

Test Specification  
For DHCPv6

Authentication Protocol

Revision Alpha 0.1

# References

This test specification focus on following DNS related RFCs.

RFC

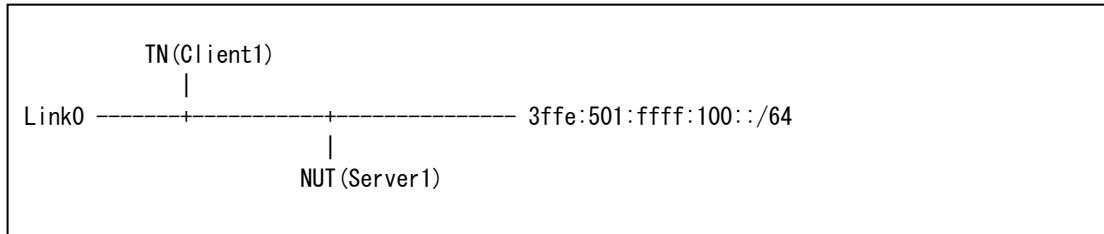
## ---TOC---

References.....	1
1. Introduction.....	4
2. Common Topology.....	5
3. Terminology .....	6
4. Description .....	7
5. Relay agent Test.....	8
5.1. Delayed Authentication Protocol Server .....	8
5.2. Multiple Authentication option are included .....	10
5.3. MD5 is mismatched.....	12
5.4. Key utilization.....	14
5.5. Receiving Solicit Message and Sending Advertise Message.....	16
5.6. Receiving Confirm Message and Sending Reply Message.....	18
5.7. Receiving Confirm Message and Sending Reply Message.....	20
5.8. Receiving Renew Message and Sending Reply Message .....	22
5.9. Receiving Renew Message and validation test is failed.....	24
5.10. Receiving Rebind Message and Sending Reply Message.....	26
5.11. Receiving rebind Message and validation test is failed .....	28
5.12. Receiving Decline Message and Sending Reply Message.....	30
5.13. Receiving Decline Message and validation test is failed.....	32
5.14. Receiving Release Message and Sending Reply Message.....	34
5.15. Receiving Release Message and validation test is failed.....	36
5.16. Receiving Information-request Message and Sending Reply Message .....	38
5.17. Receiving Information-request Message and validation test is failed.....	40
5.18. Sending Reconfigure Messages.....	42
5.19. Reconfigure Key Authentication Protocol for Server .....	44
5.20. Receiving Solicit Message and Sending Reply Message .....	46
5.21. Receiving Information -request Message and Sending Replay Message ...	48
5.22. Delayed Authentication Protocol for Client.....	50
5.23. Multiple Authentication option are included .....	52
5.24. MD5 is mismatched.....	54

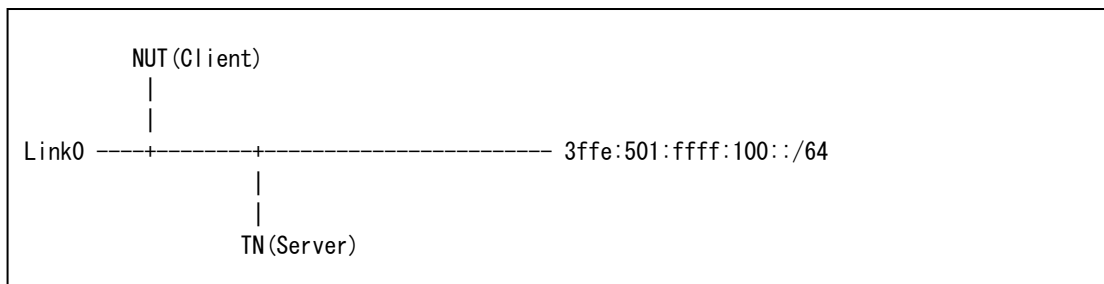
5.25.	Key Utilization .....	56
5.26.	Sending Solicit message .....	58
5.27.	Receiving Advertise Messages.....	60
5.28.	Sending Confirm message.....	62
5.29.	Sending Renew message .....	64
5.30.	Sending Rebind message .....	66
5.31.	Sending Decline message.....	68
5.32.	Sending Release message.....	70
5.33.	Sending Information-Request message.....	72
5.34.	Receiving Reply Messages and validation test is failed.....	74
5.35.	Receiving Reconfigure Messages(Renew message).....	76
5.36.	Receiving Reconfigure Messages(Informational-request message).....	78
5.37.	Receiving Reconfigure Messages and validation test is failed.....	80
5.38.	Checking Key Authentication Protocol for Client.....	82
5.39.	Sending Request Message and Receiving Reply Message.....	84
5.40.	Request/Reply Exchange finished, Receiving Reconfigure Message and validation test is failed .....	86
5.41.	Sending Solicit Message and Receiving Reply Message.....	88
5.42.	Solicit/Reply Exchange finished, Receiving Reconfigure Message and validation test is failed .....	90
5.43.	Sending Information-request Message and Receiving Reply Message.....	92
5.44.	Information-Request/Reply Exchange finished, Receiving Reconfigure Message and validation test is failed.....	94

# 1. Introduction

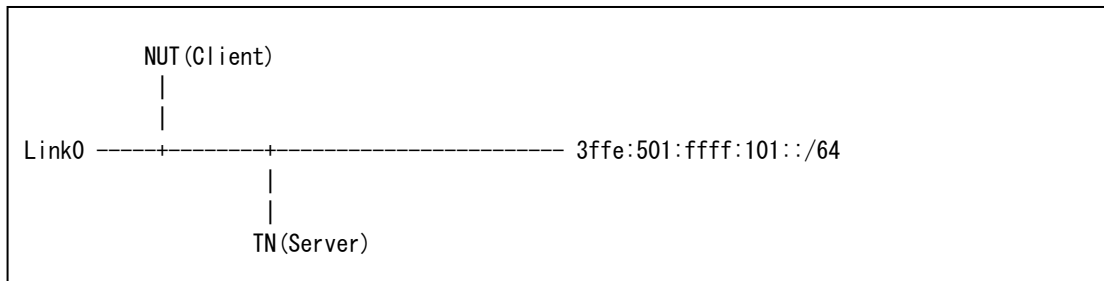
## 2. Common Topology



**Fig. 1 Topology No.1**



**Fig. 2 Topology No.2**



**Fig. 3 Topology No.3**

### 3. Terminology

## 4. Description

Each test specification consists of following parts.

**Purpose:** The Purpose is the short statement describing what the test attempts to achieve. It is usually phrased as a simple assertion of the future or capability to be tested.

**Category:** The Category shows what classification of device must satisfy the test.

**Initialization:** The Initialization describes how to initialize and configure the NUT before starting each test. If a value is not provided, then the protocol's default value is used.

**Procedure:** The Procedure describes step-by-step instructions for carrying out the test.

**Judgment:** The Judgment describes expected result. If we can observe as same result as the description of Judgment, the NUT passes the test.

**References:** The References section contains some parts of specification

## 5. Relay agent Test

### 5.1. Delayed Authentication Protocol Server

#### Purpose:

- **Verification Points**

To validate an incoming message, the receiver first checks that the value in the replay detection field is acceptable according to the replay detection method specified by the RDM field. Next, the receiver computes the MAC as described in [8]. The entire DHCP message (setting the MAC field of the authentication option to 0) is used as input to the HMAC-MD5 computation function. If the MAC computed by the receiver does not match the MAC contained in the authentication option, the receiver **MUST** discard the DHCP message.

After receiving a Solicit message that contains an Authentication option, the server selects a key for the client, based on the client's DUID and key selection policies with which the server has been configured. The server identifies the selected key in the Advertise message and uses the key to validate subsequent messages between the client and the server.

If the message passes the validation test, the server responds to the specific message as described in section 18.2. The server **MUST** include authentication information generated using the key identified in the received message, as specified in section 21.4.

#### Category:

Server

#### Initialization:

- **Network Topology**

Refer the topology "Fig. 1 Topology No.1".

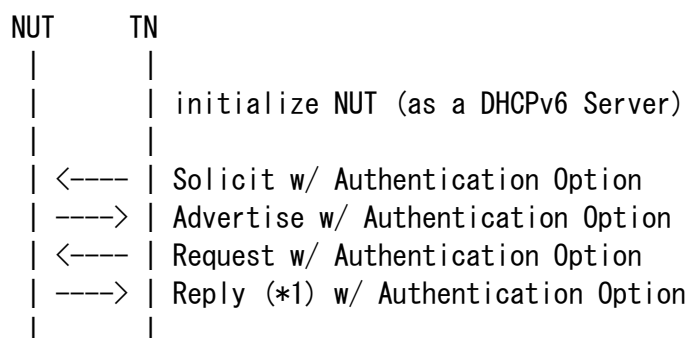
- **Configuration**

Enable Delayed Authentication Protocol Service Authentication parameter

- ✧ DHCP realm: DHCPv6.TEST.EXAMPLE.COM
- ✧ Client DUID: 00:01:00:01:00:04:93:e0:00:00:00:00:a2:a2
- ✧ Key id: 1
- ✧ Shared secret key: TEST\_VALID12

Device Name	Device Type	I/F	Assigned Prefix	Link Local Addr	MAC Addr
Server1	NUT	Link0	3ffe:501:ffff:100::/64	NUT's Linklocal address	NUT's MAC address
Client1	TN	Link0	3ffe:501:ffff:100::/64	fe80::200:ff:fe00:a2a2	00:00:00:00:a2:a2

**Procedure:**



- **Termination**

N/A

**Judgment:**

(\*1) PASS: The Solicit & Advertise & Request message must exchanged correctly. NUT will respond with Reply message. The Reply message must include Server ID option, Client ID and Authentication option, and check its 'msg-type' and 'transaction ID' OK.

**References:**

RFC3315

21.4.5 Server Considerations for Delayed Authentication protocol

22.11 Authentication Option

## 5.2. Multiple Authentication option are included

### Purpose:

- **Verification Points**

Any DHCP message that includes more than one authentication option **MUST** be discarded.

### Category:

Server

### Initialization:

- **Network Topology**

Refer the topology "Fig. 1 Topology No.1".

- **Configuration**

Enable Delayed Authentication Protocol Service Authentication parameter

✧ DHCP realm: DHCPv6. TEST. EXAMPLE. COM

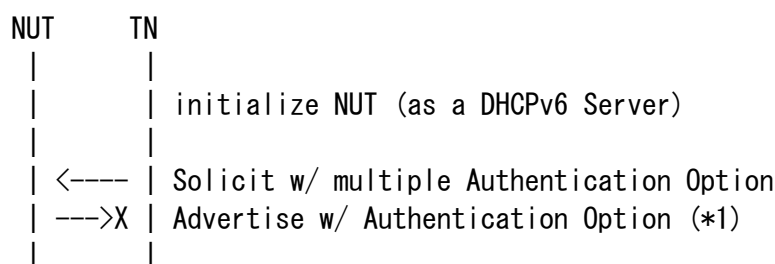
✧ Client DUID: 00:01:00:01:00:04:93:e0:00:00:00:00:a2:a2

✧ Key id: 1

✧ Shared secret key: TEST\_VALID12

Device Name	Device Type	I/F	Assigned Prefix	Link Local Addr	MAC Addr
Server1	NUT	Link0	3ffe:501:ffff:100::/64	NUT's Linklocal address	NUT's MAC address
Client1	TN	Link0	3ffe:501:ffff:100::/64	fe80::200:ff:fe00:a2a2	00:00:00:00:a2:a2

### Procedure:



- **Termination**

N/A

**Judgment:**

(\*1) PASS: If NUT received solicit message that includes more than one authentication option, NUT MUST discard it.

**References:**

RFC3315

21.4.2. Message Validation

21.4.5 Server Considerations for Delayed Authentication protocol

22.11 Authentication Option

### 5.3. MD5 is mismatched

#### Purpose:

- **Verification Points**

To validate an incoming message, the receiver first checks that the value in the replay detection field is acceptable according to the replay detection method specified by the RDM field. Next, the receiver computes the MAC as described in [8]. The entire DHCP message (setting the MAC field of the authentication option to 0) is used as input to the HMAC-MD5 computation function. If the MAC computed by the receiver does not match the MAC contained in the authentication option, the receiver **MUST** discard the DHCP message.

#### Category:

Server

#### Initialization:

- **Network Topology**

Refer the topology "Fig.1 Topology No.1".

- **Configuration**

Enable Delayed Authentication Protocol Service Authentication parameter

- ✧ DHCP realm: DHCPv6.TEST.EXAMPLE.COM
- ✧ Client DUID: 00:01:00:01:00:04:93:e0:00:00:00:00:a2:a2
- ✧ Key id: 1
- ✧ Shared secret key: TEST\_VALID12

Device Name	Device Type	I/F	Assigned Prefix	Link Local Addr	MAC Addr
Server1	NUT	Link0	3ffe:501:ffff:100::/64	NUT's Linklocal address	NUT's MAC address
Client1	TN	Link0	3ffe:501:ffff:100::/64	fe80::200:ff:fe00:a2a2	00:00:00:00:a2:a2

**Procedure:**

NUT	TN
	initialize NUT (as a DHCPv6 Server)
<----	Solicit w/ Authentication Option
---->	Advertise w/ Authentication Option
<----	Request w/ Authentication Option including invalid MAC
---->X	Reply w/ Authentication Option (*1)

- **Termination**

N/A

**Judgment:**

(\*1) PASS: If NUT received the message that includes invalid MAC, NUT discards it.

**References:**

RFC3315  
21.4.2. Message Validation  
22.11 Authentication Option

## 5.4. Key utilization

### Purpose:

- **Verification Points**

Each DHCP client has a set of keys. Each key is identified by <DHCP realm, client DUID, key id>. Each key also has a lifetime. The key may not be used past the end of its lifetime. The client's keys are initially distributed to the client through some out-of-band mechanism. The lifetime for each key is distributed with the key.

Mechanisms for key distribution and lifetime specification are beyond the scope of this document.

### Category:

Server

### Initialization:

- **Network Topology**

Refer the topology "Fig. 1 Topology No.1".

- **Configuration**

Enable Delayed Authentication Protocol Service

Authentication parameter

✧ DHCP realm: DHCPv6.TEST.EXAMPLE.COM

✧ Client DUID: 00:01:00:01:00:04:93:e0:00:00:00:00:a2:a2

✧ Key id: 1

✧ Shared secret key: TEST\_VALID12

Device Name	Device Type	I/F	Assigned Prefix	Link Local Addr	MAC Addr
Server1	NUT	Link0	3ffe:501:ffff:100::/64	NUT's Linklocal address	NUT's MAC address
Client1	TN	Link0	3ffe:501:ffff:100::/64	fe80::200:ff:fe00:a2a2	00:00:00:00:a2:a2

**Procedure:**

NUT	TN
	initialize NUT (as a DHCPv6 Server)
<----	Solicit w/ Authentication Option
---->	Advertise w/ Authentication Option
<----	Request w/ Authentication Option using Key id = 2
---->X	Reply w/ Authentication Option (*1)
<----	Solicit w/ Authentication Option
---->	Advertise w/ Authentication Option
<----	Request w/ Authentication Option using Key id = 1
---->	Reply w/ Authentication Option (*2)

- **Termination**  
N/A

**Judgment:**

- (\*1) PASS: If NUT received message that includes unrecognized Key id, NUT discards it.
- (\*2) PASS: If NUT received message that includes recognized Key id, NUT reply it.

**References:**

RFC3315  
21.4.3. Key Utilization  
21.4.5 Server Considerations for Delayed Authentication protocol  
22.11 Authentication Option

## 5.5. Receiving Solicit Message and Sending Advertise Message

### Purpose:

- **Verification Points**

The server selects a key for the client and includes authentication information in the Advertise message returned to the client as specified in section 21.4. The server **MUST** record the identifier of the key selected for the client and use that same key for validating subsequent messages with the client.

### Category:

Server

### Initialization:

- **Network Topology**

Refer the topology "Fig.1 Topology No.1".

- **Configuration**

Enable Delayed Authentication Protocol Service

Authentication parameter:

- ✧ DHCP realm: DHCPv6.TEST.EXAMPLE.COM
- ✧ Client DUID: 00:01:00:01:00:04:93:e0:00:00:00:a2:a2
- ✧ Key id: 1
- ✧ Shared secret key: TEST\_VALID12

Device Name	Device Type	I/F	Assigned Prefix	Link Local Addr	MAC Addr
Server1	NUT	Link0	3ffe:501:ffff:100::/64	NUT's Linklocal address	NUT's MAC address
Client1	TN	Link0	3ffe:501:ffff:100::/64	fe80::200:ff:fe00:a2a2	00:00:00:00:a2:a2

**Procedure:**

NUT	TN
	initialize NUT (as a DHCPv6 Server)
<----	Solicit w/ Authentication Option
---->	Advertise w/ Authentication Option
<----	Request w/ Authentication Option
---->	Reply w/ Authentication Option using key as same as Advertise (*1)

- **Termination**

N/A

**Judgment:**

(\*1) PASS: NUT MUST use that same key for validating subsequent messages with the client.

**References:**

RFC3315

21.4.5 Server Considerations for Delayed Authentication protocol

21.4.5.1. Receiving Solicit Messages and Sending Advertise Messages

22.11 Authentication Option

## 5.6. Receiving Confirm Message and Sending Reply Message

### Purpose:

- **Verification Points**

The server uses the key identified in the message and validates the message as specified in section 21.4.2.

If the message passes the validation test, the server responds to the specific message as described in section 18.2. The server **MUST** include authentication information generated using the key identified in the received message, as specified in section 21.4.

### Category:

Server

### Initialization:

- **Network Topology**

Refer the topology "Fig. 1 Topology No.1".

- **Configuration**

Enable Delayed Authentication Protocol Service Authentication parameter

✧ DHCP realm: DHCPv6.TEST.EXAMPLE.COM

✧ Client DUID: 00:01:00:01:00:04:93:e0:00:00:00:00:a2:a2

✧ Key id: 1

✧ Shared secret key: TEST\_VALID12

Device Name	Device Type	I/F	Assigned Prefix	Link Local Addr	MAC Addr
Server1	NUT	Link0	3ffe:501:ffff:100::/64	NUT's Linklocal address	NUT's MAC address
Client1	TN	Link0	3ffe:501:ffff:100::/64	fe80::200:ff:fe00:a2a2	00:00:00:00:a2:a2

**Procedure:**

NUT	TN
	initialize NUT (as a DHCPv6 Server)
<----	Solicit w/ Authentication Option
---->	Advertise w/ Authentication Option
<----	Request w/ Authentication Option
---->	Reply w/ Authentication Option
<----	Confirm (w/ IA_NA, IA Address w/o Status Code and Authentication Option)
---->	Reply (w/ Authentication Option that includes Authentication information) (*1)

- **Termination**

N/A

**Judgment:**

(\*1) PASS: If NUT received Confirm message, the message passes the validation test, the NUT respond to the message that includes Authentication option.

**References:**

RFC3315

21.4.5 Server Considerations for Delayed Authentication protocol

21.4.5.2. Receiving Request, Confirm, Renew, Rebind or Release Messages and Sending Reply Messages

22.11 Authentication Option

## 5.7. Receiving Confirm Message and Sending Reply Message

### Purpose:

- **Verification Points**

The server uses the key identified in the message and validates the message as specified in section 21.4.2. If the message fails to pass the validation test or the server does not know the key identified by the 'key ID' field, the server **MUST** discard the message and **MAY** choose to log the validation failure.

### Category:

Server

### Initialization:

- **Network Topology**

Refer the topology "Fig.1 Topology No.1".

- **Configuration**

Enable Delayed Authentication Protocol Service Authentication parameter

✧ DHCP realm: DHCPv6.TEST.EXAMPLE.COM

✧ Client DUID: 00:01:00:01:00:04:93:e0:00:00:00:00:a2:a2

✧ Key id: 1

✧ Shared secret key: TEST\_VALID12

Device Name	Device Type	I/F	Assigned Prefix	Link Local Addr	MAC Addr
Server1	NUT	Link0	3ffe:501:ffff:100::/64	NUT's Linklocal address	NUT's MAC address
Client1	TN	Link0	3ffe:501:ffff:100::/64	fe80::200:ff:fe00:a2a2	00:00:00:00:a2:a2

**Procedure:**

NUT	TN
	initialize NUT (as a DHCPv6 Server)
<----	Solicit w/ Authentication Option
---->	Advertise w/ Authentication Option
<----	Request w/ Authentication Option
---->	Reply (*1) w/ Authentication Option
<----	Confirm (w/ IA_NA, IA Address w/o Status Code and Authentication Option key id = 2)
---->X	No Reply (w/ Authentication Option that includes Authentication information) (*1)

- **Termination**

N/A

**Judgment:**

(\*1) PASS: If NUT received Confirm message, the message failed the validation test, the NUT MUST discard the message.

**References:**

RFC3315

21.4.5 Server Considerations for Delayed Authentication protocol

21.4.5.2. Receiving Request, Confirm, Renew, Rebind or Release Messages and Sending Reply Messages

22.11 Authentication Option

## 5.8. Receiving Renew Message and Sending Reply Message

### Purpose:

- **Verification Points**

The server uses the key identified in the message and validates the message as specified in section 21.4.2.

If the message passes the validation test, the server responds to the specific message as described in section 18.2. The server **MUST** include authentication information generated using the key identified in the received message, as specified in section 21.4.

### Category:

Server

### Initialization:

- **Network Topology**

Refer the topology "Fig. 1 Topology No.1".

- **Configuration**

Enable Delayed Authentication Protocol Service Authentication parameter

✧ DHCP realm: DHCPv6.TEST.EXAMPLE.COM

✧ Client DUID: 00:01:00:01:00:04:93:e0:00:00:00:00:a2:a2

✧ Key id: 1

✧ Shared secret key: TEST\_VALID12

Device Name	Device Type	I/F	Assigned Prefix	Link Local Addr	MAC Addr
Server1	NUT	Link0	3ffe:501:ffff:100::/64	NUT's Linklocal address	NUT's MAC address
Client1	TN	Link0	3ffe:501:ffff:100::/64	fe80::200:ff:fe00:a2a2	00:00:00:00:a2:a2

**Procedure:**

NUT	TN
	initialize NUT (as a DHCPv6 Server)
<----	Solicit w/ Authentication Option
---->	Advertise w/ Authentication Option
<----	Request w/ Authentication Option
---->	Reply w/ Authentication Option
<----	Renew (w/ Authentication Option)
---->	Reply (w/ Authentication Option that includes Authentication information) (*1)

- **Termination**

N/A

**Judgment:**

(\*1) PASS: If NUT received Renew message, the message passes the validation test, the NUT respond to the message that includes Authentication option.

**References:**

RFC3315

21.4.5 Server Considerations for Delayed Authentication protocol

21.4.5.2. Receiving Request, Confirm, Renew, Rebind or Release Messages and Sending Reply Messages

22.11 Authentication Option

## 5.9. Receiving Renew Message and validation test is failed

### Purpose:

- **Verification Points**

The server uses the key identified in the message and validates the message as specified in section 21.4.2. If the message fails to pass the validation test or the server does not know the key identified by the 'key ID' field, the server **MUST** discard the message and **MAY** choose to log the validation failure.

### Category:

Server

### Initialization:

- **Network Topology**

Refer the topology "Fig. 1 Topology No.1".

- **Configuration**

Enable Delayed Authentication Protocol Service Authentication parameter

✧ DHCP realm: DHCPv6.TEST.EXAMPLE.COM

✧ Client DUID: 00:01:00:01:00:04:93:e0:00:00:00:00:a2:a2

✧ Key id: 1

✧ Shared secret key: TEST\_VALID12

Device Name	Device Type	I/F	Assigned Prefix	Link Local Addr	MAC Addr
Server1	NUT	Link0	3ffe:501:ffff:100::/64	NUT's Linklocal address	NUT's MAC address
Client1	TN	Link0	3ffe:501:ffff:100::/64	fe80::200:ff:fe00:a2a2	00:00:00:00:a2:a2

**Procedure:**

NUT	TN
	initialize NUT (as a DHCPv6 Server)
<----	Solicit w/ Authentication Option
---->	Advertise w/ Authentication Option
<----	Request w/ Authentication Option
---->	Reply (*1) w/ Authentication Option
<----	Renew (w/ Authentication Option key id = 2)
---->X	No Reply (w/ Authentication Option that includes Authentication information) (*1)

- **Termination**

N/A

**Judgment:**

(\*1) PASS: If NUT received Renew message, the message failed the validation test, the NUT MUST discard the message.

**References:**

RFC3315

21.4.5 Server Considerations for Delayed Authentication protocol

21.4.5.2. Receiving Request, Confirm, Renew, Rebind or Release Messages and Sending Reply Messages

22.11 Authentication Option

## 5.10. Receiving Rebind Message and Sending Reply Message

### Purpose:

- **Verification Points**

The server uses the key identified in the message and validates the message as specified in section 21.4.2.

If the message passes the validation test, the server responds to the specific message as described in section 18.2. The server **MUST** include authentication information generated using the key identified in the received message, as specified in section 21.4.

### Category:

Server

### Initialization:

- **Network Topology**

Refer the topology "Fig. 1 Topology No.1".

- **Configuration**

Enable Delayed Authentication Protocol Service Authentication parameter

✧ DHCP realm: DHCPv6.TEST.EXAMPLE.COM

✧ Client DUID: 00:01:00:01:00:04:93:e0:00:00:00:00:a2:a2

✧ Key id: 1

✧ Shared secret key: TEST\_VALID12

Device Name	Device Type	I/F	Assigned Prefix	Link Local Addr	MAC Addr
Server1	NUT	Link0	3ffe:501:ffff:100::/64	NUT's Linklocal address	NUT's MAC address
Client1	TN	Link0	3ffe:501:ffff:100::/64	fe80::200:ff:fe00:a2a2	00:00:00:00:a2:a2

**Procedure:**

NUT	TN
	initialize NUT (as a DHCPv6 Server)
<----	Solicit w/ Authentication Option
---->	Advertise w/ Authentication Option
<----	Request w/ Authentication Option
---->	Reply (*1) w/ Authentication Option
<----	Rebind (w/ Authentication Option)
---->	Reply (w/ Authentication Option that includes Authentication information) (*1)

- **Termination**

N/A

**Judgment:**

(\*1) PASS: If NUT received Rebind message, the message passes the validation test, the NUT respond to the message that includes Authentication option.

**References:**

RFC3315

21.4.5 Server Considerations for Delayed Authentication protocol

21.4.5.2. Receiving Request, Confirm, Renew, Rebind or Release Messages and Sending Reply Messages

22.11 Authentication Option

## 5.11. Receiving rebind Message and validation test is failed

### Purpose:

- **Verification Points**

The server uses the key identified in the message and validates the message as specified in section 21.4.2. If the message fails to pass the validation test or the server does not know the key identified by the 'key ID' field, the server **MUST** discard the message and **MAY** choose to log the validation failure.

### Category:

Server

### Initialization:

- **Network Topology**

Refer the topology "Fig.1 Topology No.1".

- **Configuration**

Enable Delayed Authentication Protocol Service Authentication parameter

✧ DHCP realm: DHCPv6.TEST.EXAMPLE.COM

✧ Client DUID: 00:01:00:01:00:04:93:e0:00:00:00:00:a2:a2

✧ Key id: 1

✧ Shared secret key: TEST\_VALID12

Device Name	Device Type	I/F	Assigned Prefix	Link Local Addr	MAC Addr
Server1	NUT	Link0	3ffe:501:ffff:100::/64	NUT's Linklocal address	NUT's MAC address
Client1	TN	Link0	3ffe:501:ffff:100::/64	fe80::200:ff:fe00:a2a2	00:00:00:00:a2:a2

**Procedure:**

NUT	TN
	initialize NUT (as a DHCPv6 Server)
<----	Solicit w/ Authentication Option
---->	Advertise w/ Authentication Option
<----	Request w/ Authentication Option
---->	Reply w/ Authentication Option
<----	Rebind (w/ Authentication Option key id = 2)
---->X	No Reply (w/ Authentication Option that includes Authentication information) (*1)

- **Termination**

N/A

**Judgment:**

(\*1) PASS: If NUT received Rebind message, the message failed the validation test, the NUT MUST discard the message.

**References:**

RFC3315

21.4.5 Server Considerations for Delayed Authentication protocol

21.4.5.2. Receiving Request, Confirm, Renew, Rebind or Release Messages and Sending Reply Messages

22.11 Authentication Option

## 5.12. Receiving Decline Message and Sending Reply Message

### Purpose:

- **Verification Points**

The server uses the key identified in the message and validates the message as specified in section 21.4.2.

If the message passes the validation test, the server responds to the specific message as described in section 18.2. The server **MUST** include authentication information generated using the key identified in the received message, as specified in section 21.4.

### Category:

Server

### Initialization:

- **Network Topology**

Refer the topology "Fig. 1 Topology No.1".

- **Configuration**

Enable Delayed Authentication Protocol Service Authentication parameter

✧ DHCP realm: DHCPv6.TEST.EXAMPLE.COM

✧ Client DUID: 00:01:00:01:00:04:93:e0:00:00:00:00:a2:a2

✧ Key id: 1

✧ Shared secret key: TEST\_VALID12

Device Name	Device Type	I/F	Assigned Prefix	Link Local Addr	MAC Addr
Server1	NUT	Link0	3ffe:501:ffff:100::/64	NUT's Linklocal address	NUT's MAC address
Client1	TN	Link0	3ffe:501:ffff:100::/64	fe80::200:ff:fe00:a2a2	00:00:00:00:a2:a2

**Procedure:**

NUT	TN
	initialize NUT (as a DHCPv6 Server)
<----	Solicit w/ Authentication Option
---->	Advertise w/ Authentication Option
<----	Request w/ Authentication Option
---->	Reply w/ Authentication Option
<----	Decline (w/ Authentication Option)
---->	Reply (w/ Authentication Option that includes Authentication information) (*1)

- **Termination**

N/A

**Judgment:**

(\*1) PASS: If NUT received Decline message, the message passes the validation test, the NUT respond to the message that includes Authentication option.

**References:**

RFC3315

21.4.5 Server Considerations for Delayed Authentication protocol

21.4.5.2. Receiving Request, Confirm, Renew, Rebind or Release Messages and Sending Reply Messages

22.11 Authentication Option

## 5.13. Receiving Decline Message and validation test is failed

### Purpose:

- **Verification Points**

The server uses the key identified in the message and validates the message as specified in section 21.4.2. If the message fails to pass the validation test or the server does not know the key identified by the 'key ID' field, the server **MUST** discard the message and **MAY** choose to log the validation failure.

### Category:

Server

### Initialization:

- **Network Topology**

Refer the topology "Fig.1 Topology No.1".

- **Configuration**

Enable Delayed Authentication Protocol Service Authentication parameter

✧ DHCP realm: DHCPv6.TEST.EXAMPLE.COM

✧ Client DUID: 00:01:00:01:00:04:93:e0:00:00:00:00:a2:a2

✧ Key id: 1

✧ Shared secret key: TEST\_VALID12

Device Name	Device Type	I/F	Assigned Prefix	Link Local Addr	MAC Addr
Server1	NUT	Link0	3ffe:501:ffff:100::/64	NUT's Linklocal address	NUT's MAC address
Client1	TN	Link0	3ffe:501:ffff:100::/64	fe80::200:ff:fe00:a2a2	00:00:00:00:a2:a2

**Procedure:**

NUT	TN
	initialize NUT (as a DHCPv6 Server)
<----	Solicit w/ Authentication Option
---->	Advertise w/ Authentication Option
<----	Request w/ Authentication Option
---->	Reply (*1) w/ Authentication Option
<----	Decline (w/ Authentication Option key id = 2)
---->X	No Reply (w/ Authentication Option that includes Authentication information) (*1)

- **Termination**

N/A

**Judgment:**

(\*1) PASS: If NUT received Decline message, the message failed the validation test, the NUT MUST discard the message.

**References:**

RFC3315

21.4.5 Server Considerations for Delayed Authentication protocol

21.4.5.2. Receiving Request, Confirm, Renew, Rebind or Release Messages and Sending Reply Messages

22.11 Authentication Option

## 5.14. Receiving Release Message and Sending Reply Message

### Purpose:

- **Verification Points**

The server uses the key identified in the message and validates the message as specified in section 21.4.2.

If the message passes the validation test, the server responds to the specific message as described in section 18.2. The server **MUST** include authentication information generated using the key identified in the received message, as specified in section 21.4.

### Category:

Server

### Initialization:

- **Network Topology**

Refer the topology "Fig. 1 Topology No.1".

- **Configuration**

Enable Delayed Authentication Protocol Service Authentication parameter

✧ DHCP realm: DHCPv6.TEST.EXAMPLE.COM

✧ Client DUID: 00:01:00:01:00:04:93:e0:00:00:00:00:a2:a2

✧ Key id: 1

✧ Shared secret key: TEST\_VALID12

Device Name	Device Type	I/F	Assigned Prefix	Link Local Addr	MAC Addr
Server1	NUT	Link0	3ffe:501:ffff:100::/64	NUT's Linklocal address	NUT's MAC address
Client1	TN	Link0	3ffe:501:ffff:100::/64	fe80::200:ff:fe00:a2a2	00:00:00:00:a2:a2

**Procedure:**

NUT	TN
	initialize NUT (as a DHCPv6 Server)
<----	Solicit w/ Authentication Option
---->	Advertise w/ Authentication Option
<----	Request w/ Authentication Option
---->	Reply w/ Authentication Option
<----	Release (w/ Authentication Option)
---->	Reply (w/ Authentication Option that includes Authentication information) (*1)

• **Termination**

N/A

**Judgment:**

(\*1) PASS: If NUT received Release message, the message passes the validation test, the NUT respond to the message that includes Authentication option.

**References:**

RFC3315

21.4.5 Server Considerations for Delayed Authentication protocol

21.4.5.2. Receiving Request, Confirm, Renew, Rebind or Release Messages and Sending Reply Messages

22.11 Authentication Option

## 5.15. Receiving Release Message and validation test is failed

### Purpose:

- **Verification Points**

The server uses the key identified in the message and validates the message as specified in section 21.4.2. If the message fails to pass the validation test or the server does not know the key identified by the 'key ID' field, the server **MUST** discard the message and **MAY** choose to log the validation failure.

### Category:

Server

### Initialization:

- **Network Topology**

Refer the topology "Fig.1 Topology No.1".

- **Configuration**

Enable Delayed Authentication Protocol Service Authentication parameter

✧ DHCP realm: DHCPv6.TEST.EXAMPLE.COM

✧ Client DUID: 00:01:00:01:00:04:93:e0:00:00:00:00:a2:a2

✧ Key id: 1

✧ Shared secret key: TEST\_VALID12

Device Name	Device Type	I/F	Assigned Prefix	Link Local Addr	MAC Addr
Server1	NUT	Link0	3ffe:501:ffff:100::/64	NUT's Linklocal address	NUT's MAC address
Client1	TN	Link0	3ffe:501:ffff:100::/64	fe80::200:ff:fe00:a2a2	00:00:00:00:a2:a2

**Procedure:**

NUT	TN
	initialize NUT (as a DHCPv6 Server)
<----	Solicit w/ Authentication Option
---->	Advertise w/ Authentication Option
<----	Request w/ Authentication Option
---->	Reply (*1) w/ Authentication Option
<----	Release (w/ Authentication Option key id = 2)
---->X	No Reply (w/ Authentication Option that includes Authentication information) (*1)

- **Termination**

N/A

**Judgment:**

(\*1) PASS: If NUT received Release message, the message failed the validation test, the NUT MUST discard the message.

**References:**

RFC3315

21.4.5 Server Considerations for Delayed Authentication protocol

21.4.5.2. Receiving Request, Confirm, Renew, Rebind or Release Messages and Sending Reply Messages

22.11 Authentication Option

## 5.16. Receiving Information-request Message and Sending Reply Message

### Purpose:

- **Verification Points**

The server uses the key identified in the message and validates the message as specified in section 21.4.2.

If the message passes the validation test, the server responds to the specific message as described in section 18.2. The server **MUST** include authentication information generated using the key identified in the received message, as specified in section 21.4.

### Category:

Server

### Initialization:

- **Network Topology**

Refer the topology "Fig. 1 Topology No.1".

- **Configuration**

Enable Delayed Authentication Protocol Service Authentication parameter

✧ DHCP realm: DHCPv6.TEST.EXAMPLE.COM

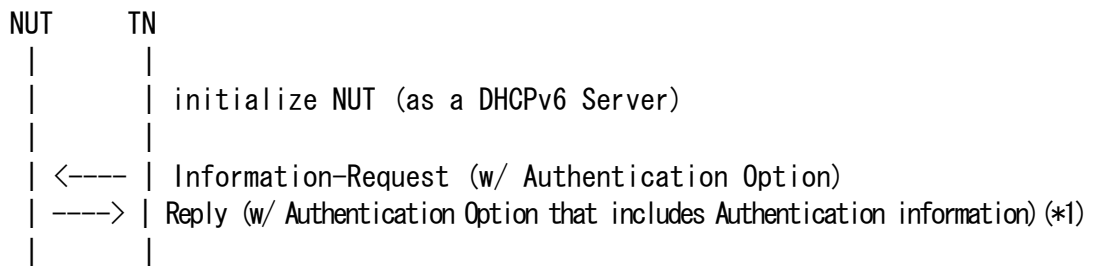
✧ Client DUID: 00:01:00:01:00:04:93:e0:00:00:00:00:a2:a2

✧ Key id: 1

✧ Shared secret key: TEST\_VALID12

Device Name	Device Type	I/F	Assigned Prefix	Link Local Addr	MAC Addr
Server1	NUT	Link0	3ffe:501:ffff:100::/64	NUT's Linklocal address	NUT's MAC address
Client1	TN	Link0	3ffe:501:ffff:100::/64	fe80::200:ff:fe00:a2a2	00:00:00:00:a2:a2

**Procedure:**



- **Termination**

N/A

**Judgment:**

(\*1) PASS: If NUT received Information-Request message, the message passes the validation test, the NUT respond to the message that includes Authentication option.

**References:**

RFC3315

21.4.5 Server Considerations for Delayed Authentication protocol

21.4.5.2. Receiving Request, Confirm, Renew, Rebind or Release Messages and Sending Reply Messages

22.11 Authentication Option

## 5.17. Receiving Information-request Message and validation test is failed

### Purpose:

- **Verification Points**

The server uses the key identified in the message and validates the message as specified in section 21.4.2. If the message fails to pass the validation test or the server does not know the key identified by the 'key ID' field, the server **MUST** discard the message and **MAY** choose to log the validation failure.

### Category:

Server

### Initialization:

- **Network Topology**

Refer the topology "Fig.1 Topology No.1".

- **Configuration**

Enable Delayed Authentication Protocol Service Authentication parameter

✧ DHCP realm: DHCPv6.TEST.EXAMPLE.COM

✧ Client DUID: 00:01:00:01:00:04:93:e0:00:00:00:00:a2:a2

✧ Key id: 1

✧ Shared secret key: TEST\_VALID12

Device Name	Device Type	I/F	Assigned Prefix	Link Local Addr	MAC Addr
Server1	NUT	Link0	3ffe:501:ffff:100::/64	NUT's Linklocal address	NUT's MAC address
Client1	TN	Link0	3ffe:501:ffff:100::/64	fe80::200:ff:fe00:a2a2	00:00:00:00:a2:a2

**Procedure:**

NUT	TN
	initialize NUT (as a DHCPv6 Server)
<----	Release (w/ Authentication Option replay detection field short (length = 32 bit))
---->X	No Reply (w/ Authentication Option that includes Authentication information) (*1)

- **Termination**

N/A

**Judgment:**

(\*1) PASS: If NUT received Information-Request message, the message failed the validation test, the NUT MUST discard the message.

**References:**

RFC3315

21.4.5 Server Considerations for Delayed Authentication protocol

21.4.5.2. Receiving Request, Confirm, Renew, Rebind or Release Messages and Sending Reply Messages

22.11 Authentication Option

## 5.18. Sending Reconfigure Messages

### Purpose:

- **Verification Points**

The server sets the "msg-type" field to RECONFIGURE. The server sets the transaction-id field to 0. The server includes a Server Identifier option containing its DUID and a Client Identifier option containing the client's DUID in the Reconfigure message.

Because of the risk of denial of service attacks against DHCP clients, the use of a security mechanism is mandated in Reconfigure messages. The server **MUST** use DHCP authentication in the Reconfigure message.

The server **MUST** include a Reconfigure Message option (defined in section 22.19) to select whether the client responds with a Renew message or an Information-Request message.

The server **MUST NOT** include any other options in the Reconfigure except as specifically allowed in the definition of individual options.

### Category:

Server

### Initialization:

- **Network Topology**

Refer the topology "Fig. 1 Topology No.1".

- **Configuration**

Enable Delayed Authentication Protocol Service Authentication parameter

✧ DHCP realm: DHCPv6.TEST.EXAMPLE.COM

✧ Client DUID: 00:01:00:01:00:04:93:e0:00:00:00:00:a2:a2

✧ Key id: 1

✧ Shared secret key: TEST\_VALID12

Device Name	Device Type	I/F	Assigned Prefix	Link Local Addr	MAC Addr
Server1	NUT	Link0	3ffe:501:ffff:100::/64	NUT's Linklocal address	NUT's MAC address
Client1	TN	Link0	3ffe:501:ffff:100::/64	fe80::200:ff:fe00:a2a2	00:00:00:00:a2:a2

**Procedure:**

NUT	TN
	initialize NUT (as a DHCPv6 Server)
<----	Solicit w/Reconfigure Accept Option w/ Authentication Option
---->	Advertise w/ Authentication Option
<----	Request w/Reconfigure Accept Option w/ Authentication Option
---->	Reply w/ Authentication Option
	Host address prefix is changed from 3ffe:501:ffff:100:: to 3ffe:501:ffff:200::
	Reload server configuration
---->	Reconfigure w/Option Request Option (IA_NA) w/IA_NA
	w/Reconfigure Message Option w/Authentication Option (*1)

- **Termination**  
N/A

**Judgment:**

(\*1) PASS: TN receives Renew w/ Authentication Option from NUT.

**References:**

RFC3315

19.1.1. Creation and Transmission of Reconfigure Messages

21.4.4.6. Receiving Reconfigure Messages

21.4.5 Server Considerations for Delayed Authentication protocol

22.11. Authentication Option

22.19. Reconfigure Message Option

## 5.19. Reconfigure Key Authentication Protocol for Server

### Purpose:

- **Verification Points**

The server selects a Reconfigure Key for a client during the Request/Reply, Solicit/Reply or Information-request/Reply message exchange. The server records the Reconfigure Key and transmits that key to the client in an Authentication option in the Reply message.

To provide authentication for a Reconfigure message, the server selects a replay detection value according to the RDM selected by the server, and computes an HMAC-MD5 of the Reconfigure message using the Reconfigure Key for the client.

The server computes the HMAC-MD5 over the entire DHCP Reconfigure message, including the Authentication option; the HMAC-MD5 field in the Authentication option is set to zero for the HMAC-MD5 computation. The server includes the HMAC-MD5 in the authentication information field in an Authentication option included in the Reconfigure message sent to the client.

### Category:

Server

### Initialization:

- **Network Topology**

Refer the topology "Fig. 1 Topology No.1".

- **Configuration**

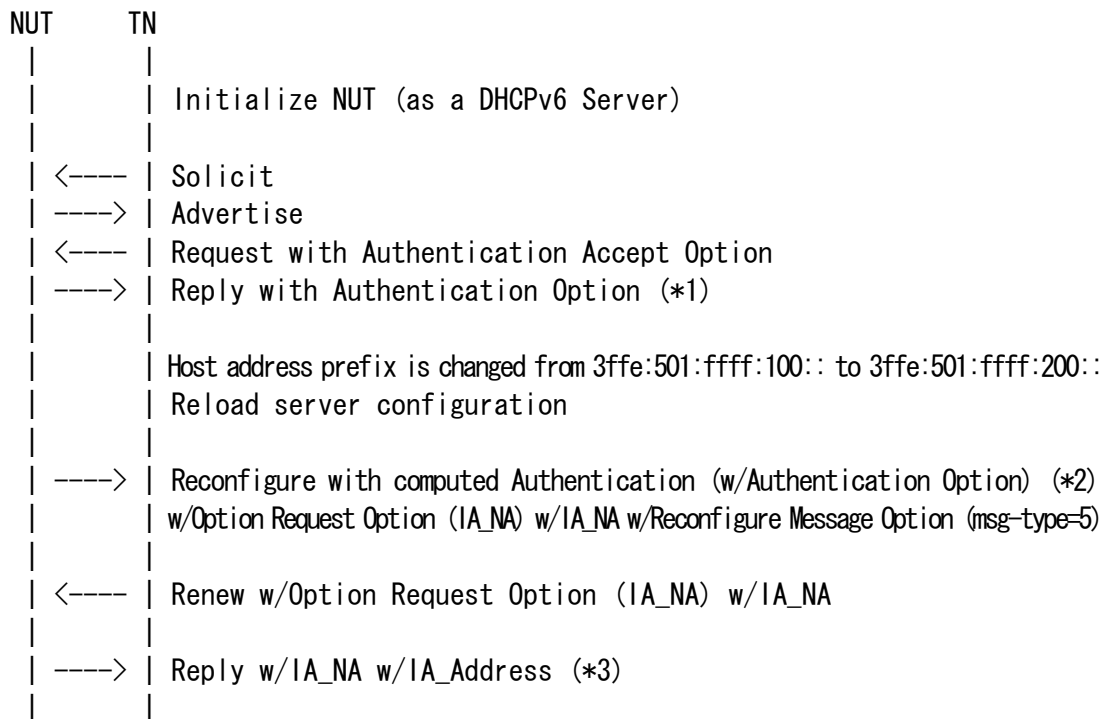
Enable Reconfigure Authentication Protocol Service

Device Name	Device Type	I/F	Assigned Prefix	Link Local Addr	MAC Addr	Op1	Op2
Server1	NUT	Link0	3ffe:501:ffff:100::/64	NUT's Linklocal address	NUT's MAC address	N/A	N/A
Client1	TN	Link0	3ffe:501:ffff:100::/64	fe80::200:ff:fe00:a2a2	00:00:00:00:a2:a2	N/A	Yes

Op1: Server ID Option

Op2: Client ID Option

## Procedure:



- Termination

N/A

## Judgment:

- (\*1) PASS: TN receive Reply message with Authentication option including key-ID.
- (\*2) PASS: TN receive Reconfigure message with Authentication option.
- (\*3) PASS: TN receive Reply message including updated IA\_NA option.

## References:

RFC3315

19.1.1. Creation and Transmission of Reconfigure Messages

21.5. Reconfigure Key Authentication Protocol

21.5.1. Use of the Authentication Option in the Reconfigure Key Authentication Protocol

## 5.20. Receiving Solicit Message and Sending Reply Message

### Purpose:

- **Verification Points**

The server selects a Reconfigure Key for a client during the Request/Reply, Solicit/Reply or Information-request/Reply message exchange. The server records the Reconfigure Key and transmits that key to the client in an Authentication option in the Reply message.

To provide authentication for a Reconfigure message, the server selects a replay detection value according to the RDM selected by the server, and computes an HMAC-MD5 of the Reconfigure message using the Reconfigure Key for the client.

The server computes the HMAC-MD5 over the entire DHCP Reconfigure message, including the Authentication option; the HMAC-MD5 field in the Authentication option is set to zero for the HMAC-MD5 computation. The server includes the HMAC-MD5 in the authentication information field in an Authentication option included in the Reconfigure message sent to the client.

### Category:

Server

### Initialization:

- **Network Topology**

Refer the topology "Fig. 1 Topology No.1".

- **Configuration**

Enable Reconfigure Authentication Protocol Service

Device Name	Device Type	I/F	Assigned Prefix	Link Local Addr	MAC Addr	Op1	Op2
Server1	NUT	Link0	3ffe:501:ffff:100::/64	NUT's Linklocal address	NUT's MAC address	N/A	N/A
Client1	TN	Link0	3ffe:501:ffff:100::/64	fe80::200:ff:fe00:a2a2	00:00:00:00:a2:a2	N/A	Yes

Op1: Server ID Option

Op2: Client ID Option

## Procedure:

NUT	TN
	Initialize NUT (as a DHCPv6 Server)
<----	Solicit with Rapid Commit and Authentication Accept Option
---->	Reply with Authentication Option (*1)
	Host address prefix is changed from 3ffe:501:ffff:100:: to 3ffe:501:ffff:200::
	Reload server configuration
---->	Reconfigure with computed Authentication (w/Authentication Option) (*2)
	w/Option Request Option (IA_NA) w/IA_NA w/Reconfigure Message Option(msg-type=5)
<----	Renew w/Option Request Option (IA_NA) w/IA_NA
---->	Reply w/IA_NA w/IA_Address (*3)

- Termination

N/A

## Judgment:

(\*1) PASS: TN receive Reply message with Authentication option including key-ID.

(\*2) PASS: TN receive Reconfigure message with Authentication option.

(\*3) PASS: TN receive Reply message including updated IA\_NA option.

## References:

RFC3315

19.1.1. Creation and Transmission of Reconfigure Messages

21.5. Reconfigure Key Authentication Protocol

21.5.1. Use of the Authentication Option in the Reconfigure Key Authentication Protocol

## 5.21. Receiving Information -request Message and Sending Replay Message

### Purpose:

- **Verification Points**

The server selects a Reconfigure Key for a client during the Request/Reply, Solicit/Reply or Information-request/Reply message exchange. The server records the Reconfigure Key and transmits that key to the client in an Authentication option in the Reply message.

To provide authentication for a Reconfigure message, the server selects a replay detection value according to the RDM selected by the server, and computes an HMAC-MD5 of the Reconfigure message using the Reconfigure Key for the client.

The server computes the HMAC-MD5 over the entire DHCP Reconfigure message, including the Authentication option; the HMAC-MD5 field in the Authentication option is set to zero for the HMAC-MD5 computation. The server includes the HMAC-MD5 in the authentication information field in an Authentication option included in the Reconfigure message sent to the client.

### Category:

Server

### Initialization:

- **Network Topology**

Refer the topology "Fig. 1 Topology No.1".

- **Configuration**

Enable Reconfigure Authentication Protocol Service

Device Name	Device Type	I/F	Assigned Prefix	Link Local Addr	MAC Addr	Op1	Op2
Server1	NUT	Link0	3ffe:501:ffff:100::/64	NUT's Linklocal address	NUT's MAC address	N/A	N/A
Client1	TN	Link0	3ffe:501:ffff:100::/64	fe80::200:ff:fe00:a2a2	00:00:00:00:a2:a2	N/A	Yes

Op1: Server ID Option

Op2: Client ID Option

## Procedure:

NUT	TN
	Initialize NUT (as a DHCPv6 Server)
<----	Information Request with Authentication Accept Option and Option Request Option (Preference Option)
---->	Reply with Authentication Option and Preference Option (10) (*1)
	Preference changed from 10 to 20 Reload server configuration
---->	Reconfigure with computed Authentication (w/Authentication Option) (*2) w/Reconfigure Message Option (msg-type=11)
<----	Information-Request with Option Request Option (Preference Option)
---->	Reply Preference Option (20) (*3)

### • Termination

N/A

## Judgment:

- (\*1) PASS: TN receive Reply message with Authentication option including key-ID.
- (\*2) PASS: TN receive Reconfigure message with Authentication option including msg-type = 11.
- (\*3) PASS: TN receive Reply message with updated Preference option.

## References:

RFC3315

9.1.1. Creation and Transmission of Reconfigure Messages

21.5. Reconfigure Key Authentication Protocol

21.5.1. Use of the Authentication Option in the Reconfigure Key  
Authentication Protocol

## 5.22. Delayed Authentication Protocol for Client

### Purpose:

- **Verification Points**

To validate an incoming message, the receiver first checks that the value in the replay detection field is acceptable according to the replay detection method specified by the RDM field. Next, the receiver computes the MAC as described in [8]. The entire DHCP message (setting the MAC field of the authentication option to 0) is used as input to the HMAC-MD5 computation function. If the MAC computed by the receiver does not match the MAC contained in the authentication option, the receiver **MUST** discard the DHCP message.

### Category:

Client

### Initialization:

- **Network Topology**

Refer the topology "Fig. 1 Topology No.1".

- **Configuration**

Enable Delayed Authentication Protocol Service

Authentication parameter

✧ DHCP realm: DHCPv6.TEST.EXAMPLE.COM

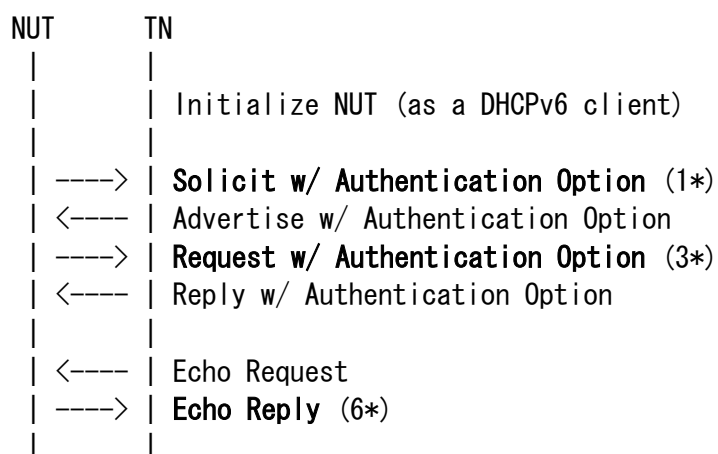
✧ Client DUID: ANY

✧ Key id: 1

✧ Shared secret key: TEST\_VALID12

Device Name	Device Type	Interface	Address	Link Local Addr	MAC Addr
Client	NUT	Link0		NUT's Linklocal address	NUT's MAC address
Server	TN	Link0	3ffe:501:ffff:100:200:ff:fe00:a1a1	fe80::200:ff:fe00:a1a1	00:00:00:00:a1:a1

### Procedure:



- **Termination**

N/A

**Judgment:**

(1\*)PASS: TN receives Solicit w/ Authentication Option from NUT.

(3\*)PASS: TN receives Request w/ Authentication Option from NUT.

(6\*)PASS: NUT should send Echo Reply to TN.

**References:**

RFC3315

21.4.4 Client Considerations for Delayed Authentication protocol

22.11 Authentication Option

## 5.23. Multiple Authentication option are included

### Purpose:

- **Verification Points**

Any DHCP message that includes more than one authentication option **MUST** be discarded.

### Category:

Client

### Initialization:

- **Network Topology**

Refer the topology "Fig.2 Topology No.2".

- **Configuration**

Enable Delayed Authentication Protocol Service

Authentication parameter

✧ DHCP realm: DHCPv6.TEST.EXAMPLE.COM

✧ Client DUID: ANY

✧ Key id: 1

✧ Shared secret key: TEST\_VALID12

Device Name	Device Type	Interface	Address	Link Local Addr	MAC Addr
Client	NUT	Link0		NUT's Linklocal address	NUT's MAC address
Server	TN	Link0	3ffe:501:ffff:100:200:ff:fe00:a1a1	fe80::200:ff:fe00:a1a1	00:00:00:00:a1:a1

### Procedure:

```

NUT      TN
|        |
|        | Initialize NUT (as a DHCPv6 client)
|        |
| ----> | Solicit w/ Authentication Option
| <---- | Advertise w/ Multiple Authentication Option
| ----> | Solicit w/ Authentication Option (*3)
|        |

```

- **Termination**

N/A

**Judgment:**

(3\*)PASS: TN discards previous Advertise from NUT.  
TN retransmits Solicit message with Authentication.

**References:**

RFC3315

21.4.4 Client Considerations for Delayed Authentication protocol

22.11 Authentication Option

## 5.24. MD5 is mismatched

### Purpose:

- **Verification Points**

To validate an incoming message, the receiver first checks that the value in the replay detection field is acceptable according to the replay detection method specified by the RDM field. Next, the receiver computes the MAC as described in [8]. The entire DHCP message (setting the MAC field of the authentication option to 0) is used as input to the HMAC-MD5 computation function. If the MAC computed by the receiver does not match the MAC contained in the authentication option, the receiver **MUST** discard the DHCP message.

### Category:

Client

### Initialization:

- **Network Topology**

Refer the topology "Fig.2 Topology No.2".

- **Configuration**

Enable Delayed Authentication Protocol Service

Authentication parameter

✧ DHCP realm: DHCPv6.TEST.EXAMPLE.COM

✧ Client DUID: ANY

✧ Key id: 1

✧ Shared secret key: TEST\_VALID12

Device Name	Device Type	Interface	Assigned Prefix	Link Local Addr	MAC Addr
Client	NUT	Link0	3ffe:501:ffff:101::/64	NUT's Linklocal address	NUT's MAC address
Server	TN	Link0	3ffe:501:ffff:101::/64	fe80::200:ff:fe00:a1a1	00:00:00:00:a1:a1

**Procedure:**

NUT	TN
	Initialize NUT (as a DHCPv6 client)
---->	Solicit w/ Authentication Option
<----	Advertise w/ Authentication Option
	including shared secret key ="TEST_INVALID"
<----	Advertise w/ Authentication Option
	including shared secret key ="TEST_VALID12"
---->	<b>Request w/ Authentication Option (4*)</b>

- **Termination**  
N/A

**Judgment:**

(4\*)PASS: TN discards 1st Advertise message  
TN responds to 2nd received Advertise message from NUT.

**References:**

RFC3315  
21.4.2 Message Validation  
22.11 Authentication Option

## 5.25. Key Utilization

### Purpose:

- **Verification Points**

To validate an incoming message, the receiver first checks that the value in the replay detection field is acceptable according to the replay detection method specified by the RDM field. Next, the receiver computes the MAC as described in [8]. The entire DHCP message (setting the MAC field of the authentication option to 0) is used as input to the HMAC-MD5 computation function. If the MAC computed by the receiver does not match the MAC contained in the authentication option, the receiver **MUST** discard the DHCP message.

### Category:

Client

### Initialization:

- **Network Topology**

Refer the topology "Fig.2 Topology No.2".

- **Configuration**

Enable Delayed Authentication Protocol Service

Authentication parameter

✧ DHCP realm: DHCPv6.TEST.EXAMPLE.COM

✧ Client DUID: ANY

✧ Key id: 1

✧ Shared secret key: TEST\_VALID12

Device Name	Device Type	Interface	Address	Link Local Addr	MAC Addr
Client	NUT	Link0		NUT's Linklocal address	NUT's MAC address
Server	TN	Link0	3ffe:501:ffff:100:200:ff:fe00:a1a1	fe80::200:ff:fe00:a1a1	00:00:00:00:a1:a1

**Procedure:**

NUT	TN
	Initialize NUT (as a DHCPv6 client)
---->	Solicit w/ Authentication Option
<----	Advertise w/ Authentication Option
	including shared secret key ="TEST_INVALID"
<----	Advertise w/ Authentication Option
	including shared secret key ="TEST_VALID12"
---->	<b>Request w/ Authentication Option (4*)</b>

- **Termination**  
N/A

**Judgment:**

(4\*)PASS: TN discards 1st Advertise message  
TN responds to 2nd received Advertise message from NUT.

**References:**

RFC3315  
21.4.2 Message Validation  
22.11 Authentication Option

## 5.26. Sending Solicit message

### Purpose:

- **Verification Points**

When the client sends a Solicit message and wishes to use authentication, it includes an Authentication option with the desired protocol, algorithm and RDM. The client does not include any replay detection or authentication information in the Authentication option.

### Category:

Client

### Initialization:

- **Network Topology**

Refer the topology "Fig. 2 Topology No.2".

- **Configuration**

Enable Delayed Authentication Protocol Service

Authentication parameter

✧ DHCP realm: DHCPv6.TEST.EXAMPLE.COM

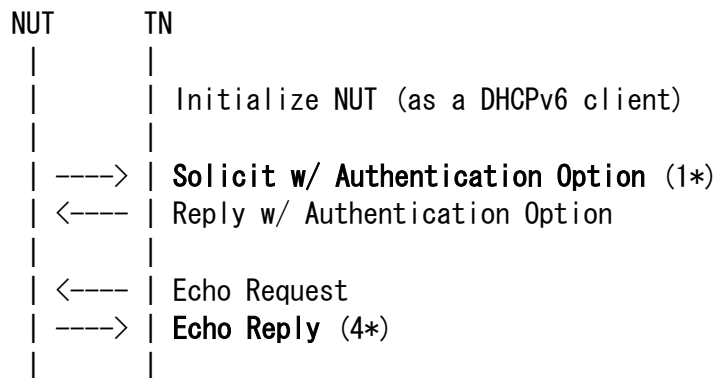
✧ Client DUID: ANY

✧ Key id: 1

✧ Shared secret key: TEST\_VALID12

Device Name	Device Type	Interface	Address	Link Local Addr	MAC Addr
Client	NUT	Link0		NUT's Linklocal address	NUT's MAC address
Server	TN	Link0	3ffe:501:ffff:100:200:ff:fe00:a1a1	fe80::200:ff:fe00:a1a1	00:00:00:00:a1:a1

**Procedure:**



- **Termination**

N/A

**Judgment:**

(1\*)PASS: TN receives Solicit w/ Authentication Option from NUT.

(4\*)PASS: NUT should send Echo Reply to TN.

**References:**

RFC3315

21.4.4 Client Considerations for Delayed Authentication protocol

21.4.4.1. Sending Solicit Messages

22.11 Authentication Option

## 5.27. Receiving Advertise Messages

### Purpose:

- **Verification Points**

The client validates any Advertise messages containing an Authentication option specifying the delayed authentication protocol using the validation test.

The client authenticated the Advertise message through which the client selected the server, the client **MUST** generate authentication information for subsequent Request messages sent to the server.

When the client sends a subsequent message, it **MUST** use the same key used by the server to generate the authentication information.

### Category:

Client

### Initialization:

- **Network Topology**

Refer the topology "Fig. 2 Topology No.2".

- **Configuration**

Enable Delayed Authentication Protocol Service

Authentication parameter

✧ DHCP realm: DHCPv6.TEST.EXAMPLE.COM

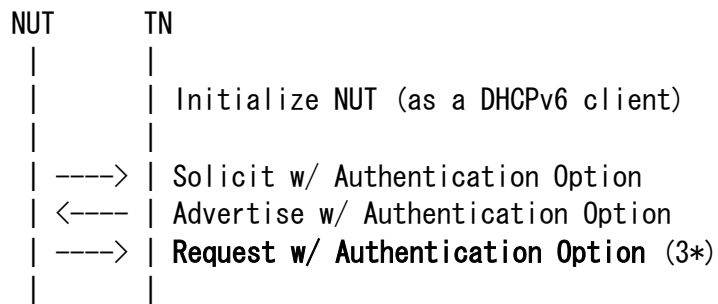
✧ Client DUID: ANY

✧ Key id: 1

✧ Shared secret key: TEST\_VALID12

Device Name	Device Type	Interface	Address	Link Local Addr	MAC Addr
Client	NUT	Link0		NUT's Linklocal address	NUT's MAC address
Server	TN	Link0	3ffe:501:ffff:100:200:ff:fe00:a1a1	fe80::200:ff:fe00:a1a1	00:00:00:00:a1:a1

**Procedure:**



- **Termination**  
N/A

**Judgment:**

(3\*)PASS: TN receives Request w/ Authentication Option from NUT.

**References:**

RFC3315

21.4.2. Message Validation

21.4.4. Client Considerations for Delayed Authentication protocol

21.4.4.2. Receiving Advertise Messages

21.4.4.3. Sending Request, Confirm, Renew, Rebind, Decline or Release Messages

22.11 Authentication Option

## 5.28. Sending Confirm message

### Purpose:

- **Verification Points**

If the client authenticated the Advertise message through which the client selected the server, the client **MUST** generate authentication information for subsequent Confirm messages sent to the server.

When the client sends a subsequent message, it **MUST** use the same key used by the server to generate the authentication information.

### Category:

Client

### Initialization:

- **Network Topology**

Refer the topology "Fig.2 Topology No.2".

- **Configuration**

Enable Delayed Authentication Protocol Service

Authentication parameter

✧ DHCP realm: DHCPv6.TEST.EXAMPLE.COM

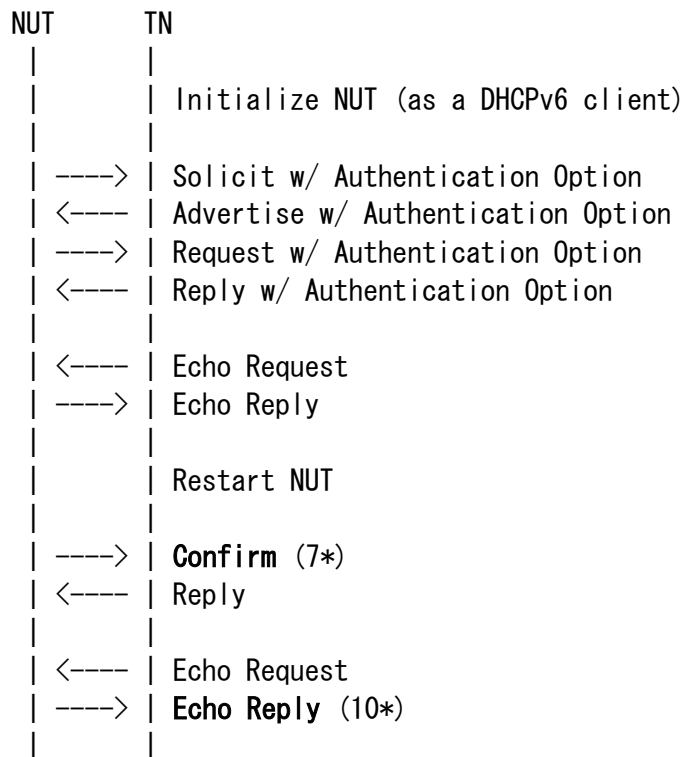
✧ Client DUID: ANY

✧ Key id: 1

✧ Shared secret key: TEST\_VALID12

Device Name	Device Type	Interface	Assigned Prefix	Link Local Addr	MAC Addr
Client	NUT	Link0		NUT's Linklocal address	NUT's MAC address
Server	TN	Link0	3ffe:501:ffff:100:200:ff:fe00:a1a1	fe80::200:ff:fe00:a1a1	00:00:00:00:a1:a1

**Procedure:**



• **Termination**

N/A

**Judgment:**

(7\*)PASS: TN receives Confirm w/ Authentication Option from NUT.

(10\*)PASS: NUT should send Echo Reply to TN.

**References:**

RFC3315

21.4.4 Client Considerations for Delayed Authentication protocol

21.4.4.3. Sending Request, Confirm, Renew, Rebind, Decline or Release Messages

## 5.29. Sending Renew message

### Purpose:

- **Verification Points**

If the client authenticated the Advertise message through which the client selected the server, the client **MUST** generate authentication information for subsequent Renew messages sent to the server.

When the client sends a subsequent message, it **MUST** use the same key used by the server to generate the authentication information.

### Category:

Client

### Initialization:

- **Network Topology**

Refer the topology "Fig.2 Topology No.2".

- **Configuration**

Enable Delayed Authentication Protocol Service

Authentication parameter

✧ DHCP realm: DHCPv6.TEST.EXAMPLE.COM

✧ Client DUID: ANY

✧ Key id: 1

✧ Shared secret key: TEST\_VALID12

Device Name	Device Type	Interface	Assigned Prefix	Link Local Addr	MAC Addr
Client	NUT	Link0		NUT's Linklocal address	NUT's MAC address
Server	TN	Link0	3ffe:501:ffff:100:200:ff:fe00:a1a1	fe80::200:ff:fe00:a1a1	00:00:00:00:a1:a1

## Procedure:

NUT	TN
	Initialize NUT (as a DHCPv6 client)
---->	Solicit w/ Authentication Option
<----	Advertise w/ Authentication Option
---->	Request w/ Authentication Option
<----	Reply w/ Authentication Option that includes IA_NA option (T1=50, T2=80)
<----	Echo Request
---->	Echo Reply
	Before T1 time expired
---->	<b>Renew w/ Authentication Option (7*)</b>
<----	Reply w/ Authentication Option
<----	Echo Request
---->	<b>Echo Reply (10*)</b>

- **Termination**

N/A

## Judgment:

(7\*)PASS: TN receives Renew w/ Authentication Option from NUT.

(10\*)PASS: NUT should send Echo Reply to TN.

## References:

RFC3315

21.4.4 Client Considerations for Delayed Authentication protocol

21.4.4.3. Sending Request, Confirm, Renew, Rebind, Decline or Release Messages

## 5.30. Sending Rebind message

### Purpose:

- **Verification Points**

If the client authenticated the Advertise message through which the client selected the server, the client **MUST** generate authentication information for subsequent Rebind messages sent to the server.

When the client sends a subsequent message, it **MUST** use the same key used by the server to generate the authentication information.

### Category:

Client

### Initialization:

- **Network Topology**

Refer the topology "Fig.2 Topology No.2".

- **Configuration**

Enable Delayed Authentication Protocol Service

Authentication parameter

✧ DHCP realm: DHCPv6.TEST.EXAMPLE.COM

✧ Client DUID: ANY

✧ Key id: 1

✧ Shared secret key: TEST\_VALID12

Device Name	Device Type	Interface	Assigned Prefix	Link Local Addr	MAC Addr
Client	NUT	Link0		NUT's Linklocal address	NUT's MAC address
Server	TN	Link0	3ffe:501:ffff:100:200:ff:fe00:a1a1	fe80::200:ff:fe00:a1a1	00:00:00:00:a1:a1

## Procedure:

NUT	TN
	Initialize NUT (as a DHCPv6 client)
---->	Solicit w/ Authentication Option
<----	Advertise w/ Authentication Option
---->	Request w/ Authentication Option
<----	Reply w/ Authentication Option that includes IA_NA option (T1=50, T2=80)
<----	Echo Request
---->	Echo Reply
	Before T1 time expired
---->	Renew w/ Authentication Option
	Before T2 time expired
---->	<b>Rebind w/ Authentication Option (8*)</b>
<----	Reply w/ Authentication Option
<----	Echo Request
---->	<b>Echo Reply (11*)</b>

- **Termination**

N/A

## Judgment:

(8\*)PASS: TN receives Rebind w/ Authentication Option from NUT.

(11\*)PASS: NUT should send Echo Reply to TN.

## References:

RFC3315

21.4.4 Client Considerations for Delayed Authentication protocol

21.4.4.3. Sending Request, Confirm, Renew, Rebind, Decline or Release Messages

## 5.31. Sending Decline message

### Purpose:

- **Verification Points**

If the client authenticated the Advertise message through which the client selected the server, the client **MUST** generate authentication information for subsequent Decline messages sent to the server.

When the client sends a subsequent message, it **MUST** use the same key used by the server to generate the authentication information.

### Category:

Client

### Initialization:

- **Network Topology**

Refer the topology "Fig.2 Topology No.2".

- **Configuration**

Enable Delayed Authentication Protocol Service

Authentication parameter

✧ DHCP realm: DHCPv6.TEST.EXAMPLE.COM

✧ Client DUID: ANY

✧ Key id: 1

✧ Shared secret key: TEST\_VALID12

Device Name	Device Type	Interface	Assigned Prefix	Link Local Addr	MAC Addr
Client	NUT	Link0		NUT's Linklocal address	NUT's MAC address
Server	TN	Link0	3ffe:501:ffff:100:200:ff:fe00:a1a1	fe80::200:ff:fe00:a1a1	00:00:00:00:a1:a1

## Procedure:

NUT	TN
	Initialize NUT (as a DHCPv6 client)
---->	Solicit w/ Authentication Option
<----	Advertise w/ Authentication Option
---->	Request w/ Authentication Option
<----	Reply w/ Authentication Option
---->	Wait DAD NS
<----	DAD NA (the address is found to be use on the link)
---->	<b>Decline (7*)</b>
<----	Reply
<----	Echo Request
-->X	<b>Echo Reply (10*)</b>

- **Termination**

N/A

## Judgment:

(7\*)PASS: TN receives Decline w/ Authentication Option from NUT.

(10\*)PASS: NUT must not send Echo Reply to TN.

## References:

RFC3315

21.4.4 Client Considerations for Delayed Authentication protocol

21.4.4.3. Sending Request, Confirm, Renew, Rebind, Decline or Release Messages

## 5.32. Sending Release message

### Purpose:

- **Verification Points**

If the client authenticated the Advertise message through which the client selected the server, the client **MUST** generate authentication information for subsequent Release messages sent to the server.

When the client sends a subsequent message, it **MUST** use the same key used by the server to generate the authentication information.

### Category:

Client

### Initialization:

- **Network Topology**

Refer the topology "Fig.2 Topology No.2".

- **Configuration**

Enable Delayed Authentication Protocol Service

Authentication parameter

✧ DHCP realm: DHCPv6.TEST.EXAMPLE.COM

✧ Client DUID: ANY

✧ Key id: 1

✧ Shared secret key: TEST\_VALID12

Device Name	Device Type	Interface	Assigned Prefix	Link Local Addr	MAC Addr
Client	NUT	Link0		NUT's Linklocal address	NUT's MAC address
Server	TN	Link0	3ffe:501:ffff:100:200:ff:fe00:a1a1	fe80::200:ff:fe00:a1a1	00:00:00:00:a1:a1

**Procedure:**

NUT	TN
	Initialize NUT (as a DHCPv6 client)
---->	Solicit w/ Authentication Option
<----	Advertise w/ Authentication Option
---->	Request w/ Authentication Option
<----	Reply w/ Authentication Option
	Release binding address on NUT
---->	<b>Release</b> (5*)
<----	Reply
<----	Echo Request
-->X	<b>Echo Reply</b> (8*)

• **Termination**

N/A

**Judgment:**

(5\*)PASS: TN receives Release w/ Authentication Option from NUT.

(8\*)PASS: NUT must not send Echo Reply to TN.

**References:**

RFC3315

21.4.4 Client Considerations for Delayed Authentication protocol

21.4.4.3. Sending Request, Confirm, Renew, Rebind, Decline or Release Messages

### 5.33. Sending Information-Request message

#### Purpose:

- **Verification Points**

If the server has selected a key for the client in a previous message exchange, the client **MUST** use the same key to generate the authentication information throughout the session.

#### Category:

Client

#### Initialization:

- **Network Topology**

Refer the topology "Fig.2 Topology No.2".

- **Configuration**

Enable Delayed Authentication Protocol Service

Authentication parameter

✧ DHCP realm: DHCPv6.TEST.EXAMPLE.COM

✧ Client DUID: ANY

✧ Key id: 1

✧ Shared secret key: TEST\_VALID12

Device Name	Device Type	Interface	Address	Link Local Addr	MAC Addr
Client	NUT	Link0		NUT's Linklocal address	NUT's MAC address
Server	TN	Link0	3ffe:501:ffff:100:200:ff:fe00:a1a1	fe80::200:ff:fe00:a1a1	00:00:00:00:a1:a1

**Procedure:**

NUT	TN
	Initialize NUT (as a DHCPv6 client)
---->	Solicit w/ Authentication Option
<----	Advertise w/ Authentication Option
---->	Request w/ Authentication Option
<----	Reply w/ Authentication Option
---->	<b>Information-Request w/ Authentication Option (1*)</b>
<----	Reply w/ Authentication Option
--X->	No Information-Request (2*)

• **Termination**

N/A

**Judgment:**

(1\*)PASS: TN receives Information-Request w/ Authentication Option from NUT.

(1\*)PASS: TN doesn't receive Information-Request w/ Authentication Option from NUT.

**References:**

RFC3315

21.4.4 Client Considerations for Delayed Authentication protocol

21.4.4.4. Sending Information-request Messages

22.11 Authentication Option

## 5.34. Receiving Reply Messages and validation test is failed

### Purpose:

- **Verification Points**

If the client authenticated the Advertise it accepted, the client **MUST** validate the associated Reply message from the server. The client **MUST** discard the Reply if the message fails to pass the validation test and **MAY** log the validation failure. If the Reply fails to pass the validation test, the client **MUST** restart the DHCP configuration process by sending a Solicit message.

### Category:

Client

### Initialization:

- **Network Topology**

Refer the topology "Fig. 2 Topology No.2".

- **Configuration**

Enable Delayed Authentication Protocol Service  
Authentication parameter  
✧ DHCP realm: DHCPv6.TEST.EXAMPLE.COM  
✧ Client DUID: ANY  
✧ Key id: 1  
✧ Shared secret key: TEST\_VALID12

Device Name	Device Type	Interface	Address	Link Local Addr	MAC Addr
Client	NUT	Link0		NUT's Linklocal address	NUT's MAC address
Server	TN	Link0	3ffe:501:ffff:100:200:ff:fe00:a1a1	fe80::200:ff:fe00:a1a1	00:00:00:00:a1:a1

**Procedure:**

NUT	TN
	Initialize NUT (as a DHCPv6 client)
---->	Solicit w/ Authentication Option
<----	Advertise w/ Authentication Option
---->	Request w/ Authentication Option
<----	Reply w/ invalid Authentication Option (Key id =2)
---->	<b>Solicit w/ Authentication Option (5*)</b>

- **Termination**

N/A

**Judgment:**

(5\*)PASS: TN receives Solicit w/ Authentication Option from NUT.

**References:**

RFC3315

21.4.4 Client Considerations for Delayed Authentication protocol

21.4.4.5. Receiving Reply Messages

22.11 Authentication Option

## 5.35. Receiving Reconfigure Messages (Renew message)

### Purpose:

- **Verification Points**

Upon receipt of a valid Reconfigure message, the client responds with either a Renew message or an Information-request message as indicated by the Reconfigure Message option.

The client ignores the transaction-id field in the received Reconfigure message.

### Category:

Client

### Initialization:

- **Network Topology**

Refer the topology "Fig.2 Topology No.2".

- **Configuration**

Enable Delayed Authentication Protocol Service

Authentication parameter

✧ DHCP realm: DHCPv6.TEST.EXAMPLE.COM

✧ Client DUID: ANY

✧ Key id: 1

✧ Shared secret key: TEST\_VALID12

Device Name	Device Type	Interface	Assigned Prefix	Link Local Addr	MAC Addr
Client	NUT	Link0		NUT's Linklocal address	NUT's MAC address
Server	TN	Link0	3ffe:501:ffff:100:200:ff:fe00:a1a1	fe80::200:ff:fe00:a1a1	00:00:00:00:a1:a1

## Procedure:

NUT	TN
	Initialize NUT (as a DHCPv6 client)
---->	Solicit w/ Authentication Option
<----	Advertise w/Reconfigure Accept Option w/ Authentication Option
---->	Request w/ Authentication Option
<----	Reply w/Reconfigure Accept Option w/ Authentication Option
<----	Reconfigure w/Reconfigure Message Option (msg-type=5) w/ Authentication Option
---->	<b>Renew w/ Authentication Option (6*)</b>

- **Termination**

N/A

## Judgment:

(6\*)PASS: TN receives Renew w/ Authentication Option from NUT.

## References:

RFC3315

19.1.1. Creation and Transmission of Reconfigure Messages

19.4.1. Receipt of Reconfigure Messages

21.4.4. Client Considerations for Delayed Authentication protocol

21.4.4.6. Receiving Reconfigure Messages

22.11. Authentication Option

22.19. Reconfigure Message Option

## 5.36. Receiving Reconfigure Messages (Informational-request message)

### Purpose:

- **Verification Points**

Upon receipt of a valid Reconfigure message, the client responds with either a Renew message or an Information-request message as indicated by the Reconfigure Message option.

The client ignores the transaction-id field in the received Reconfigure message.

### Category:

Client

### Initialization:

- **Network Topology**

Refer the topology "Fig. 2 Topology No.2".

- **Configuration**

Enable Delayed Authentication Protocol Service

Authentication parameter

✧ DHCP realm: DHCPv6.TEST.EXAMPLE.COM

✧ Client DUID: ANY

✧ Key id: 1

✧ Shared secret key: TEST\_VALID12

Device Name	Device Type	Interface	Assigned Prefix	Link Local Addr	MAC Addr
Client	NUT	Link0		NUT's Linklocal address	NUT's MAC address
Server	TN	Link0	3ffe:501:ffff:100:200:ff:fe00:a1a1	fe80::200:ff:fe00:a1a1	00:00:00:00:a1:a1

## Procedure:

NUT	TN
	Initialize NUT (as a DHCPv6 client)
---->	Solicit w/ Authentication Option
<----	Advertise w/Reconfigure Accept Option w/ Authentication Option
---->	Request w/ Authentication Option
<----	Reply w/Reconfigure Accept Option w/ Authentication Option
<----	Reconfigure w/Reconfigure Message Option (msg-type=11) w/ Authentication Option
---->	<b>Information-request w/ Authentication Option (6*)</b>

- **Termination**

N/A

## Judgment:

(6\*)PASS: TN receives Information-request w/ Authentication Option from NUT.

## References:

RFC3315

19.1.1. Creation and Transmission of Reconfigure Messages

19.4.1. Receipt of Reconfigure Messages

21.4.4. Client Considerations for Delayed Authentication protocol

21.4.4.6. Receiving Reconfigure Messages

22.11. Authentication Option

22.19. Reconfigure Message Option

## 5.37. Receiving Reconfigure Messages and validation test is failed

### Purpose:

- **Verification Points**

The client MUST discard the Reconfigure if the message fails to pass the validation test and MAY log the validation failure.

### Category:

Client

### Initialization:

- **Network Topology**

Refer the topology "Fig.2 Topology No.2".

- **Configuration**

Enable Delayed Authentication Protocol Service

Authentication parameter

✧ DHCP realm: DHCPv6.TEST.EXAMPLE.COM

✧ Client DUID: ANY

✧ Key id: 1

✧ Shared secret key: TEST\_VALID12

Device Name	Device Type	Interface	Assigned Prefix	Link Local Addr	MAC Addr
Client	NUT	Link0		NUT's Linklocal address	NUT's MAC address
Server	TN	Link0	3ffe:501:ffff:100:200:ff:fe00:a1a1	fe80::200:ff:fe00:a1a1	00:00:00:00:a1:a1

**Procedure:**

NUT	TN
	Initialize NUT (as a DHCPv6 client)
---->	Solicit w/ Authentication Option
<----	Advertise w/Reconfigure Accept Option w/ Authentication Option
---->	Request w/ Authentication Option
<----	Reply w/Reconfigure Accept Option w/ Authentication Option
<----	<del>Reconfigure w/Reconfigure Message Option (msg-type=5)</del> w/ invalid Authentication Option(Key id=2)
--> X	<b>Renew w/ Authentication Option (6*)</b>

- **Termination**

N/A

**Judgment:**

(6\*)PASS: TN does not receive Renew w/ Authentication Option from NUT.

**References:**

RFC3315

19.1.1. Creation and Transmission of Reconfigure Messages

19.4.1. Receipt of Reconfigure Messages

21.4.4. Client Considerations for Delayed Authentication protocol

21.4.4.6. Receiving Reconfigure Messages

22.11. Authentication Option

22.19. Reconfigure Message Option

## 5.38. Checking Key Authentication Protocol for Client

### Purpose:

- **Verification Points**

The client will receive a Reconfigure Key from the server in the initial Reply message from the server. The client records the Reconfigure Key for use in authenticating subsequent Reconfigure messages.

To authenticate a Reconfigure message, the client computes an HMAC-MD5 over the DHCP Reconfigure message, using the Reconfigure Key received from the server. If this computed HMAC-MD5 matches the value in the Authentication option, the client accepts the Reconfigure message.

### Category:

Client

### Initialization:

- **Network Topology**

Refer the topology "Fig.2 Topology No.2".

- **Configuration**

Enable Reconfigure Key Authentication Protocol Service

Device Name	Device Type	Interface	Assigned Prefix	Link Local Addr	MAC Addr
Client	NUT	Link0	3ffe:501:ffff:101::/64	NUT's Linklocal address	NUT's MAC address
Server	TN	Link0	3ffe:501:ffff:101::/64	fe80::200:ff:fe00:a1a1	00:00:00:00:a1:a1

## Procedure:

NUT	TN
	Initialize NUT (as a DHCPv6 client)
---->	Solicit
<----	Advertise
---->	<b>Request with Authentication Accept Option (*3)</b>
<----	Reply with Authentication Option
	Host address prefix is changed from 3ffe:501:ffff:100:: to 3ffe:501:ffff:200::
	Reload server configuration
<----	Reconfigure with computed Authentication (w/Authentication Option)
	w/Option Request Option (IA_NA) w/IA_NA w/Reconfigure Message Option (msg-type=5)
---->	<b>Renew w/Option Request Option IA_NA) w/IA_NA (*6)</b>
<----	Reply w/IA_NA w/IA_Address
<----	Echo Request (send to NUT's new address)
---->	<b>Echo Reply (*9)</b>

- **Termination**

N/A

## Judgment:

- (\*3) PASS: TN receive Request message with Authentication Accept option.
- (\*6) PASS: TN receive Renew message with Option Request Option (IA\_NA) and IA\_NA Option.
- (\*9) PASS: TN receive Echo Reply message.

## References:

RFC3315

19.4.2. Creation and Transmission of Renew Messages

21.5. Reconfigure Key Authentication Protocol

21.5.3. Client considerations for Reconfigure Key protocol

## 5.39. Sending Request Message and Receiving Reply Message

### Purpose:

- **Verification Points**

The client will receive a Reconfigure Key from the server in the initial Reply message from the server. The client records the Reconfigure Key for use in authenticating subsequent Reconfigure messages.

To authenticate a Reconfigure message, the client computes an HMAC-MD5 over the DHCP Reconfigure message, using the Reconfigure Key received from the server. If this computed HMAC-MD5 matches the value in the Authentication option, the client accepts the Reconfigure message.

### Category:

Client

### Initialization:

- **Network Topology**

Refer the topology "Fig.3 Topology No.3".

- **Configuration**

Enable Reconfigure Key Authentication Protocol Service

Device Name	Device Type	Interface	Assigned Prefix	Link Local Addr	MAC Addr
Client	NUT	Link0	3ffe:501:ffff:101::/64	NUT's Linklocal address	NUT's MAC address
Server	TN	Link0	3ffe:501:ffff:101::/64	fe80::200:ff:fe00:a1a1	00:00:00:00:a1:a1

## Procedure:

NUT	TN
	Initialize NUT (as a DHCPv6 client)
---->	Solicit
<----	Advertise
---->	<b>Request with Authentication Accept Option (*3)</b>
<----	Reply with Authentication Option
	Host address prefix is changed from 3ffe:501:ffff:100:: to 3ffe:501:ffff:200::
	Reload server configuration
<----	Reconfigure with computed Authentication (w/Authentication Option)
	w/Option Request Option (IA_NA) w/IA_NA w/Reconfigure Message Option (msg-type=5)
---->	<b>Renew w/Option Request Option (IA_NA) w/IA_NA (*6)</b>

- Termination

N/A

## Judgment:

(\*3) PASS: TN receive Request message with Authentication Accept option.

(\*6) PASS: TN receive Renew message with Option Request Option (IA\_NA) and IA\_NA Option.

## References:

RFC3315

19.4.2. Creation and Transmission of Renew Messages

21.5. Reconfigure Key Authentication Protocol

21.5.3. Client considerations for Reconfigure Key protocol

## 5. 40. Request/Reply Exchange finished, Receiving Reconfigure Message and validation test is failed

### Purpose:

- **Verification Points**

The client will receive a Reconfigure Key from the server in the initial Reply message from the server. The client records the Reconfigure Key for use in authenticating subsequent Reconfigure messages.

To authenticate a Reconfigure message, the client computes an HMAC-MD5 over the DHCP Reconfigure message, using the Reconfigure Key received from the server. If this computed HMAC-MD5 matches the value in the Authentication option, the client accepts the Reconfigure message.

### Category:

Client

### Initialization:

- **Network Topology**

Refer the topology "Fig.3 Topology No.3".

- **Configuration**

Enable Reconfigure Key Authentication Protocol Service

Device Name	Device Type	Interface	Assigned Prefix	Link Local Addr	MAC Addr
Client	NUT	Link0	3ffe:501:ffff:101::/64	NUT's Linklocal address	NUT's MAC address
Server	TN	Link0	3ffe:501:ffff:101::/64	fe80::200:ff:fe00:a1a1	00:00:00:00:a1:a1

## Procedure:

NUT	TN
	Initialize NUT (as a DHCPv6 client)
---->	Solicit
<----	Advertise
---->	<b>Request with Authentication Accept Option (*3)</b>
<----	Reply with Authentication Option
	Host address prefix is changed from 3ffe:501:ffff:100:: to 3ffe:501:ffff:200::
	Reload server configuration
<----	Reconfigure w/Invalid Authentication Option (Value field is invalid)
	w/Option Request Option (IA_NA) w/IA_NA w/Reconfigure Message Option (msg-type=5)
--> X	<b>Renew w/Option Request Option (IA_NA) w/IA_NA (*6)</b>

- **Termination**

N/A

## Judgment:

- (\*3) PASS: TN receive Request message with Authentication Accept option.
- (\*6) PASS: TN does not receive Renew message.

## References:

RFC3315

19.4.2. Creation and Transmission of Renew Messages

21.5. Reconfigure Key Authentication Protocol

21.5.3. Client considerations for Reconfigure Key protocol

## 5.41. Sending Solicit Message and Receiving Reply Message

### Purpose:

- **Verification Points**

The client will receive a Reconfigure Key from the server in the initial Reply message from the server. The client records the Reconfigure Key for use in authenticating subsequent Reconfigure messages.

To authenticate a Reconfigure message, the client computes an HMAC-MD5 over the DHCP Reconfigure message, using the Reconfigure Key received from the server. If this computed HMAC-MD5 matches the value in the Authentication option, the client accepts the Reconfigure message.

### Category:

Client

### Initialization:

- **Network Topology**

Refer the topology "Fig.3 Topology No.3".

- **Configuration**

Enable Reconfigure Key Authentication Protocol Service

Device Name	Device Type	Interface	Assigned Prefix	Link Local Addr	MAC Addr
Client	NUT	Link0	3ffe:501:ffff:101::/64	NUT's Linklocal address	NUT's MAC address
Server	TN	Link0	3ffe:501:ffff:101::/64	fe80::200:ff:fe00:a1a1	00:00:00:00:a1:a1

## Procedure:

NUT	TN
	Initialize NUT (as a DHCPv6 client)
---->	<b>Solicit w/Rapid Commit Option w/Authentication Accept Option (*1)</b>
<----	Reply with Authentication Option
	Host address prefix is changed from 3ffe:501:ffff:100:: to 3ffe:501:ffff:200::
	Reload server configuration
<----	Reconfigure with computed Authentication (w/Authentication Option)
	w/Option Request Option (IA_NA) w/IA_NA w/Reconfigure Message Option (msg-type=5)
---->	<b>Renew w/Option Request Option (IA_NA) w/IA_NA (*4)</b>

- **Termination**

N/A

## Judgment:

(\*1) PASS: TN receive Solicit message with Authentication Accept option and Rapid Commit Option

(\*4) PASS: TN receive Renew message with Option Request Option (IA\_NA) and IA\_NA Option.

## References:

RFC3315

19.4.2. Creation and Transmission of Renew Messages

21.5. Reconfigure Key Authentication Protocol

21.5.3. Client considerations for Reconfigure Key protocol

## 5.42. Solicit/Reply Exchange finished, Reconfigure Message and validation test is failed

### Purpose:

- **Verification Points**

The client will receive a Reconfigure Key from the server in the initial Reply message from the server. The client records the Reconfigure Key for use in authenticating subsequent Reconfigure messages.

To authenticate a Reconfigure message, the client computes an HMAC-MD5 over the DHCP Reconfigure message, using the Reconfigure Key received from the server. If this computed HMAC-MD5 matches the value in the Authentication option, the client accepts the Reconfigure message.

### Category:

Client

### Initialization:

- **Network Topology**

Refer the topology "Fig.3 Topology No.3".

- **Configuration**

Enable Reconfigure Key Authentication Protocol Service

Device Name	Device Type	Interface	Assigned Prefix	Link Local Addr	MAC Addr
Client	NUT	Link0	3ffe:501:ffff:101::/64	NUT's Linklocal address	NUT's MAC address
Server	TN	Link0	3ffe:501:ffff:101::/64	fe80::200:ff:fe00:a1a1	00:00:00:00:a1:a1

## Procedure:

NUT	TN
	Initialize NUT (as a DHCPv6 client)
---->	<b>Solicit w/Rapid Commit Option w/Authentication Accept Option (*1)</b>
<----	Reply with Authentication Option
	Host address prefix is changed from 3ffe:501:ffff:100:: to 3ffe:501:ffff:200::
	Reload server configuration
<----	Reconfigure w/Invalid Authentication Option (Value field is invalid)
	w/Option Request Option (IA_NA) w/IA_NA w/Reconfigure Message Option (msg-type=5)
--> X	<b>Renew w/Option Request Option (IA_NA) w/IA_NA (*4)</b>

- **Termination**  
N/A

## Judgment:

- (\*1) PASS: TN receive Solicit message with Authentication Accept option and Rapid Commit Option
- (\*4) PASS: TN does not receive Renew message.

## References:

- RFC3315
- 19.4.2. Creation and Transmission of Renew Messages
- 21.5. Reconfigure Key Authentication Protocol
- 21.5.3. Client considerations for Reconfigure Key protocol

## 5.43. Sending Information-request Message and Receiving Reply Message

### Purpose:

- **Verification Points**

The client will receive a Reconfigure Key from the server in the initial Reply message from the server. The client records the Reconfigure Key for use in authenticating subsequent Reconfigure messages.

To authenticate a Reconfigure message, the client computes an HMAC-MD5 over the DHCP Reconfigure message, using the Reconfigure Key received from the server. If this computed HMAC-MD5 matches the value in the Authentication option, the client accepts the Reconfigure message.

### Category:

Client

### Initialization:

- **Network Topology**

Refer the topology "Fig.3 Topology No.3".

- **Configuration**

Enable Reconfigure Key Authentication Protocol Service

Device Name	Device Type	Interface	Assigned Prefix	Link Local Addr	MAC Addr
Client	NUT	Link0	3ffe:501:ffff:101::/64	NUT's Linklocal address	NUT's MAC address
Server	TN	Link0	3ffe:501:ffff:101::/64	fe80::200:ff:fe00:a1a1	00:00:00:00:a1:a1

## Procedure:

NUT	TN
	Initialize NUT (as a DHCPv6 client)
---->	<b>Information-Request w/Authentication Accept Option and Option Request Option (Preference Option) (*1)</b>
<----	Reply with Authentication Option and Preference Option (10)
	Preference changed from 10 to 20
	Reload server configuration
<----	Reconfigure with computed Authentication (w/Authentication Option) w/Reconfigure Message Option (msg-type=11)
---->	<b>Information-Request with Option Request Option (Preference Option) (*4)</b>

- **Termination**

N/A

## Judgment:

(\*1) PASS: TN receive Information-Request message with Authentication Accept option and Option Request Option (Preference Option).

(\*4) PASS: TN receives Information-Request with Option Request Option (Preference Option).

## References:

RFC3315

19.4.2. Creation and Transmission of Renew Messages

21.5. Reconfigure Key Authentication Protocol

21.5.3. Client considerations for Reconfigure Key protocol

## 5.44. Information-Request/Reply Exchange finished, Receiving Reconfigure Message and validation test is failed

### Purpose:

- **Verification Points**

The client will receive a Reconfigure Key from the server in the initial Reply message from the server. The client records the Reconfigure Key for use in authenticating subsequent Reconfigure messages.

To authenticate a Reconfigure message, the client computes an HMAC-MD5 over the DHCP Reconfigure message, using the Reconfigure Key received from the server. If this computed HMAC-MD5 matches the value in the Authentication option, the client accepts the Reconfigure message.

### Category:

Client

### Initialization:

- **Network Topology**

Refer the topology "Fig.3 Topology No.3".

- **Configuration**

Enable Reconfigure Key Authentication Protocol Service

Device Name	Device Type	Interface	Assigned Prefix	Link Local Addr	MAC Addr
Client	NUT	Link0	3ffe:501:ffff:101::/64	NUT's Linklocal address	NUT's MAC address
Server	TN	Link0	3ffe:501:ffff:101::/64	fe80::200:ff:fe00:a1a1	00:00:00:00:a1:a1

**Procedure:**

NUT	TN
	Initialize NUT (as a DHCPv6 client)
---->	<b>Information-Request w/Authentication Accept Option</b>
	<b>and Option Request Option (Preference Option) (*1)</b>
<----	Reply with Authentication Option and Preference Option (10)
	Preference changed from 10 to 20
	Reload server configuration
<----	Reconfigure with w/Invalid Authentication Option (Value field is invalid)
	w/Reconfigure Message Option (msg-type=11)
--> X	<b>Information-Request with Option Request Option (Preference Option) (*4)</b>

• **Termination**

N/A

**Judgment:**

(\*1) PASS: TN receive Information-Request message with Authentication Accept option and Option Request Option (Preference Option).

(\*4) PASS: TN does not receive Information-Request with Option Request Option (Preference Option).

**References:**

RFC3315

19.4.2. Creation and Transmission of Renew Messages

21.5. Reconfigure Key Authentication Protocol

21.5.3. Client considerations for Reconfigure Key protocol