NTT Communications

# .com Master

ADVANCE

OFFICIAL TEXT

# Internet Certificate Examination

NTT Communications

notified contents comply with the contents of M (Managed) flag and O (Other) flag in RA. (see below).

- **Stateful DHCPv6 (Stateful Address Automatic Configuration)**

Stateful DHCPv6 (RFC 3315) runs when the bit value of M (Managed) flag in RA is 1. Stateful DHCPv6 is a method in which it is possible to pool the IPv6 address in the DHCPv6 server beforehand, and allot an IPv6 address to the host from the pool.
The basic function is the same as IPv4, but since the default gateway information is not notified, RA notification of manual settings in the host is required. Further, server information such as DNS server etc. is notified from the DHCPv6 server.

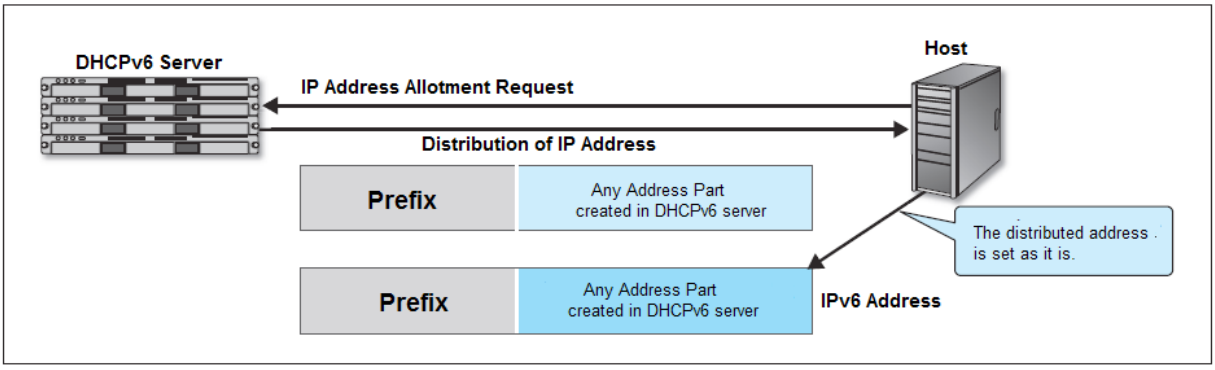


Fig. 1.24 • Stateful DHCPv6

- **Stateful DHCPv6**

Stateless DHCPv6 (RFC 3736) runs when the bit value of O (Other) flag in RA is 1. The stateless DHCPv6 notifies only server information such as DNS server etc., and does not notify IP address. In this case, setting the IP address in host is combined with the stateful address automatic configuration or manual configuration is required.

- **DHCPv6-PD**

DHCPv6-PD (RFC 3633) is a method of allocating address prefix from ISP etc. For example, when one address prefix is allotted to the router, it is possible to redistribute the IP address to the host using RA or DHCPv6 from the address prefix to which the router is allotted.

## ■ Multi-Prefix

In IPv6, IPv6 address with different prefixes is supported as a standard in configurable multiprefix in one network interface*26.

However, if a host gives a prefix from both IPv6 network and IPv6 internet generally known as closed IPv6 network such as NTT NGN and FLET's network that cannot mutually communicate with the Internet, and becomes a multi-prefix, it may be possible route selection and source address selection (see Reference) may not be done properly and communication may not be established appropriately. (Fig. 1.25)

**Reference** **Selection of Source Address in Multi-Prefix**

In IPv6, if there are more than two choices for the source address during the transmission of packets, according to the rules known as longest match, the address with the longest match with destination address is selected.

Lets take the example of IP addresses 2001:db8::2003 and 2001:db8::2007. Which of these addresses have the longest match when compared to 2001:db8::2004.

2001:db8::2004 ends with …0010 0000 0000 0100, and 2001:db8::2003 ends with …0010 0000 0000 0011 and matches upto 125 digits. The IP address 2001:db8::2007 ends with 0010 0000 0000 0111 and matches upto 126 digits. Therefore, 2001:db8::2007 is the longest match.

*26 Interface for connecting to the network. In this case, it refers to an interface for allocating IP address to connect with TCP/IP. In some cases, it is possible to allocate multiple IP addresses to one network interface.

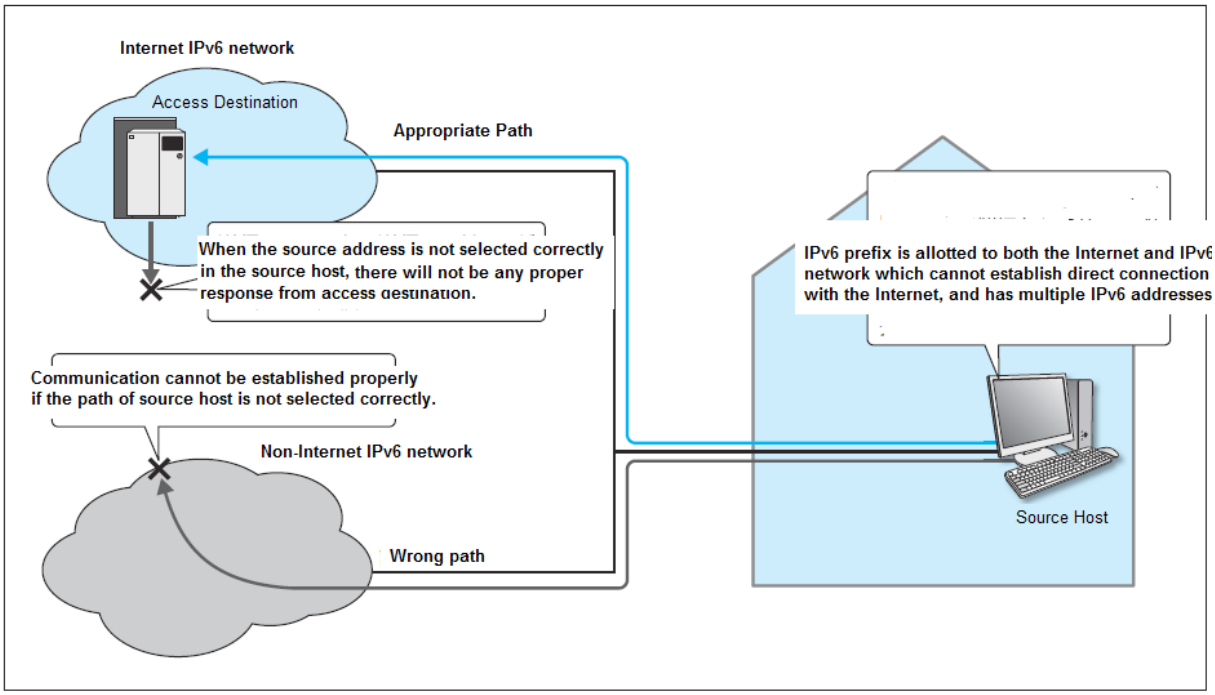


Fig. 1.25 • An example of a multi-IPv6 prefix problem

### ■ Compatibility with IPv4 Equipment

When communication is established in IPv6, the router device such as broadband router etc. must support IPv6. NIC (Network Interface Card), LAN cable, hubs etc. do not use the IP address, and can use the same one as used in IPv4 as it is.

In addition, IPv4 address and IPv6 address can be set at the same time in various OS such as Windows 8 etc., and this is supported in IPv4 as well as IPv6. This is known as dual stack when it is compatible with both IPv4 and IPv6.

### ■ Using IPv6 on IPv4 Network

The corresponding ISP in IPv6 is increasing, but it does not mean that all the servers and clients on the Internet can use the IPv6 address.

However, even in IPv4 networks that do not support IPv6, there are various technologies to allow the IPv6 communication between hosts. For example, it is possible to pass through the IPv4 network by storing all the IPv6 packets in IPv4 packet, in a technology known as IPv6 over IPv4 tunnel.

## ⑩ ICMP, ICMPv6

ICMP (Internet Control Message Protocol) is a protocol that complements IP which is used to ensure reliability and error notification and also used to determine the status of the network. 'ping' and 'traceroute' are used as network test applications using ICMP, and is used to determine the disconnection point of network and reason for delay in communication speed etc.

In addition to network inspection, ICMPv6 used in IPv6 is also used to search MAC address from the IP address and for automatic configuration of IP address. Further, ICMPv6 is used in RA, error notification, neighbor discovery, duplicate address detection, path MTU discovery etc., and controls communication. However, IPv6 communication may not be established properly, when ICMPv6 is configured such that transmission is not possible due to enhanced security etc.

### ■ Neighbor Discovery

Neighbor Discovery (ND) is a function used to discover the host and router which exists in the same link, and is used for link-layer address resolution (Fig. 1.26), automatic configuration of IPv6 address, determination of network prefix, discovery of neighboring router etc.

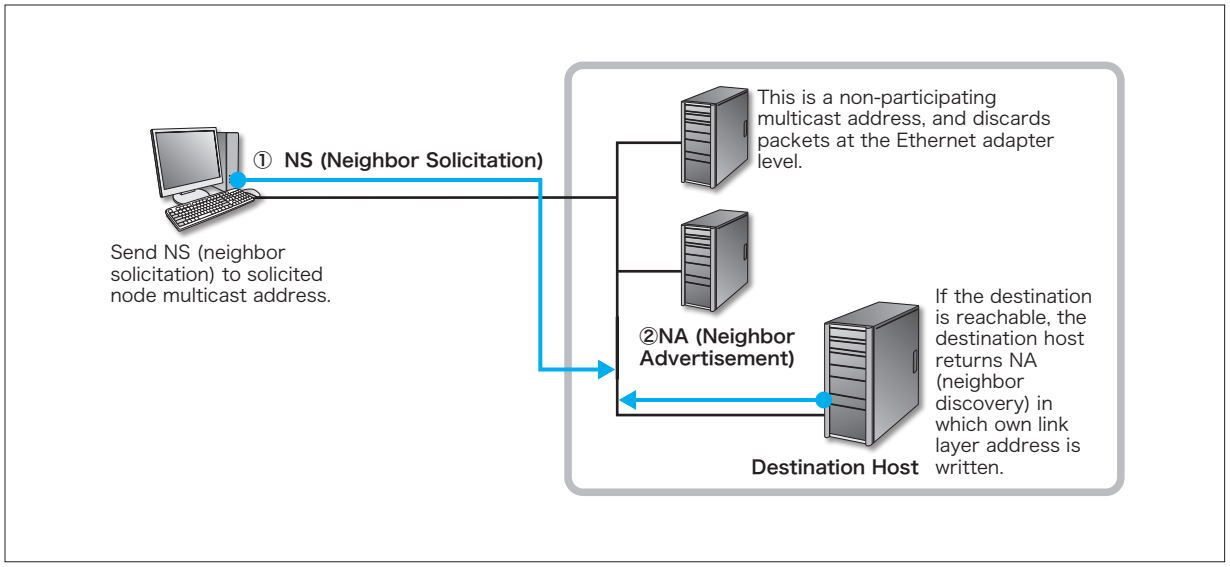


**Fig. 1.26 • Link Layer Address Resolution**

The protocol used for neighbor discovery is NDP (Neighbor Discovery Protocol). In addition, the neighbor discovery ICMPv6 messages are as shown in Table 1.7.

In order to resolve the link-layer address from the IP address of neighbor node, ARP was used in case of Ethernet in IPv4. In IPv6, ARP is not used, and link-layer address resolution is done using neighbor discovery which is independent of a particular media. Unlike IPv4 ARP, neighbor discovery uses multicast rather than broadcast.

In case of IPv4, IPv4 address and MAC address (link-layer address) information of the neighbor node was managed in ARP table. Unlike IPv4, IPv6 address and MAC address of neighbor node is managed in a table known as neighbor cache in IPv6.

In addition, neighbor cache is maintained and managed using a mechanism known as Neighbor Unreachability Detection (NUD).

**Table 1.7 Examples of ICMPv6 Neighbor Discovery Messages**

| Message | Role |
|---|---|
| NS: Neighbor Solicitation | • Duplicate Address Detection (DAD) and checking reachability/non-reachability<br>• Resolution of link layer address (Similar to ARP in IPv4) |
| NA: Neighbor Advertisement | • Response to neighbor solicitation<br>• Notification of change in own address |
| RS: Router Solicitation | • Used for discovery of router in segment<br>• Sent while obtaining router advertisement immediately |
| RA: Router Advertisement | • Notification of default route by router<br>• Automatic address settings are enabled with the distribution of prefix information |

## ■ Path MTU Discovery

In IPv4, intermediate routers perform fragmentation. In IPv6, division of packets is prohibited in router in order to speed up data transfer. Therefore, fragmentation is done only by the source in IPv6. The source confirms the packet size that can pass between the destinations.
This function is known as **Path MTU Discovery**.

In the Path MTU Discovery, data communication is established between destination hosts using local link MTU to which source host is connected. As shown in Fig. 1.27, when the packet to be transmitted is 1,500 bytes and MTU of the passing router is 1,400 bytes, packet is discarded as MTU is small in the passing router, and the router transmits the ICMPv5 message (Packet Too Big) to the source along with own MTU information. The source retransmits with the MTU included in this message and repeats until it reaches the destination host, and discovers the path MTU which is the smallest MTU. The source sends to the path MTU value after division of packets.