Case Studies of Recent IP Problems in Homes

Abstract

In this article, we explain some case studies of recent IP (Internet protocol) problems that have occurred in homes. This is the nineteenth in a bimonthly series on the theme of practical field information on telecommunication technologies. This month's contribution is from the Network Interface Engineering Group, Technical Assistance and Support Center, Maintenance and Service Operations Department, Network Business Headquarters, NTT EAST.

Keywords: IP problem, IPv6, case study

1. Introduction

A wide variety of terminals have come to be connected to the Internet protocol (IP) network in unison with the rapid expansion of Internet services in society. At NTT EAST, the Technical Assistance and Support Center has seen the number of problem incidents in the IP system increase annually as FLET'S and other IP communication services grow, and it has been working to identify and explain the causes of these IP communication problems using packet-capture analysis. This month's article describes recent developments in Internet technologies and introduces case studies of IP problems that have been solved by packet-capture analysis.

2. IPv4

This section describes recent developments in Internet Protocol version 4 (IPv4) and an associated problem.

2.1 IPv4 global addresses

On February 3, 2011, the Internet Assigned Numbers Authority (IANA), the organization that manages the allocation of IPv4 global addresses used mainly for establishing Internet connections, announced that these addresses had been exhausted. Then, about two months later on April 15, the Japan Network Information Center (JPNIC), the organization in charge of allocating and registering IP addresses in Japan, also announced the exhaustion of IPv4 addresses. At present, this applies only to IPv4 global addresses allocated to Internet service providers (ISPs) and corporations; the efficient use of existing addresses means that Internet usage is continuing as usual. However, as new allocation of IPv4 global addresses is no longer possible, it may not be possible to launch new services using the Internet via IPv4 connections.

2.2 Case study: slow Internet access

The following describes a problem related to the allocation and exhaustion of IPv4 global addresses. Specifically, a customer using the FLET'S service reported that Internet access was sometimes slow.

2.2.1 Customer's equipment configuration and conditions at time of problem occurrence

The equipment and systems used to establish this customer's Internet connection are shown in **Fig. 1**. In this setup, a Point-to-Point Protocol over Ethernet (PPPoE) session is established at the broadband router, while the customer equipment is connected on the local area network (LAN) side. After connecting to the Internet from a home personal computer (PC), the customer sometimes found that the connection was slow. A check of the broadband router log around the times the problem occurred revealed that PPPoE sessions had been released ten or more times in one day, as shown in **Fig. 2**.

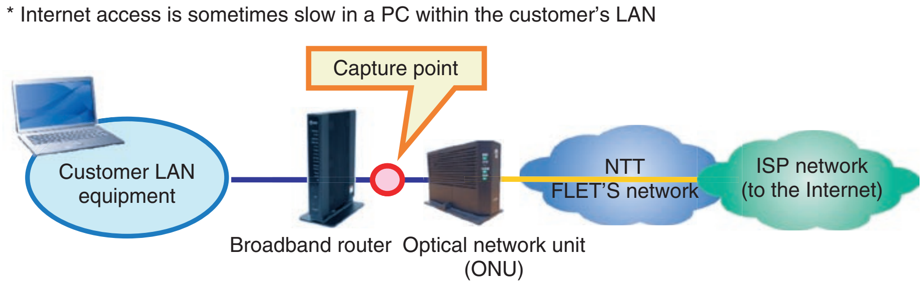
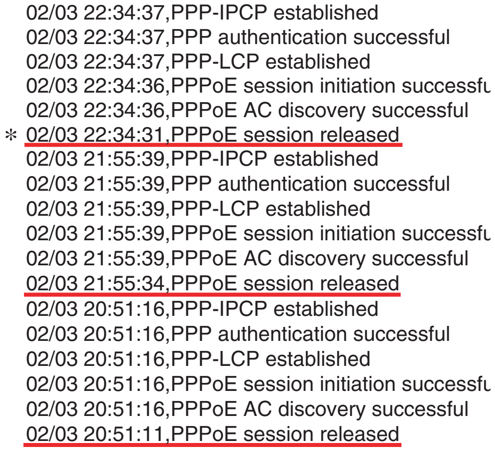

* Internet access is sometimes slow in a PC within the customer's LAN
Capture point
Customer LAN equipment
Broadband router
Optical network unit (ONU)
NTT FLET'S network
ISP network (to the Internet)

Fig. 1. Customer's Internet connection configuration.



```
  02/03 22:34:37,PPP-IPCP established
  02/03 22:34:37,PPP authentication successful
  02/03 22:34:37,PPP-LCP established
  02/03 22:34:36,PPPoE session initiation successfu
  02/03 22:34:36,PPPoE AC discovery successful
* 02/03 22:34:31,PPPoE session released
  02/03 21:55:39,PPP-IPCP established
  02/03 21:55:39,PPP authentication successful
  02/03 21:55:39,PPP-LCP established
  02/03 21:55:39,PPPoE session initiation successfu
  02/03 21:55:39,PPPoE AC discovery successful
  02/03 21:55:34,PPPoE session released
  02/03 20:51:16,PPP-IPCP established
  02/03 20:51:16,PPP authentication successful
  02/03 20:51:16,PPP-LCP established
  02/03 20:51:16,PPPoE session initiation successfu
  02/03 20:51:16,PPPoE AC discovery successful
  02/03 20:51:11,PPPoE session released
```

Fig. 2. Excerpt of PPPoE session release log in broadband router.

2.2.2 Inspection method and analysis results

We performed packet capture on the wide area network (WAN) side of the broadband router at the times the problem was occurring and then analyzed in detail all of the captured data corresponding to the time of that PPPoE session release indicated in the broadband router log. By doing this, we were able to determine why the problem was occurring.

(1) Log analysis at PPPoE session release time

We analyzed captured data before and after a PPPoE session release time as recorded on the broadband router log (Fig. 2). As shown in **Fig. 3**, the broadband router first receives and acknowledges a PPP Termination Request from the network side and then receives and acknowledges a PPPoE Active Discovery Terminate (PADT) signal, also from the network side. These actions result in the release of the PPPoE session.

(2) Captured data before/after PPPoE session release

Captured data before and after a PPPoE session release (marked by * in the broadband router log of Fig. 2) are outlined on the log and shown in **Fig. 4**. The data indicate that the 10-minute period prior to the PPP Termination Request from the network was an idle state between the broadband router and ISP (in this case, an idle Internet connection). The same was true for PPPoE session releases in other time slots; all were preceded by a 10-minute idle state. As shown in the figure, about 6 seconds was needed to reestablish a PPPoE session after its release, so it can be assumed that the system response would seem slow to the user if an Internet connection were to be attempted during such a session-reestablishment period.

2.2.3 Discussion based on analysis results

The analysis results (1) and (2) above indicated that communications control on the ISP side would release a PPPoE connection (perform disconnection processing) if an idle state existed for at least 10 minutes. The ISP most likely does this for allocated addresses that are not being actively used, with the intention being to achieve more effective use of IPv4 global addresses.

2.2.4 Cause of problem

The results of analysis suggested that this problem was caused by communications-control measures on the ISP side and not by any problems in the FLET'S network. We therefore contacted the ISP manager in question and confirmed that processing to release a PPPoE connection would indeed be initiated on the ISP side to recover IPv4 global addresses if an idle state continued for at least 10 minutes.

Looking forward, we can envision a large-scale rollout of the IPv6 next-generation Internet protocol

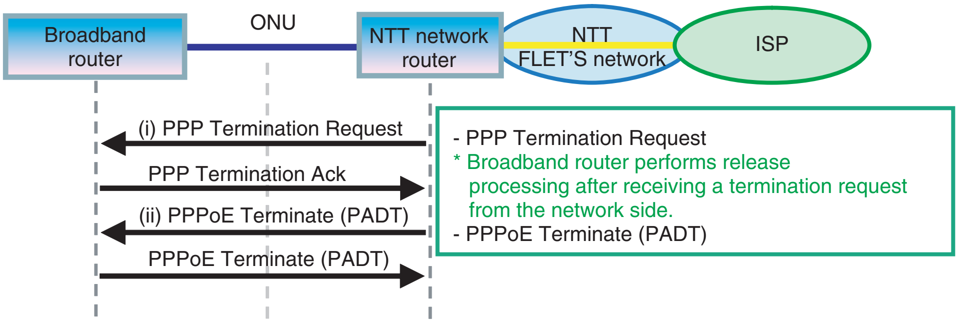
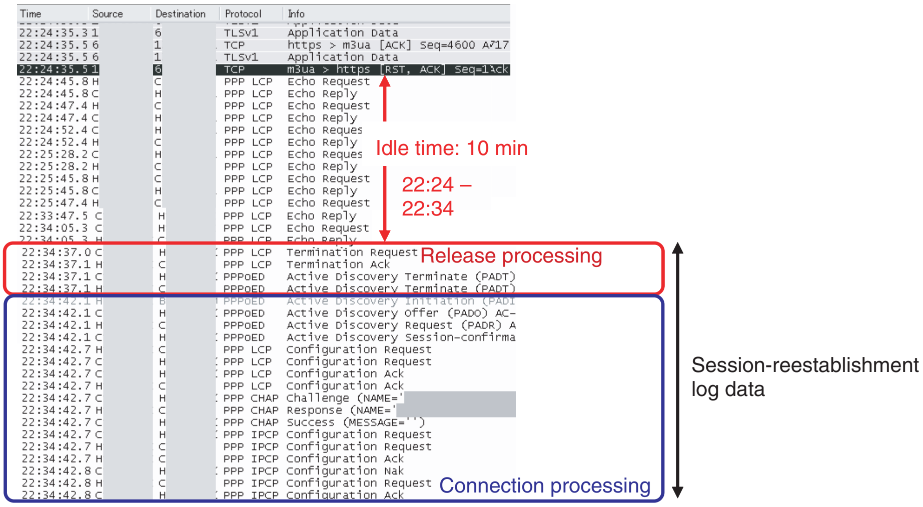

Broadband router
ONU
NTT network router
NTT FLET'S network
ISP
(i) PPP Termination Request
PPP Termination Ack
(ii) PPPoE Terminate (PADT)
PPPoE Terminate (PADT)
- PPP Termination Request
* Broadband router performs release processing after receiving a termination request from the network side.
- PPPoE Terminate (PADT)

Fig. 3. Session release sequence.



```
Time          Source     Destination   Protocol   Info
22:24:35.3 1             6             TLSv1      Application Data
22:24:35.5 6             1             TCP        https > m3ua [ACK] Seq=4600 A?17
22:24:35.5 6             1             TLSv1      Application Data
22:24:35.5 1             6             TCP        m3ua > https [RST, ACK] Seq=1\ck
22:24:45.8 H             C             PPP LCP    Echo Request
22:24:45.8 C             H             PPP LCP    Echo Reply
22:24:47.4 H             C             PPP LCP    Echo Request
22:24:47.4 C             H             PPP LCP    Echo Reply
22:24:52.4 C             H             PPP LCP    Echo Reques
22:24:52.4 H             C             PPP LCP    Echo Reply
22:25:28.2 C             H             PPP LCP    Echo Reques
22:25:28.2 H             C             PPP LCP    Echo Reply
22:25:45.8 H             C             PPP LCP    Echo Request
22:25:45.8 C             H             PPP LCP    Echo Reply
22:25:47.4 H             C             PPP LCP    Echo Request
22:33:47.5 C             H             PPP LCP    Echo Reply
22:34:05.3 C             H             PPP LCP    Echo Request
22:34:05.3 H             C             PPP LCP    Echo Reply
22:34:37.0 C             H             PPP LCP    Termination Request
22:34:37.1 H             C             PPP LCP    Termination Ack
22:34:37.1 C             H             PPPoED     Active Discovery Terminate (PADT)
22:34:37.1 H             C             PPPoED     Active Discovery Terminate (PADT)
22:34:42.1 H             B             PPPoED     Active Discovery Initiation (PADI
22:34:42.1 C             H             PPPoED     Active Discovery Offer (PADO) AC-
22:34:42.1 H             C             PPPoED     Active Discovery Request (PADR) A
22:34:42.1 C             H             PPPoED     Active Discovery Session-confirma
22:34:42.7 H             C             PPP LCP    Configuration Request
22:34:42.7 C             H             PPP LCP    Configuration Request
22:34:42.7 C             H             PPP LCP    Configuration Ack
22:34:42.7 H             C             PPP LCP    Configuration Ack
22:34:42.7 C             H             PPP CHAP   Challenge (NAME='
22:34:42.7 H             C             PPP CHAP   Response (NAME='
22:34:42.7 C             H             PPP CHAP   Success (MESSAGE='')
22:34:42.7 C             H             PPP IPCP   Configuration Request
22:34:42.7 H             C             PPP IPCP   Configuration Request
22:34:42.7 H             C             PPP IPCP   Configuration Ack
22:34:42.8 C             H             PPP IPCP   Configuration Nak
22:34:42.8 H             C             PPP IPCP   Configuration Request
22:34:42.8 C             H             PPP IPCP   Configuration Ack
```

Fig. 4. Captured data before and after session release.

in response to this problem, and we can also consider the introduction of a mechanism to achieve more efficient use of IPv4 global addresses.

3. IPv6

This section describes recent developments in Internet Protocol version 6 (IPv6) and an IPv6 Internet connection problem.

3.1 IPv6 features

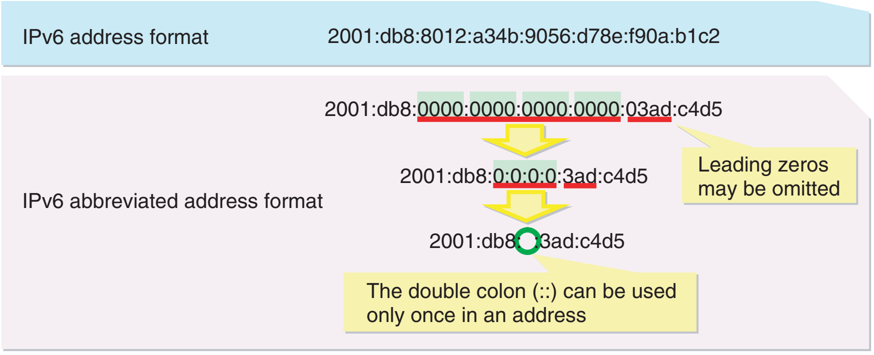
IPv6 was developed as the next-generation IP to succeed IPv4, which has been the protocol used to support Internet connections to date. As the scale of the Internet grew over the years, a number of shortcomings in IPv4 came to light, the most obvious of which is the exhaustion of IPv4 global addresses. Another problem is network address translation (NAT) traversal.

The aim of NAT traversal is to use IPv4 global addresses efficiently (economically) on the WAN side. With this method, a broadband router can increase the number of connected terminals by using private addresses on the LAN side and converting addresses by NAT (more accurately, network address and port translation (NAPT) since the process includes port translation). This method, however, prevents a terminal on the LAN side from being directly specified from the outside, thereby hampering bidirectional communications. Specifically, it can result in complicated settings and problematic communications in such applications as 050-type IP telephony and online multiplayer games.

In contrast to the above, IPv6 extends the address

Table 1. IPv4 and IPv6 features.

Version	IPv4	IPv6
Address length (number of addresses)	32 bits (about 4.3 billion)	128 bits (about 3.4 × 10^{38})
Address notation method	Decimal notation	Hexadecimal notation
Address allocation method	Specifications do not provide for automatic allocation of addresses, so other mechanisms must be used.	Specifications provide for automatic allocation of addresses.


IPv6 address format
2001:db8:8012:a34b:9056:d78e:f90a:b1c2
IPv6 abbreviated address format
2001:db8:0000:0000:0000:0000:03ad:c4d5
2001:db8:0:0:0:0:3ad:c4d5
Leading zeros may be omitted
2001:db8::3ad:c4d5
The double colon (::) can be used only once in an address

- Leading zeros in each section of four hexadecimal digits are to be omitted. For example, 0db8 is written as db8, and 0000 is simply written as 0.
- Consecutive four-digit sections of 0s are replaced by a double colon (::) wherever possible.
- If only one four-digit section of 0s appears in the address, it is not replaced by a double colon (::).
- If there are multiple fields that can be replaced by a double colon (::), the field with the most four-digit sections of 0s is to be replaced by a double colon (::). However, if the number of four-digit sections of 0s is the same for all replaceable fields, the forward field shall be replaced by a double colon (::).

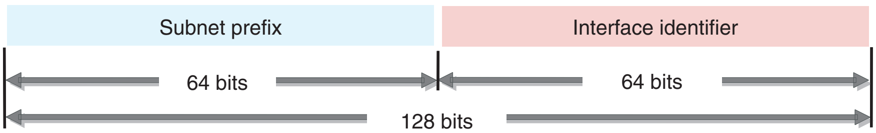
Fig. 5. IPv6 address notation.

space to 128 bits, thereby resolving the problem of an insufficient number of global IP addresses. The features of IPv4 and IPv6 are listed in **Table 1**. IPv4 uses 32-bit addresses, which means that it can handle 2^{32} or about 4.3 billion IP addresses. However, with 128-bit addresses, IPv6 can handle 2^{128} or about 3.4 × 10^{38} IP addresses, a significantly larger number. If all of these IP addresses were to be allocated to the entire human race (which we set to 7 billion people for calculation purposes), the number of addresses per person would turn out to be 480 × 10^{26}. It can therefore be said that the number of IPv6 addresses that can be implemented is essentially infinite. The IPv6 specifications also feature enhanced security functions and the addition of Internet Protocol Security (IPsec) as a standard function enabling the creation of a secure communications environment.

3.2 IPv6 address notation

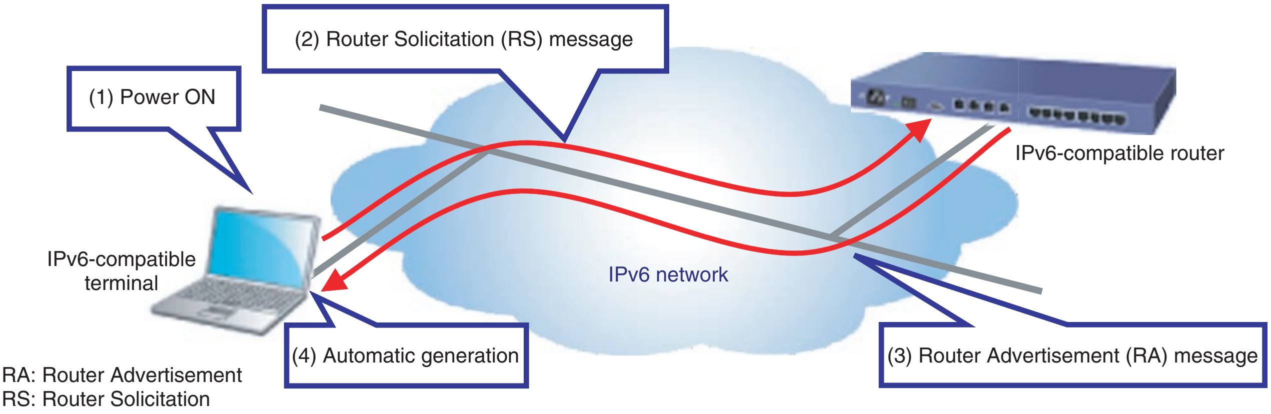
The IPv6 address notation method is shown in **Fig. 5**. Since the address space has been extended to 128 bits in IPv6, a hexadecimal (0–f) notation method has been adopted that divides the 128 bits (16 bits × 8) into 8 groups of 16 bits connected by colons.

Furthermore, as shown in **Fig. 6**, the IPv6 unicast address used for Internet connections treats the first 64 bits of the 128-bit address as a subnet prefix and the last 64 bits as an interface identifier making for a clearly defined address format. In IPv4 addresses, the bit sequences for the network address and host address could change, which means that address processing at network interfaces has been mainly



- The interface identifier of a unicast address beginning with other than binary 000 is configured in Modified EUI-64 format with a length of 64 bits.
- The boundary between the network-identifying and node-identifying sections is variable in IPv4 but fixed in IPv6.

Fig. 6. IPv6 unicast address structure.



RA: Router Advertisement
RS: Router Solicitation

Fig. 7. IPv6 automatic address generation method.

handled by software. In short, while achieving high-speed processing was problematic with IPv4 addresses, this uniform method of using bit sequences in IPv6 addresses means that high-speed processing can be achieved by hardware.

3.3 IPv6 address allocation method

Unlike IPv4, the address allocation method specified by IPv6 automatically allocates IP addresses for establishing IPv6 connections. This IPv6 automatic address generation scheme, called IPv6 plug and play, is shown in **Fig. 7**. The convenience of IPv6 plug and play is analogous to the ease of using a home appliance by simply plugging it into a power outlet on a wall. When a LAN cable is connected to an IPv6-compatible terminal (and authentication is performed in the case of a wireless LAN) (1), the terminal transmits a Router Solicitation (RS) message (2), and an IPv6 router in the network returns a Router Advertisement (RA) message (3). The IPv6-compatible terminal then extracts from this RA message the information needed to automatically generate an IPv6 unicast address (4). The above process can be mainly accomplished by hardware, which means that an IPv6 unicast address can be configured in even less time that it takes to boot up the OS (operating system) on a PC running Windows.

3.4 Toward full-scale deployment of IPv6

The *World IPv6 Launch* was held on June 6, 2012 as a global event to introduce the new protocol. The intention behind this event was to convey the idea that IPv6 would be supported on an ongoing basis well beyond the launch date. This includes support for IPv6 standards by IP-network-compatible terminals to be marketed in the future as well as IPv6 support for website connections. The holding of this event signified a transition to a full-scale IPv6 deployment stage.

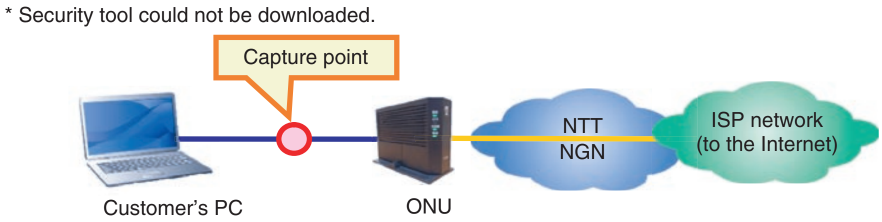

* Security tool could not be downloaded.
Capture point
Customer's PC
ONU
NTT NGN
ISP network (to the Internet)

Fig. 8. Customer's Internet connection configuration.

3.5 Case study: Security Tools cannot be downloaded on FLET'S HIKARI NEXT

We present here a case study of a problem related to IPv6 connections. Specifically, a customer subscribing to the *FLET'S HIKARI NEXT High-speed Type* broadband access service was unable to download Security Tools (the name of this service at NTT WEST, but called FLET'S VIRUS CLEAR v6 at NTT EAST) from FLET'S simple setup tools. Additionally, while IPv4 Internet communications presented no problems, connections to IPv6 sites such as an IPv6 service information site could not be achieved.

3.5.1 Customer's equipment configuration and conditions at time of problem occurrence

The customer's Internet connection configuration is shown in **Fig. 8**. Here, one PC running Windows 7 was connected to the ONU, and Internet connections to the PC were established using installed startup tools (i.e., PPPoE connection functions in the OS). In this environment, IPv4 Internet communications were able to be performed without incident, but Security Tools could not be downloaded from the FLET'S simple setup tools.

3.5.2 Inspection method and analysis results

We performed packet capture between the ONU and PC at the time the problem occurred. We also performed packet capture when connecting a test PC that was shown to be capable of downloading Security Tools, and we compared and analyzed the captured data between these two PCs.

(1) Problem trigger

The sequence flow at the time of a Security Tools download-destination connection failure is shown in **Fig. 9**. To begin with, the series of operations from turning on the PC to determining the IPv6 unicast address for connecting to the FLET'S HIKARI NEXT service (NGN: Next-Generation Network), was executed normally. This was followed by name resolution (DNS: Domain Name Service) of the URL (uniform resource locator) for the Security Tools download destination, which was likewise performed without any problems.

Next, the PC transmitted a hypertext transfer protocol (HTTP) synchronize (SYN) request to initiate the HTTP connection process. Immediately after this, the NTT network router transmitted a Neighbor Solicitation (NS) message (media access control (MAC) address request in IPv6 communications) to the PC's NGN unicast address. However, no Neighbor Advertisement (NA) message (MAC address reply in IPv6 communications) was subsequently transmitted from the PC side, so the NTT network router entered a state in which it could not move to the next sequence. Finally, after the PC repeated the transmission of the HTTP SYN request three to four times, the connection terminated. At this time, the message "Cannot Display" appeared on the PC browser's screen. The above analysis led us to conclude that there was some reason why NA messages were not being transmitted from the PC side.

(2) PC operation at time of problem occurrence

In searching for the reason why no NA messages were being transmitted from the PC, we found that NA transmission for that NGN unicast address was being blocked by the PC's Windows firewall.

3.5.3 Discussion based on analysis results

We also found that default settings for the Windows firewall do not block NA transmissions. However, depending on the security software preinstalled in PCs, settings that restrict IPv6 communications can also be made, and we surmise that those default settings were changed at the time of product shipment.

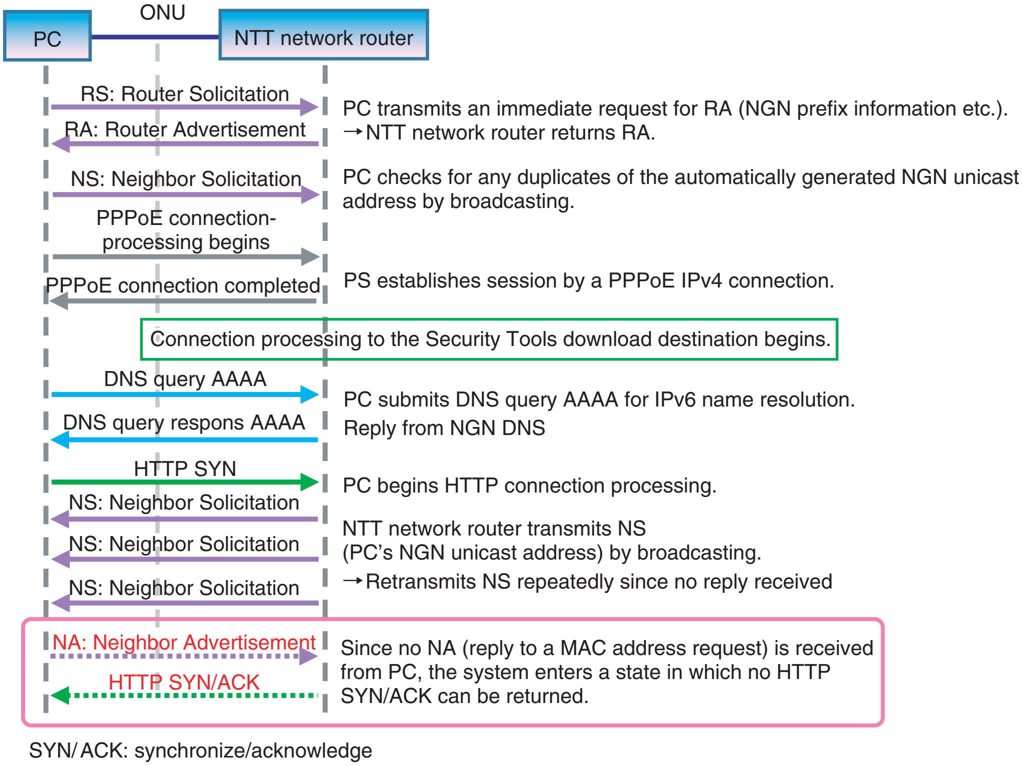

PC
ONU
NTT network router
RS: Router Solicitation
RA: Router Advertisement
PC transmits an immediate request for RA (NGN prefix information etc.).
→NTT network router returns RA.
NS: Neighbor Solicitation
PC checks for any duplicates of the automatically generated NGN unicast address by broadcasting.
PPPoE connection-processing begins
PPPoE connection completed
PS establishes session by a PPPoE IPv4 connection.
Connection processing to the Security Tools download destination begins.
DNS query AAAA
DNS query respons AAAA
PC submits DNS query AAAA for IPv6 name resolution.
Reply from NGN DNS
HTTP SYN
PC begins HTTP connection processing.
NS: Neighbor Solicitation
NS: Neighbor Solicitation
NS: Neighbor Solicitation
NTT network router transmits NS
(PC's NGN unicast address) by broadcasting.
→Retransmits NS repeatedly since no reply received
NA: Neighbor Advertisement
HTTP SYN/ACK
Since no NA (reply to a MAC address request) is received from PC, the system enters a state in which no HTTP SYN/ACK can be returned.
SYN/ ACK: synchronize/acknowledge

Fig. 9. Sequence at time of Security Tools download-destination connection failure.

3.5.4 Cause of problem

The search for the reason why no NA messages were being issued by the customer's PC revealed that NA transmissions for that NGN unicast address were being blocked due to that PC's Windows firewall settings. This is why the PC entered into a state in which it could not connect with an IPv6 site. Consequently, changing the Windows firewall settings or temporarily disabling the firewall made it possible to connect to the Security Tools download site and download those tools. This case study underscores the importance of checking PC settings in the event that specific types of communications cannot be performed.

4. Conclusion

In this article, we gave an overview of the IPv4 and IPv6 protocols and introduced two case studies of recent IP problems experienced by customers in their homes. New services and products using IP connections are constantly being launched, and the IP network within customers' homes is becoming increasingly diversified and complex. The Technical Assistance and Support Center is committed to uncovering the causes of IP-related problems and to finding early solutions.