 	 2.Binding Update 3.Binding Acknowledgement
 <=== <===	:	 	 	c.IKE Phase2 (IPsec SA3/SA4) d.IKE Phase2 (IPsec SA7/SA8)
 ====	 -> <	 	 	(It is if required) 4.ICMP Echo Request
 <=== 	-			r 5.Home Test Init 6.Care-of Test Init
 ====	< :> <	 		7.Care-of Test 8.Home test
 <=== 	•			I 9.ICMP Echo Reply 10.Binding Update
 	i			11.ICMP Echo Reply
 	NUTO ·>	 	 	 12.Router Advertisement
 <	:		 	 13.Binding Update
 		 	 	14.Binding Acknowledgement e.(inactive IPsec SA3/SA4)
 <	 	 	 	 15.Neighbor Advertisement
 		 	I >	 16.Home Test Init (*1) 17.Home Test
		 	>	 18.Binding Update (*2)



- 1. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)
- a. IKE Phase1 (ISAKMP SA)
- b. IKE Phase2 (IPsec SA1/SA2)
- 2. Receive Binding Update. (NUTX -> HA0) (Refer to 5.14.1)
- 3. Send Binding Acknowledgement. (HA0 -> NUTX) (Refer to 5.15.1)
- c. IKE Phase2 (IPsec SA3/SA4)
- d. IKE Phase2 (IPsec SA7/SA8)
- 4. Send ICMP Echo Request. (out: HA0 -> NUTX, in: CN0 -> NUT0) (Refer to 5.7.2)
- 5. Receive Home Test Init. (out: NUTX -> HA0, in: NUT0 -> CN0) (Refer to 5.10.2)
- 6. Receive Care-of Test Init. (NUTX -> CN0) (Refer to 5.11.1)
- 7. Send Care-of Test. (CN0 -> NUTX) (Refer to 5.13.1)
- 8. Send Home Test. (out: HAO -> NUTX, in: CNO -> NUTO) (Refer to 5.12.2)
- 9. Receive ICMP Echo Reply or [11]. (out: NUTX -> HA0, in: NUT0 -> CN0) (Refer to 5.8.2)
- 10. Receive Binding Update. (NUTX -> CN0) (Refer to 5.14.3)
- 11. [9] or Receive ICMP Echo Reply. (NUTX -> CN0 with Home Address Option) (Refer to 5.8.3)
- 12. Send Router Advertisement. (HA0 -> HA0_allnode_multi) (Refer to 5.2.2)
- 13. Receive Binding Update. (NUT0 -> HA0) (Refer to 5.14.1)
- 14. Send Binding Acknowledgement. (HA0 -> NUT0) (Refer to 5.15.1)
- e. (inactive IPsec SA3/SA4)
- 15. Receive Neighbor Advertisement. (NUT0(Unspecified) -> HA0_allnode_multi) (Refer to 5.4.1)
- 16. Receive Home Test Init. (NUT0 -> CN0) (*1) (Refer to 5.10.1)

Γ	IPv6 Header	Source Address	MN home
			(global)
		Destination Address	CN
			(global)
	Mobility Header	MH Type	1

- 17. Send Home Test. (CN0 -> NUT0) (Refer to 5.12.1)
- 18. Receive Binding Update to CN0. (NUT0 -> CN0) (*2) (Refer to 5.14.3)

[JUDGMENT]

(*1) PASS: CN0 receives Home Test Init.

Then, check whether this packet fills all of the following,

- The security policy entries is inactive.
- (*2) PASS: CN0 receives Binding Update.

[REFERENCES]



 $RFC3776\ Using\ IPsec$ to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents

See Section 4.2



6.13.2.2.6 MN-1-2-2-1-010 - Sending HoTI (Foreign -> home -> Foreign, ISAKMP SA expired, IPsec SA3/SA4 expired)

[PURPOSE]

 $MN\mbox{-}1\mbox{-}2\mbox{-}2\mbox{-}1\mbox{-}010$ - Sending HoTI (Foreign -> home -> Foreign, ISAKMP SA expired, IPsec SA3/SA4 expired)

[CATEGORY]

HOST: ADVANCED FUNCTION (IKE (AND RETURN ROUTABILITY))

[REQUIREMENT OF TEST]

Function of IKE: YES

Function of Return Routability: YES Function of Real Home Link: YES

[TOPORGY]

Refer to 2.1.1.1 Common Topology-1

[TEST SETUP]

Refer to 3.1 Common Setup-1

[INITIALIZATION]

	_			
HAO	NUT0	R1	R2	CNO
		- 1		1
	>			1.Router Advertisement
				I
	NUTX			I
				I
	<			2.Router Advertisement
		- 1		1
<-				3.Neighbor Solicitation
		1		4.(no reply)
1	1	- 1		

- 1. Send Router Advertisement. (HA0 -> HA0_allnode_multi) (Refer to 5.2.2)
- 2. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)
- 3. Receive Neighbor Solicitation. (NUT0 -> HA0) (Refer to 5.3.3)
- 4. (no reply)

_	-			
HA0	NUTX	R1	R2	CNO
		1	- 1	T
	<		- 1	1.Router Advertisement
		1	- 1	1
<=	==>	- 1	1	a.IKE Phase1 (ISAKMP SA)



<===>		b.IKE Phase2 (IPsec SA1/SA2)
<		2.Binding Update
>		3.Binding Acknowledgement
<===>		r c.IKE Phase2 (IPsec SA3/SA4)
<===>	i i i	d.IKE Phase2 (IPsec SA7/SA8)
j	i i	(It is if required)
====>	<	4.ICMP Echo Request
		<u> </u>
	>	
l I	>	b.Care-of lest init 7.Care-of Test
 ====>	' !	7.care-or rest 8.Home test
/	`	0.1101110 1031
<====	>	9.ICMP Echo Reply
-	, >	
1	>	11.ICMP Echo Reply
1		
l NU	ΤΟ	
>		12.Router Advertisement
 <		l 13.Binding Update
>		14.Binding Acknowledgement
i	' ' ' 	
İ	i i i	e.(inactive IPsec SA3/SA4)
Ì	l l	
<		15.Neighbor Advertisement
1		
	>	16.Home Test Init
	<	17.Home Test
l		I 18.Binding Update
1		10.binding opdate
i		:
1		f.(expire ISAKMP SA)
1		
1		:
		g.(expire IPsec SA3/SA4)
l NU ⁻		
I NU	1/	I



		1
	<	19.Router Advertisement
		1
<		20.Binding Update
>		21.Binding Acknowledgement
		1
<===>		h.IKE Phase1 (ISAKMP SA)
<===>		i.IKE Phase2 (IPsec SA3/SA4) (*1)
		1
====>	<	22.ICMP Echo Request
		1
<====	>	23.Home Test Init (*2)
	>	24.Care-of Test Init
	<	25.Care-of Test
====>	<	26.Home test
		1
<====	>	27.ICMP Echo Reply
	>	28.Binding Update (*3)
1	>	29.ICMP Echo Reply
		1

- 1. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)
- a. IKE Phase1 (ISAKMP SA)
- b. IKE Phase2 (IPsec SA1/SA2)
- 2. Receive Binding Update. (NUTX -> HA0) (Refer to 5.14.1)
- 3. Send Binding Acknowledgement. (HA0 -> NUTX) (Refer to 5.15.1)
- c. IKE Phase2 (IPsec SA3/SA4)
- d. IKE Phase2 (IPsec SA7/SA8)
- 4. Send ICMP Echo Request. (out: HA0 -> NUTX, in: CN0 -> NUT0) (Refer to 5.7.2)
- 5. Receive Home Test Init. (out: NUTX -> HA0, in: NUT0 -> CN0) (Refer to 5.10.2)
- 6. Receive Care-of Test Init. (NUTX -> CN0) (Refer to 5.11.1)
- 7. Send Care-of Test. (CN0 -> NUTX) (Refer to 5.13.1)
- 8. Send Home Test. (out: HA0 -> NUTX, in: CN0 -> NUT0) (Refer to 5.12.2)
- 9. Receive ICMP Echo Reply or [11]. (out: NUTX -> HA0, in: NUT0 -> CN0) (Refer to 5.8.2)
- 10. Receive Binding Update. (NUTX -> CN0) (Refer to 5.14.3)
- 11. [9] or Receive ICMP Echo Reply. (NUTX -> CN0 with Home Address Option) (Refer to 5.8.3)
- 12. Send Router Advertisement. (HA0 -> HA0_allnode_multi) (Refer to 5.2.2)
- 13. Receive Binding Update. (NUT0 -> HA0) (Refer to 5.14.1)



- 14. Send Binding Acknowledgement. (HA0 -> NUT0) (Refer to 5.15.1)
- e. (inactive IPsec SA3/SA4)
- 15. Receive Neighbor Advertisement. (NUT0(Unspecified) -> HA0_allnode_multi) (Refer to 5.4.1)
- 16. Receive Home Test Init. (NUT0 -> CN0) (Refer to 5.10.1)
- 17. Send Home Test. (CN0 -> NUT0) (Refer to 5.12.1)
- 18. Receive Binding Update to CN0. (NUT0 -> CN0) (Refer to 5.14.3)
- f. (expire ISAKMP SA)
- g. (expire IPsec SA3/SA4)
- 19. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)
- 20. Receive Binding Update. (NUTX -> HA0) (Refer to 5.14.1)
- 21. Send Binding Acknowledgement. (HA0 -> NUTX) (Refer to 5.15.1)
- h. IKE Phase1 (ISAKMP SA)
- i. IKE Phase2 (IPsec SA3/SA4) (*1)
- 22. Send ICMP Echo Request. (out: HA0 -> NUTX, in: CN0 -> NUT0) (Refer to 5.7.2)
- 23. Receive Home Test Init. (out: NUTX -> HA0, in: NUT0 -> CN0) (*2) (Refer to 5.10.2)

cici to 3.10. <i>≥)</i>			
IPv6 Header	Source Address	MN Care-of (global)	
	Destination Address	HA (global)	
Encapsulating	Security Parameters Index	Any	
Security	Sequence Number	Any	
Payload	Initialization Vector	Any	
IPv6 Header	Source Address	MN home (global)	
	Destination Address	CN (global)	
Mobility Header	MH Type	1	

- 24. Receive Care-of Test Init. (NUTX -> CN0) (Refer to 5.11.1)
- 25. Send Care-of Test. (CN0 -> NUTX) (Refer to 5.13.1)
- 26. Send Home Test. (out: HA0 -> NUTX, in: CN0 -> NUT0) (Refer to 5.12.2)
- 27. Receive ICMP Echo Reply or [29]. (out: NUTX -> HA0, in: NUT0 -> CN0) (Refer to 5.8.2)
- 28. Receive Binding Update. (NUTX -> CN0) (*3) (Refer to 5.14.3)

Source Address	IVIIN Care-or	
Destination Address		CN
	(global)	
Home Address		MN home
		(global)
MH Type		5
Nonce	Option Type	4
Indices	Option Length	4
	Home Nonce Index	Any
	Care-of Nonce Index	Any
Binding	Option Type	5
	Option Length	12
Data	Authenticator	Any
	Destination Add Home Address MH Type Nonce Indices	Destination Address Home Address MH Type Nonce Indices Option Type Option Length Home Nonce Index Care-of Nonce Index Binding Authorization Option Length Option Length Option Length Option Length

29. [27] or Receive ICMP Echo Reply. (NUTX -> CN0 with Home Address Option) (Refer to 5.8.3)



[JUDGMENT]

- (*1) PASS: IPsec SA3/SA4 is re-established after re-establishing ISAKMP SA.
- (*2) PASS: CN0 receives Home Test Init.
 - Then, check whether this packet fills all of the following,
 - using new IPsec SA3.
- (*3) PASS: CN0 receives Binding Update.

[REFERENCES]

RFC3776 Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents

See Section 4.2



6.13.2.2.7 MN-1-2-2-1-014 - Sending HoTI (Foreign -> home -> Foreign, ISAKMP SA exist, IPsec SA3/SA4 expired)

[PURPOSE]

MN-1-2-2-1-014 - Sending HoTI (Foreign -> home -> Foreign, ISAKMP SA exist, IPsec SA3/SA4 expired)

[CATEGORY]

HOST: ADVANCED FUNCTION (IKE (AND RETURN ROUTABILITY))

[REQUIREMENT OF TEST]

Function of IKE: YES

Function of Real Home Link: YES Function of Return Routability: YES

NUT sets (K) bit in BU which is transmitted to HA: YES

[TOPORGY]

Refer to 2.1.1.1 Common Topology-1

[TEST SETUP]

Refer to 3.1 Common Setup-1

[INITIALIZATION]

HA0	NUT0	R1	R2	CNO
	1	1		1
	->			1.Router Advertisement
				1
	NUTX			1
				1
	<	-		2.Router Advertisement
				1
<				3.Neighbor Solicitation
				4.(no reply)
				1

- 1. Send Router Advertisement. (HA0 -> HA0_allnode_multi) (Refer to 5.2.2)
- 2. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)
- 3. Receive Neighbor Solicitation. (NUT0 -> HA0) (Refer to 5.3.3)
- 4. (no reply)

HA0	NUTX	R1	R2	CNO
-		1	- 1	I
	<			1.Router Advertisement
		- 1		



	<===>		a.IKE Phase1 (ISAKMP SA)
	<===>		b.IKE Phase2 (IPsec SA1/SA2)
	<		I 2.Binding Update
	>		3.Binding Acknowledgement
ĺ			
i	<===>		c.IKE Phase2 (IPsec SA3/SA4)
ĺ	<===>		d.IKE Phase2 (IPsec SA7/SA8)
			(It is if required)
	====>	<	4.ICMP Echo Request
			<u> </u>
		>	
		> <	6.Care-of Test Init
		•	7.Care-or lest 8.Home test
			O.Home test
	<====	>	ı I 9.ICMP Echo Reply
ĺ			10.Binding Update
i		>	
	NU	ΤΟ	
	>		12.Router Advertisement
	<		13.Binding Update
	>		14.Binding Acknowledgement
			ı e.(inactive IPsec SA3/SA4)
			0.(maeriva ii 000 0/10/0/11)
	<		15.Neighbor Advertisement
ĺ			
		>	16.Home Test Init
		<	17.Home Test
		>	18.Binding Update
			;
			l f.(expire ISAKMP SA)
		ı ı l 	1.(0xp110 10\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
			' :
	NU	TX	



1	<	19.Router Advertisement	
		I	
<		20.Binding Update	
>		21.Binding Acknowledgement	
		1	
<===>		g.IKE Phase2 (IPsec SA3/SA	4) (*1)
		1	
====>	<	22.ICMP Echo Request	
		I	
<====		> 23.Home Test Init (*2)	
		> 24.Care-of Test Init	
	<	25.Care-of Test	
====>	<	26.Home test	
1		1	
<====		> 27.ICMP Echo Reply	
1		> 28.Binding Update (*3)	
		> 29.ICMP Echo Reply	
		1	

- 1. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)
- a. IKE Phase1 (ISAKMP SA)
- b. IKE Phase2 (IPsec SA1/SA2)
- 2. Receive Binding Update. (NUTX -> HA0) (Refer to 5.14.1)
- 3. Send Binding Acknowledgement. (HA0 -> NUTX) (Refer to 5.15.1)
- c. IKE Phase2 (IPsec SA3/SA4)
- d. IKE Phase2 (IPsec SA7/SA8)
- 4. Send ICMP Echo Request. (out: HA0 -> NUTX, in: CN0 -> NUT0) (Refer to 5.7.2)
- 5. Receive Home Test Init. (out: NUTX -> HA0, in: NUT0 -> CN0) (Refer to 5.10.2)
- 6. Receive Care-of Test Init. (NUTX -> CN0) (Refer to 5.11.1)
- 7. Send Care-of Test. (CN0 -> NUTX) (Refer to 5.13.1)
- 8. Send Home Test. (out: HA0 -> NUTX, in: CN0 -> NUT0) (Refer to 5.12.2)
- 9. Receive ICMP Echo Reply or [11]. (out: NUTX -> HA0, in: NUT0 -> CN0) (Refer to 5.8.2)
- 10. Receive Binding Update. (NUTX -> CN0) (Refer to 5.14.3)
- 11. [9] or Receive ICMP Echo Reply. (NUTX -> CN0 with Home Address Option) (Refer to 5.8.3)
- 12. Send Router Advertisement. (HA0 -> HA0_allnode_multi) (Refer to 5.2.2)
- 13. Receive Binding Update. (NUT0 -> HA0) (Refer to 5.14.1) # (K)bit on
- 14. Send Binding Acknowledgement. (HA0 -> NUT0) (Refer to 5.15.1)



- # (K)bit on
- e. (inactive IPsec SA3/SA4)
- 15. Receive Neighbor Advertisement. (NUT0(Unspecified) -> HA0_allnode_multi) (Refer to 5.4.1)
- 16. Receive Home Test Init. (NUT0 -> CN0) (Refer to 5.10.1)
- 17. Send Home Test. (CN0 -> NUT0) (Refer to 5.12.1)
- 18. Receive Binding Update to CN0. (NUT0 -> CN0) (Refer to 5.14.3)
- f. (expire IPsec SA3/SA4)
- 19. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)
- 20. Receive Binding Update. (NUTX -> HA0) (Refer to 5.14.1)
- 21. Send Binding Acknowledgement. (HA0 -> NUTX) (Refer to 5.15.1)
- g. IKE Phase2 (IPsec SA3/SA4) (*1)
- 22. Send ICMP Echo Request. (out: HAO -> NUTX, in: CNO -> NUT0) (Refer to 5.7.2)
- 23. Receive Home Test Init. (out: NUTX -> HA0, in: NUT0 -> CN0) (*2) (Refer to 5.10.2)

IPv6 Header	Source Address	MN Care-of (global)
	Destination Address	HA (global)
Encapsulating	Security Parameters Index	Any
Security	Sequence Number	Any
Payload	Initialization Vector	Any
IPv6 Header	Source Address	MN home (global)
	Destination Address	CN (global)
Mobility Header	MH Type	1

- 24. Receive Care-of Test Init. (NUTX -> CN0) (Refer to 5.11.1)
- 25. Send Care-of Test. (CN0 -> NUTX) (Refer to 5.13.1)
- 26. Send Home Test. (out: HA0 -> NUTX, in: CN0 -> NUT0) (Refer to 5.12.2)
- 27. Receive ICMP Echo Reply or [29]. (out: NUTX -> HA0, in: NUT0 -> CN0) (Refer to 5.8.2)
- 28. Receive Binding Update. (NUTX -> CN0) (*3) (Refer to 5.14.3)

IPv6 Header	Source Address	5	MN care-of
	Destination Add	CN (global)	
Destination Option Header	Home Address		MN home (global)
Mobility Header	MH Type		5
Mobility options	Nonce Option Type		4
	Indices	Option Length	4
		Home Nonce Index	Any
	Care-of Nonce Index		Any
	Binding Authorization	Option Type	5
		Option Length	12
	Data	Authenticator	Any

29. [27] or Receive ICMP Echo Reply. (NUTX -> CN0 with Home Address Option) (Refer to 5.8.3)

[JUDGMENT]

(*1) PASS: IPsec SA3/SA4 is re-established.



(*2) PASS: CN0 receives Home Test Init.

Then, check whether this packet fills all of the following,

- using new IPsec SA3.

(*3) PASS: CN0 receives Binding Update.

[REFERENCES]

RFC3776 Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents

See Section 4.2



6.13.2.3 Prefix Discovery

6.13.2.3.1 MN-1-2-3-1-001 - Sending MPS (Establishing New SA5/SA6)

[PURPOSE]

MN-1-2-3-1-001 - Sending MPS (Establishing New SA5/SA6)

[CATEGORY]

HOST: ADVANCED FUNCTION (IKE (AND MPD))

[REQUIREMENT OF TEST]

Function of IKE: YES

Function of Mobile Prefix Discovery: YES

[TOPORGY]

Refer to 2.1.1.1 Common Topology-1

[TEST SETUP]

Refer to 3.1 Common Setup-1

[INITIALIZATION]

HAO	NUT0	R1	R2	CNO
		1		I
	>	- 1		1.Router Advertisement
		1		I
	NUTX	- 1		I
		- 1		I
	<			2.Router Advertisement
				I
<-		- 1		3.Neighbor Solicitation
		- 1		4.(no reply)
		-		1

- 1. Send Router Advertisement. (HA0 -> HA0_allnode_multi) (Refer to 5.2.2)
- 2. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)
- 3. Receive Neighbor Solicitation. (NUT0 -> HA0) (Refer to 5.3.3)
- 4. (no reply)
- In the case of Virtual Home Link

HA0	NUTX	R1	R2	CNO
	1	1		I
	<			1.Router Advertisement



1. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)

HA0	NUTX	R1	R2	CNO
		1		T
	<			1.Router Advertisement
				I
<==	==>			a.IKE Phase1 (ISAKMP SA)
<==	==>			b.IKE Phase2 (IPsec SA1/SA2)
				I
<				2.Binding Update
	·->			3.Binding Acknowledgement
				I
<==	==>			c.IKE Phase2 (IPsec SA5/SA6)
				I
<				4.Mobile Prefix Solicitation (*1)
	·->			5.Mobile Prefix Advertisement
				I
<				6.Binding Update (*2)
	·->			7.Binding Acknowledgement
				1

- 1. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)
- a. IKE Phase1 (ISAKMP SA)
- b. IKE Phase2 (IPsec SA1/SA2)
- 2. Receive Binding Update. (NUTX -> HA0) (Refer to 5.14.1)
- 3. Send Binding Acknowledgement. (HA0 -> NUTX) (Refer to 5.15.1) # The Status field is set to 1(accepted but prefix discovery necessary).
- c. IKE Phase2 (IPsec SA5/SA6)
- 4. Receive Mobile Prefix Solicitation. (NUTX -> HA0 with Home Address Option) (*1) (Refer to 5.19.1)

	(1) (Refer to 0.10.1)						
	IPv6 Header	Source Address	MN care-of (global)				
		Destination Address	HA (global)				
	Destination Option Header	Home Address of Mobile Node	MN home (global)				
	Encapsulating	Security Parameters Index	Any				
	Security	Sequence Number	Any				
	Payload	Initialization Vector	Any				
	Mobility Header	Type	146				

- 5. Send Mobile Prefix Advertisement. (HA0 -> NUTX with Type2 Routing Header) (Refer to 5.20.1)
 - # The Prefix Information option is included, and,



- # The Valid Lifetime is set less than the remaining lifetime of the home registration.
- # The Preferred Lifetime is set less than the remaining lifetime of the home registration.
- 6. Receive Binding Update. (NUTX -> HA0) (*2) (Refer to 5.14.1)
- 7. Send Binding Acknowledgement. (HA0 -> NUTX) (Refer to 5.15.1)

[JUDGMENT]

(*1) PASS: HA0 receives Mobile Prefix Solicitation.

Then, check whether this packet fills all of the following,

- using new IPsec SA5.

(*2) PASS: HA0 receives Binding Update.

[REFERENCES]

RFC3775 Mobility Support in IPv6 See Section 11.3.2



6.13.2.3.2 MN-1-2-3-1-002 - Sending MPS (Foreign -> Stay, ISAKMP SA expired, IPsec SA5/SA6 expired)

[PURPOSE]

MN-1-2-3-1-002 - Sending MPS (Foreign -> Stay, ISAKMP SA expired, IPsec SA5/SA6 expired)

[CATEGORY]

HOST: ADVANCED FUNCTION (IKE (AND MPD))

[REQUIREMENT OF TEST]

Function of IKE: YES

Function of Mobile Prefix Discovery: YES

[TOPORGY]

Refer to 2.1.1.1 Common Topology-1

[TEST SETUP]

Refer to 3.1 Common Setup-1

[INITIALIZATION]

HAO	NUTO	R1	R2	CNO
				1
	>			1.Router Advertisement
				I
	NUTX			I
				I
	<	-		2.Router Advertisement
				I
<-				3.Neighbor Solicitation
				4.(no reply)
				1

- 1. Send Router Advertisement. (HA0 -> HA0_allnode_multi) (Refer to 5.2.2)
- 2. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)
- 3. Receive Neighbor Solicitation. (NUT0 -> HA0) (Refer to 5.3.3)
- 4. (no reply)
- In the case of Virtual Home Link

HA0	NUTX	R1	R2	CNO
	1	1		I
	<			1.Router Advertisement



1. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)

HA0	NUTX	R1	R2	CNO
1	- 1		1	
	<		1	1.Router Advertisement
				I
<==	=>			a.IKE Phase1 (ISAKMP SA)
<==	=>		-	b.IKE Phase2 (IPsec SA1/SA2)
			I	
<			I	2.Binding Update
	->			3.Binding Acknowledgement
!	ļ		1	
<==	=>			c.IKE Phase2 (IPsec SA5/SA6)
1	l l		1	A Mahilla Basti Oaliaitatiaa (*A)
'		l	I	4.Mobile Prefix Solicitation (*1)
	->	l	l	5.Mobile Prefix Advertisement
1	l I	l	l I	1
	l I	I	1	1 ·
i	l I	l I	l I	 d.(expire ISAKMP SA)
 <==	 =>	l I	İ	e1.IKE Phase1 (ISAKMP SA)
'	1	! 	i	1
i	i	i	i	i :
i	i	İ	i	i
i	i	İ	i	f.(expire IPsec SA5/SA6)
<==	=>	i	i	e2.IKE Phase1 (ISAKMP SA)
<==	=>		1	g.IKE Phase2 (IPsec SA5/SA6) (*1)
1	- 1		1	
	->		1	6.Mobile Prefix Advertisement
<			1	7.Mobile Prefix Solicitation (*2)
	->		1	8.Mobile Prefix Advertisement
- 1			- 1	

- 1. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)
- a. IKE Phase1 (ISAKMP SA)
- b. IKE Phase2 (IPsec SA1/SA2)
- 2. Receive Binding Update. (NUTX -> HA0) (Refer to 5.14.1)
- 3. Send Binding Acknowledgement. (HA0 -> NUTX) (Refer to 5.15.1) # The Status field is set to 1(accepted but prefix discovery necessary).



- c. IKE Phase2 (IPsec SA5/SA6)
- 4. Receive Mobile Prefix Solicitation. (NUTX -> HA0 with Home Address Option) (Refer to 5.19.1)
- 5. Send Mobile Prefix Advertisement. (HA0 -> NUTX with Type2 Routing Header) (Refer to 5.20.1)
- d. (expire ISAKMP SA)
- e1. IKE Phase1 (ISAKMP SA) or [e2]
- f. (expire IPsec SA5/SA6)
- e2. [e1] or IKE Phase1 (ISAKMP SA)
- g. IKE Phase2 (IPsec SA5/SA6) (*1)
- 6. Send unsolicited Mobile Prefix Advertisement. (HA0 -> NUTX with Type2 Routing Header) (Refer to 5.20.1)
- 7. Receive Mobile Prefix Solicitation. (NUTX -> HA0 with Home Address Option) (*2) (Refer to 5.19.1)

	· ·	
IPv6 Header	Source Address	MN care-of (global)
	Destination Address	HA (global)
Destination Option Header	Home Address of Mobile Node	MN home (global)
Encapsulating	Security Parameters Index	Any
Security	Sequence Number	Any
Payload	Initialization Vector	Any
Mobility Header	Туре	146

8. Send Mobile Prefix Advertisement. (HA0 -> NUTX with Type2 Routing Header) (Refer to 5.20.1)

[JUDGMENT]

- (*1) PASS: IPsec SA5/SA6 is re-established after re-establishing ISAKMP SA.
- (*2) PASS: HA0 receives Mobile Prefix Solicitation.

Then, check whether this packet fills all of the following,

- using new IPsec SA5.

[REFERENCES]

RFC3775 Mobility Support in IPv6 See Section 11.3.2



6.13.2.3.3 MN-1-2-3-1-004 - Sending MPS (Foreign -> Foreign -> Stay, ISAKMP SA discard, IPsec SA5/SA6 expired)

[PURPOSE]

MN-1-2-3-1-004 - Sending MPS (Foreign -> Foreign -> Stay, ISAKMP SA discard, IPsec SA5/SA6 expired)

[CATEGORY]

HOST: ADVANCED FUNCTION (IKE (AND MPD))

[REQUIREMENT OF TEST]

Function of IKE: YES

Function of Mobile Prefix Discovery: YES

[TOPORGY]

Refer to 2.1.1.1 Common Topology-1

[TEST SETUP]

Refer to 3.1 Common Setup-1

[INITIALIZATION]

HAO	NUTO	R1	R2	CNO
				1
	>			1.Router Advertisement
				I
	NUTX			I
				I
	<	-		2.Router Advertisement
				I
<-				3.Neighbor Solicitation
				4.(no reply)
				1

- 1. Send Router Advertisement. (HA0 -> HA0_allnode_multi) (Refer to 5.2.2)
- 2. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)
- 3. Receive Neighbor Solicitation. (NUT0 -> HA0) (Refer to 5.3.3)
- 4. (no reply)
- In the case of Virtual Home Link

HA0	NUTX	R1	R2	CNO
	1	1		I
	<			1.Router Advertisement



1. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)

HA0	NUTX	R1	R2	CNO
 	 < 	 	 	 1.Router Advertisement
	=> =>	i I		a.IKE Phase1 (ISAKMP SA) b.IKE Phase2 (IPsec SA1/SA2)
	 ->	 		2.Binding Update 3.Binding Acknowledgement
 <== 	 => 	 	 	 c.IKE Phase2 (IPsec SA5/SA6)
	 ->	i !	 	4.Mobile Prefix Solicitation 5.Mobile Prefix Advertisement
	I NUTY	1		
	<	 		 6.Router Advertisement
	 >			 7.Binding Update 8.Binding Acknowledgement
 <==	 =>		 	d.(discard ISAKMP SA) e1.IKE Phase1 (ISAKMP SA)
	 => =>			f.(expire IPsec SA5/SA6) e2.IKE Phase1 (ISAKMP SA) g.IKE Phase2 (IPsec SA5/SA6) (*1)
	-> 	 	 	9.Mobile Prefix Advertisement 10.Mobile Prefix Solicitation (*2) 11.Mobile Prefix Advertisement
i	İ	İ	İ	·

- 1. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)
- a. IKE Phase1 (ISAKMP SA)
- b. IKE Phase2 (IPsec SA1/SA2)



- 2. Receive Binding Update. (NUTX -> HA0) (Refer to 5.14.1)
- 3. Send Binding Acknowledgement. (HA0 -> NUTX) (Refer to 5.15.1) # The Status field is set to 1(accepted but prefix discovery necessary).
- c. IKE Phase2 (IPsec SA5/SA6)
- 4. Receive Mobile Prefix Solicitation. (NUTX -> HA0 with Home Address Option) (Refer to 5.19.1)
- 5. Send Mobile Prefix Advertisement. (HA0 -> NUTX with Type2 Routing Header) (Refer to 5.20.1)
- 6. Send Router Advertisement. (R2 -> R2_allnode_multi) (Refer to 5.2.1)
- 7. Receive Binding Update. (NUTY -> HA0) (Refer to 5.14.1) # (K)bit on/off
- 8. Send Binding Acknowledgement. (HA0 -> NUTY) (Refer to 5.15.1) # (K)bit off
- d. (discard ISAKMP SA)
- e1. IKE Phase1 (ISAKMP SA) or [e2]
- f. (expire IPsec SA5/SA6)
- e2. [e1] or IKE Phase1 (ISAKMP SA)
- g. IKE Phase2 (IPsec SA5/SA6) (*1)
- 9. Send unsolicited Mobile Prefix Advertisement. (HA0 -> NUTY with Type2 Routing Header) (Refer to 5.20.1)
- 10. Receive Mobile Prefix Solicitation. (NUTY -> HA0 with Home Address Option) (*2) (Refer to 5.19.1)

` / `	,	
IPv6 Header	Source Address	MN care-of (global)
	Destination Address	HA (global)
Destination Option Header	Home Address of Mobile Node	MN home (global)
Encapsulating	Security Parameters Index	Any
Security	Sequence Number	Any
Payload	Initialization Vector	Any
Mobility Header	Type	146

11. Send Mobile Prefix Advertisement. (HA0 -> NUTY with Type2 Routing Header) (Refer to 5.20.1)

[JUDGMENT]

- (*1) PASS: IPsec SA5/SA6 is re-established after re-establishing ISAKMP SA.
- (*2) PASS: HA0 receives Mobile Prefix Solicitation.

Then, check whether this packet fills all of the following,

- using new IPsec SA5.

[REFERENCES]

RFC3775 Mobility Support in IPv6 See Section 11.7.3



6.13.2.3.4 MN-1-2-3-1-006 - Sending MPS (Foreign -> Foreign -> Stay, ISAKMP SA update, IPsec SA5/SA6 expired)

[PURPOSE]

 $MN\mbox{-}1\mbox{-}2\mbox{-}3\mbox{-}1\mbox{-}006$ - Sending MPS (Foreign -> Foreign -> Stay, ISAKMP SA update, IPsec SA5/SA6 expired)

[CATEGORY]

HOST: ADVANCED FUNCTION (IKE (AND MPD))

[REQUIREMENT OF TEST]

Function of IKE: YES

Function of Mobile Prefix Discovery: YES

NUT sets (K) bit in BU which is transmitted to HA: YES

[TOPORGY]

Refer to 2.1.1.1 Common Topology-1

[TEST SETUP]

Refer to 3.1 Common Setup-1

[INITIALIZATION]

• In the case of Real Home Link

HA0	NUT0	R1	R2	CNO
			- 1	I
	>			1.Router Advertisement
				I
	NUTX			I
				I
	<			2.Router Advertisement
				I
<-				3.Neighbor Solicitation
				4.(no reply)
1				

- 1. Send Router Advertisement. (HA0 -> HA0_allnode_multi) (Refer to 5.2.2)
- 2. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)
- 3. Receive Neighbor Solicitation. (NUT0 -> HA0) (Refer to 5.3.3)
- 4. (no reply)
- In the case of Virtual Home Link

HA0	NUTX	R1	R2	CNO
1	I	1	- 1	- 1



| | <---- | | | 1.Router Advertisement

1. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)

LDUNI		., -			
HAO	NUT.	X F	₹1 F	R2 C	NO
		 <	 		1.Router Advertisement
	 > >	 	 		a.IKE Phase1 (ISAKMP SA) b.IKE Phase2 (IPsec SA1/SA2)
\	I	l I	 		b. IKE THASEZ (11 Sec 5A17 5A2)
		į	į		2.Binding Update
	·-> 				3.Binding Acknowledgement
 <== 	 > 	 	 		c.IKE Phase2 (IPsec SA5/SA6)
		ļ			4.Mobile Prefix Solicitation
	·-> 	l I	l I		5.Mobile Prefix Advertisement
	NUT	Y			
		 <	ا ا		6.Router Advertisement
<	 	 	 		7.Binding Update
	->	ĺ	ĺ		8.Binding Acknowledgement
		 	 		d.(update ISAKMP SA)
					 :
l	 	 	 		e.(expire IPsec SA5/SA6)
<==	==>	į	į		f.IKE Phase2 (IPsec SA5/SA6) (*1)
	 				9.Mobile Prefix Advertisement
-	· ·	 	 		10.Mobile Prefix Solicitation (*2)
	·->	i	i		11.Mobile Prefix Advertisement
		I	I		I

- 1. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)
- a. IKE Phase1 (ISAKMP SA)
- b. IKE Phase2 (IPsec SA1/SA2)



- 2. Receive Binding Update. (NUTX -> HA0) (Refer to 5.14.1)
- 3. Send Binding Acknowledgement. (HA0 -> NUTX) (Refer to 5.15.1) # The Status field is set to 1(accepted but prefix discovery necessary).
- c. IKE Phase2 (IPsec SA5/SA6)
- 4. Receive Mobile Prefix Solicitation. (NUTX -> HA0 with Home Address Option) (Refer to 5.19.1)
- 5. Send Mobile Prefix Advertisement. (HA0 -> NUTX with Type2 Routing Header) (Refer to 5.20.1)
- 6. Send Router Advertisement. (R2 -> R2_allnode_multi) (Refer to 5.2.1)
- 7. Receive Binding Update. (NUTY -> HA0) (Refer to 5.14.1) # (K)bit on
- 8. Send Binding Acknowledgement. (HA0 -> NUTY) (Refer to 5.15.1) # (K)bit on
- d. (update ISAKMP SA)
- e. (expire IPsec SA5/SA6)
- f. IKE Phase2 (IPsec SA5/SA6) (*1)
- 9. Send unsolicited Mobile Prefix Advertisement. (HA0 -> NUTY with Type2 Routing Header) (Refer to 5.20.1)
- 10. Receive Mobile Prefix Solicitation. (NUTY -> HA0 with Home Address Option) (*2) (Refer to 5.19.1)

IPv6 Header	Source Address	MN care-of (global)
	Destination Address	HA (global)
Destination Option Header	Home Address of Mobile Node	MN home (global)
Encapsulating	Security Parameters Index	Any
Security	Sequence Number	Any
Payload	Initialization Vector	Any
Mobility Header	Type	146

11. Send Mobile Prefix Advertisement. (HA0 -> NUTY with Type2 Routing Header) (Refer to 5.20.1)

[JUDGMENT]

- (*1) PASS: IPsec SA5/SA6 is re-established without re-establishment of ISAKMP SA.
- (*2) PASS: CN0 receives Mobile Prefix Solicitation.

Then, check whether this packet fills all of the following,

- using new IPsec SA5.

[REFERENCES]

RFC3775 Mobility Support in IPv6 See Section 11.7.1, 11.7.3



6.13.2.3.5 MN-1-2-3-1-010 - Sending MPS (Foreign -> Home -> Foreign, ISAKMP SA expired, IPsec SA5/SA6 expired)

[PURPOSE]

MN-1-2-3-1-010 - Sending MPS (Foreign -> Home -> Foreign, ISAKMP SA expired, IPsec SA5/SA6 expired)

[CATEGORY]

HOST: ADVANCED FUNCTION (IKE (AND MPD))

[REQUIREMENT OF TEST]

Function of IKE: YES

Function of Mobile Prefix Discovery: YES

Function of Real Home Link: YES

[TOPORGY]

Refer to 2.1.1.1 Common Topology-1

[TEST SETUP]

Refer to 3.1 Common Setup-1

[INITIALIZATION]

HA0	NUT0	R1	R2	CNO
	1		1	1
	->		- 1	1.Router Advertisement
			- 1	I
	NUTX		- 1	I
			- 1	I
	<	-	-	2.Router Advertisement
			- 1	I
<				3.Neighbor Solicitation
				4.(no reply)
	1			I

- 1. Send Router Advertisement. (HA0 -> HA0_allnode_multi) (Refer to 5.2.2)
- 2. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)
- 3. Receive Neighbor Solicitation. (NUT0 -> HA0) (Refer to 5.3.3)
- 4. (no reply)

_				
HA0	NUTX	R1	R2	CNO
			- 1	
	<		- 1	1.Router Advertisement
			- 1	1
<=	==>		1	a.IKE Phase1 (ISAKMP SA)



<==>	b.IKE Phase2 (IPsec SA1/SA2)
	2.Binding Update 3.Binding Acknowledgement
	c.IKE Phase2 (IPsec SA5/SA6)
	4.Mobile Prefix Solicitation 5.Mobile Prefix Advertisement
NUTO	
	6.Router Advertisement
<	7.Binding Update
>	8.Binding Acknowledgement
	9.Neighbor Advertisement
	į :
	d.(expire ISAKMP SA)
	 :
	e.(expire IPsec SA5/SA6)
NUTX	
	10.Router Advertisement
<	11.Binding Update
>	12.Binding Acknowledgement
	f.IKE Phase1 (ISAKMP SA)
<===>	g.IKE Phase2 (IPsec SA5/SA6) (*1)
	13.Mobile Prefix Solicitation (*2)
>	14.Mobile Prefix Advertisement
	 15.Binding Update (*3)
>	16.Binding Acknowledgement
	I

1. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)



- a. IKE Phase1 (ISAKMP SA)
- b. IKE Phase2 (IPsec SA1/SA2)
- 2. Receive Binding Update. (NUTX -> HA0) (Refer to 5.14.1)
- 3. Send Binding Acknowledgement. (HA0 -> NUTX) (Refer to 5.15.1)# The Status field is set to 1(accepted but prefix discovery necessary).
- c. IKE Phase2 (IPsec SA5/SA6)
- 4. Receive Mobile Prefix Solicitation. (NUTX -> HA0 with Home Address Option) (Refer to 5.19.1)
- 5. Send Mobile Prefix Advertisement. (HA0 -> NUTX with Type2 Routing Header) (Refer to 5.20.1)
- 6. Send Router Advertisement. (HA0 -> HA0_allnode_multi) (Refer to 5.2.2)
- 7. Receive Binding Update. (NUT0 -> HA0) (Refer to 5.14.1)
- 8. Send Binding Acknowledgement. (HA0 -> NUT0) (Refer to 5.15.1)
- 9. Receive Neighbor Advertisement. (NUT0(Unspecified) -> HA0_allnode_multi) (Refer to 5.4.1)
- d. (expire ISAKMP SA)
- e. (expire IPsec SA5/SA6)
- 10. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)
- 11. Receive Binding Update. (NUTX -> HA0) (Refer to 5.14.1)
- 12. Send Binding Acknowledgement. (HA0 -> NUTX) (Refer to 5.15.1) # The Status field is set to 1(accepted but prefix discovery necessary).
- f. IKE Phase1 (ISAKMP SA)
- g. IKE Phase2 (IPsec SA5/SA6) (*1)
- 13. Receive Mobile Prefix Solicitation. (NUTX -> HA0 with Home Address Option) (*2) (Refer to 5.19.1)

IPv6 Header	Source Address	MN care-of (global)
	Destination Address	HA (global)
Destination Option Header	Home Address of Mobile Node	MN home (global)
Encapsulating	Security Parameters Index	Any
Security	Sequence Number	Any
Payload	Initialization Vector	Any
Mobility Header	Туре	146

- 14. Send Mobile Prefix Advertisement. (HA0 -> NUTX with Type2 Routing Header) (Refer to 5.20.1)
 - # The Prefix Information option is included, and,
 - # The Valid Lifetime is set less than the remaining lifetime of the home registration.
 - # The Preferred Lifetime is set less than the remaining lifetime of the home registration.



15. Receive Binding Update. (NUTX -> HA0) (*3) (Refer to 5.14.1)

IPv6 Header	Source Address	5	MN care-of (global)
	Destination Add	HA (global)	
Destination Option Header	Home Address		MN home (global)
Encapsulating	Security Param	eter Index	Any
Security	Sequence		Any
Payload	Initialization Ve	ctor	Any
Mobility Header	MH Type		5
Mobility options	ns Alternate Care-of	Туре	3
		Option Length	16
	Address	Address	MN care-of

16. Send Binding Acknowledgement. (HA0 -> NUTX) (Refer to 5.15.1)

[JUDGMENT]

- (*1) PASS: IPsec SA5/SA6 is re-established after re-establishing ISAKMP SA.
- (*2) PASS: HA0 receives Mobile Prefix Solicitation.
 - Then, check whether this packet fills all of the following,
 - using new IPsec SA5.
- (*3) PASS: HA0 receives Binding Update.

[REFERENCES]

RFC3776 Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents

See Section 4.2



6.13.2.3.6 MN-1-2-3-1-014 - Sending MPS (Foreign -> Home -> Foreign, ISAKMP SA exist, IPsec SA5/SA6 expired)

[PURPOSE]

 $MN\mbox{-}1\mbox{-}2\mbox{-}3\mbox{-}1\mbox{-}014$ - Sending MPS (Foreign -> Home -> Foreign, ISAKMP SA exist, IPsec SA5/SA6 expired)

[CATEGORY]

HOST: ADVANCED FUNCTION (IKE (AND MPD))

[REQUIREMENT OF TEST]

Function of IKE: YES

Function of Mobile Prefix Discovery: YES

Function of Real Home Link: YES

NUT sets (K) bit in BU which is transmitted to HA: YES

[TOPORGY]

Refer to 2.1.1.1 Common Topology-1

[TEST SETUP]

Refer to 3.1 Common Setup-1

[INITIALIZATION]

HA0	NUT0	R1	R2	CNO
		1		1
	>	1		1.Router Advertisement
		1		I
	NUTX	1		I
		1		I
	<			2.Router Advertisement
				I
<-				3.Neighbor Solicitation
				4.(no reply)
		1		I

- 1. Send Router Advertisement. (HA0 -> HA0_allnode_multi) (Refer to 5.2.2)
- 2. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)
- 3. Receive Neighbor Solicitation. (NUT0 -> HA0) (Refer to 5.3.3)
- 4. (no reply)

HA0	NUTX	R1	R2	CNO	
	1	1	1	1	
	<		1	1.Router Advertiseme	ent
- 1			- 1	1	



١	<==>		a.IKE Phase1 (ISAKMP SA)
 	<==>		b.IKE Phase2 (IPsec SA1/SA2)
i	<	i i	2.Binding Update
	>		3.Binding Acknowledgement
	<===>		 c.IKE Phase2 (IPsec SA5/SA6)
i	<	i i	4.Mobile Prefix Solicitation
١	>		5.Mobile Prefix Advertisement
	NUTO		
	>		 6.Router Advertisement
İ	<		7.Binding Update
	>		8.Binding Acknowledgement
 	< 		l 9.Neighbor Advertisement
į	į		 :
			l d.(expire IPsec SA5/SA6)
	NUTX		
 	 <		 10.Router Advertisement
i	<		11.Binding Update
١	>		12.Binding Acknowledgement
	 <==> 		 e.IKE Phase2 (IPsec SA5/SA6) (*1)
İ	<		1 13.Mobile Prefix Solicitation (*2)
	>		14.Mobile Prefix Advertisement
	<		ı 15.Binding Update (*3)
ا	>		16.Binding Acknowledgement
	I		

- 1. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)
- a. IKE Phase1 (ISAKMP SA)
- b. IKE Phase2 (IPsec SA1/SA2)



- 2. Receive Binding Update. (NUTX -> HA0) (Refer to 5.14.1)
- 3. Send Binding Acknowledgement. (HA0 -> NUTX) (Refer to 5.15.1) # The Status field is set to 1(accepted but prefix discovery necessary).
- c. IKE Phase2 (IPsec SA5/SA6)
- 4. Receive Mobile Prefix Solicitation. (NUTX -> HA0 with Home Address Option) (Refer to 5.19.1)
- 5. Send Mobile Prefix Advertisement. (HA0 -> NUTX with Type2 Routing Header) (Refer to 5.20.1)
- 6. Send Router Advertisement. (HA0 -> HA0_allnode_multi) (Refer to 5.2.2)
- 7. Receive Binding Update. (NUT0 -> HA0) (Refer to 5.14.1)
- 8. Send Binding Acknowledgement. (HA0 -> NUT0) (Refer to 5.15.1)
- 9. Receive Neighbor Advertisement. (NUT0(Unspecified) -> HA0_allnode_multi) (Refer to 5.4.1)
- d. (expire IPsec SA5/SA6)
- 10. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)
- 11. Receive Binding Update. (NUTX -> HA0) (Refer to 5.14.1) # (K)bit on
- 12. Send Binding Acknowledgement. (HA0 -> NUTX) (Refer to 5.15.1)
 - # (K)bit on
 - # The Status field is set to 1(accepted but prefix discovery necessary).
- e. IKE Phase2 (IPsec SA5/SA6) (*1)
- 13. Receive Mobile Prefix Solicitation. (NUTX -> HA0 with Home Address Option) (*2) (Refer to 5.19.1)

`	,	
IPv6 Header	Source Address	MN care-of (global)
	Destination Address	HA (global)
Destination Option Header	Home Address of Mobile Node	MN home (global)
Encapsulating	Security Parameters Index	Any
Security	Sequence Number	Any
Payload	Initialization Vector	Any
Mobility Header Type		146

- 14. Send Mobile Prefix Advertisement. (HA0 -> NUTX with Type2 Routing Header) # The Prefix Information option is included, and,
 - # The Valid Lifetime is set less than the remaining lifetime of the home registration.
 - # The Preferred Lifetime is set less than the remaining lifetime of the home registration.
- 15. Receive Binding Update. (NUTX -> HA0) (*3) (Refer to 5.14.1)

IPv6 Header	Source Address	MN care-of (global)
	Destination Address	HA (global)
Destination Option Header	Home Address	MN home (global)
Encapsulating	Security Parameter Index	Any
Security	Sequence	Any
Payload	Initialization Vector	Any



Mobility Header	MH Type		5
Mobility options	Alternate	Туре	3
	Care-of	Option Length	16
	Address	Address	MN care-of

16. Send Binding Acknowledgement. (HA0 -> NUTX)

[JUDGMENT]

(*1) PASS: IPsec SA5/SA6 is re-established.

(*2) PASS: HA0 receives Mobile Prefix Solicitation.

Then, check whether this packet fills all of the following,

- using new IPsec SA5.

(*3) PASS: HA0 receives Binding Update.

[REFERENCES]

RFC3776 Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents

See Section 4.2



6.13.2.3.7 MN-1-2-3-1-017 - Sending MPS (Foreign -> Home -> Foreign, IPsec SA5/SA6 exist)

[PURPOSE]

MN-1-2-3-1-017 - Sending MPS (Foreign -> Home -> Foreign, IPsec SA5/SA6 exist)

[CATEGORY]

HOST: ADVANCED FUNCTION (IKE (AND MPD))

[REQUIREMENT OF TEST]

Function of IKE: YES

Function of Mobile Prefix Discovery: YES

Function of Real Home Link: YES

[TOPORGY]

Refer to 2.1.1.1 Common Topology-1

[TEST SETUP]

Refer to 3.1 Common Setup-1

[INITIALIZATION]

HA0	NUT0	R1	R2	CNO
1	1	- 1	- 1	1
	>		- 1	1.Router Advertisement
	1		1	1
	NUTX		1	1
	1		1	1
1	<		- 1	2.Router Advertisement
	1		1	1
<-				3.Neighbor Solicitation
1	1			4.(no reply)
1	1		- 1	1

- 1. Send Router Advertisement. (HA0 -> HA0_allnode_multi) (Refer to 5.2.2)
- 2. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)
- 3. Receive Neighbor Solicitation. (NUT0 -> HA0) (Refer to 5.3.3)
- 4. (no reply)

HA0	NUTX	R1	R2	CNO
			- 1	I
	<		- 1	1.Router Advertisement
				I
<=	==>			a.IKE Phase1 (ISAKMP SA)
<=	==>	1	1	l b.IKE Phase2 (IPsec SA1/SA2)



	I
<	2.Binding Update
>	3.Binding Acknowledgement
	I Stricting Acknowledgement
<===>	c.IKE Phase2 (IPsec SA5/SA6)
	I C. TRE THASEZ (TI SEC SASTONO)
	I 4.Mobile Prefix Solicitation
<	!
>	5.Mobile Prefix Advertisement
NUTO	
!!!!!	
>	6.Router Advertisement
<	7.Binding Update
>	8.Binding Acknowledgement
<	9.Neighbor Advertisement
NUTX	
	10.Router Advertisement
	[
<	11.Binding Update
>	12.Binding Acknowledgement
	_
<	13.Mobile Prefix Solicitation (*1)
>	14.Mobile Prefix Advertisement
i i i	i I
<	15.Binding Update (*2)
>	16.Binding Acknowledgement
	1

- 1. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)
- a. IKE Phase1 (ISAKMP SA)
- b. IKE Phase2 (IPsec SA1/SA2)
- 2. Receive Binding Update. (NUTX -> HA0) (Refer to 5.14.1)
- 3. Send Binding Acknowledgement. (HA0 -> NUTX) (Refer to 5.15.1) # The Status field is set to 1(accepted but prefix discovery necessary).
- c. IKE Phase2 (IPsec SA5/SA6)
- 4. Receive Mobile Prefix Solicitation. (NUTX -> HA0 with Home Address Option) (Refer to 5.19.1)



- 5. Send Mobile Prefix Advertisement. (HA0 -> NUTX with Type2 Routing Header) (Refer to 5.20.1)
- 6. Send Router Advertisement. (HA0 -> HA0_allnode_multi) (Refer to 5.2.2)
- 7. Receive Binding Update. (NUT0 -> HA0) (Refer to 5.14.1)
- 8. Send Binding Acknowledgement. (HA0 -> NUT0) (Refer to 5.15.1)
- 9. Receive Neighbor Advertisement. (NUT0(Unspecified) -> HA0_allnode_multi) (Refer to 5.4.1)
- 10. Send Router Advertisement. (R1 -> R1_allnode_multi) (Refer to 5.2.1)
- 11. Receive Binding Update. (NUTX -> HA0) (Refer to 5.14.1)
- 12. Send Binding Acknowledgement. (HA0 -> NUTX) (Refer to 5.15.1)
 - # The Status field is set to 1(accepted but prefix discovery necessary).
- 13. Receive Mobile Prefix Solicitation. (NUTX -> HA0 with Home Address Option) (*1) (Refer to 5.19.1)

(-) ()					
IPv6 Header	Source Address	MN care-of (global)			
	Destination Address	HA (global)			
Destination Option Header	Home Address of Mobile Node	MN home (global)			
Encapsulating	Security Parameters Index	Any			
Security	Sequence Number	Any			
Payload	Initialization Vector	Any			
Mobility Header	Type	146			

- 14. Send Mobile Prefix Advertisement. (HA0 -> NUTX with Type2 Routing Header) # The Prefix Information option is included, and,
 - * The Valid Lifetime is set less than the remaining lifetime of the home registration.
 - # The Preferred Lifetime is set less than the remaining lifetime of the home registration.
- 15. Receive Binding Update. (NUTX -> HA0) (*2) (Refer to 5.14.1)
- 16. Send Binding Acknowledgement. (HA0 -> NUTX)

[JUDGMENT]

(*1) PASS: CN0 receives Mobile Prefix Solicitation.

Then, check whether this packet fills all of the following,

- using old IPsec SA5.
- (*2) PASS: HA0 receives Binding Update.

[REFERENCES]

RFC3776 Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents

See Section 4.2



AUTHOR'S LIST

Yasushi Takagi (NTT)

Masaya Tanaka (NTT)

Masaharu Sasaki (NTT)

Keisuke Sakitani (NTT)

Masamitsu Yoshida (NTT)

Harutaka Ueno (NTT)

Takaaki Sato (NTT)

Yoshio Yoshida (NTT-AT)

Noriko Mizusawa (NTT-AT)

Taisuke Sako (NTT-AT)

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)

Tamami Miyazaki (YASKAWA INFORMATION SYSTEMS Corporation)

Shiho Homan (YASKAWA INFORMATION SYSTEMS Corporation)

Copyright (C) 2005 - 2007 Nippon Telegraph and Telephone Corporation (NTT), NTT Advanced Technology Corporation (NTT-AT), YASKAWA INFORMATION SYSTEMS Corporation, Yokogawa Electric Corporation, and IPv6 Forum. All Rights Reserved.

No part of this documentation may be reproduced for any purpose without prior permission.