International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2053

(02/2008)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

Next Generation Networks – Frameworks and functional architecture models

Functional requirements for IPv6 migration in NGN

Recommendation ITU-T Y.2053

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	**Y.2000–Y.2099**
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Numbering, naming and addressing	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899

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

Recommendation ITU-T Y.2053

Functional requirements for IPv6 migration in NGN

Summary

Recommendation ITU-T Y.2053 provides feasible IPv6 migration scenarios and functional requirements necessary for them.

Source

Recommendation ITU-T Y.2053 was approved on 29 February 2008 by ITU-T Study Group 13 (2005-2008) under Recommendation ITU-T A.8 procedure.

Keywords

IPv4, IPv6, migration, NGN

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/.

CONTENTS

Recommendation ITU-T Y.2053

Functional requirements for IPv6 migration in NGN

1 Scope

The objective of this Recommendation is to identify IPv6 migration scenarios and functional requirements necessary for them.

NGN transport stratum provides IP connectivity services to NGN users, but the current NGN assumes no specific version of IP. It means that IPv4 and IPv6 could coexist in NGN while IPv4 is being replaced with IPv6. So the interim solution like IPv6 transition mechanism (see clauses 6 and 7) is required for this period.

If the IPv6 transition mechanism is introduced to NGN, there could be various migration scenarios satisfying various application's requirements or service provider's requirements, and these migration scenarios will also impact on existing FEs of NGN.

Thus, this Recommendation provides feasible IPv6 migration scenarios, and functional requirements required to support each scenario.

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.

[ITU-T Y.2011] Recommendation ITU-T Y.2011 (2004), *General principles and general reference model for Next Generation Networks*.

[ITU-T Y.2012] Recommendation ITU-T Y.2012 (2006), *Functional requirements and architecture of the NGN release 1*.

[ITU-T Y.2111] Recommendation ITU-T Y.2111 (2006), *Resource and admission control functions in Next Generation Networks*.

[ITU-T Y.2701] Recommendation ITU-T Y.2701 (2007), *Security requirements for NGN release 1*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 host [b-ITU-T Y.1540]: A computer that communicates using the Internet protocols. A host implements routing functions (i.e., it operates at the IP layer) and may implement additional functions including higher layer protocols (e.g., TCP in a source or destination host) and lower layer protocols (e.g., ATM).

3.1.2 router [b-ITU-T Y.1540]: A host that enables communication between other hosts by forwarding IP packets based on the content of their IP destination address field.

3.1.3 dual IP layer [b-IETF RFC 4213]: Dual IP layer is a technique for providing support for both Internet Protocols – IPv4 and IPv6 – in a node. Dual IP layer is also known as dual stack.

3.1.4 configured tunneling [b-IETF RFC 4213]: The configured tunneling is a technique for establishing point-to-point tunnels by encapsulating IPv6 packets within IPv4 headers to carry them over IPv4 infrastructures (or vice versa).

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 node: A node is a device that is connected as part of a computer network. Nodes can be computers, cell phones, or various other network appliances, such as routers, switches, and hubs.

3.2.2 subnet: A subnet is a physical network served by one router, for instance an Ethernet network (consisting of one or several Ethernet segments or local area networks, interconnected by switches and bridges) or a virtual local area network (VLAN).

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations:

ALG Application Layer Gateway

CPE Customer Premises Equipment

FE Functional Entity

NAT-PT Network Address Translation and Protocol Translation

SCF Service Control Function

SIIT Stateless IP/ICMP Translation Algorithm

5 Conventions

5.1 Native IPv6 device

A device that only has IPv6 stack.

5.2 IPv6 transition mechanism

An IPv6 transition mechanism means a mechanism that supports transition between IPv4 and IPv6. There are many kinds of IPv6 transition mechanisms available, and the user can choose one that fits into a deployment environment.

5.3 Basic IPv6 transition mechanisms

Basic IPv6 transition mechanisms means "Dual IP layer" and "Configured tunneling" which can be implemented on the IPv6 node [b-IETF RFC 4213].

6 IP as a transport function of NGN

NGN functions are divided into service stratum functions and transport stratum functions as described in [ITU-T Y.2011]. The transport stratum provides IP connectivity to NGN service stratum and users under the control of transport control functions. This means that IP plays the key role of transport function of NGN.

In NGN, most of services are carried over IP, although IP itself may in turn be carried over a number of underlying technologies like ATM, Ethernet, etc. According to the NGN release 1, it is assumed that the version of IP is not fixed. This means that IPv4 and IPv6 could coexist in NGN

while IPv4 is being replaced with IPv6, thus a mechanism that supports migration into IPv6 is required for this period.

IETF introduced several IPv6 transition mechanisms as recommendations for migration to IPv6 [b-IETF RFC 4213]. These mechanisms could also be recommendations for the NGN which uses IP as a transport function. The study of IPv6 with NGN has not yet been completed.

The IPv6 transition mechanisms used in this Recommendation are dual stack, configured tunnelling, and network address translation/protocol translation (NAT-PT) [b-IETF RFC 4213]. These mechanisms are explained in more details in clause 7.

When the IPv6 transition mechanisms are introduced to NGN, various migration scenarios could be possible. This Recommendation also shows such feasible scenarios.

7 Basic approaches for interworking and migration

The network consists of various IPv4-based and IPv6-based networks at different geographic locations which are connected via an underlying transport network.

There are three major approaches in providing interworking and migration between the IPv4-based network and the IPv6-based network: dual IP layer, configured tunnelling and NAT-PT.

For more information on these mechanisms, see Appendix I.

7.1 Dual IP layer (Dual stack)

The node that has dual IP layer provides implementations of both versions of the Internet Protocol (IPv4 and IPv6) which are also enabled at the same time. This node can directly interoperate with IPv4-only node using IPv4 packets, and also directly interoperate with IPv6-only node using IPv6 packets. There will be no IP protocol conversion necessary when communicating with a dual stack node on either the media path or the signalling path. Details on dual IP layer node have been identified in [b-IETF RFC 4213].

7.2 Configured tunnelling

The configured tunnelling is a technique for establishing point-to-point tunnels by encapsulating IPv6 packets within IPv4 headers to carry them over IPv4 infrastructures (or vice versa).

In most deployment scenarios, the IPv6 routing infrastructure will be built up over time. While the IPv6 infrastructure is being deployed, the existing IPv4 routing infrastructure can still remain and can be used to carry IPv6 traffic. Tunnelling provides a way to utilize an existing IPv4 routing infrastructure to carry IPv6 traffic.

Dual stack nodes can tunnel IPv6 packets over regions of IPv4 routing topology by encapsulating them within IPv4 packets. Tunnelling can be used in a variety of ways:

- router-to-router;
- host-to-router;
- host-to-host.

Configured tunnelling can be used in all of the above cases, but it is most likely to be used in router-to-router due to the need to explicitly configure the tunnelling endpoints.

7.3 Network address translation and protocol translation

NAT-PT uses address translation like NAT and IPv6/IPv4 protocol translation as described in stateless IP/ICMP translation (SIIT) [b-IETF RFC 2765] to provide transparent routing to end-hosts in IPv6 realm trying to communicate with end-hosts in IPv4 realm and vice versa.

The SIIT identifies a protocol translation mechanism that allows communication between IPv6-only and IPv4-only hosts via protocol independent translation of IPv4 and IPv6 packets, requiring no state information for the session.

Some applications carry network addresses in payloads. The NAT-PT is application unaware and does not snoop the payload. Application layer gateway (ALG) could work in conjunction with the NAT-PT to provide support for many such applications.

Generally the NAT-PT function is placed on the edge of network. If the NAT-PT function is placed in the core of the network, the overall performance of the network would decrease seriously because the NAT-PT function reconstructs all IP packets that pass through it.

NAPT-PT extends the notion of translation one step further by also translating transport identifier (e.g., TCP and UDP port numbers, ICMP query identifiers). The NAPT-PT, which stands for "Network Address Port Translation + Protocol Translation", would allow IPv6 nodes to communicate with the IPv4 nodes transparently using a single IPv4 address. The TCP/UDP ports of the IPv6 nodes are translated into TCP/UDP ports of the registered IPv4 address.

8 Migration scenarios

There are various IPv6 migration scenarios satisfying the user/application or provider requirements. In this clause, several migration scenarios from the transport stratum's viewpoint are shown. Each scenario is referred to in clause 9 to explain the functional requirements for the relevant functional entity (FE). See Table 1.

Legend for Table 1

- IPv6/dual stack: IPv6-only node, or dual stack node
- IPv4/dual stack: IPv4-only node, or dual stack node
- IPv4: IPv4-only node
- IPv6: IPv6-only node
- Blue cell: IPv6-enabled entity
- Red cell: IPv4-enabled entity

Table 1 – Role of functional elements for various migration scenarios

		End-user function A	EN-FE	ABG-FE	IBG-FE	NACF	RACF	End-user function B
NAT-PT	CASE 1	IPv6/ dual stack	NAT-PT	IPv4	IPv4	–	Offer NAT-PT control	IPv4/ dual stack
	CASE 2	IPv6/ dual stack	IPv6/ dual stack	NAT-PT	IPv4	–	Offer NAT-PT control	IPv4/ dual stack
	CASE 3	IPv6/ dual stack	IPv6/ dual stack	IPv6/ dual stack	NAT-PT	–	Offer NAT-PT control	IPv4/ dual stack
Tunnelling	CASE 4	Tunnel end-point	IPv4	IPv4	IPv4	Offer tunnel end-point information	–	IPv6/ dual stack
	CASE 5	IPv6/ dual stack	Tunnel end-point	IPv4	IPv4	–	–	IPv6/ dual stack
	CASE 6	IPv6/ dual stack	IPv6/ dual stack	Tunnel end-point	IPv4	–	–	IPv6/ dual stack
	CASE 7	IPv6/ dual stack	IPv6/ dual stack	IPv6/ dual stack	Tunnel end-point	–	–	IPv6/ dual stack
NAT-PT	CASE 8	IPv6 Customer Network (NAT-PT)	IPv4	IPv4	IPv4	–	Offer NAT-PT control	IPv4/dual stack
Tunnelling	CASE 9	Dual stack Customer Network (tunnel end-point)	IPv4	IPv4	IPv4	Offer tunnel end-point information	–	IPv6/ dual stack
Dual stack	CASE 10	Dual stack	Dual stack	Dual stack	Dual stack	–	–	Dual stack
	CASE 11	Dual stack Customer Network	Dual stack	Dual stack	Dual stack	–	–	Dual stack
IPv6	CASE 12	IPv6	IPv6	IPv6	IPv6	–	–	IPv6

8.1 CASE 1 ~ 3 (NAT-PT cases)

From CASE 1 to CASE 3, both end-user functions have different versions of IP stack (or an end-user function is a dual stack, but a service/application only supports a different IP stack from the other end-user functions). NAT-PT enables end-user functions which have different IP stacks to communicate with each other by translating IPv6 packet into IPv4 packet (or vice versa). To do this, one of the FEs in the path between the end-user functions should provide the NAT-PT function.

Usually, the NAT-PT function should not be placed on the core FE because it snoops and rebuilds all packets. If the NAT-PT function is placed on the core FE, the overall performance of the network could be decreased. So an interconnection border gateway FE (IBG-FE) is not recommended for a NAT-PT function.

For CASE 1, the following requirements are defined:

- EN-FE shall have dual stack.
- EN-FE shall have public IPv4 address for IPv4 side, global scope IPv6 address for IPv6 side.
- EN-FE shall have NAT-PT function.
- EN-FE could have an appropriate ALG for a specific application.
- RACF shall provide NAT-PT control functions.

CASES 2 and 3 have the same requirements as CASE 1 except that the NAT-PT function is placed on ABG-FE or IBG-FE.

8.2 CASE 4 ~ 7 (configured tunnelling cases)

From CASE 4 to CASE 7, both end-user functions are IPv6 nodes and networks between two end-user functions are IPv4 only. To communicate with each other in this situation, configured tunnelling mechanisms can be used. Configured tunnelling needs two tunnel end-points for encapsulation and decapsulation of IPv4 packets. Two FEs in the communication path should be tunnel end-point.

For CASE 5, the following requirements are defined:

- EN-FE shall have dual stack.
- EN-FE shall have public IPv4 address for tunnel end-point, global scope IPv6 address for IPv6 side.
- EN-FE shall have tunnel end-point function.
- Tunnel end-point for the end-user function B could be any FE among EN-FE, ABG-FE, IBG-FE on the side of end-user functions B.

CASES 6 and 7 have the same requirements as CASE 5 except that tunnel end-point for end-user function A is ABG-FE or IBG-FE.

Sometimes, an end-user function itself could be a tunnel end-point. CASE 4 shows this case. In this case, NACF should provide information for other tunnel end-point.

8.3 CASE 8 (NAT-PT case)

In this case, end-user function A has an IPv6 customer network, and the other end-user function is IPv4 node; thus end-user function A should have NAT-PT function. The other situations are the same as CASE 1 ~ 3.

For CASE 8, the following requirements are defined:

- End-user function A shall have dual-stack.
- End-user function A shall have public IPv4 address for IPv4 side, global scope IPv6 address for IPv6 side.
- End-user function A shall have NAT-PT function.
- End-user function A could have an appropriate ALG for a specific application.
- RACF shall provide NAT-PT control functions.

8.4 CASE 9 (configured tunnelling cases)

In this case, end-user function A is an IPv6 customer network and the other end-user function is IPv6 node; thus end-user function A should be a tunnel end-point. The other situations are the same as CASE 4.

8.5 CASE 10 ~ 11 (dual stack cases)

CASES 10 ~ 11 are the most ideal case. In this case, every FE has dual stack, so most of the applications/services can communicate with each other without any consideration of the specific IP version.

8.6 CASE 12 (native IPv6 case)

CASE 12 is the final stage of IPv6 migration. In this case, every FE and every application/service is IPv6-only.

9 Functional requirements for IPv6 migration at transport stratum

As described in clause 8, some FEs in transport stratum should support IPv6 transition function according to a specific IPv6 migration scenario. In this clause, the FEs related to IPv6 migration are identified and the functional requirements for these FEs are described.

9.1 Transport stratum functions

The transport functions of NGN provide IP connectivity to the NGN service stratum and end-user equipments under the control of NACF and RACF components. Figure 9-1 shows an example configuration of NGN from the viewpoint of transport stratum.

The set of FEs related to IPv6 migration could be different according to each possible migration scenario.

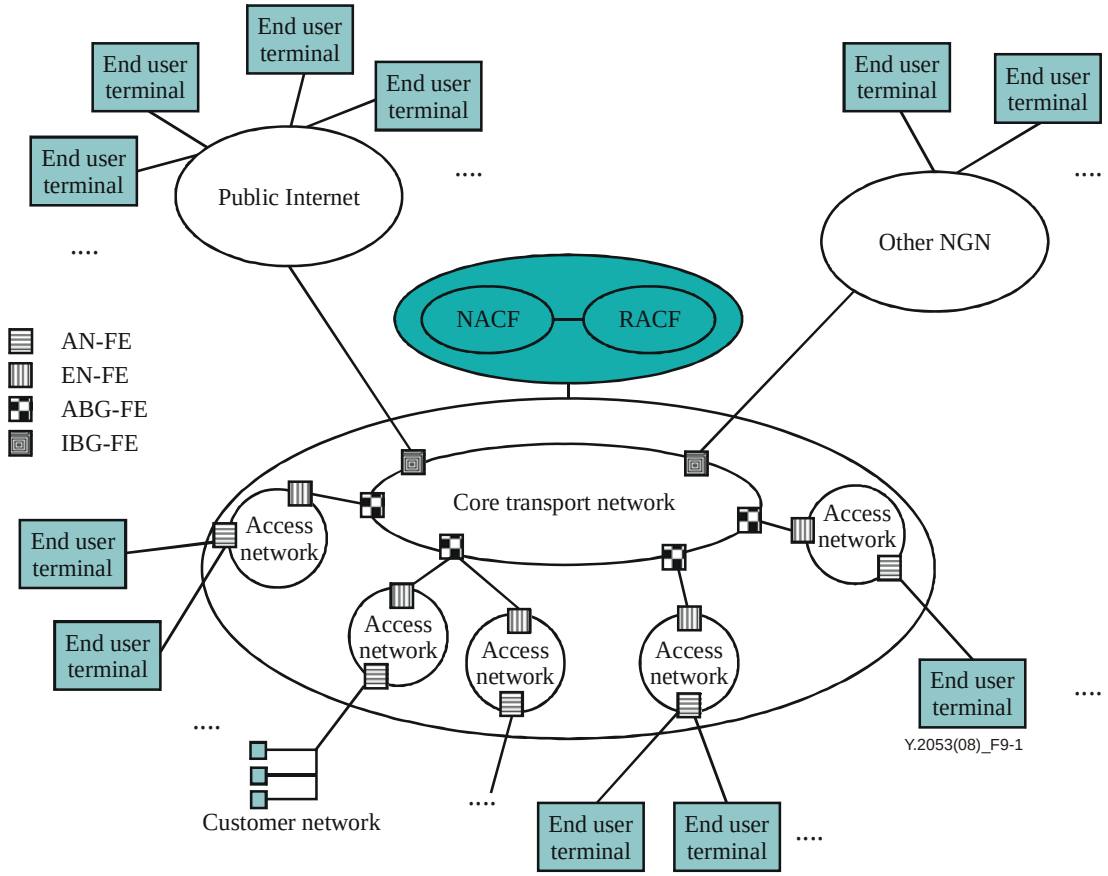

Figure 9-1 – An example configuration of NGN (view point at transport stratum)

9.1.1 Transport functions

Transport functions are comprised of access transport functions and core transport functions. Among those transport functions EN-FE, ABG-FE, IBG-FE are related to IPv6 migration.

9.1.1.1 Access transport functions

Access transport functions process end-users' access to the network as well as collecting and aggregating the traffic coming from these accesses towards the core network. Thus, tunnel end-point function and NAT-PT function are suitable for access transport functions.

a) *Access node FE (AN-FE)*

In this Recommendation, the AN-FE is assumed to be a layer 2 device; therefore, it is not involved in access protocol functionality.

b) *Edge node FE (EN-FE)*

The EN-FE in the access transport functions connects to core packet transport functions. In the case of connection to IP-based core transport functions, it shall be a layer 3 device with IP forwarding capabilities.

The EN-FE could be a tunnel end-point and/or NAT-PT device in CASE 1 or CASE 5. In both cases, the EN-FE should be dual stack.

- Tunnel end-point: An IPv6 end-user function tries to communicate with another IPv6 end-user function in other network over IPv4 core transport network, then the EN-FE should be a tunnel end-point (CASE 5). When the EN-FE receives IPv6 packets from IPv6 end-user functions, it encapsulates them in IPv4 header and forwards then to the other tunnel end-point.

– Scenario CASE 5: End-user function A and end-user function B are IPv6 nodes. One tunnel end-point for end-user function A is EN-FE, and the other tunnel end-point could be either EN-FE or ABG-FE or IBG-FE on the side of the end-user function B. FEs in the path between both tunnel end-points are IPv4.

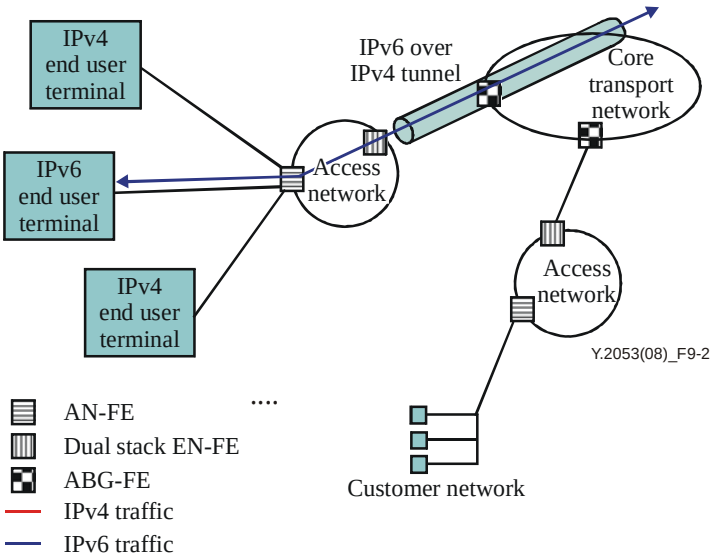

Figure 9-2 – An EN-FE as tunnel end-point

- NAT-PT: If an EN-FE supports NAT-PT function, an IPv6 end-user function can communicate with other IPv4 end-user functions. When the EN-FE supports NAT-PT function, the EN-FE translates the IPv6 packets from the IPv6 end-user terminals into IPv4 packets or vice versa. If the EN-FE has NAT-PT function, it should be controlled by RACF [ITU-T Y.2111].
  – Scenario CASE 1: IPv6 end-user function A tries to communicate with IPv4-only end-user function B. EN-FE in the side of end-user function A has NAT-PT function. Other FEs in the path are IPv4.

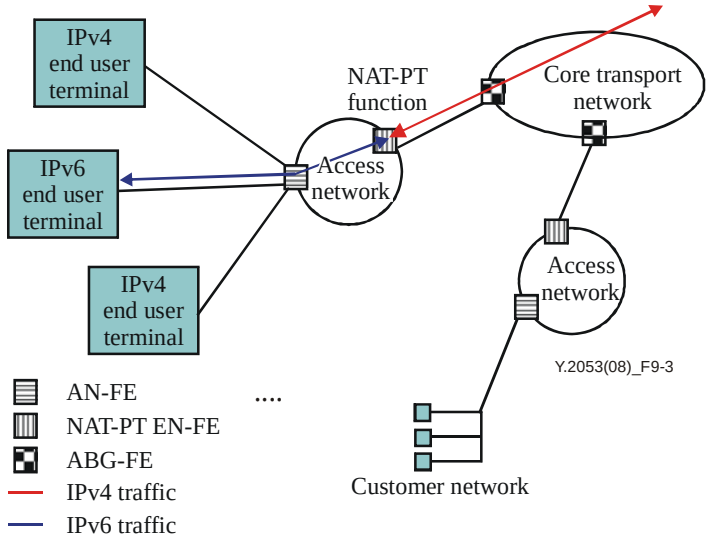

Figure 9-3 – An EN-FE as NAT-PT

- Native IPv6 deployment: If there is no IPv4 end-user terminal attached to AN-FE(s) that an EN-FE manages, the EN-FE could be a native IPv6 device. If the EN-FE is upgraded to a native IPv6 device, it just forwards IPv6 traffic to the ABG-FE.
  - Scenario CASE 2: If IPv6 end-user function wants to communicate with other IPv4 end-user functions, the ABG-FE should be a NAT-PT device.
  - Scenario CASE 6: If IPv6 end-user function wants to communicate with other IPv6 end-user functions, the ABG-FE should be a tunnel end-point.

9.1.1.2 Core transport functions

The core transport functions are responsible for ensuring information transport throughout the core network. Tunnel end-point function and NAT-PT function could be placed on ABG-FE and IBG-FE, but it is not recommended to place NAT-PT function on core transport FEs.

a) *Access border gateway FE (ABG-FE)*

The ABG-FE is a packet gateway between an access network and a core transport network. The EN-FE(s) which aggregate NGN user traffic connect to the ABG-FE. The ABG-FE could be a tunnel end-point and/or NAT-PT device in CASE 2 or CASE 6. In both cases, the EN-FE should be dual stack.

- Tunnel end-point: If the EN-FE does not support tunnel end-point, the ABG-FE should be a tunnel end-point for IPv6 traffic from end-user terminals. In this case, the ABG-FE has more functions to execute than in CASE 5, because, additionally, the ABG-FE serves as a terminal end-point through which all IPv6 traffic from attached EN-FE(s) is concentred.
  - Scenario CASE 6: If the EN-FE is dual stack but does not support tunnel end-point or all end-user functions and the EN-FE are upgraded to the native IPv6 device, the ABG-FE should be a tunnel end-point for IPv6 traffic from end-user terminals. The other tunnel end-point could be either EN-FE or ABG-FE or IBG-FE on the side of the other end-user function.

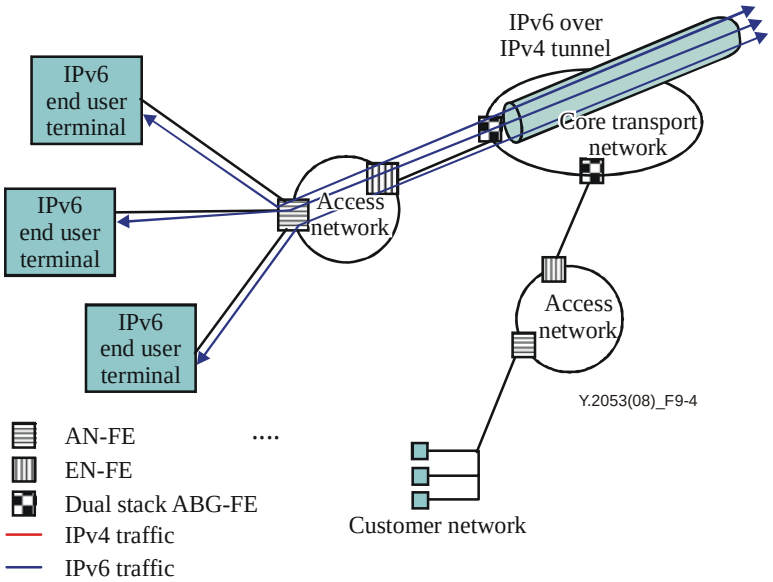

Figure 9-4 – An ABG-FE as tunnel end-point

- NAT-PT: If an IPv6 end-user function wants to communicate with IPv4 end-user function and the EN-FE does not support NAT-PT, the ABG-FE should support NAT-PT function.

– Scenario CASE 2: IPv6-only end-user function A tries to communicate with IPv4-only end-user function B. The EN-FE could be native IPv6 or dual stack. In this case, ABG-FE should have NAT-PT function. Other FEs are IPv4.

- Native IPv6 deployment: If all EN-FE(s) and all ABG-FE(s) are upgraded to native IPv6 device;
  – Scenario CASE 3: If IPv6 end-user function wants to communicate with other IPv4 end-user functions, the IBG-FE should be a NAT-PT device.
  – Scenario CASE 7: if IPv6 end-user function wants to communicate with other IPv6 end-user functions, the IBG-FE should be a tunnel end-point.

b) *Interconnection border gateway FE (IBG-FE)*

The IBG-FE is a packet gateway used to interconnect an operator's core transport network with another operator's core transport network supporting the packet-based services (refer to Figure 9-1). In the initial stage, most of the IBG-FEs only support IPv4, but, in the end, core transport network would be completely dual stack and finally be native IPv6 (CASE 10, CASE 11, CASE 12). During this transitional period, if the ABG-FE attached to the IBG-FE is upgraded to native IPv6 device, the IBG-FE should be a tunnel end-point or NAT-PT (CASE 3, CASE 7).

- Scenario CASE 7: If the ABG-FE is dual stack but does not support tunnel end-point or all end-user functions, EN-FE, and the ABG-FE are upgraded to the native IPv6 device, the IBG-FE should be a tunnel end-point for IPv6 traffic from end-user functions. The other tunnel end-point may be either IBG-FE, ABG-FE, or EN-FE on the side of the other end-user function.

If an IPv6 end-user function wants to communicate with IPv4 end-user function and the ABG-FE does not support NAT-PT, the IBG-FE should support NAT-PT function (CASE 3). But it is not recommended that the NAT-PT function be used between the core transport networks.

- Scenario CASE 3: IPv6-only end-user function A tries to communicate with IPv4-only end-user function B. The ABG-FE could be native IPv6 or dual stack. In this case, IBG-FE should have NAT-PT function. Other FEs are IPv4.

9.1.2 Transport control functions

9.1.2.1 Network access control functions (NACF)

a) *Network access configuration FE (NAC-FE)*

The NAC-FE is responsible for IP address allocation to terminals [ITU-T Y.2012] . It may also distribute other network configuration parameters like the address of DNS servers or signalling proxies, and so on. Thus, if the end-user function is tunnel end-point or dual stack the NAC-FE should provide the following additional information:

- End-user function is dual stack: If an end-user function is dual stack, the NAC-FE shall allocate IPv6 and IPv4 address to the end-user function.
- End-user function is tunnel end-point: If an end-user function is a dual stack terminal or a customer network, it could be a tunnel end-point (CASE 4, CASE 9). In this case the NAC-FE shall allocate the other tunnel end-point configuration information (refer to [b-IETF draft-03]).

9.1.2.2 Resource and admission control functions (RACF)

The RACF [ITU-T Y.2111] defines related requirements and functional architecture covering aspects such as resource reservation, admission control and gate control, network address port translation (NAPT) and firewall control, and network address translation (NAT) traversal. Thus, if

NAT-PT is used as IPv6 transition mechanism, RACF should consider requirements for NAT-PT scenarios (CASE 1, CASE 2, CASE 3, and CASE 8).

9.2 End-user functions

9.2.1 Terminal

An end-user terminal could be a tunnel end-point by itself (CASE 4). In this case, the other tunnel end-point could be another end-user terminal: EN-FE, ABG-FE, or IBG-FE.

9.2.2 Customer network

In this case, CPE of customer network could be a tunnel end-point or NAT-PT device (CASE 8, CASE 9).

9.3 Other non-NGN network functions

If NGN user function tries to communicate with other non-NGN network functions, an appropriate entity of non-NGN network should do a similar role as the one described in clause 8.

10 Security considerations

This Recommendation does not require any specific security considerations and aligns with the security requirements in [ITU-T Y.2701].

Appendix I

IPv6 migrations in NGN

(This appendix does not form an integral part of this Recommendation)

I.1 IPv6 transition mechanisms

This clause shows three IPv6 transition architectures from the viewpoint of IPv6 transition mechanisms architecture.

a) *Dual stack*

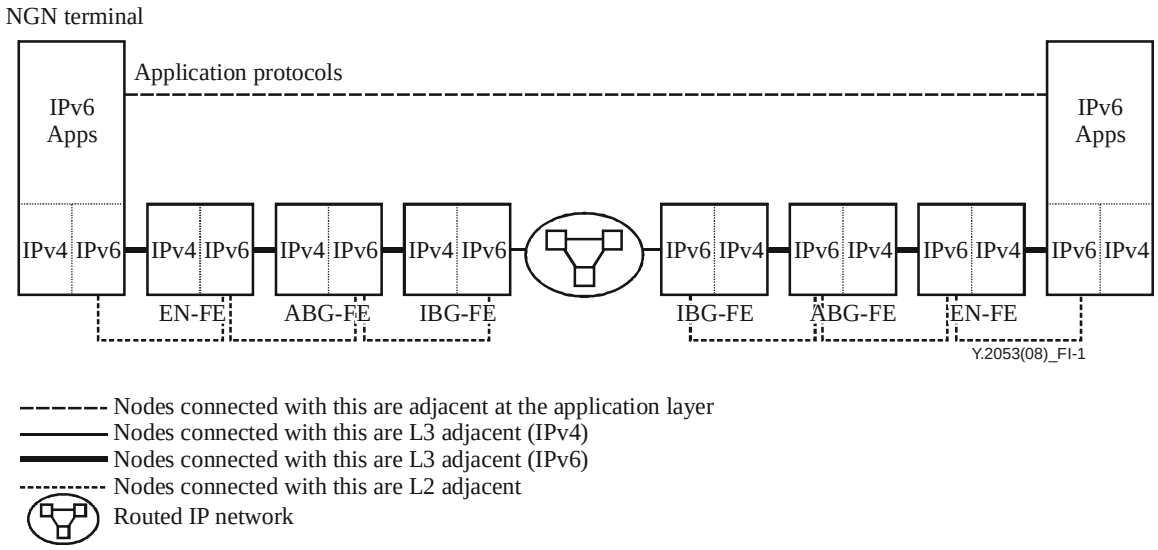

Figure I.1 – An example communication scenario with full dual stack

The most straightforward way for IPv6 nodes to remain compatible with IPv4-only nodes is by providing a complete IPv4 implementation. IPv6 nodes that provide complete IPv4 and IPv6 implementations are called "dual stack nodes". Dual stack nodes have the ability to send and receive both IPv4 and IPv6 packets. They can directly interoperate with IPv4 nodes using IPv4 packets, and also directly interoperate with IPv6 nodes using IPv6 packets.

Figure I.1 shows the case where the IPv6 services communicate with each other on dual stack network.

b) *Configured tunnel*

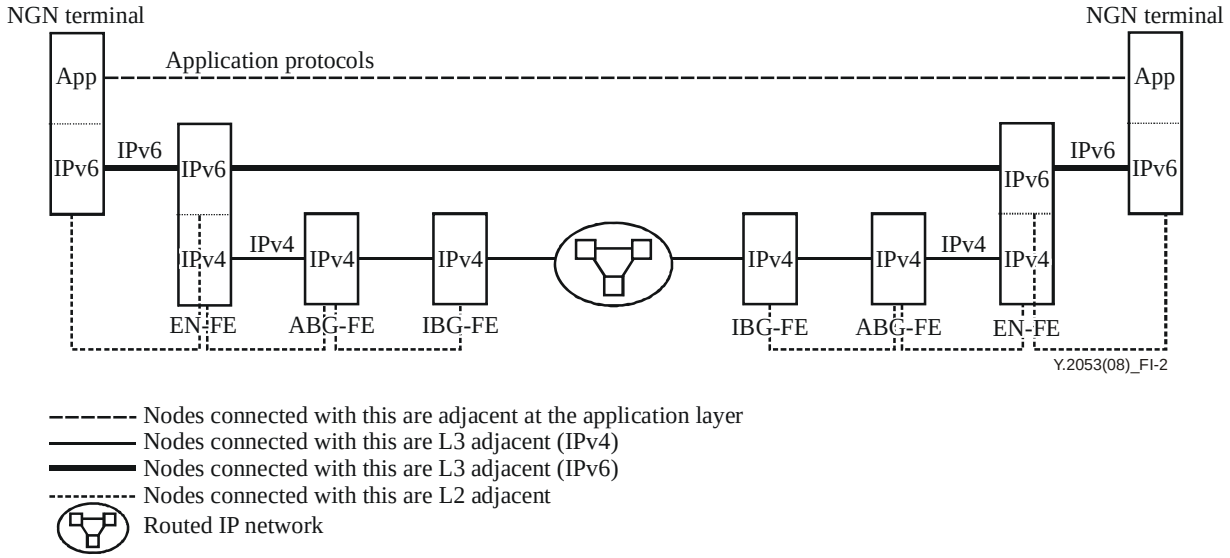

Figure I.2 – Example communication scenario with a configured tunnel

In the initial stage of IPv6 transition, most of the nodes are IPv4-only. Thus, a small set of routers in the core transport network has IPv6 capabilities. The use of a configured tunnel is adequate during this step.

In this case, there are dual stack nodes. IPv6 applications run on both end nodes communicating on IPv6 stack, and IPv6 packets are delivered over IPv4 stack of the core transport network. From this point of view, the L3 adjacency of EN-FE, tunnel end-point, is another EN-FE.

In this scenario, the EN-FE aggregates traffic of IPv6 NGN terminals and it is a dual stack node. Some of the NGN terminals attached to the EN-FE want to use IPv6 services. A configured tunnel is the adequate way to provide IPv6 service to them because most of the core transport functional entities are IPv4-only. The two tunnel end-points are EN-FEs in this case. The EN-FE aggregates tunnel end-points from several NGN terminals which want to use IPv6 services.

c) *NAT-PT*

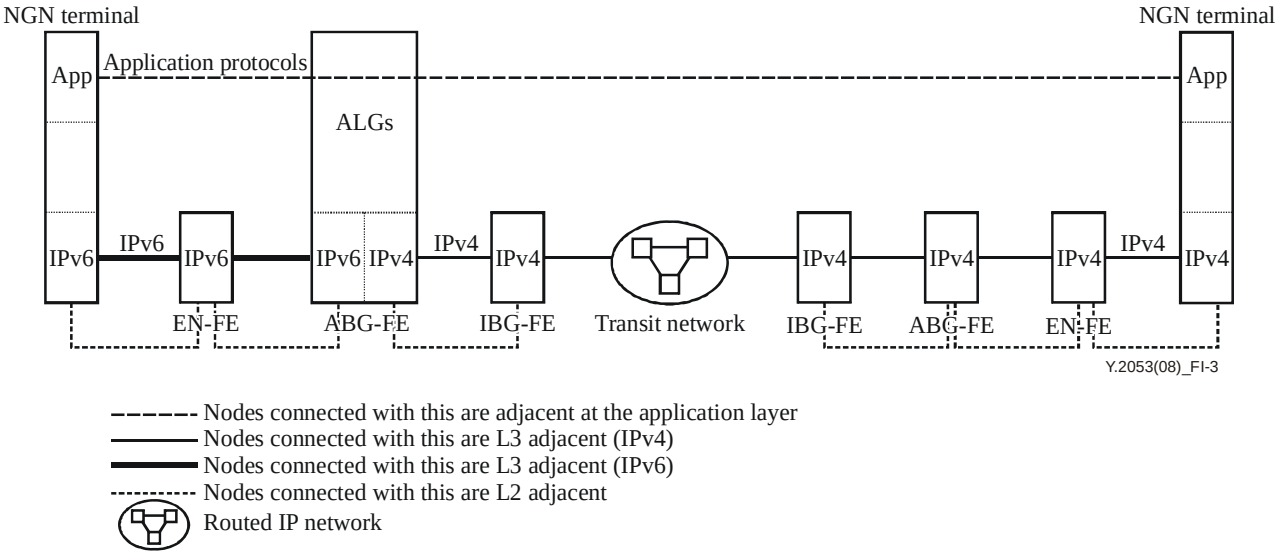

Figure I.3 – An example deployment scenario with NAT-PT

The NAT-PT mechanism (IPv4/IPv6 translation) is usually for edge IPv6 island subnets. The IPv6 NGN terminals behind the NAT-PT box can communicate with other IPv6 NGN terminals or other IPv4 NGN terminals through it.

The NAT-PT translates IPv6 header into IPv4 header or vice versa. The ALG translates application protocol header if it contains any IP layer information.

All packets which pass through the NAT-PT box will be reconstructed if each end-node of the connection has a different version of the IP stack. This results in a decline of performance. So the NAT-PT mechanism usually is not to be used in the core network.

I.2 Example migration scenarios according to Table 1

During the period of migration to IPv6, several types of nodes like dual stack, IPv6-only, IPv4-only nodes may coexist. In this clause, possible deployment scenarios during this period are introduced case by case.

A) *Scenario CASES 10, 11– Dual stack*

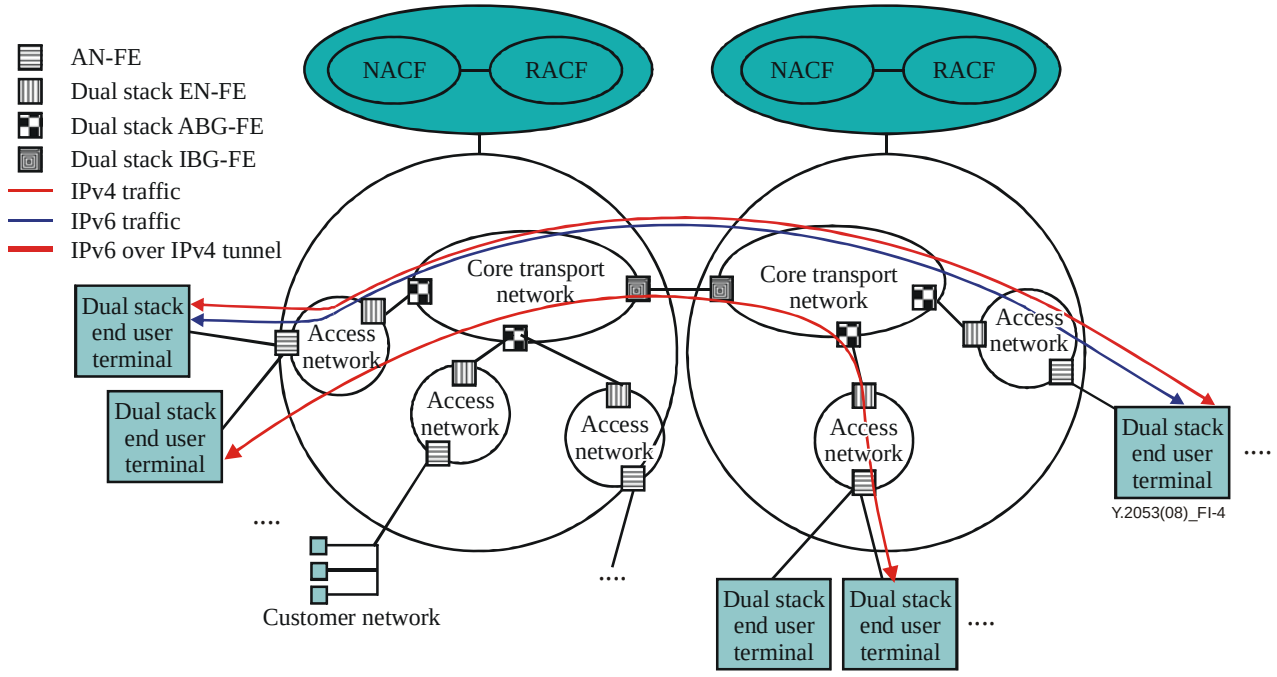

Figure I.4 – Dual stack node – dual stack node scenario

This scenario is the most ideal case. All end-user terminals and access/core transition FEs are dual stack and have IPv4/IPv6 routable address. IPv4 and IPv6 application can run on a dual-stack end-user terminal and can communicate with other applications which run on another dual-stack end-user terminal without any help from other IPv6 transition mechanisms.

- DNS:

  In this case the role of DNS is important.

  The Domain Name System (DNS) is used in both IPv4 and IPv6 to map between hostnames and IP addresses. The DNS resolver library on dual stack node should be able to handle A and AAAA record. If a DNS query result contains A records and AAAA records at the same time, the resolver library may reorder the results returned to the application in order to influence the version of IP packets used to communicate with that specific node – IPv6 first, or IPv4 first.

The applications should be able to specify whether they want IPv4, IPv6, or both records. This defines which address families the resolver looks up. Since most applications try the addresses in the order they are returned by the resolver, this can affect the IP version "preference" of applications.

The issues and operational guidelines for using IPv6 with DNS are described in more detail in [b-IETF RFC 4472].

B) *Scenario CASE 4 (CASES 5, 6, 7, 9 are similar cases) – Configured tunnelling*

If the core transport network runs on IPv4, a configured tunnel can be used to forward IPv6 traffic to the destination access network.

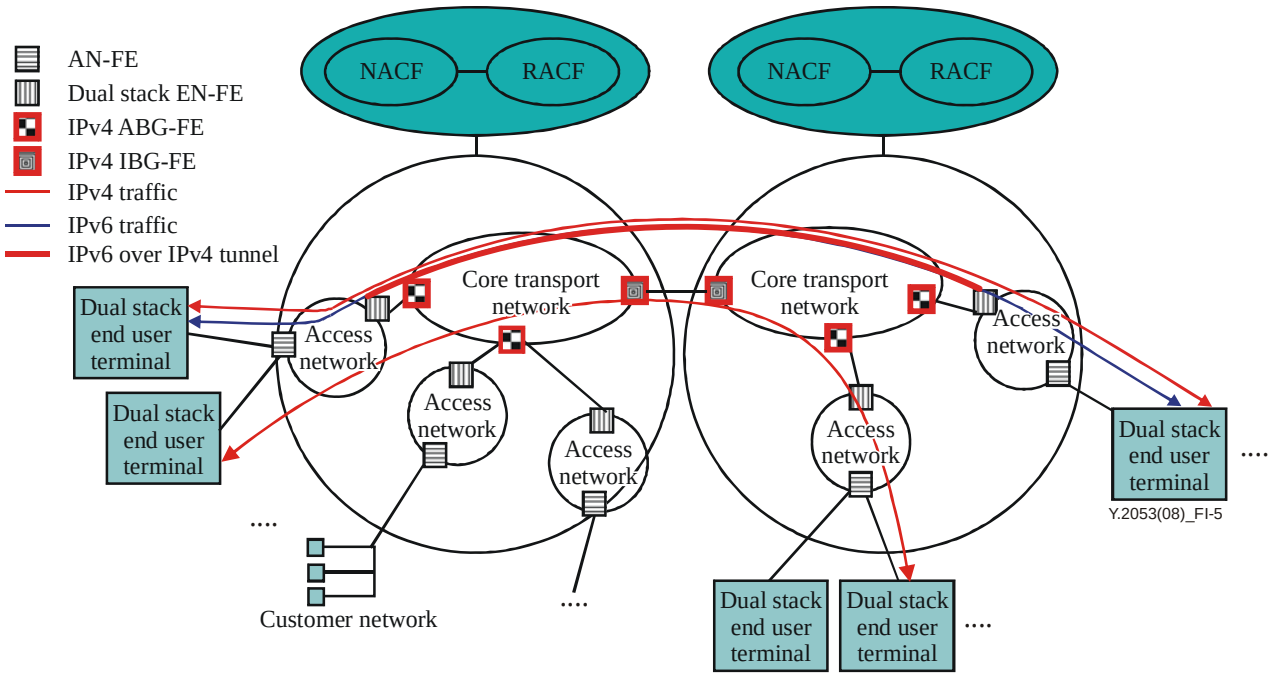

Figure I.5 – Dual stack node – dual stack node (IPv4 core transport) scenario

C) *Scenario CASE 4 (CASES 5, 6, 7, 9 are similar cases) – dual stack ←→ IPv4-only*

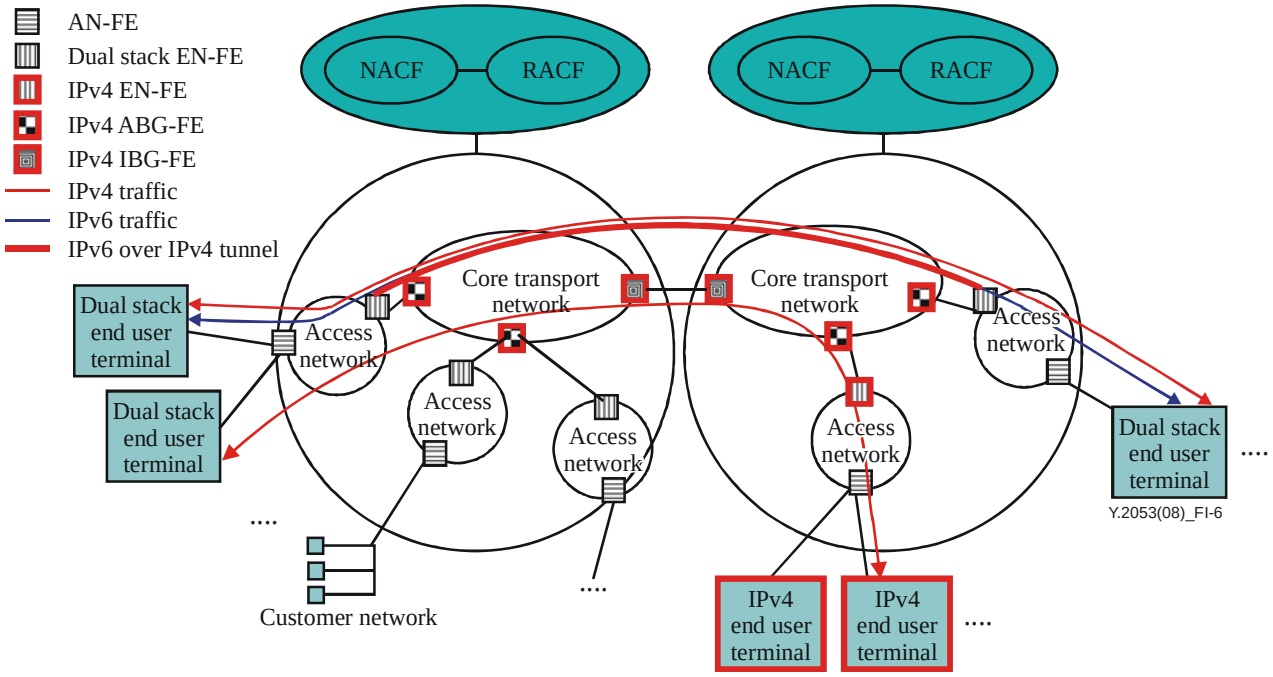

Figure I.6 – Dual stack node – IPv4 node (IPv4 core transport)

The following case is another example derived from C.

D) *Scenario CASE 4 (CASES 5, 6, 7, 9 are similar cases) – dual stack ←→ IPv6-only*

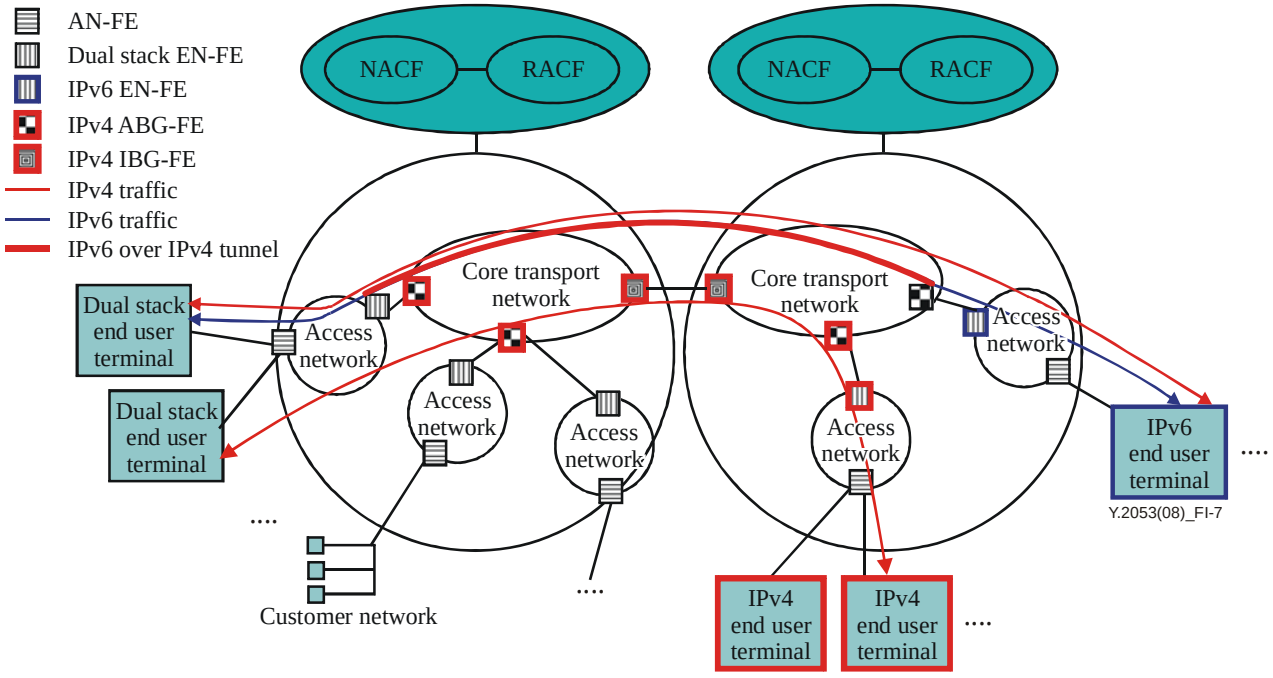

Figure I.7 – Dual stack node – IPv6 node (IPv4 core transport)

The following case is another example derived from C.

E) *Scenario CASE 1 (CASES 2, 3, 8 are similar cases) – NAT-PT*

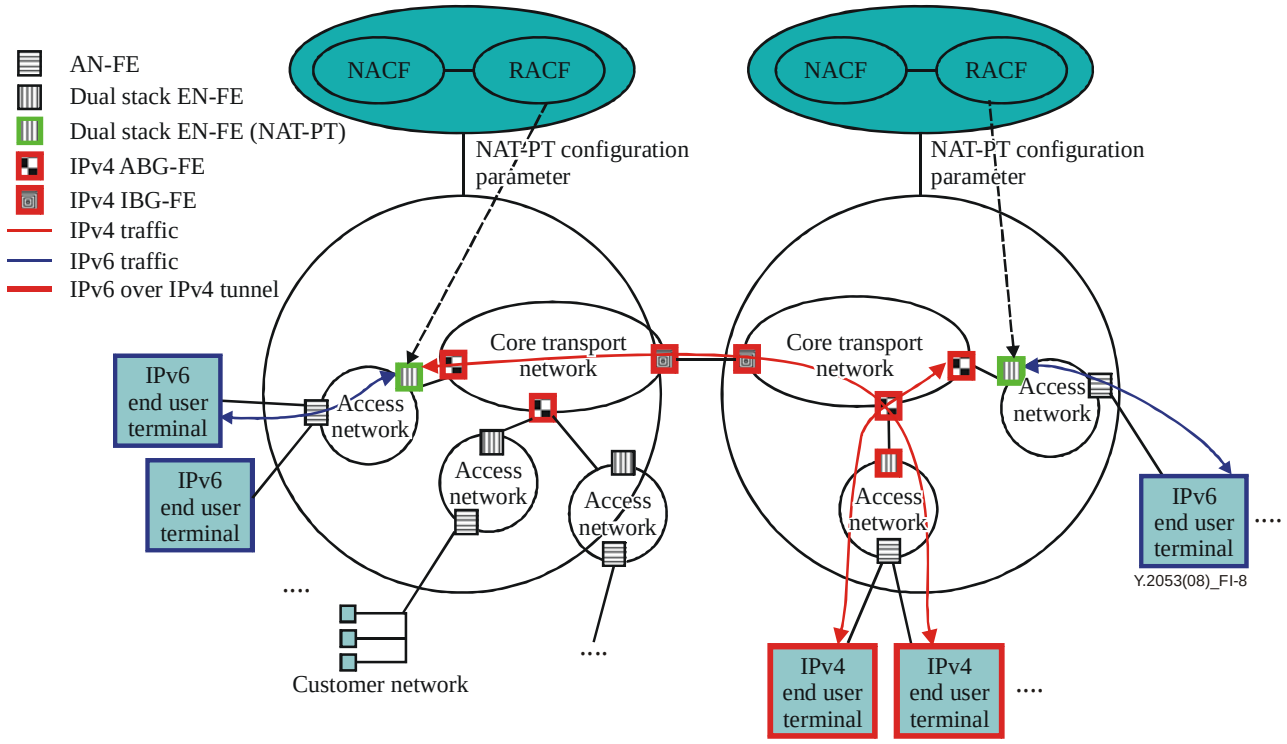

Figure I.8 – IPv4 node – IPv6 node (IPv4 core transport)

IPv6 end-user terminal can communicate with IPv4 terminal through NAT-PT device. In this example, NAT-PT is installed on the EN-FE. NAT-PT can also be installed on ABG-FE or IBG-FE. The NAT-PT device translates IPv6 packets into IPv4 packets or vice versa.

RACF manages NAT-PT translation policy and other configuration parameters. The RACF provides such information to NAT-PT device whenever it is necessary.

F) *Scenario CASE 4 (CASES 5, 6, 7, 9 are similar cases) – IPv6-only ←→ IPv4-only*

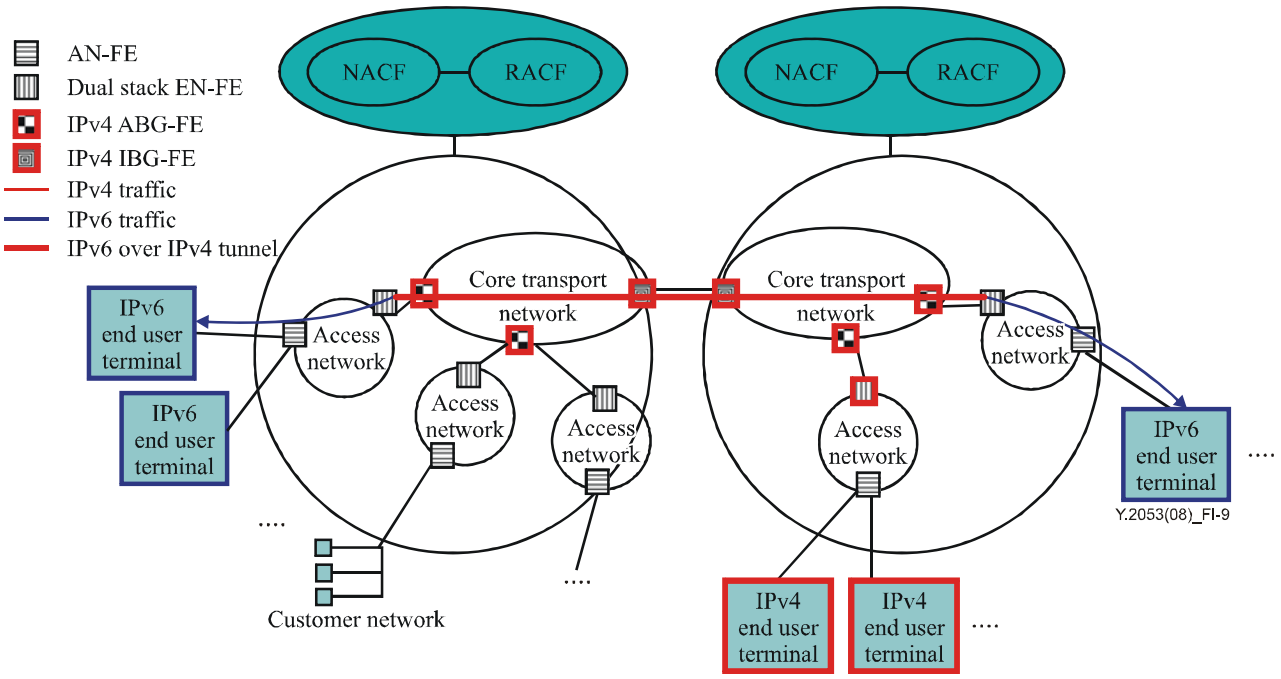

Figure I.9 – IPv6 node – IPv6 node (IPv4 core transport)

This case is similar to B. To traverse IPv4 core transport network, a configured tunnel is used in this scenario.

Bibliography

[b-ITU-T Y.1540] Recommendation ITU-T Y.1540 (2007), *Internet protocol data communication service – IP packet transfer and availability performance parameters*.

[b-IETF RFC 2765] IETF RFC 2765 (2000), *Stateless IP/ICMP Translation Algorithm (SIIT)*, (Standards Track). <http://www.ietf.org/rfc/rfc2765.txt?number=2765>

[b-IETF RFC 2766] IETF RFC 2766 (2000), *Network Address Translation – Protocol Translation (NAT-PT)*, (Standards Track). <http://www.ietf.org/rfc/rfc2766.txt?number=2766>

[b-IETF RFC 4213] IETF RFC 4213 (2005), *Basic Transition Mechanisms for IPv6 Hosts and Routers*, (Standards Track). <http://www.ietf.org/rfc/rfc4213.txt?number=4213>

[b-IETF RFC 4472] IETF RFC 4472 (2006), *Operational Considerations and Issues with IPv6 DNS*. <http://www.ietf.org/rfc/rfc4472.txt?number=4472>

[b-IETF draft-03] IETF draft-03, *IPv6 Tunnel Broker with the Tunnel Setup Protocol (TSP)*. <http://tool.ietf.org/html/draft-blanchet-v6ops-tunnelbroker-tsp-03>

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
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	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
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 and next-generation networks**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2008