Modern Applied Science

www.ccsenet.org/journal.html

Vol. 3, No. 11

November 2009

# Research on Next Generation Dynamic Host Configuration Protocol and Security of Application

Ziqian Xiao, Jingyou Chen & Chaobo Yang

Department of Software Engineering, Hainan Software Profession Institute

Qionghai 571400, China

E-mail: xiaoziqian1234@163.com

**Abstract**

In this paper, the author studies on next generation of Dynamic Host Configuration Protocol (DHCPv6), expounds the principle of DHCPv6 and its message exchange process. And also point out that the security issues may exist, hence several strategies have been put forward to improve the safety of message exchange, as well as the security of network. The author discusses DHCPv6 as being independent of its interaction with Neighbor Discovery in this paper.

**Keywords:** Stateless Services, Identity Association, Message exchange, Relay Agents

## 1. Introduction

With the Internet's rapid development and expansion, IP address is about to face the depletion of resources. The next generation of IP Protocol (Ipv6) is ripe in theory. Although there are many problems in transition, we will eventually enter the world of IPv6. In IPv6 networks, the number of fixed nodes will become mobile. How to quickly and easily allow network nodes to connect to the Internet is a major issue we are facing. The current DHCPv4 resolved auto-configuration of network nodes, however, in the IPv6 network DHCPv6 will play as the protagonist, which will become indispensable to the future of network members, DHCPv6 is developed from the DHCPv4, more simple and more powerful. Unavoidably, some security issues existed. After the study on DHCPv6, we found that some strategies can be adopted to improve the security of the application of DHCPv6.

## 2. Define about DHCPv6

### *2.1 DHCP Unique Identifier (DUID)*

A DHCP Unique Identifier (DUID) is variable length data which uniquely identifies each individual DHCPv6 client or server. This is similar to the client or server identifier in DHCPv4, but is designed to ensure better uniqueness of the identifier among all clients and servers; [RFC3315] defines a standard format of DUIDs in order to help ensure that DUIDs are unique. They are the following three types: DUID-LLT, DUID-EN and DUID-LL, Figure 2.1 shows the detailed characteristics of their respective.

In Figure 2.1, DUID-EN in the Enterprise-number refers to IANA for a specified integer manufacturers, Identifier manufacturers refer to each specific marking of variable length.

### *2.2 Identity Association*

An Identity Association (IA) is a conceptual structure that identifies a set of DHCPv6 configuration information. Each IA is identified by a 32-bit identifier (Identity Association Identifier, IAID). An IAID must uniquely identify one particular IA within each client. The notion of an IA was introduced in DHCPv6 because of the property of IPv6 that an interface can have multiple IP addresses. The primary goal of IAs is to define multiple identities within a single client, each of which is associated with a different IPv6 address. The lease duration is managed per IA, not per address. Three types of IA:

• Identity association for non-temporary addresses (IA_NA): An IA_NA defines a set of normal, that is, not temporary; IPv6 addresses to be allocated for a client’s interface. Addresses in an IA_NA are expected to be used as long as the client wants to renew these addresses as necessary.

• Identity association for temporary addresses (IA_TA): An IA_TA defines a set of temporary IPv6 addresses to be allocated for a client’s interface, where temporary refers to the privacy extension. Due to the nature of temporary addresses, an IA_TA does not have the T1 and T2 parameters and is not expected to be renewed.

• Identity association for prefix delegation (IA_PD): An IA_PD defines a set of IPv6 prefixes to be allocated from a delegating router to a requesting router for prefix delegation. Like IA_NA, an IA_PD is expected to be renewed using the T1 and T2 parameters.

### *2.3 Binding*

A binding is a conceptual structure maintained by a server, which represents particular configuration information currently assigned to a client. For configuration information associated with an IA, the binding is identified by the tuple of <client's DUID, IA-type, IAID>, where IA-type is one of IA_NA, IA_TA, and IA_PD.

## 3. Working principle of DHCPv6

All DHCPv6 messages are carried in IPv6 UDP packets. The following well-known IPv6 addresses and UDP ports are used in DHCPv6 exchanges:

• All_DHCP_Relay_Agents_and_Servers (ff02::1:2): The well-known link-scope multicast address for relay agents and servers. All relay agents and servers must join this group on the interface accepting incoming messages.

• All_DHCP_Servers (ff05::1:3): The well-known site-scope multicast address for servers. All servers must join this group on the interface accepting incoming messages.

• UDP port 546: The well-known UDP port that clients listen on.

• UDP port 547: The well-known UDP port that servers and relay agents listen on.

### *3.1 Message Name and Descriptions*

Table 1 lists message name and descriptions.

### *3.2 Common Message exchange process*

The DHCPv6 protocol consists of various types of message exchanges. The exchanges for some common scenarios will be described next.

a. Exchanges for Address Allocation

A client starts DHCPv6 exchanges for address allocation with a Solicit message specifying an IA_TA or IA_NA for which the client wants to configure addresses. Servers receiving the Solicit message consult their local configurations, determine whether they can allocate addresses for the IA, and return Advertise messages containing their offers. When a server prepares the Advertise message, it attempts to send the same options that it will send to the client in its Reply message if the client chooses this server. This allows the client to compare the options and addresses advertised by different DHCP servers and choose the set of options and addresses that fit its particular needs. In practice, the contents of the Advertise message may not matter much; the client may simply choose the server that sends the first Advertise message as long as the server has the same preference.

Figure 3-1 shows that there are two servers, server1 and server2, respond to the Solicit message, and the client selects server1.

In Figure 3-1, Client receive the advertise message which send by Server1 earlier, so Client choose Server1 as DHCP server. And this can be done using the Rapid Commit option. The use of the Rapid Commit option primarily assumes an environment where at most one server is available for the client.

b. Exchanges for Prefix Delegation

DHCPv6 message exchanges for prefix delegation are mostly the same as those for address allocation described before with the following minor exceptions:

• The Confirm and Decline messages are not used for prefix delegation.

• When the requesting router (i.e., the DHCPv6 client) detects that it may have attached to a new uplink, it uses Rebind and Reply exchanges to confirm the previous binding, instead of using the Confirm message.

c. Exchanges for the Stateless Services

For the stateless DHCPv6 service—that is, getting configuration information that does not need per-client binding—Information-request and Reply exchanges are used. These exchanges are simple: the client sends an Information-request message, usually without including the DUID of any particular server. Servers receive the message, and respond with a Reply message containing any stateless configuration information. But this simple mechanism has turned out to be insufficient in practice, due to the lack of renewal operation. The IETF has standardized a new DHCPv6 option, called the Information Refresh Time (IRT) option, for the Information-request and Reply exchanges. This option specifies the interval with which the client needs to perform another exchange of Information-request and Reply messages so that the client can update the information with no more delay than the refresh interval.

An implementation that supports this option also has the notion of a default refresh time. Even if the Reply message to Information-request does not include an Information Refresh Time option, the client will perform another exchange about every 24 hours.

Figure 3-3 shows an example of exchanges with the Information Refresh Time option. In the first exchange, the Reply to the Information-request message contains a recursive DNS server address, 2000:db8:1111::35, and an Information Refresh Time option with the interval of 1 hour. Then the site starts renumbering, and the DNS server will have a new address, 2000:db8:ffff::35. During the migration period, both the old and new addresses are valid. In about 1 hour, the client starts the second exchange. This time, the two addresses of the recursive DNS server are provided. Eventually, the Reply message will contain the new address only, and then the site can stop using the old address(es).

d. Exchanges with Relay Agents

If there is no server on a link to which a client is attached, the client needs to contact servers via a DHCPv6 relay agent. The basic notion of relay agents is the same as that of relay agents in DHCPv4, but unlike DHCPv4, separate types of messages are used for communication between servers and relay agents. This is described in the table in section 3.Figure 3-4 shows procedure for a Solicit-Advertise exchange.

e. Other message exchanges

There are some else message exchange process, such as Renewal of Addresses, Server-initiated Exchanges and Other Exchanges for Address Allocation. Because these process are not the focus of this paper, so these are no longer described in detail.

## 4. We are faced with security issues in the use of DHCPv6

### *4.1 Stateless address allocation brings security risks*

It is convenient and low cost when using Stateless address configuration, but any nodes can be free to access the network, and easily obtain the relevant configuration information, which will bring about security threats.

### *4.2 Fake DHCP server sends configuration information*

In case there is a fake DHCP server in the network, sending incorrect configuration information to the computer to obtain configuration information, which will cause confusion in the network.

### *4.3 Explicitly send a message, may be illegal to obtain*

Message exchanges without encryption, may be accessed by an attacker, which will lead to the leakage of sensitive information.

### *4.4 Illegal client access to configuration information*

Message exchanges without authentication, the configuration information may be accessed by illegal clients.

## 5. Strategies to improve security

### *5.1 Strategies to protect the safety of the network*

Compared with IPv4, IPv6 has a lot of great improvements. Most notably, IPsec will be integrated into the IPv6 protocol, then IPSec will no longer stand alone, but as an inherent part of IPv6 protocol, and cross-cutting.

For the physical layer of security risks, we can configure redundant equipment, redundant lines, security power supply, environment protection, as well as electromagnetic compatibility to enhance the protection of safety management. Level above the physical layer of security risks, we can use the following means of protection: such as AAA, TACACS +, RADIUS access control protocol, and security control user access to the network to prevent attacks against the application layer; through the MAC address and IP address binding to restrict the MAC addresses per port to use and the number of broadcast packets per port to establish the threshold volume, the use of Port-based VLAN and ACL, users establish a secure tunnel such as to prevent attacks against the two networks; routing through the filter of the routing information encryption and authentication, multicast directional control and improve routing convergence speed and reduce the impact of routing oscillation measures to strengthen the security of three-tier network. IPSec routers and switches guarantee the perfect support for the network data and the validity of information, consistency and integrity, and provide a number of network security solutions.

### *5.2 Initiative Detect illegal DHCP server*

If there is an illegal server on the network, that will be a great danger and can lead to paralysis of the entire network. It is difficult to think the culprit is an illegal server. Even if there existence of an illegal server on the network, but it is also difficult to identify the location of illegal server if in a large enterprise network. So, we can use some methods to detect illegal servers, for example, the establishment of a computer program to achieve this objective.

### *5.3 Exchanges with Authentication can improve security between DHCP Client and DHCP Server*

DHCPv6 has a built-in security mechanism between a client and a server in its base protocol specification. This security mechanism primarily aims to ensure integrity of DHCPv6 messages (particularly ones from a server to a client). It does not provide any confidentiality for message contents.

Overall, the integrity in the DHCPv6 security mechanism is ensured based on the HMAC (Keyed Hashing for Message Authentication Code) protocol. [RFC3315] defines two variations of the mechanism: The delayed authentication protocol and the reconfigure key protocol. Both protocols use a special-purpose DHCPv6 option—the Authentication option—as a common framework.

In the delayed authentication protocol, it is assumed that the client and the server(s) share the key beforehand by some out-of-band method. Figure 4-1 shows message exchanges using the delayed authentication protocol.

In the reconfigure key protocol is used specifically to secure a Reconfigure message. The client and the server do not have to share a key beforehand. Figure 4-2 shows message exchanges including a Reconfigure message with the reconfigure key protocol. Note that the key is sent to the client in the first Reply message without being encrypted. Thus, if an attacker can snoop between the server and the client, it can steal the key and mount an attack using a Reconfigure message with the valid HMAC digest. The reconfigure key protocol is thus not entirely secure, and that is why [RFC3315] states that this protocol be used only when there is not another mechanism available.

### *5.4 Authenticating communication between DHCP relay agent and server or between DHCP relay agents*

In practice, we can use IPsec to achieve the exchange of information security.IPsec was designed such that it is independent of the IP protocol versions. Currently, IPsec is widely deployed in IPv4 as a method to connect multiple remote sites for creating a single Virtual Private Network (VPN) over the Internet. In IPv6, supporting IPsec-related protocols is a mandatory requirement for any IPv6 node, which means all IPv6 nodes have IPsec enabled by default. This requirement will accelerate the deployment of IPsec not only for creating VPNs but also to encourage secure communications among IPv6 nodes. IPsec is a set of mechanisms that adds authentication and encryption to the IP layer.

Figure4-3 shows an example of use IP security for communication between a relay agent and a server or between relay agents.

AH offers connectionless data integrity and data origin authentication for IP packets with optional protection against packet replays. The authentication covers the IPv6 header, the extension headers and upper layer protocol data. Figure 4-4 shows Original Packet of IPv6, Figure 4-5 shows after applying AH.

ESP provides all of the security services offered by AH. In addition, ESP offers data confidentiality by means of encryption and limited traffic flow confidentiality. The header coverage is the primary difference between the authentication service provided by AH and that provided by ESP. ESP does not cover the IPv6 header and the extension headers unless these are encapsulated in the tunnel. Figure 4-6 shows Insertion of the ESP header.

The Authentication Data portion of the ESP packet is optional and is included when the SA has selected the authentication service. The length of the Authentication Data depends on the chosen authentication function. The authentication algorithm performs the computation covering the entire ESP header as shown in Figure 4-6. Since data integrity protection is provided only for the ESP header, we must use AH in addition to ESP if the IPv6 header and the extension headers placed before ESP also require integrity protection. Figure 4-7 shows details of ESP Placement with AH.

## 6. Conclusion

In the above paragraphs, we have discussed the definition of DHCPv6, and its principle and process for the information exchange. And some feasible strategies to ensure the next generation Ipv6 network DHCP services in security applications have also been given, which is based on the experiences of current Ipv4 network.

## References

Chen, lijun. (2008). Security Project Analysis and Investigation Based on DHCP. *Beijing University of Posts and Telecommunications*. 2008. 9. 17.

M. Bellar. R. Canetti. (1997). HMAC: Keyed-Hashing for Message Authentication .*RFC2104*. February 1997.

Qing Li, Tatuya Jinmei and Keiichi Shima. (2007). *IPv6 Advanced Protocols Implementation*. Morgan Kaufmann Publish. 2007.

R. Dorms et al. (2003). "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)," *RFC3315*. July 2003.

R.Droms, W. Arbaugh. (2001). Authentication for DHCP Messages .*RFC3118*. June 2001.

S. Frankel and S. Kelly. (2002). *"The HMAC-SHA-256-128 Algorithm and Its Use with IPsec"*. Internet Draft:

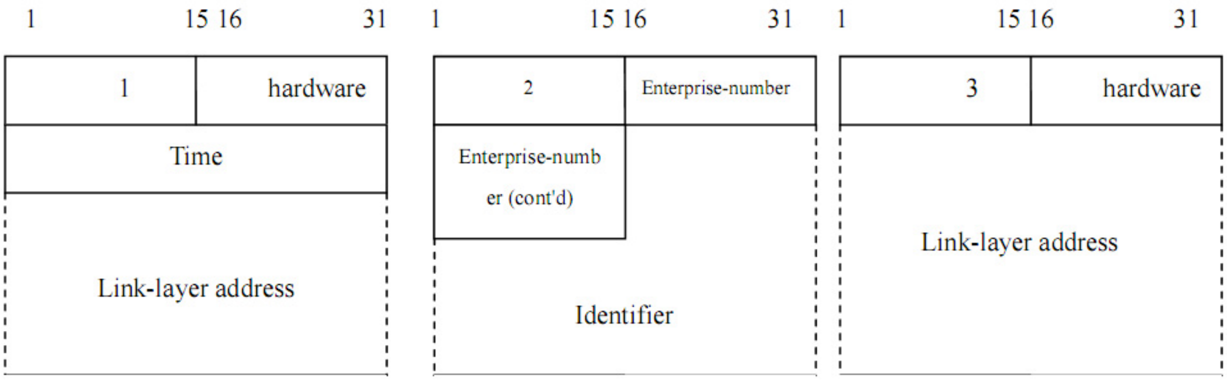
draft-ietf-ipsec-ciph-sha-256-01.txt. June 2002.

T. Narten and R. Draves. (2001). "Privacy Extensions for Stateless Address Autoconfiguration in IPv6".*RFC3041*. January 2001.

Xiao, shaobin. (2005). Research and Implementation for DHCPv6.*Southwest Jiaotong University*.2005.8.16.

Table 1. Message Name and Descriptions

| Type | Name | Description |
|---|---|---|
| 1 | Solicit | Sent by a client to find available DHCPv6 servers |
| 2 | Advertise | Sent by a server in response to a Solicit message with configuration information. |
| 3 | Request | Sent by a client to a particular server to perform resource (e.g., address) allocation. |
| 4 | Confirm | Sent by a client when it may have moved to a different link in order to check whether the prefix of allocated addresses (if any) is still valid. |
| 5 | Renew | Sent by a client to the server that has allocated a configuration resource to renew the use of that resource. |
| 6 | Rebind | Sent by a client to servers to renew an allocated information resource when the attempt using Renew messages fails. |
| 7 | Reply | Sent by a server in response to various messages from a client, mainly for confirming or rejecting the request that the client made. |
| 8 | Release | Sent by a client to the server that allocated a configuration resource in order to inform the server that the resource can be released. |
| 9 | Decline | Sent by a client when it detects that an allocated address is already in use. It informs the server that the address cannot be used. |
| 10 | Reconfigure | Sent by a server to initiate exchanges starting with a Renew or Information request message. It forces the client to refresh the information allocated to it. |
| 11 | Information-request | Sent by a client for the stateless service. |
| 12 | Relay-forward | Sent by a relay agent, encapsulating a message from a client to the server. |
| 13 | Relay-reply | Sent by a server, encapsulating a message returned to a client through relay agents. |



Format of DUID-LLT

Format of DUID-EN

Format of DUID-LL

Figure 2.1 Three types of DUIDs

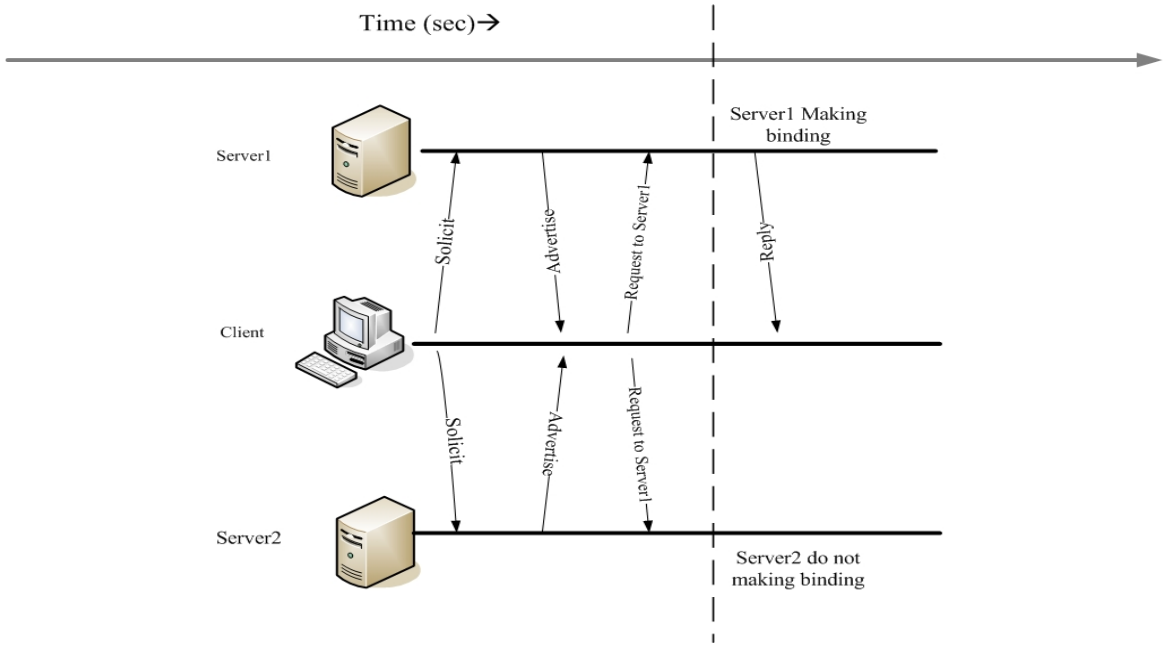


Figure 3-1. Initial message exchanges for address allocation

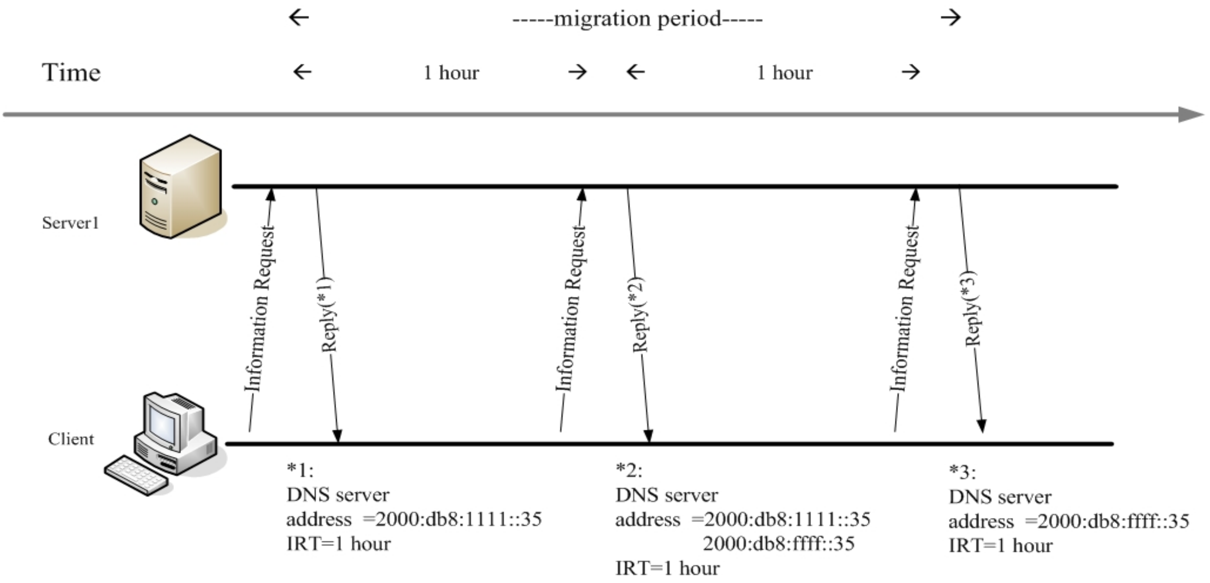


Figure 3-3. Renumbering procedure for stateless exchanges

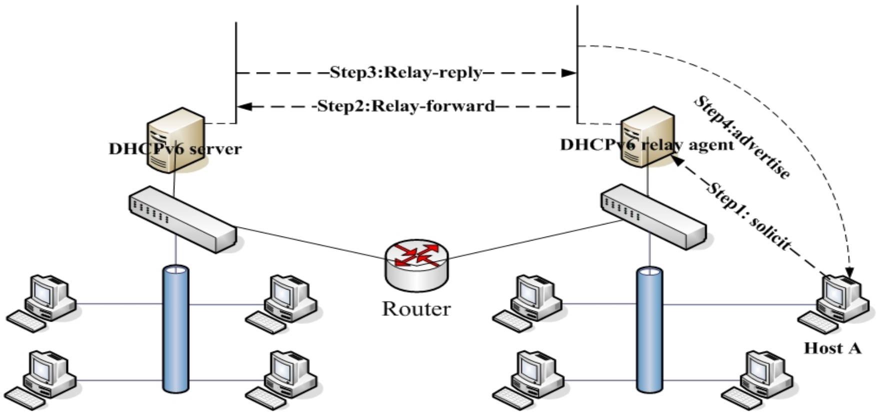


Figure 3-4. Solicit-Advertise exchange via a relay agent

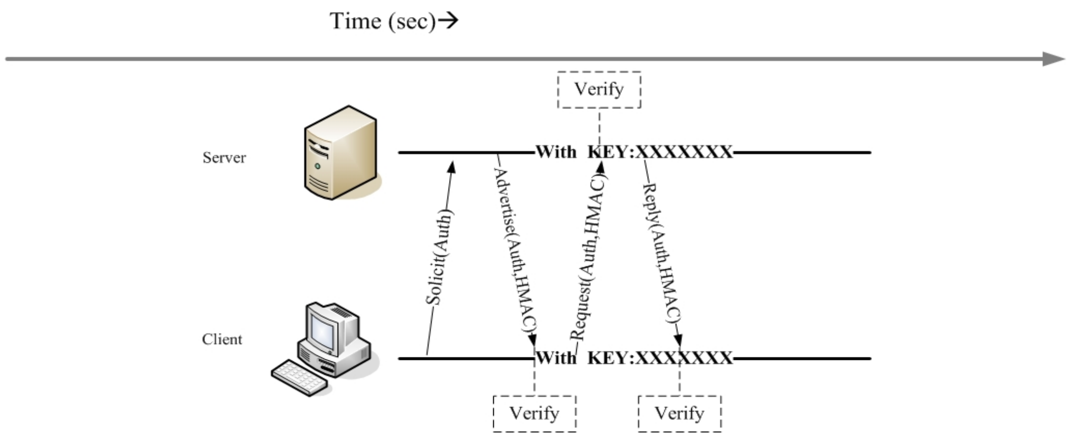


Figure 4-1. DHCPv6 message exchanges using the delayed authentication protocol

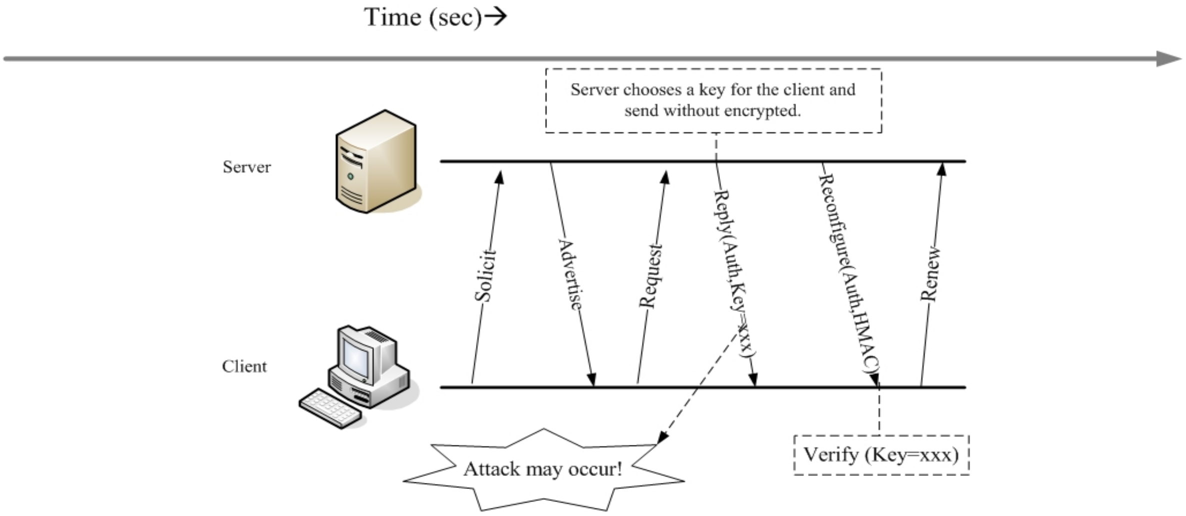


Figure 4-2. DHCPv6 message exchanges using the reconfigure key protocol.

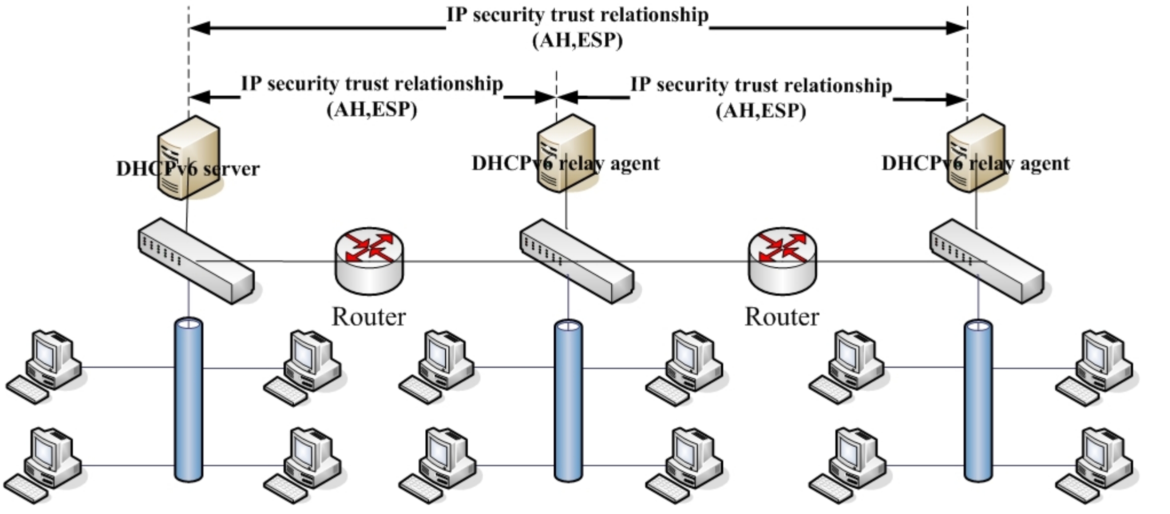

IP security trust relationship (AH,ESP)
IP security trust relationship (AH,ESP)
IP security trust relationship (AH,ESP)
DHCPv6 server
DHCPv6 relay agent
DHCPv6 relay agent
Router
Router

Figure 4-3. Use IP security for communication between a relay agent and a server or between relay agents.

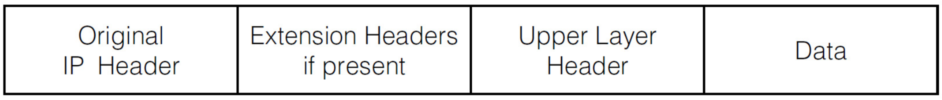


Figure 4-4. Original Packet of IPv6

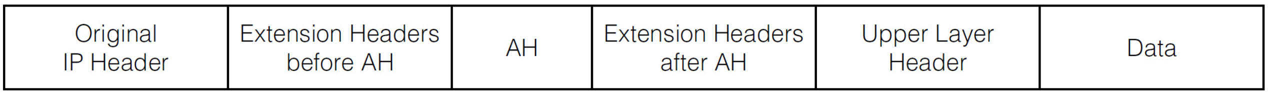


Figure 4-5. After applying AH

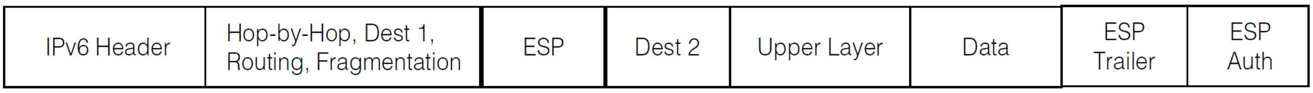


Figure 4-6. Insertion of the ESP header

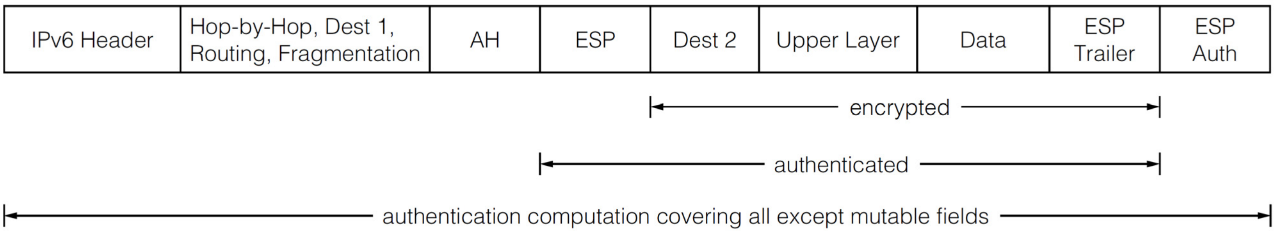

IPv6 Header
Hop-by-Hop, Dest 1, Routing, Fragmentation
AH
ESP
Dest 2
Upper Layer
Data
ESP Trailer
ESP Auth
encrypted
authenticated
authentication computation covering all except mutable fields

Figure 4-7. ESP Placement with AH