International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Q.3405

(10/2018)

SERIES Q: SWITCHING AND SIGNALLING, AND ASSOCIATED MEASUREMENTS AND TESTS

Signalling requirements and protocols for the NGN – Service and session control protocols

IPv6 protocol procedures for broadband services

Recommendation ITU-T Q.3405

ITU-T Q-SERIES RECOMMENDATIONS

SWITCHING AND SIGNALLING, AND ASSOCIATED MEASUREMENTS AND TESTS

SIGNALLING IN THE INTERNATIONAL MANUAL SERVICE	Q.1–Q.3
INTERNATIONAL AUTOMATIC AND SEMI-AUTOMATIC WORKING	Q.4–Q.59
FUNCTIONS AND INFORMATION FLOWS FOR SERVICES IN THE ISDN	Q.60–Q.99
CLAUSES APPLICABLE TO ITU-T STANDARD SYSTEMS	Q.100–Q.119
SPECIFICATIONS OF SIGNALLING SYSTEMS No. 4, 5, 6, R1 AND R2	Q.120–Q.499
DIGITAL EXCHANGES	Q.500–Q.599
INTERWORKING OF SIGNALLING SYSTEMS	Q.600–Q.699
SPECIFICATIONS OF SIGNALLING SYSTEM No. 7	Q.700–Q.799
Q3 INTERFACE	Q.800–Q.849
DIGITAL SUBSCRIBER SIGNALLING SYSTEM No. 1	Q.850–Q.999
PUBLIC LAND MOBILE NETWORK	Q.1000–Q.1099
INTERWORKING WITH SATELLITE MOBILE SYSTEMS	Q.1100–Q.1199
INTELLIGENT NETWORK	Q.1200–Q.1699
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR IMT-2000	Q.1700–Q.1799
SPECIFICATIONS OF SIGNALLING RELATED TO BEARER INDEPENDENT CALL CONTROL (BICC)	Q.1900–Q.1999
BROADBAND ISDN	Q.2000–Q.2999
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR THE NGN	Q.3000–Q.3709
General	Q.3000–Q.3029
Network signalling and control functional architecture	Q.3030–Q.3099
Network data organization within the NGN	Q.3100–Q.3129
Bearer control signalling	Q.3130–Q.3179
Signalling and control requirements and protocols to support attachment in NGN environments	Q.3200–Q.3249
Resource control protocols	Q.3300–Q.3369
Service and session control protocols	**Q.3400–Q.3499**
Service and session control protocols – supplementary services	Q.3600–Q.3616
Service and session control protocols – supplementary services based on SIP-IMS	Q.3617–Q.3639
VoLTE/ViLTE network signalling	Q.3640–Q.3655
NGN applications	Q.3700–Q.3709
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR SDN	Q.3710–Q.3899
TESTING SPECIFICATIONS	Q.3900–Q.4099
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR IMT-2020	Q.5000–Q.5049
COMBATING COUNTERFEITING AND STOLEN ICT DEVICES	Q.5050–Q.5069

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T Q.3405

IPv6 protocol procedures for broadband services

Summary

Recommendation ITU-T Q.3405 identifies the Internet Protocol version 6 (IPv6) procedures which support broadband services with IPv6 transition. The protocol procedures are specified according to three basic IPv6 transition modes: dual stack, tunnelling and translation.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Q.3405	2018-10-14	11	11.1002/1000/13696

Keywords

DS-Lite, IPoE, IPv6, NAT, PPPoE.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Page

Recommendation ITU-T Q.3405

IPv6 protocol procedures for broadband services

1 Scope

This Recommendation identifies the Internet Protocol version 6 (IPv6) procedures which support broadband services with IPv6 transition. The protocol procedures are specified according to three basic IPv6 transition modes: dual stack, tunnelling and translation.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[IETF RFC 3315]	IETF RFC 3315 (2003), *Dynamic Host Configuration Protocol for IPv6 (DHCPv6).*
[IETF RFC 3633]	IETF RFC 3633 (2003), *IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6*.
[IETF RFC 4291]	IETF RFC 4291 (2006), *IP Version 6 Addressing Architecture*.
[IETF RFC 4861]	IETF RFC 4861 (2007), *Neighbor Discovery for IP version 6 (IPv6).*
[IETF RFC 6333]	IETF RFC 6333 (2011), *Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion*.
[IETF RFC 6598]	IETF RFC 6598 (2012), *IANA-Reserved IPv4 Prefix for Shared Address Space*.

3 Definitions

3.1 Terms defined elsewhere

None.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

BRAS	Broadband Remote Access Server
CPE	Customer Premise Equipment
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol version 6
DHCPv6-PD	Dynamic Host Configuration Protocol version 6 – Prefix Delegation

DNS	Domain Name Server
DS-Lite	Dual Stack-Lite
IP	Internet Protocol
IPoE	Internet Protocol over Ethernet
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
MAC	Media Access Control
NAT	Network Address Translation
NDP	Neighbour Discovery Protocol
PPPoE	Point-to-Point Protocol over Ethernet
WAN	Wide Area Network

5 Conventions

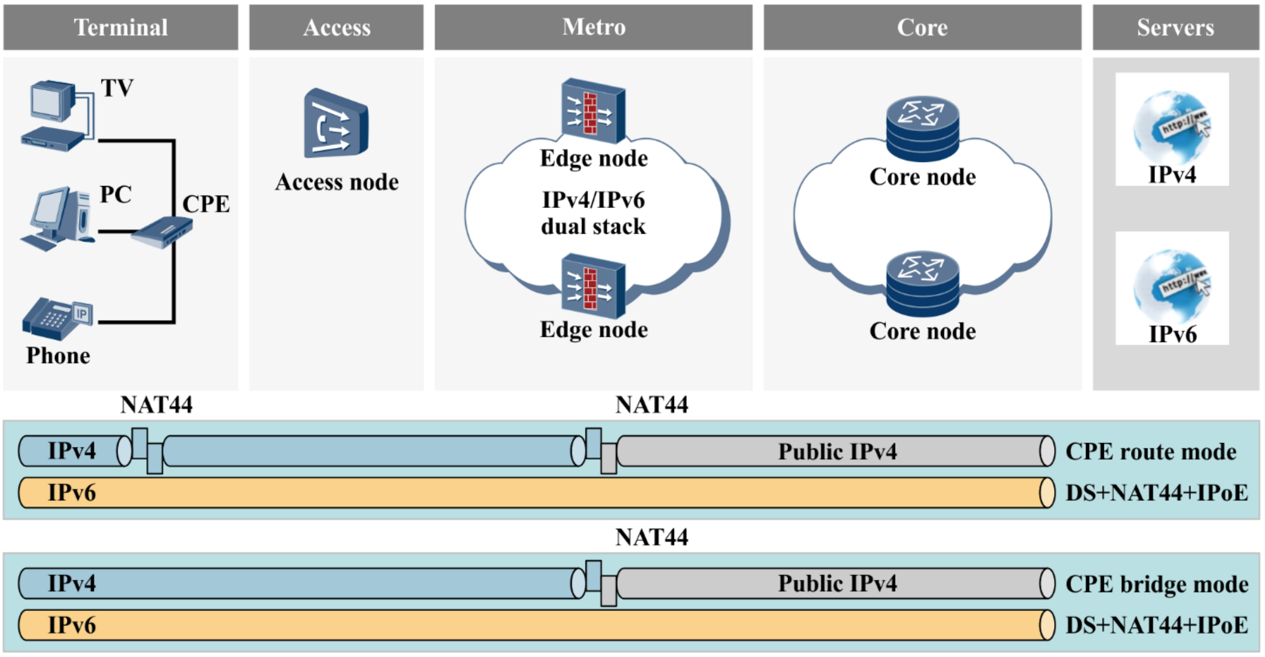
In this Recommendation:

The keyword "should" indicates a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

6 Basic IPv6 transition modes to support broadband services

6.1 Dual stack + NAT mode with IPoE access

Figure 6-1 depicts the dual stack + network address translation (NAT) mode with Internet Protocol over Ethernet (IPoE) access to support end-to-end broadband services. Depending on the working mode of customer premise equipment (CPE), i.e., either route mode or bridge mode, the transition is divided into two further sub-modes.



Q.3405(18)_F6-1

Figure 6-1 – Dual stack +NAT mode with IPoE access to support broadband services

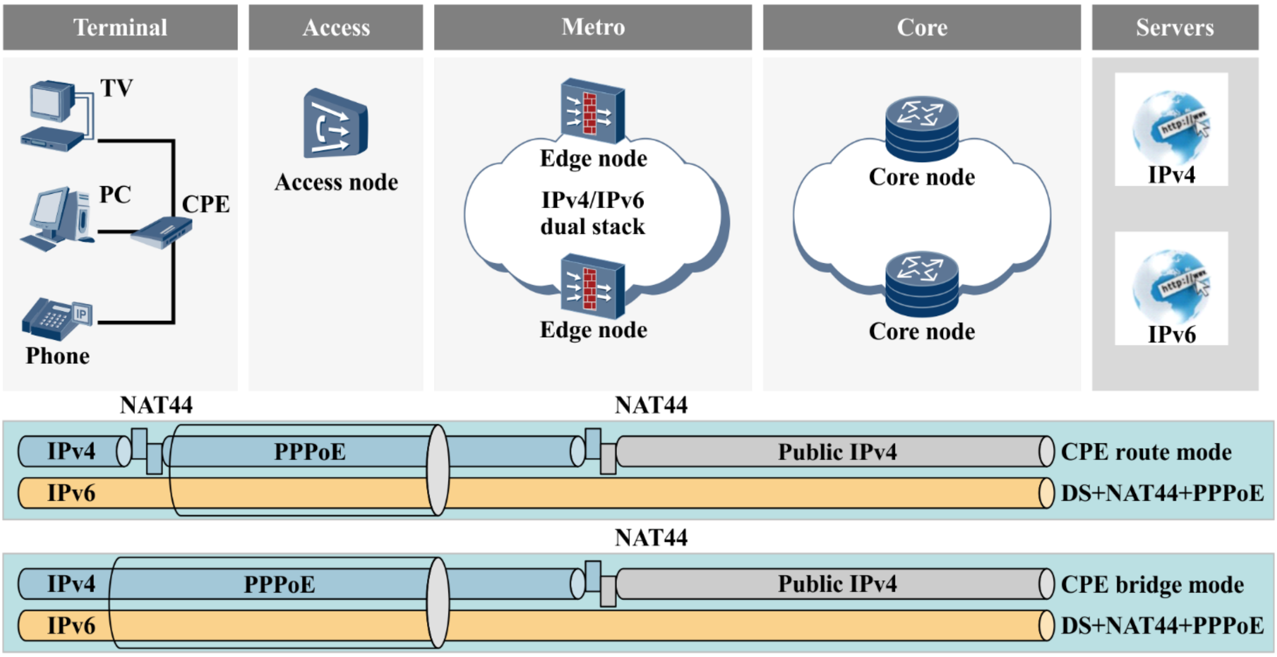
When the CPE works in route mode, user Internet Protocol version 4 (IPv4) traffic passes through two devices which perform NAT functions. The first NAT function is executed in the CPE to perform translation from the IPv4 address of the user private network to an IPv4 address of the carrier private network (see [IETF RFC 6598]). The second NAT function is executed in the carrier network to perform translation from the IPv4 address of the carrier private network to an IPv4 address in the public network.

When the CPE works in bridge mode, user IPv4 traffic passes through only one device performing a NAT function. This NAT function is executed in the carrier network to perform translation from the IPv4 address of the user private network to an IPv4 address in the public network.

For both sub-modes, the procedures for IPv6 traffic end-to-end transmission are described in clause 7.1.

6.2 Dual stack + NAT mode with PPPoE access

Figure 6-2 depicts the dual stack + NAT mode with point-to-point protocol over Ethernet (PPPoE) access to support end-to-end broadband services; both IPv4 and IPv6 access are required to support a PPPoE session. Depending on the working mode of the CPE, i.e., either route mode or bridge mode, the transition is divided into two further sub-modes.



Q.3405(18)_F6-2

Figure 6-2 – Dual stack +NAT mode with PPPoE access to support broadband services

When the CPE works in route mode, a PPPoE session, which is required to support IPv4 and IPv6 protocols, is initiated in the CPE and terminated in a carrier edge device, such as a broadband remote access server (BRAS). User IPv4 traffic passes through two devices performing NAT functions. The first NAT function is executed in the CPE to perform translation from the IPv4 address of the user private network to an IPv4 address of the carrier private network (see [IETF RFC 6598]). The second NAT function is executed in the carrier network to perform translation from the IPv4 address of the carrier private network to an IPv4 address in the public network.

When the CPE works in bridge mode, a PPPoE session, which is required to support IPv4 and IPv6 protocols, is initiated in the user's terminal and terminated in a carrier edge device, such as a BRAS. User IPv4 traffic passes through only one device performing a NAT function. User traffic is initiated in user equipment and terminated in a carrier edge device, such as BRAS. The NAT function is executed on the carrier network side to perform translation from the IPv4 address of the user private network to an IPv4 address in the public network.

For both sub-modes, IPv6 traffic is encapsulated into a PPPoE session in the CPE or in the user's terminal, and is decapsulated in a carrier edge device (e.g., BRAS). The procedures for IPv6 traffic end-to-end transmission are described in clause 7.2.

6.3 DS-Lite with PPPoE access

Figure 6-3 depicts dual stack-lite (DS-Lite) [IETF RFC 6333] mode with PPPoE access to support end-to-end broadband services. In this mode, the CPE is generally required to be configured to work in route mode.

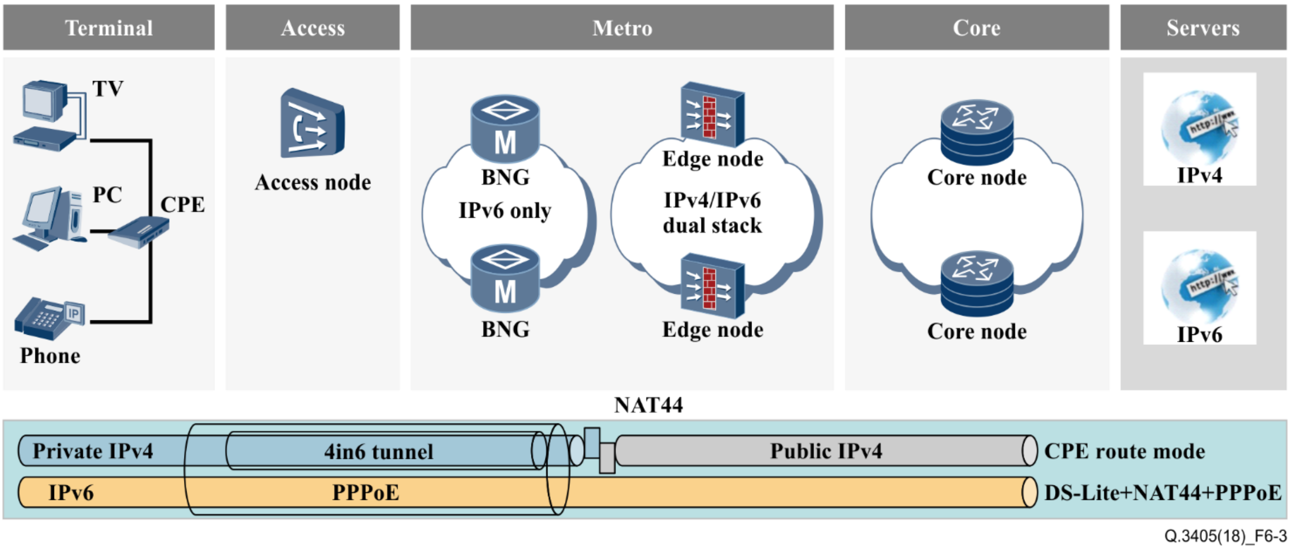


Figure 6-3 – DS-Lite with PPPoE access to support broadband services

A DS-Lite tunnel established between the CPE and a carrier edge device (e.g., BRAS), and a PPPoE session supporting IPv6 is required. The user IPv4 traffic initiated from the CPE is encapsulated into a DS-Lite tunnel, and then transmitted to the carrier edge device in a PPPoE session. The carrier edge device (e.g., BRAS) terminates the PPPoE session and decapsulates the IPv4 traffic from the DS-Lite tunnel, and then performs translation from the IPv4 address of the user private network to an IPv4 address in the public network. User IPv6 traffic is also encapsulated into a PPPoE session in the CPE and decapsulated in the carrier edge device (e.g., BRAS).

7 Protocol procedures

7.1 Procedures for dual stack + NAT with IPoE access

In the mode "dual stack + NAT with IPoE access", user IPv4 packets require one or two NAT operations to be performed when transmitted, but user IPv6 packet do not require any NAT operations. In this mode, the CPE and/or the edge node must maintain a NAT44 mapping table and implement the IP address mapping from private IPv4 addresses to public IPv4 addresses.

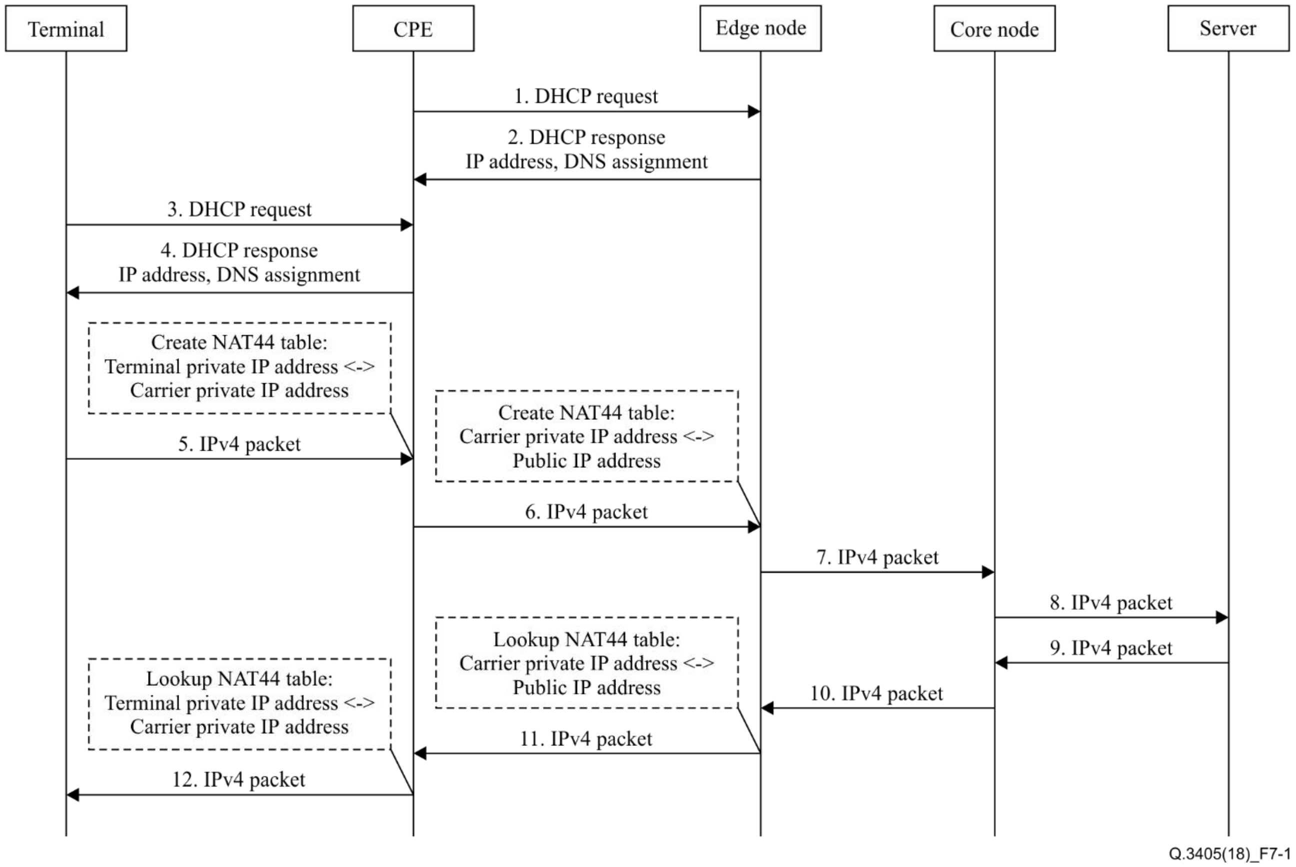


Figure 7-1 – Procedure for dual stack + NAT with IPoE access with CPE working in route mode

Figure 7-1 depicts the procedure for user IPv4 packet transmission with the CPE working in route mode with the mode of "dual stack + NAT with IPoE access". In this mode, the CPE obtains IPv4 address and domain name server (DNS)-related information from the carrier edge device through the dynamic host configuration protocol (DHCP). The user then also obtains their IPv4 address and DNS-related information from the CPE through DHCP. When user traffic is transmitted end-to-end, it needs to go through two levels of NAT mapping. The first level of NAT mapping is executed in the CPE device and maps from the user private IPv4 address to the carrier private IPv4 address; the second level of NAT mapping is executed in the carrier edge device (e.g., BRAS) and maps from the carrier private IPv4 address to the public IPv4 address. In this case, both the CPE and the carrier edge device must maintain a NAT mapping table.

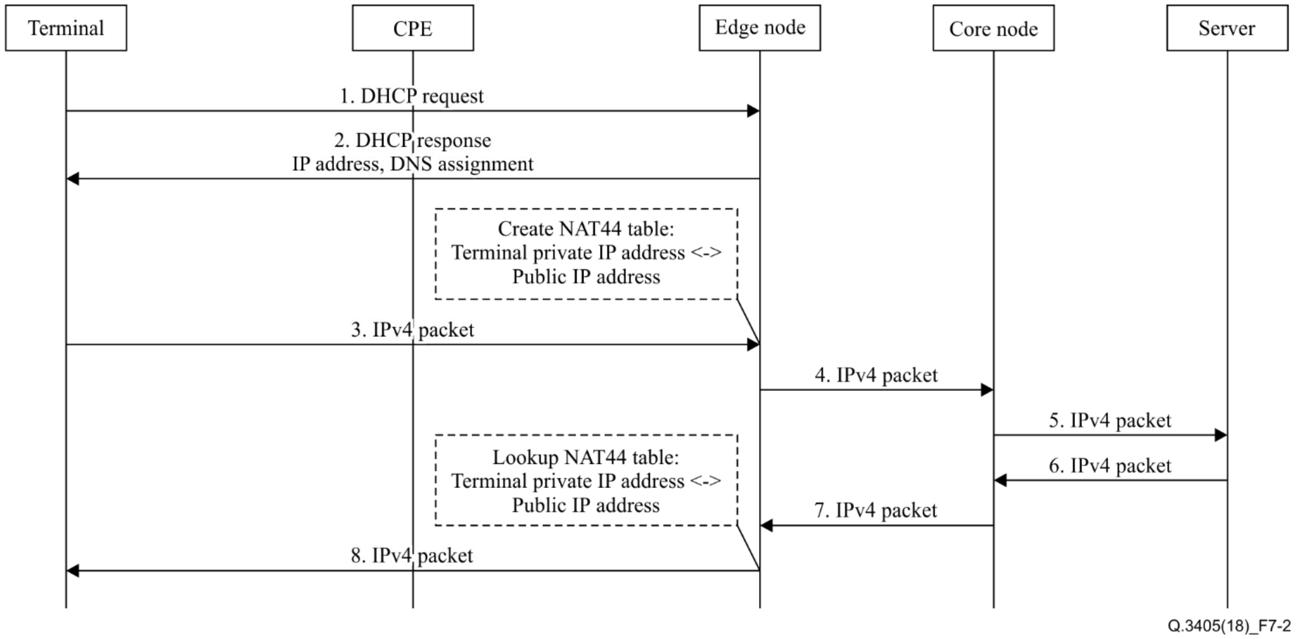
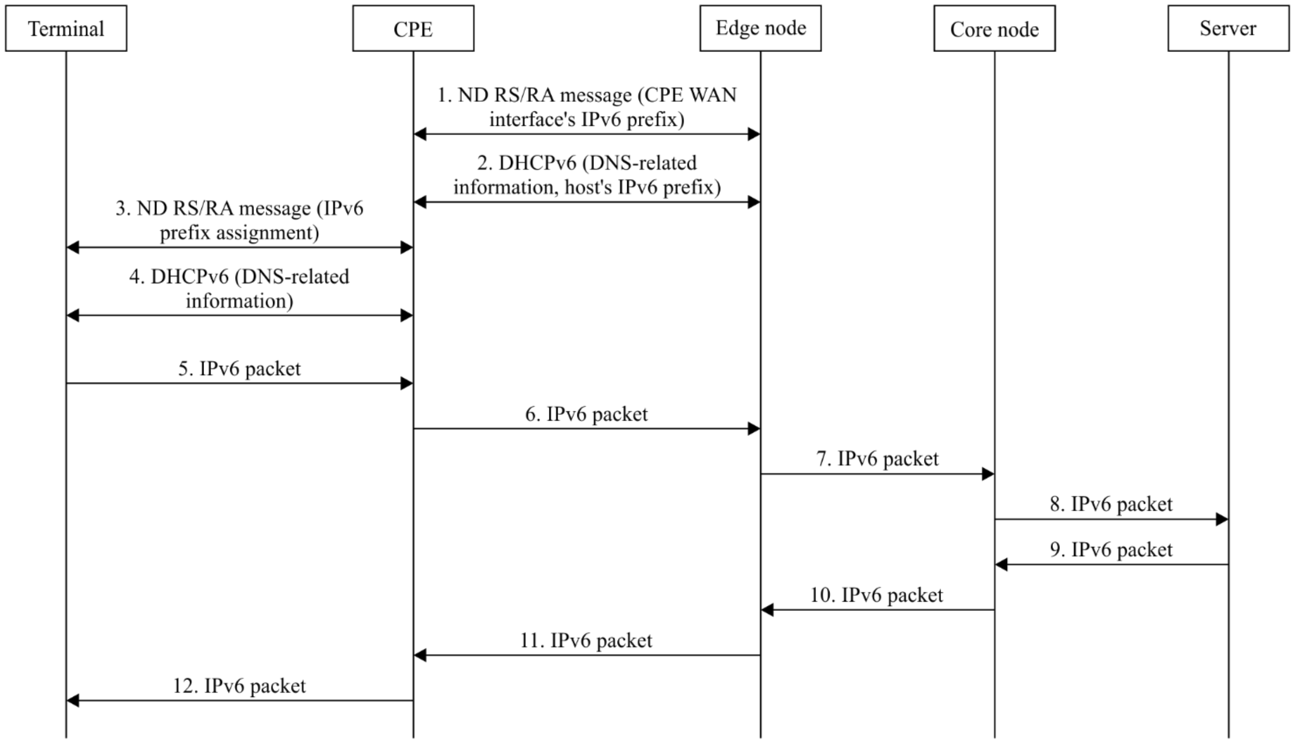


Figure 7-2 – Procedure for dual stack + NAT with IPoE access with CPE working in bridge mode

Figure 7-2 depicts the procedure for user IPv4 packet transmission with the CPE working in bridge mode with the mode of "dual stack + NAT with IPoE access". In this mode, the difference from the procedure described in Figure 7-1 is that the user IPv4 packet end-to-end transmission only needs to go through one level of NAT mapping. The NAT mapping is executed at the carrier edge device (e.g., BRAS), from the user private IPv4 address to the public IPv4 address. Only the carrier edge device needs to maintain a NAT mapping table.

In the mode "dual stack + NAT with IPoE access", terminals can transmit IPv6 traffic directly without NAT. According to different CPE working modes and IPv6 address configuration methods, there are several IPv6 traffic transmission procedure options; for any one of these options, the basic procedure is similar. In this Recommendation, a CPE working in route mode is chosen as a typical mode to explain the IPv6 traffic transmission procedure. Referring to Figure 7-3 and Figure 7-4, two different IPv6 address configuration methods in the terminal are described. The first method uses neighbour discovery protocol (NDP) [IETF RFC 4861] while the second method uses dynamic host configuration protocol version 6 (DHCPv6) [IETF RFC 3315].

An IPv6 address consists of an IPv6 prefix and interface identifier (ID) [IETF RFC 4291]. The IPv6 prefix assigned for a terminal should be allocated by the carrier using dynamic host configuration protocol version 6 - prefix delegation (DHCPv6-PD) [IETF RFC 3633]. The terminal can then obtain its IPv6 prefix by the Router Advertisement message in NDP or by DHCPv6. An interface ID can be calculated based on the interface's media access control (MAC) value [IETF RFC 4291].


Terminal
CPE
Edge node
Core node
Server
1. ND RS/RA message (CPE WAN interface's IPv6 prefix)
2. DHCPv6 (DNS-related information, host's IPv6 prefix)
3. ND RS/RA message (IPv6 prefix assignment)
4. DHCPv6 (DNS-related information)
5. IPv6 packet
6. IPv6 packet
7. IPv6 packet
8. IPv6 packet
9. IPv6 packet
10. IPv6 packet
11. IPv6 packet
12. IPv6 packet

Q.3405(18)_F7-3

Figure 7-3 – Procedure for user IPv6 packet transmission with CPE working in route mode, and terminal IPv6 address assigned by NDP

Figure 7-3 depicts the mode of IPv4/IPv6 dual stack with the CPE working in route mode, and with the CPE obtaining its wide area network (WAN) IPv6 prefix from the network using NDP. At the same time, the CPE requests an IPv6 prefix delegation from the carrier edge device (e.g., BRAS) using DHCPv6. After obtaining an IPv6 prefix for the user network, a CPE can announce this IPv6 prefix to the terminal using NDP. When obtaining an IPv6 prefix, the CPE and terminal automatically generate an IPv6 address with an interface ID. The CPE and terminal can obtain DNS-related information using DHCPv6. User data are all encapsulated into IPv6 packets for transmission.

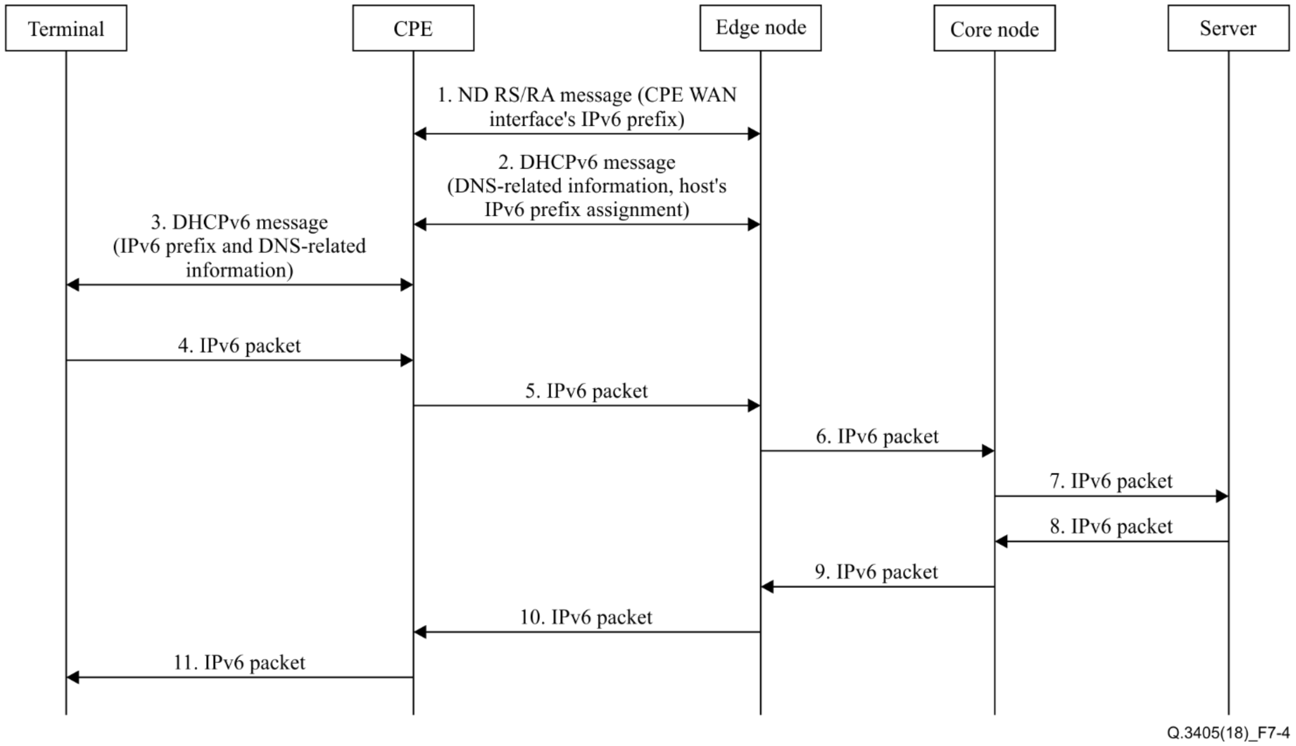

Terminal
CPE
Edge node
Core node
Server
1. ND RS/RA message (CPE WAN interface's IPv6 prefix)
2. DHCPv6 message (DNS-related information, host's IPv6 prefix assignment)
3. DHCPv6 message (IPv6 prefix and DNS-related information)
4. IPv6 packet
5. IPv6 packet
6. IPv6 packet
7. IPv6 packet
8. IPv6 packet
9. IPv6 packet
10. IPv6 packet
11. IPv6 packet
Q.3405(18)_F7-4

Figure 7-4 – Procedure for user IPv6 packet transmission with CPE working in route mode, and terminal IPv6 address assigned by DHCPv6

Figure 7-4 depicts the mode of IPv4/IPv6 dual stack with the CPE working in route mode. However, as differentiated from the procedure of Figure 7-3, in this case the terminal obtains an IPv6 prefix and DNS information from the CPE using DHCPv6, and automatically generates an IPv6 address with an interface ID.

7.2 Procedures for dual stack + NAT with PPPoE access

Figure 7-5 depicts the IPv4 traffic transmission procedure with the CPE working in route mode. IPv4 data sent along the transmission path will be processed by two NAT devices. The first NAT device is the CPE, which translates a user private network IPv4 address to a carrier private network IPv4 address; the second NAT device is a carrier edge node (e.g., BRAS), which translates a carrier private network IPv4 address to a public network IPv4 address.

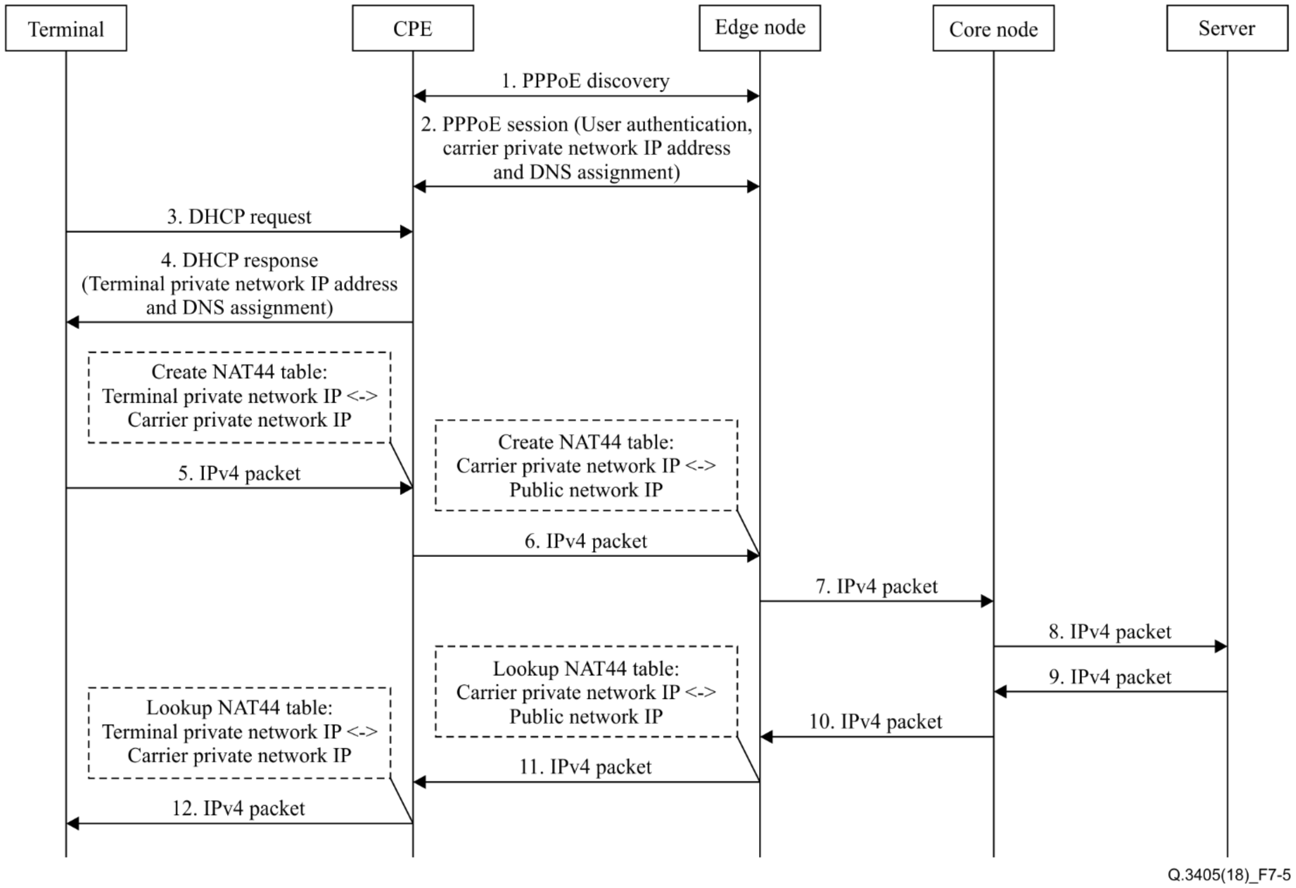

Terminal
CPE
Edge node
Core node
Server
1. PPPoE discovery
2. PPPoE session (User authentication, carrier private network IP address and DNS assignment)
3. DHCP request
4. DHCP response (Terminal private network IP address and DNS assignment)
Create NAT44 table: Terminal private network IP <-> Carrier private network IP
Create NAT44 table: Carrier private network IP <-> Public network IP
5. IPv4 packet
6. IPv4 packet
7. IPv4 packet
8. IPv4 packet
9. IPv4 packet
Lookup NAT44 table: Carrier private network IP <-> Public network IP
Lookup NAT44 table: Terminal private network IP <-> Carrier private network IP
10. IPv4 packet
11. IPv4 packet
12. IPv4 packet
Q.3405(18)_F7-5

Figure 7-5 – Procedure for dual stack + NAT with PPPoE access with CPE working in route mode

In route mode, as shown in Figure 7-5, the CPE obtains a carrier private IPv4 address and DNS-related information from a carrier edge node using the PPPoE protocol. The terminal obtains a private IPv4 address and DNS-related information from the CPE using DHCP. When sending user data, the CPE executes the first level of NAT mapping from a user private IPv4 address to a carrier private IPv4 address. Then, the carrier edge node executes the second level of NAT mapping from a carrier private IPv4 address to a public IPv4 address. When receiving user data, the carrier edge node executes the first level of NAT mapping from the public IPv4 address to the carrier private IPv4 address. The CPE then executes the second level of NAT mapping from the carrier private IPv4 address to the user private IPv4 address. Both the CPE and carrier edge node must maintain NAT mapping tables.

Figure 7-6 depicts the IPv4 traffic transmission procedure with CPE working in bridge mode. IPv4 data sent along the transmission path will be processed by one NAT device, the carrier edge node (e.g., BRAS), which translates a user private network IP address to a public network IP address.

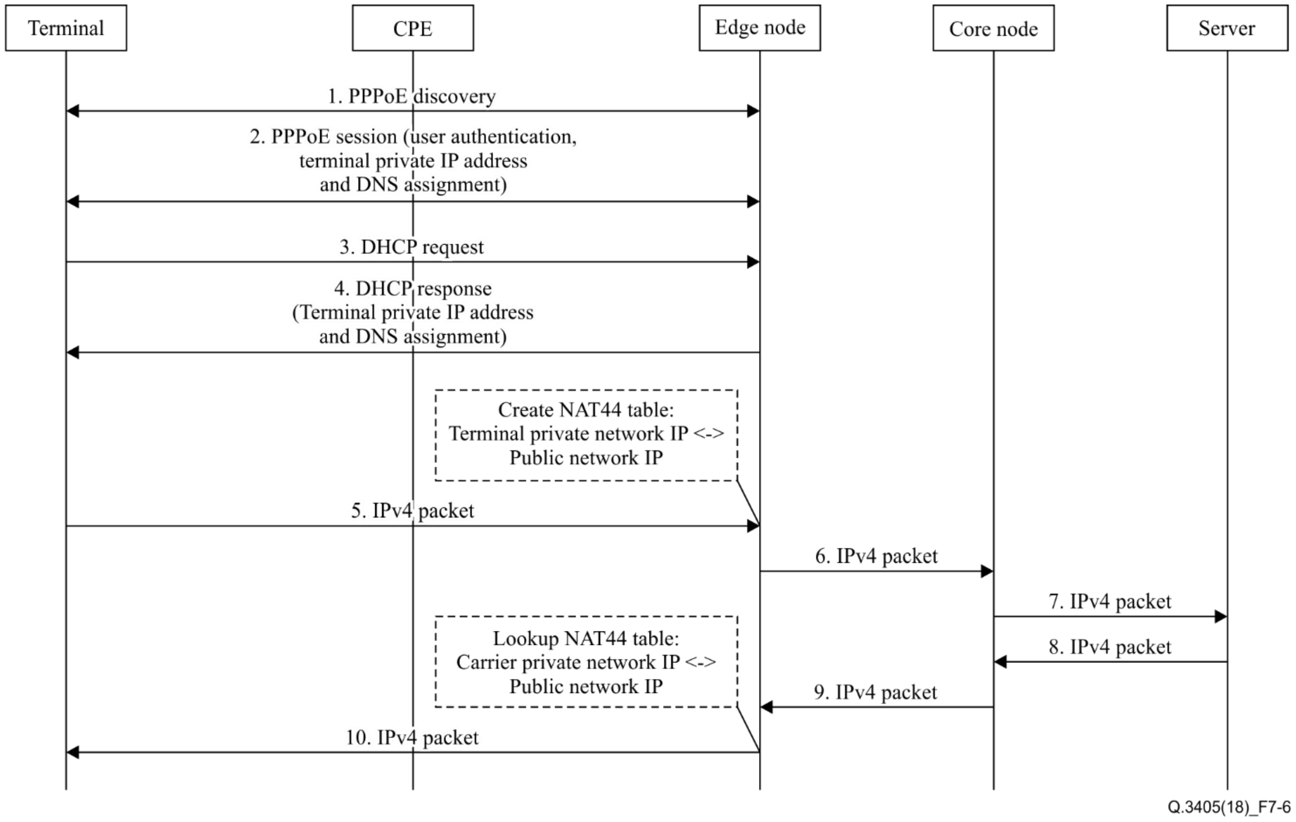

Terminal
CPE
Edge node
Core node
Server
1. PPPoE discovery
2. PPPoE session (user authentication, terminal private IP address and DNS assignment)
3. DHCP request
4. DHCP response (Terminal private IP address and DNS assignment)
Create NAT44 table: Terminal private network IP <-> Public network IP
5. IPv4 packet
6. IPv4 packet
7. IPv4 packet
Lookup NAT44 table: Carrier private network IP <-> Public network IP
8. IPv4 packet
9. IPv4 packet
10. IPv4 packet
Q.3405(18)_F7-6

Figure 7-6 – Procedure for dual stack + NAT with PPPoE access with CPE working in bridge mode

In bridge mode, as shown in Figure 7-6, the terminal obtains a user private network IPv4 address and DNS-related information from a carrier edge node using the PPPoE protocol or DHCP. When a terminal is transmitting user data, the carrier edge node executes the NAT mapping from a user private network IPv4 address to a public network IPv4 address. When the terminal is receiving data, the carrier edge node executes the NAT mapping from the public network IPv4 address to the user private network IPv4 address. The carrier edge node must maintain the NAT mapping table.

Figure 7-7 and Figure 7-8 depict IPv6 traffic transmission procedures with the CPE working in route mode. The main difference between these two procedures is the method by which the terminal acquires its IPv6 prefix, either via NDP or DHCPv6 respectively.

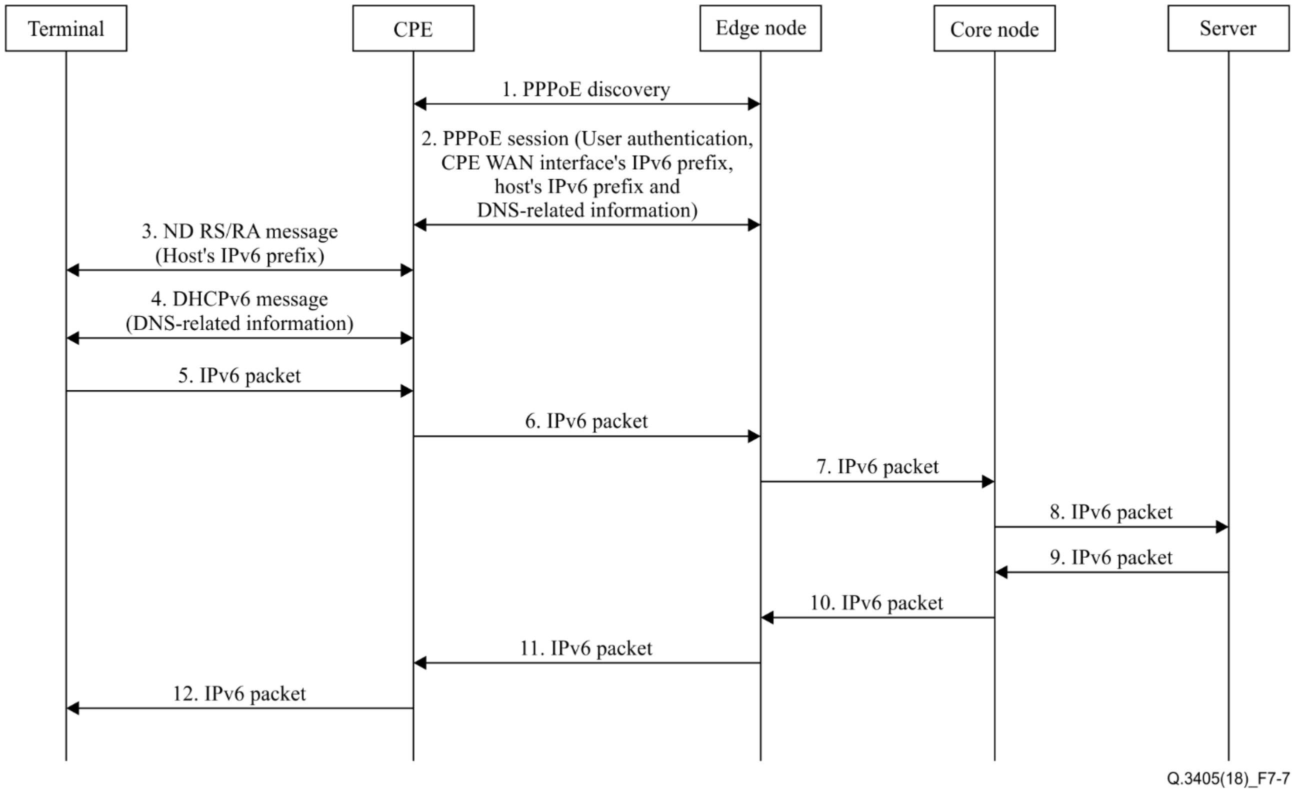

Terminal
CPE
Edge node
Core node
Server
1. PPPoE discovery
2. PPPoE session (User authentication, CPE WAN interface's IPv6 prefix, host's IPv6 prefix and DNS-related information)
3. ND RS/RA message (Host's IPv6 prefix)
4. DHCPv6 message (DNS-related information)
5. IPv6 packet
6. IPv6 packet
7. IPv6 packet
8. IPv6 packet
9. IPv6 packet
10. IPv6 packet
11. IPv6 packet
12. IPv6 packet
Q.3405(18)_F7-7

Figure 7-7 – Procedure for user IPv6 packet transmission with CPE working in route mode, IPv6 address of a terminal assigned by NDP

As shown in Figure 7-7, a CPE obtains a terminal IPv6 prefix and DNS-related information from a carrier edge node using PPPoE. The CPE then announces the IPv6 prefix to the terminal using NDP and assigns the DNS-related information to the terminal using DHCPv6 when the O flag in the Router Advertisement message of NDP is set [IETF RFC 4861]. The terminal automatically generates an IPv6 address based on the received IPv6 prefix and the calculated interface ID. User data are all encapsulated into IPv6 packets for transmission.

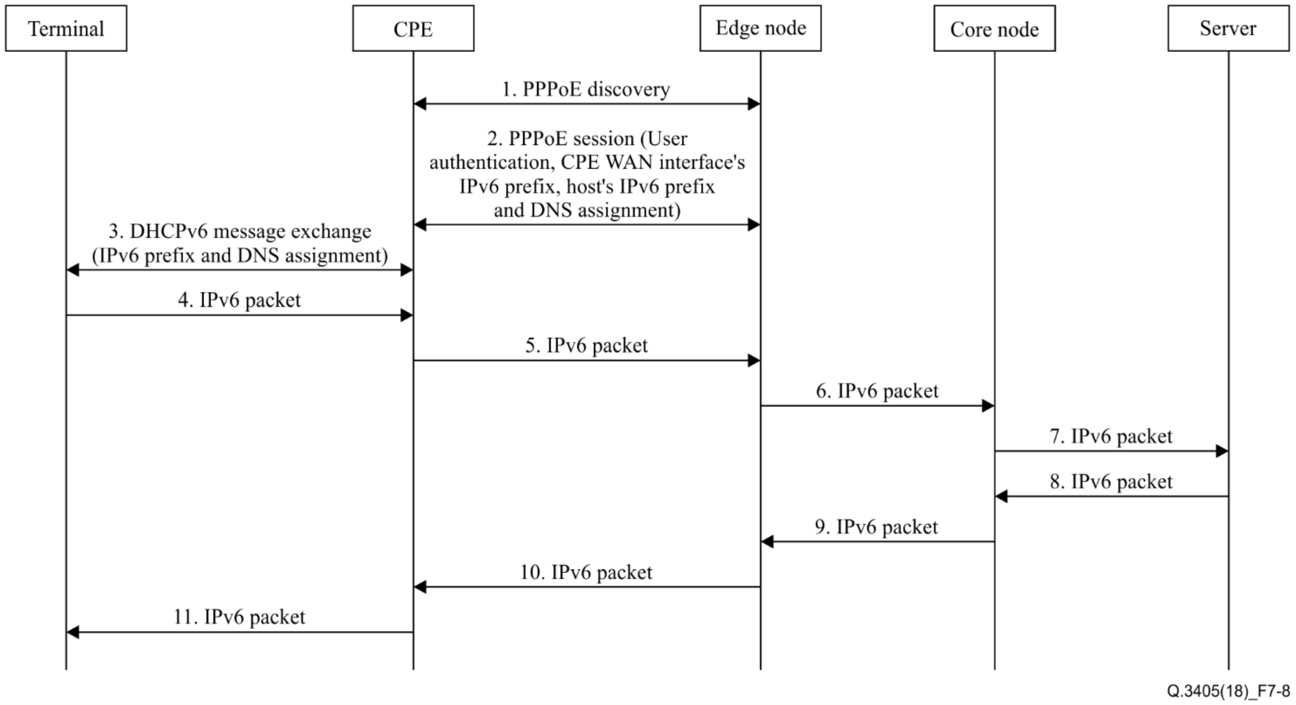


Figure 7-8 – Procedure for user IPv6 packet transmission with CPE working in route mode, IPv6 address of a terminal assigned by DHCPv6

As differentiated from the procedure of Figure 7-7, in Figure 7-8, the terminal obtains the IPv6 prefix and DNS-related information from the CPE using DHCPv6.

7.3 Procedures for DS-Lite with PPPoE access

Figure 7-9 depicts the IPv4 traffic transmission procedure in DS-Lite + PPPoE mode. IPv4 data sent along the transmission path are orderly encapsulated in a DS-Lite tunnel (IPv4 in IPv6 tunnel) [IETF RFC 6333] and the PPPoE session at the CPE, and then decapsulated in the PPPoE session and DS-Lite tunnel. The user data IPv4 address is translated from a user private network IPv4 address to a public network IPv4 address at the carrier edge node (e.g., BRAS).

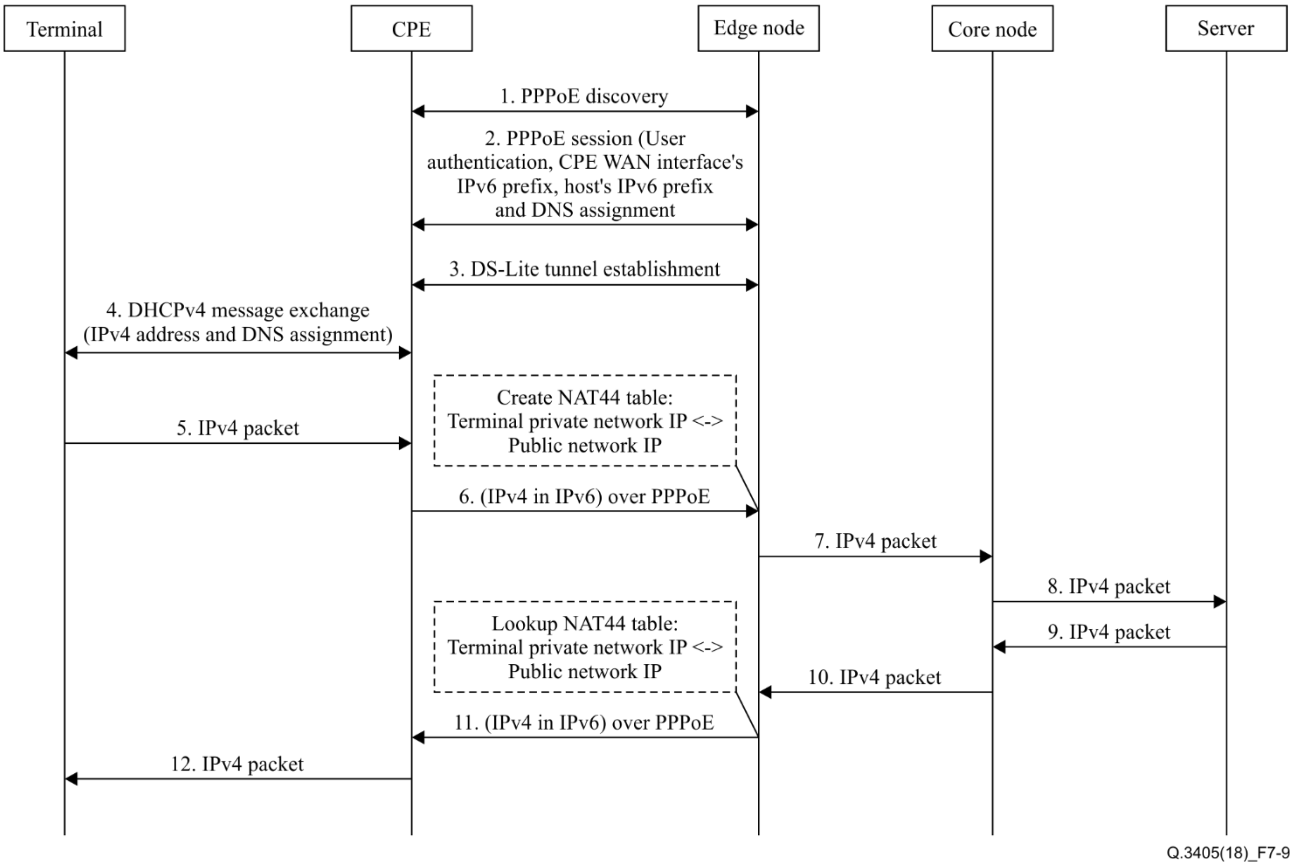

Terminal
CPE
Edge node
Core node
Server
1. PPPoE discovery
2. PPPoE session (User authentication, CPE WAN interface's IPv6 prefix, host's IPv6 prefix and DNS assignment
3. DS-Lite tunnel establishment
4. DHCPv4 message exchange (IPv4 address and DNS assignment)
Create NAT44 table: Terminal private network IP <-> Public network IP
5. IPv4 packet
6. (IPv4 in IPv6) over PPPoE
7. IPv4 packet
8. IPv4 packet
Lookup NAT44 table: Terminal private network IP <-> Public network IP
9. IPv4 packet
10. IPv4 packet
11. (IPv4 in IPv6) over PPPoE
12. IPv4 packet
Q.3405(18)_F7-9

Figure 7-9 – Procedure for DS-Lite with PPPoE access when CPE working in route mode

As shown in Figure 7-9, the CPE obtains IPv6 prefix and DNS-related information from a carrier edge node using PPPoE and then sets up a DS-Lite tunnel with the carrier edge node. The terminal obtains private IPv4 address and DNS-related information from the CPE using DHCP. When a terminal is sending user data, the CPE encapsulates these data into a DS-Lite tunnel. The carrier edge node decapsulates the packets, and translates a user private IPv4 address into a public IPv4 address which creates a NAT mapping item. When a terminal is receiving data, the carrier edge node translates a public IPv4 address into a user private network IPv4 address according to the NAT mapping table, and encapsulates the packet into a DS-Lite tunnel. A CPE decapsulates the packet by removing the IPv6 header and sends it to a terminal.

Figure 7-10 and Figure 7-11 depicts the IPv6 traffic transmission procedure in DS-Lite + PPPoE mode. The main difference between these two procedures is the method used by the terminal to acquire the IPv6 prefix.

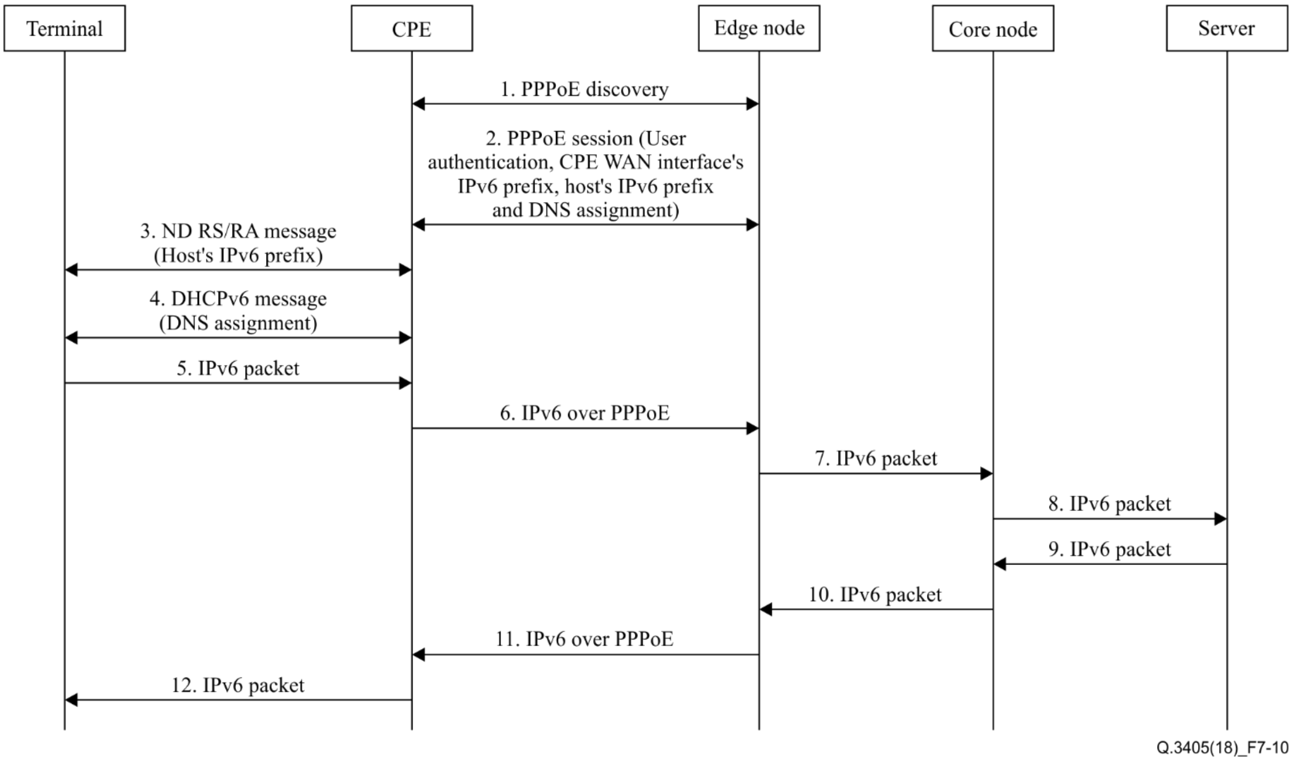


Figure 7-10 – Procedure for user IPv6 packet transmission with CPE working in route mode, IPv6 address of terminal assigned by NDP

As shown in Figure 7-10, a CPE obtains IPv6 prefix and DNS-related information from the carrier edge node using PPPoE. The terminal obtains an IPv6 prefix using NDP, and automatically generates an IPv6 address based on the received IPv6 prefix and the calculated interface ID. The terminal configures DNS-related information using DHCP when the O flag in the Router Advertisement message of NDP is set. User data are all encapsulated into IPv6 packets for transmission.

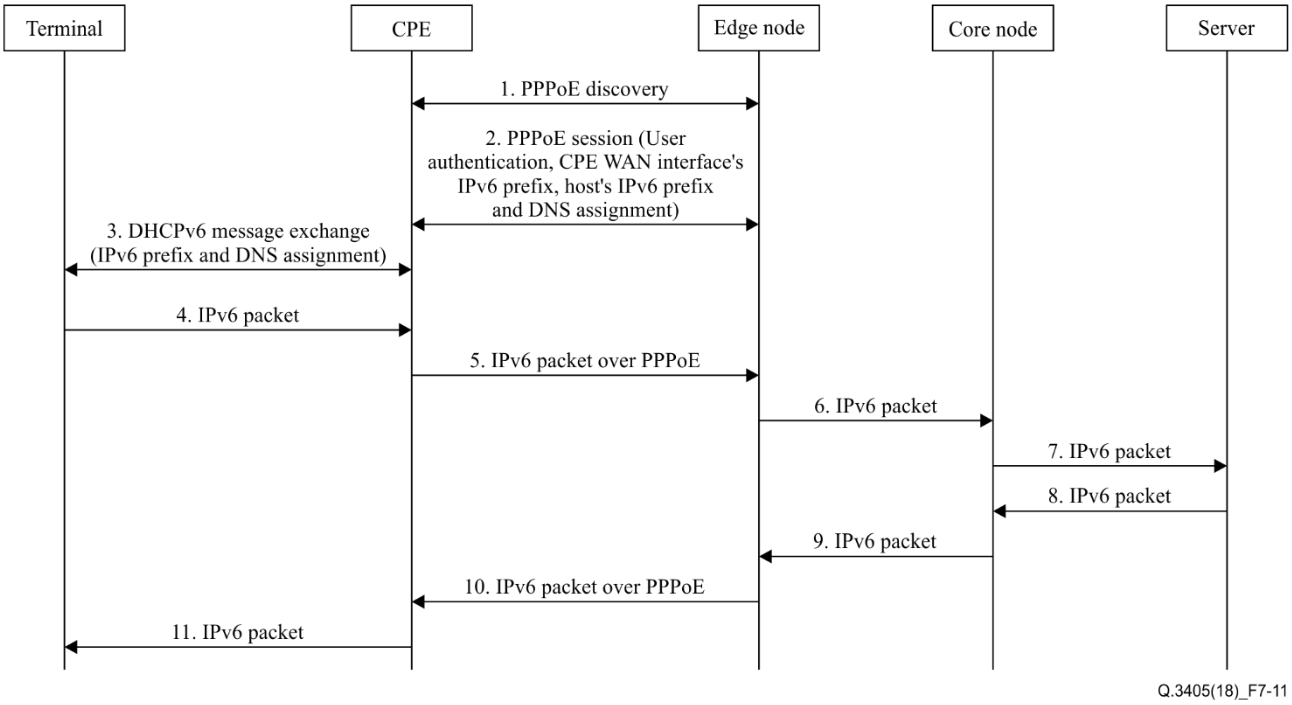

Terminal
CPE
Edge node
Core node
Server
1. PPPoE discovery
2. PPPoE session (User authentication, CPE WAN interface's IPv6 prefix, host's IPv6 prefix and DNS assignment)
3. DHCPv6 message exchange (IPv6 prefix and DNS assignment)
4. IPv6 packet
5. IPv6 packet over PPPoE
6. IPv6 packet
7. IPv6 packet
8. IPv6 packet
9. IPv6 packet
10. IPv6 packet over PPPoE
11. IPv6 packet
Q.3405(18)_F7-11

Figure 7-11 – Procedure for user IPv6 packet transmission with CPE working in route mode, IPv6 address of terminal assigned by DHCPv6

As differentiated from the procedure of Figure 7-10, in Figure 7-11 a terminal obtains IPv6 prefix and DNS-related information from a CPE using DHCPv6.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	**Switching and signalling, and associated measurements and tests**
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2018