International Telecommunication Union

ITU-T

TELECOMMUNICATION STANDARDIZATION SECTOR OF ITU

Y.2052

(02/2008)

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

Next Generation Networks – Frameworks and functional architecture models

---

Framework of multi-homing in IPv6-based NGN

Recommendation ITU-T Y.2052

ITU-T

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.2052

Framework of multi-homing in IPv6-based NGN

Summary

Recommendation ITU-T Y.2052 describes a framework of multi-homing in Internet Protocol version 6 (IPv6)-based next generation network (NGN). This Recommendation identifies the requirements, the usage models, the functional architecture, and the applications of multi-homing in IPv6-based NGN.

Source

Recommendation ITU-T Y.2052 was approved on 29 February 2008 by ITU-T Study Group 13 (2005-2008) under Recommendation ITU-T A.8 procedure.

Keywords

IPv6, IPv6-based NGN, multi-homing.

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.2052

Framework of multi-homing in IPv6-based NGN

1 Scope

One of the primary features of Internet Protocol version 6 (IPv6) is 'multi-homing'. Using IPv6 multi-homing features, a network (or site) and/or a user terminal (or host) is able to have multiple network connections with multiple network interfaces and multiple IPv6 addresses. In IPv6-based next generation network (NGN), NGN users will have, using multi-homing features, always-on connectivity, improved fault tolerance, performance improvement by load balancing, and session continuity, etc.

This Recommendation describes a framework of multi-homing in IPv6-based NGN. For this purpose, this Recommendation identifies the requirements, the usage models, the functional architecture, and some applications of multi-homing so as to facilitate the deployment of the enhanced services in IPv6-based NGN.

The scope of this Recommendation includes:

- requirements of multi-homing in IPv6-based NGN;
- usage models of multi-homing in IPv6-based NGN;
- functional architecture to support multi-homing in IPv6-based NGN;
- applications of multi-homing in IPv6-based NGN.

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

[ITU-T Y.2051] Recommendation ITU-T Y.2051 (2008), *General overview of IPv6-based NGN*.

[ITU-T Y.2201] Recommendation ITU-T Y.2201 (2007), *NGN release 1 requirements*.

[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 fault tolerance [ITU-T E.800]: An attribute of an item that makes it able to perform a required function in the presence of certain given sub-item faults.

3.1.2 IPv6-based NGN [ITU-T Y.2051]: This refers to NGN that supports addressing, routing protocols and services associated with IPv6. An IPv6-based NGN shall recognize and process the

IPv6 headers and options, operating over various underlying transport technologies in the transport stratum.

3.1.3 session continuity [b-ITU-T Q.1702]: The ability of the user to maintain continuity of ongoing sessions while changing between terminal devices and across various access and core networks.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 always-on connectivity: A capability that a NGN user or user equipment can connect to the networks at any time and at any place.

3.2.2 host multi-homing: A multi-homing feature that a host has multiple connections to networks.

3.2.3 IPv6 multi-homing: A feature of an IPv6 host and/or IPv6 network that enables the host or network to be multi-homed to networks through multiple network interfaces and multiple IPv6 addresses.

3.2.4 IPv6 network provider: An entity that provides IPv6 network connection by advertising IPv6 prefix information (e.g., ISP).

3.2.5 load balancing: A scheme by which the traffic load could be separated and balanced to effectively utilize the network resources (e.g., link bandwidth).

3.2.6 network interface: A device to be used by a node to connect to a network.

3.2.7 site: An entity autonomously operating a network using IP.

3.2.8 site multi-homing: A multi-homing feature that a site (network) has multiple connections to other networks.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

BGP	Border Gateway Protocol
DCCP	Datagram Congestion Control Protocol
DHCPv6	Dynamic Host Configuration Protocol for IPv6
FE	Functional Entity
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISP	Internet Service Provider
NACF	Network Attachment Control Function
NGN	Next Generation Network
RACF	Resource and Admission Control Function
SCTP	Stream Control Transmission Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

5 Conventions

None.

6 Features of multi-homing in IPv6-based NGN

The primary purpose of multi-homing is to provide multiple network connections to increase the reliability of network connections. Besides increasing reliability, the multi-homing feature enables the site and/or host to effectively utilize network connections to provide load balancing, session continuity, etc. In Internet Protocol version 4 (IPv4)-based networks, multi-homing is mainly deployed by using border gateway protocol (BGP) mechanism between network domains [b-IETF RFC 2260].

In IPv6-based NGN, multi-homing should be given more importance due to the following observations:

– A node has multiple IPv6 addresses for different scope and renumbering.

– A node has multiple network interfaces (physical interfaces by heterogeneous access networks and tunnelling interfaces).

– A node has multiple network prefixes for routing scaling.

IPv6 can provide a user terminal with multiple IPv6 addresses, which are allocated hierarchically by network providers. Although the purpose of multi-homing in IPv6-based NGN is the same as IPv4-based network, the requirements/considerations and mechanisms are different. In IPv6-based NGN, it disallows IPv4-style multi-homing [b-IETF RFC 2772].

– IPv6 network providers (e.g., Internet service provider (ISP)) cannot advertise prefixes of other network providers.

– Sites cannot advertise to upstream providers prefixes longer than their assigned prefix.

Because of these restrictions and the requirement of session continuity during the change of network connection by multi-homing, different mechanisms are needed for IPv6 multi-homing. The Internet Engineering Task Force (IETF) has carried out many studies for developing solutions, see [b-IETF RFC 3582], [b-IETF RFC 4116], [b-IETF RFC 4177], [b-IETF RFC 4218], [b-IETF RFC 4219].

In IPv6-based NGN, a NGN transport stratum comprises a wide variety of IPv6-based access networks and IPv6-based core network. IPv6-based access networks may be heterogeneous using different access technologies [ITU-T Y.2012]. Figure 1 shows an example of an IPv6-based NGN network architecture that consists of an IPv6-based core network and heterogeneous access networks which support IPv6-based IP connectivity. Those access networks use different access technologies and are interconnected with each other through IPv6-based core network.

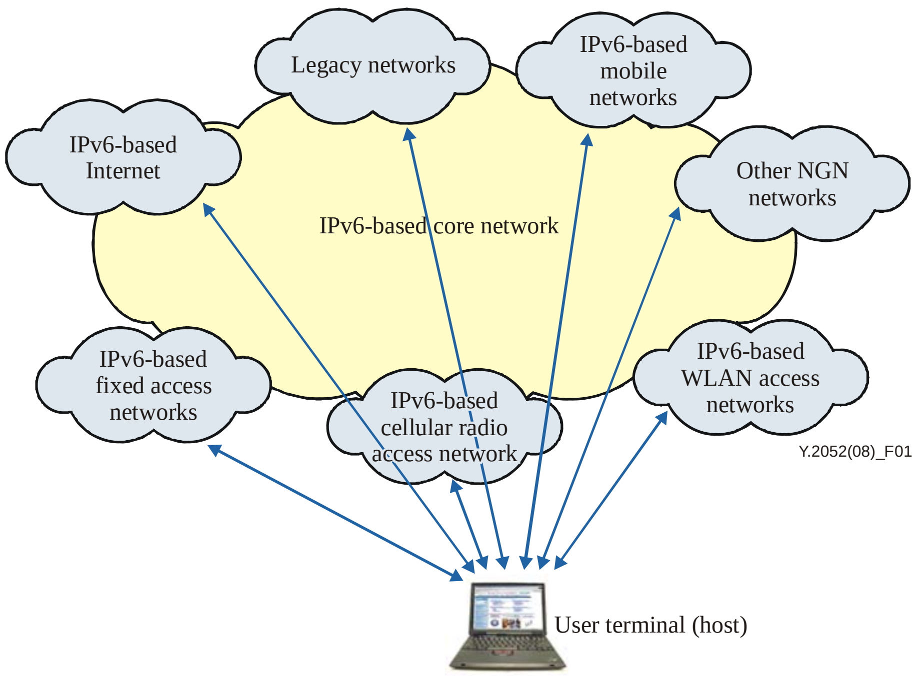

Figure 1 – Overall configuration model of IPv6-based NGN

In this configuration, a user terminal could use multiple IPv6 addresses and multiple network interfaces and be multiply connected to IPv6-based NGN. Also, each access network could use multiple network connections through multiple network prefixes. In this way, multi-homing features in IPv6-based NGN could be used to provide more enhanced services and connectivity for the users.

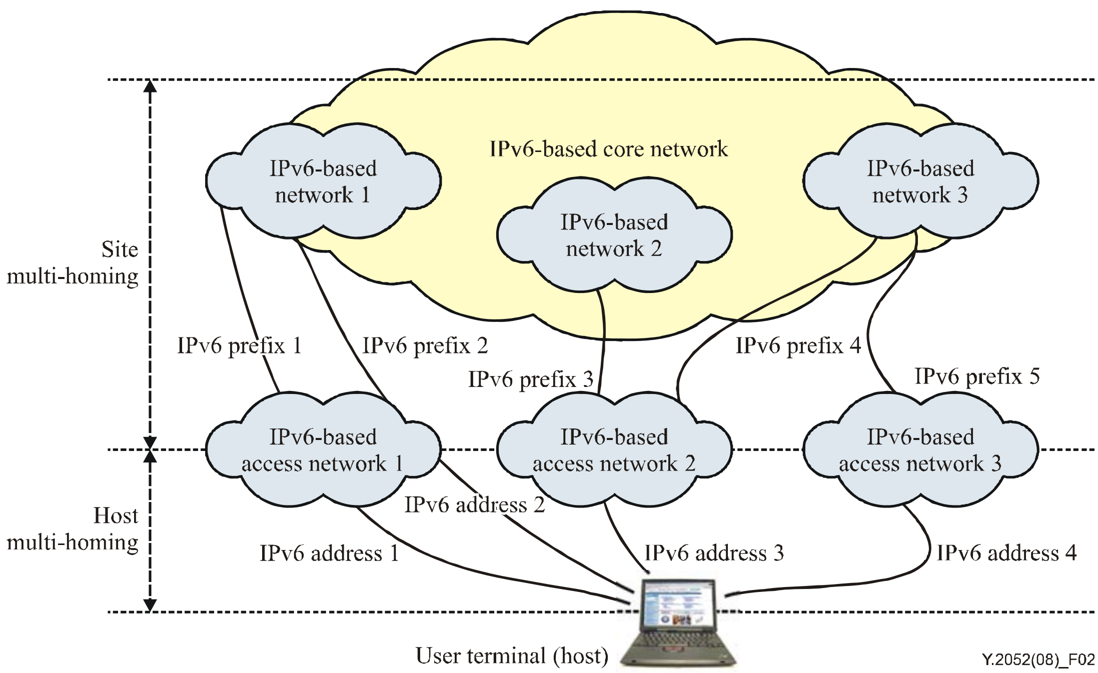

Figure 2 – Example of multi-homing in IPv6-based NGN

In Figure 2, a user terminal is connected to three different access networks using different access technologies. Each access network is also connected to different IPv6-based networks. In this case, the user terminal could simultaneously use multiple network connections to communicate with the other network nodes. The user terminal could use two network connections through access network 1 with two different IPv6 addresses, and it could use each network connection through access network 2 and access network 3. Also, access network could be multiply connected to other networks. Access network 1 could use two network connections (using different IPv6 prefixes through IPv6-based network 1). Also, access network 2 could use two network connections (one is through IPv6-based network 2 and the other through IPv6-based network 3).

7 Requirements of multi-homing in IPv6-based NGN

7.1 General requirements of multi-homing in IPv6-based NGN

To provide more enhanced services and applications for the users, IPv6-based NGN shall be considered to support multi-homing. In this respect, the following are defined as general requirements to support multi-homing in IPv6-based NGN:

– IPv6-based NGN transport stratum shall provide users with multiple access capabilities to the network.
– IPv6-based NGN shall provide multiple accesses to heterogeneous access networks.
– A network shall have multiple network connections with other networks.
– A user terminal shall have multiple network connections with the network.
– A user terminal shall support multiple network interfaces.
– A user terminal shall have multiple IPv6 addresses in a network interface.
– A user terminal shall have the capability to use multiple connections simultaneously.
– A user terminal shall acquire (or relinquish) additional IPv6 addresses dynamically via a user terminal's mobility or host renumbering protocol.
– A user terminal shall acquire (or relinquish) additional network interface dynamically via multiple network interfaces or tunnel configuration.
– A network shall acquire (or relinquish) additional prefixes dynamically via the router renumbering protocol [b-IETF RFC 2894].

7.2 Requirements of site multi-homing

In IPv6-based NGN, each user is expected to use a wide variety of application services, which include broadband multimedia services, video-conferencing, streaming, and advanced telephony services. In particular, these advanced services are required to be accessed through diverse transport technologies and capabilities [ITU-T Y.2201]. In addition, IPv6-based NGN shall support various types of communication modes: one-to-one, one-to-many, many-to-many, many-to-one. To support these services and capabilities, IPv6-based NGN will benefit from the ability to support site multi-homing capability. With the help of site multi-homing capability, each access network can connect to a core network with multiple network connections and each access network can connect to other access networks via the core network with multiple network connections.

Site multi-homing in IPv6-based NGN shall be used for a site (network) to be multi-homed to a single IPv6 network provider (e.g., ISP), or to different IPv6 network providers. Figure 3 shows the scenarios of site multi-homing in IPv6-based NGN. In Figure 3-a, a site is connected to a single network provider via different network connections, whereas a site is multiply connected to two different network providers in Figure 3-b.

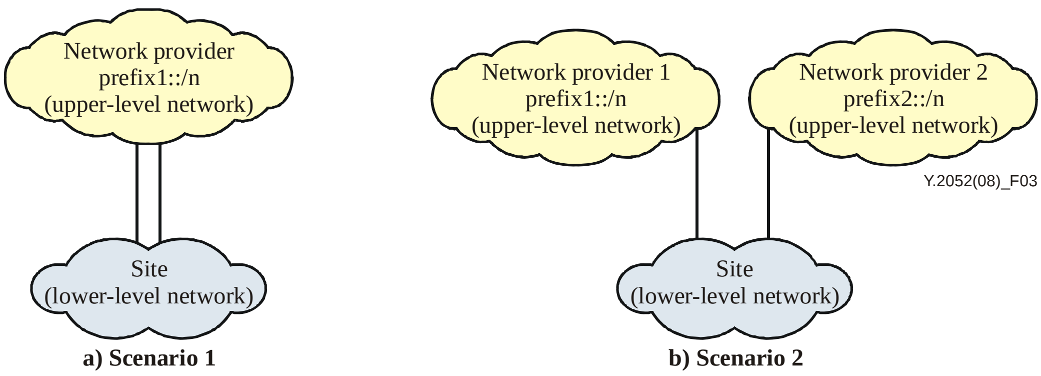

Figure 3 – Site multi-homing scenarios in IPv6-based NGN

It is noted that 'site' is already defined in IETF. In IPv6-based NGN environments, a site can be regarded as a network. In IPv6-based NGN architecture, a site represents any networks such as access network and core network. Site multi-homing in IPv6-based NGN could be realized by the interaction between the upper-level networks and the lower-level networks. The upper-level networks usually advertise prefix information, and the lower-level networks make their routing policy based on the prefix information received from the upper-level networks.

To support site multi-homing in IPv6-based NGN, the following requirements shall be considered:

– Core network shall be able to provide multiple network connections to other networks.

– Access network shall be able to provide multiple network connections to other networks.

7.3 Requirements of host multi-homing

A traditional paradigm to communicate between network nodes is characterized as described in Figure 4-a. Logically, each layer (application layer, transport layer (transmission control protocol (TCP)/user datagram protocol (UDP)/stream control transmission protocol (SCTP)/datagram congestion control protocol (DCCP)), network layer (IPv4/IPv6), link layer, and physical layer) at host 1 is interconnected with the corresponding layer at host 2. This interconnection relationship is maintained from the start of the communication until the end. The important element in this relationship is a one-to-one connection between each layer.

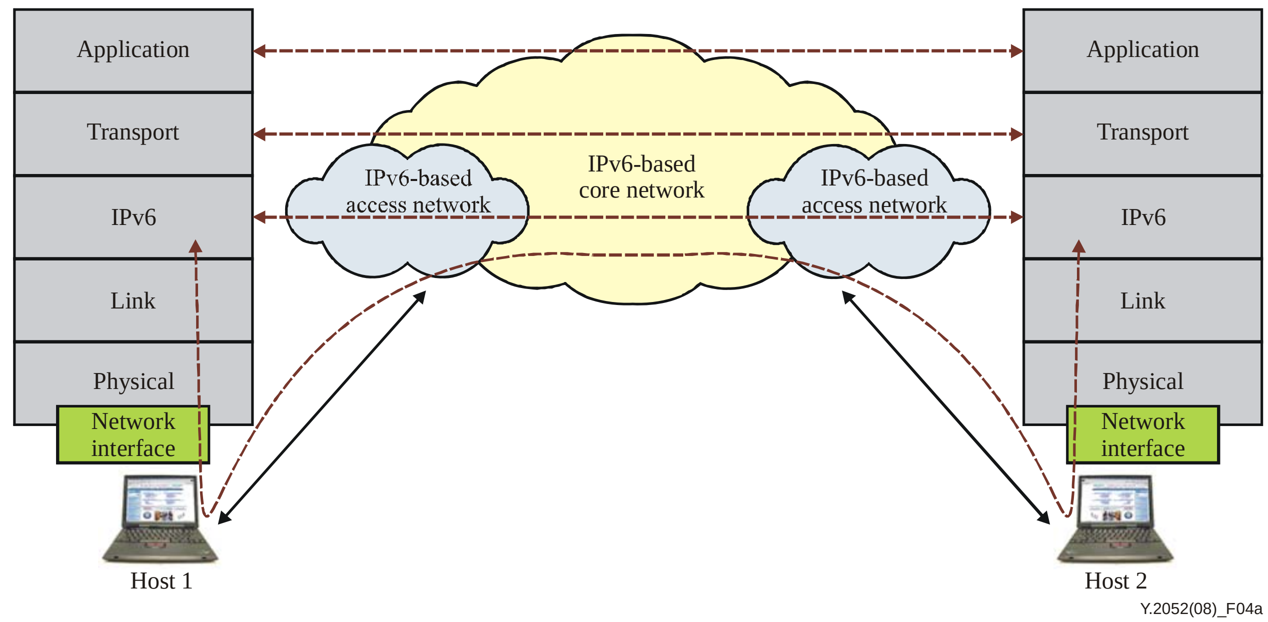

Figure 4-a – Traditional paradigm to communicate between network nodes

As multiple network interfaces and multiple IPv6 addresses are used in a network node, the communication paradigm is changed. In a traditional communication paradigm, although a host has multiple network interfaces, only one network interface is selected and used to communicate at a time. But, for a host in IPv6-based NGN, multiple network interfaces are used to communicate simultaneously and the host might have the capability to access to multiple heterogeneous access networks at the same time. Figure 4-b shows this scenario. Host 1 uses multiple network interfaces to communicate with host 2 and there might be multiple link layer (layer 2) connections. Also, host 1 could use multiple IPv6 addresses to communicate with host 2 and there might be multiple network connections.

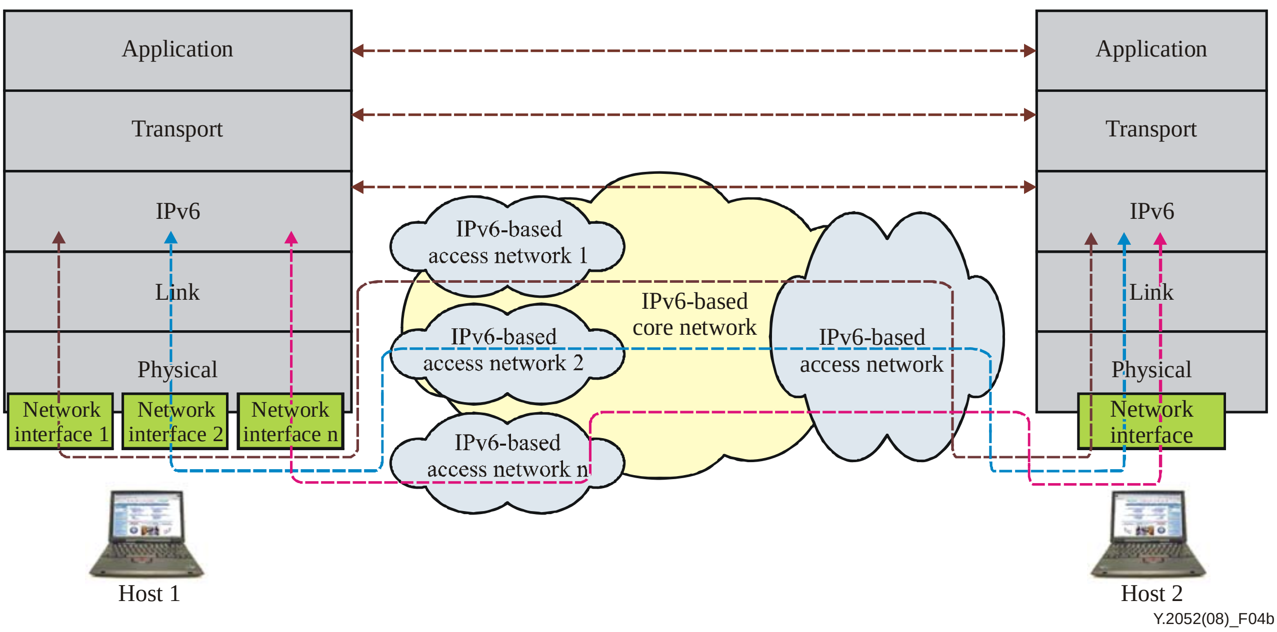

Figure 4-b – Usage of multiple network interfaces in a host

In IPv6-based NGN, a host might have multiple IPv6 addresses in a network interface and/or multiple network interfaces. In Figure 4-c, host 1 has multiple IPv6 addresses and uses multiple network (layer 3) connections to communicate with the other node.

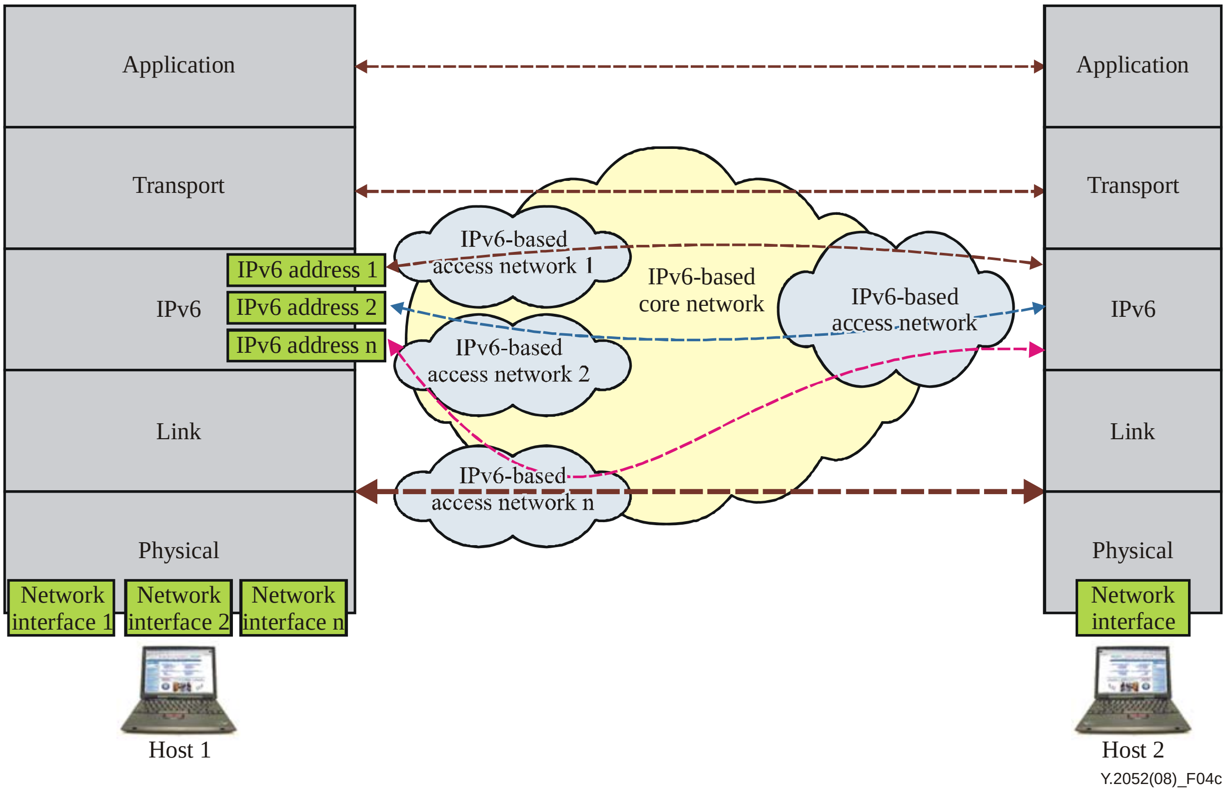

Figure 4-c – Usage of multiple IPv6 addresses in a host

Due to the multiplicity of network interfaces and IPv6 addresses in transport layer, there can be multiple transport (layer 4) sessions using SCTP and DCCP. Figure 4-d shows this scenario.

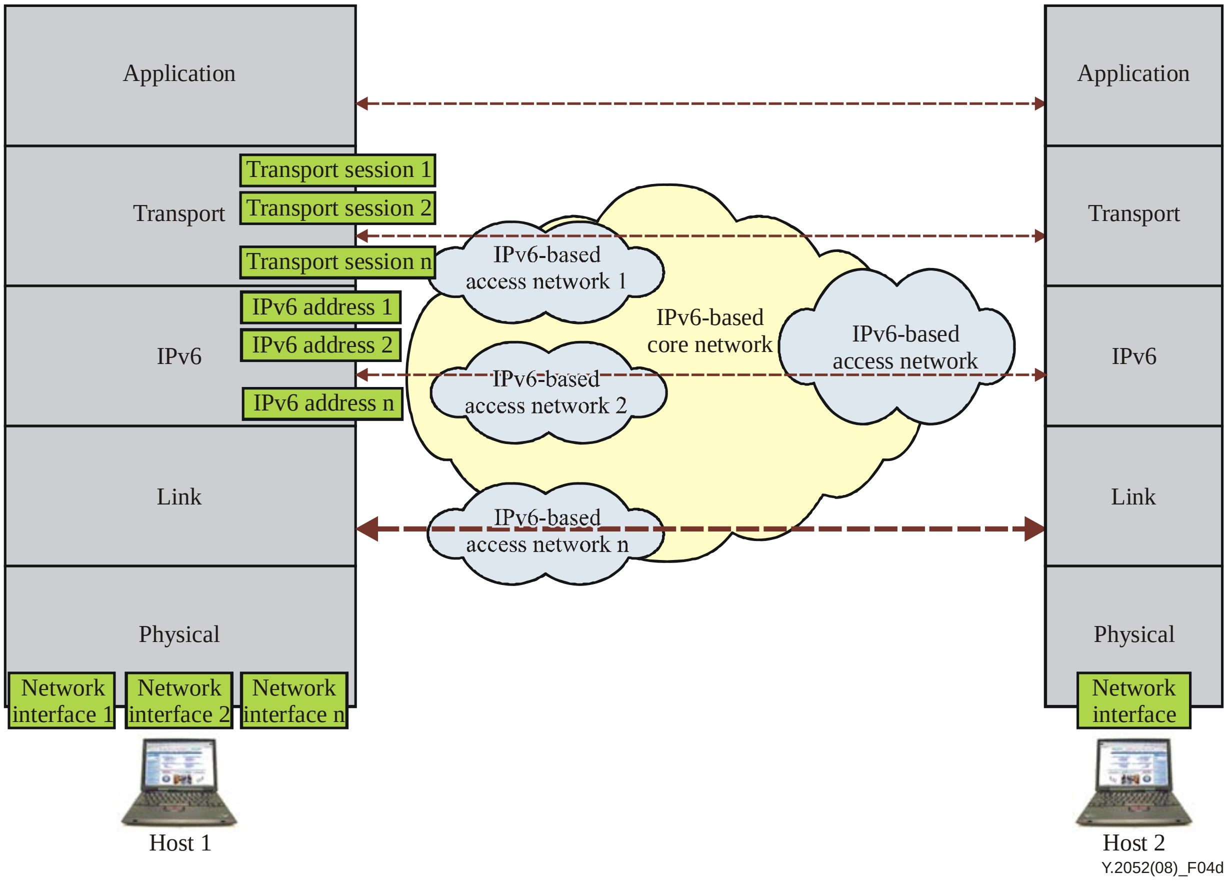

Figure 4-d – Usage of multiple transport sessions in a host

To support host multi-homing in IPv6-based NGN, the following requirements shall be considered:

– A user terminal shall be able to have multiple network connections to access networks with multiple IPv6 addresses and/or multiple network interfaces.

– A user terminal shall be able to have multiple IPv6 addresses and/or multiple network interfaces and shall be able to connect to multiple heterogeneous access networks with multiple IPv6 addresses and/or multiple network interfaces.

– A user terminal shall be able to activate those multiple network interfaces/multiple IPv6 addresses simultaneously.

– A mobile user using host multi-homing feature in IPv6-based NGN shall be able to continue the services, even though the mobile user continues to move from one access network to the other access network using different access network technologies.

8 Multi-homing models in IPv6-based NGN

One of the primary goals in IPv6-based NGN is to provide NGN users with enhanced services and applications by using the multi-homing features: site multi-homing and host multi-homing. By a protocol layering concept, the multi-homing functionality could be further classified into a network layer (IPv6) multi-homing and a transport layer (TCP/UDP/SCTP/DCCP) multi-homing. In the network layer, site multi-homing and host multi-homing could be both used whereas in the transport layer, the host (end-to-end) multi-homing could be used between the two end-to-end hosts together.

8.1 Usage model of multi-homing in a network layer

Multi-homing in a network layer is associated with an IPv6 protocol (e.g., layer 3). In a network layer, a user terminal (host) and/or user group (site) will be multi-homed to multiple access networks, hence connected to the NGN core network. Furthermore, multi-homing in a network layer could be classified into site multi-homing and host multi-homing.

Figure 5 shows a network model of site multi-homing in a network layer.

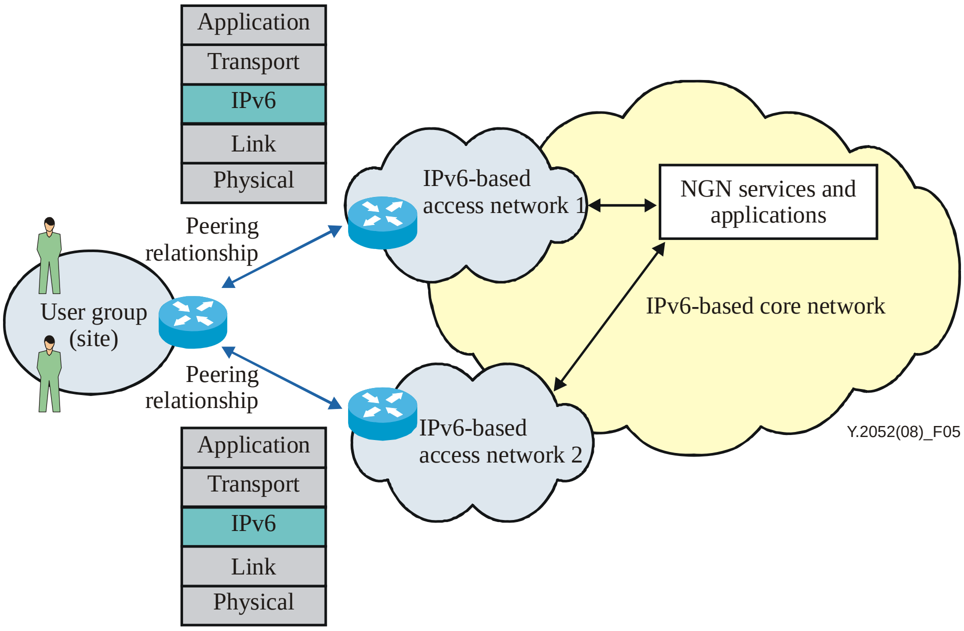

Figure 5 – Site multi-homing in a network layer

In Figure 5, a site or a network of a user group is multi-homed to multiple access networks in IPv6-based NGN. The gateway or router of the site will be interconnected to those of the access networks with the peer-to-peer relationship in a network layer. Such peering relationship might be subject to an agreed negotiation between the two associated networks.

With the help of this site multi-homing capability, IPv6-based NGN users located in the site could use the enhanced NGN services and applications provided by the NGN service provider via the core network.

Typical application areas of this type of site multi-homing include:

– Traffic load sharing: for improvement of the utilization of network bandwidth;

– Traffic engineering: for enhancement of the network utilization and for routing optimization.

Figure 6 shows a network model for the host multi-homing in a network layer.

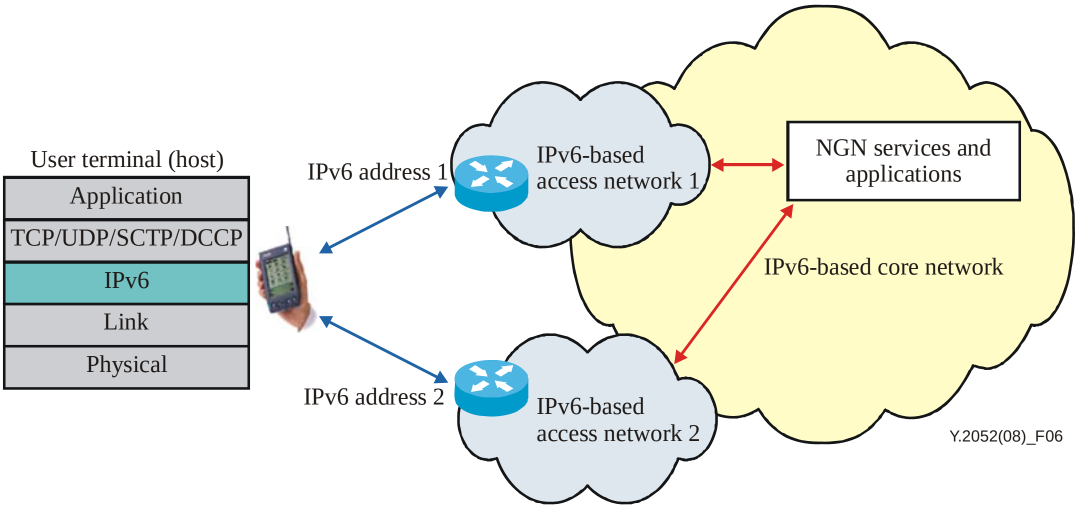

Figure 6 – Host multi-homing in a network layer

As shown in Figure 6, multi-homing could also be used with the capability of the individual IPv6 hosts in a network layer. In the figure, the IPv6 host (user terminal) is multi-homed to multiple access networks in IPv6-based NGN. In this model, the IPv6 host would use two different IPv6 addresses with the different subnet prefixes to each of the access networks.

With the help of this host multi-homing capability, IPv6-based NGN users (hosts) could use the enhanced NGN services and applications provided by the NGN service provider via the core network.

Typical application areas of this host multi-homing include:

– Traffic load sharing: for improvement of the utilization of link bandwidth assigned to the host;
– Fault tolerance with redundancy: to recover the host connection from the network failure.

8.2 Usage model of multi-homing in a transport layer

IPv6 multi-homing could also be used in the transport layer in IPv6-based NGN. In this case, multi-homing in a network layer is associated with transport protocols (e.g., layer 4), developed in the IETF, which support the transport-layer multi-homing such as SCTP and DCCP [b-IETF RFC 2960] and [b-IETF RFC 4340]. In the perspective of TCP/IP socket programming, TCP and UDP are not relevant to transport layer multi-homing.

It is noted that transport-layer multi-homing would intrinsically be based on the support of the underlying network layer multi-homing feature. That is, the SCTP/DCCP multi-homing would operate on the IPv6 multi-homing for the services and applications in IPv6-based NGN. In this way, each SCTP/DCCP session will be made using multiple IPv6 addresses, which are given in a network layer.

In a transport layer, a user terminal (host) will be multi-homed to the access networks and further to the corresponding IPv6 host over multiple IPv6 addresses. In this regard, the transport layer multi-homing can be considered as the 'end-to-end host multi-homing', since the multi-homing connection will be established between the two end-to-end hosts, with the help of the host multi-homing in IPv6-based NGN.

Figure 7 shows a network model for the multi-homing in a transport layer.

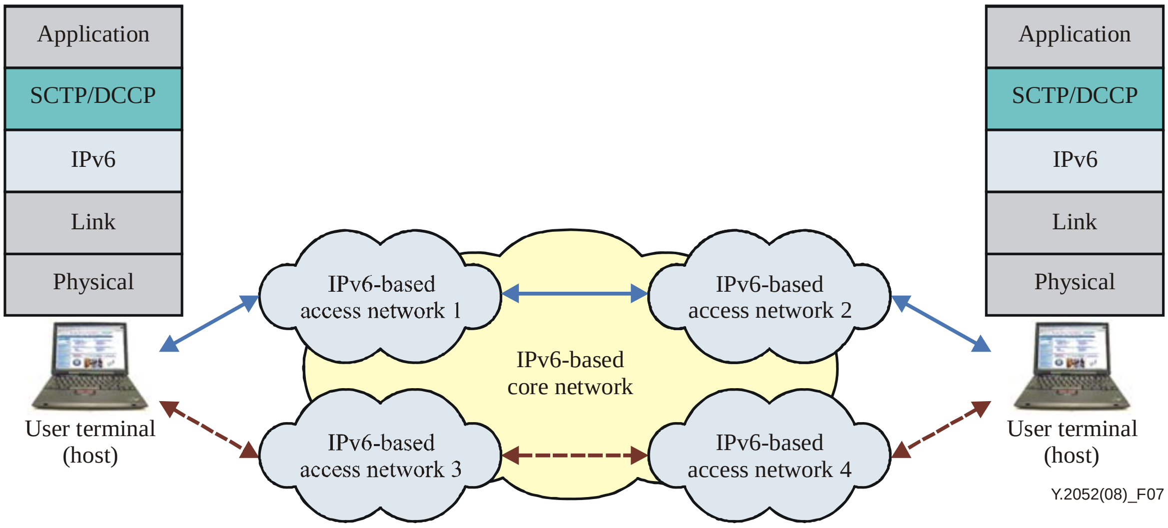

Figure 7 – Multi-homing with transport layer multi-homing

As shown in Figure 7, IPv6 multi-homing could also be used in the end-to-end transport layer between the two endpoints, with the help of the capability of multi-homing in the network layer. In the figure, the two IPv6 hosts are multi-homed to the networks, and establish multi-homed connections using the two IPv6 addresses. Those two hosts will use SCTP or DCCP as the associated transport protocol so as to exploit the capability of IPv6 multi-homing.

It needs to be noted that to exploit multi-homing in a transport layer, each IPv6 host needs to ensure that the upper-layer applications are made using SCTP or DCCP as the transport layer protocol. With the help of this transport layer multi-homing capability, IPv6-based NGN users could benefit from the NGN services and applications provided by the NGN service providers.

Typical application areas of the IPv6 transport layer multi-homing include:

– Fault tolerance with redundancy: to recover the host connection from the network failure.

– Session continuity across different access networks: to support the seamless handover.

9 Functional architecture to support multi-homing in IPv6-based NGN

9.1 Overall architecture to support multi-homing

The functional architecture in [ITU-T Y.2012] makes a clear distinction between the services aspects provided by the NGN (service stratum) and the data transport used to support those services (transport stratum). [ITU-T Y.2012] describes the functional architecture of the NGN. From the viewpoint of the functional architecture defined in [ITU-T Y.2012], this clause identifies the functions and functional elements used to support multi-homing features in IPv6-based NGN.

Multi-homing feature shall be realized in the NGN transport stratum. The NGN transport stratum is further classified into transport functions and transport control functions. The transport functions provide the connectivity for all components and physically separated functions within the NGN. It is noted that the purpose of multi-homing features is to provide multiple network connections between networks and hosts in IPv6-based NGN. Accordingly, multi-homing features shall be supported in NGN transport functions, which include access network functions, edge functions, and core transport functions. In Figure 8, functions associated with multi-homing features in IPv6-based NGN are marked as the shaded boxes.

Access network functions are used to deal with end-users' access to the network and collection/aggregation of the traffic coming from end users. In IPv6-based NGN, there might be a lot of heterogeneous access networks which use different access technologies. The access network function shall support multi-homing capability to provide multiple network connections to the users over a variety of heterogeneous access networks.

NGN edge functions are responsible for media and traffic processing for aggregated traffic coming from access networks toward the core network. There might be single or multiple network connections between access networks and the core network. To support multiple network connections between them, multi-homing capability shall be provided in the NGN edge function.

NGN core transport functions are used to interconnect a wide variety of access networks and to transport the services over the core network with a certain level of QoS provisioning. The multiple network connections might be used to enhance the QoS concerned with data transport over the core network. For this purpose, the core transport functions shall be able to support IPv6 multi-homing capability.

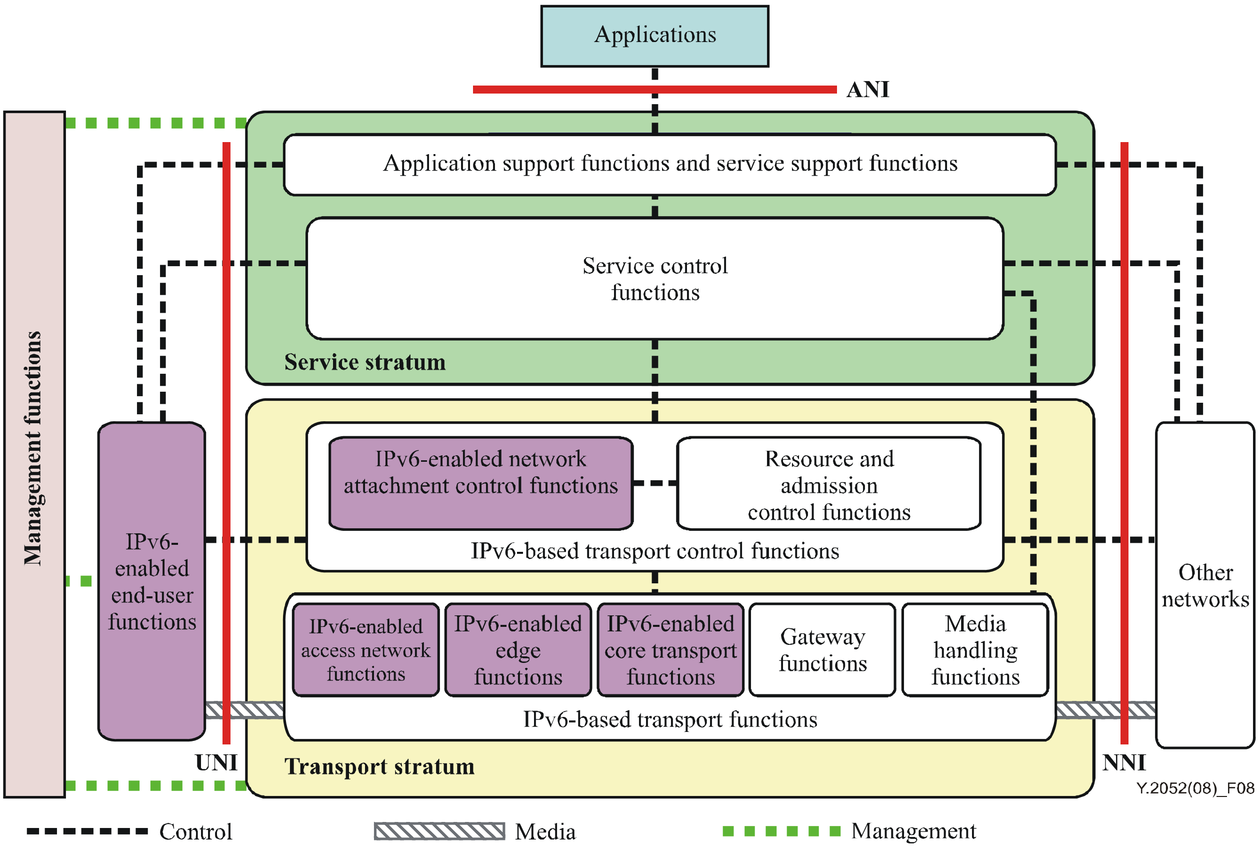

Figure 8 – NGN architecture related to multi-homing

In transport control functions, network attachment control functions (NACFs) shall be able to support IPv6 multi-homing. The NACF is responsible for dynamic configuration of IPv6 addresses and other configuration parameters associated with user equipment. Multi-homing capability shall be provided by NACF to support efficient IPv6 address allocation for multiple network connections.

Multi-homing shall also be supported in end-user functions. With the help of multi-homing in end-user functions, more enhanced services/applications could be provided for the user terminal with multiple network interfaces and multiple IPv6 addresses.

9.2 Functional architecture to support multi-homing

To provide more enhanced services and applications using multi-homing features in IPv6-based NGN, multi-homing capability shall be supported by the associated functional entities in

IPv6-based NGN. Figure 9 shows NGN functional entities associated with multi-homing in IPv6-based NGN. As shown in the figure, the functional entities (FEs) in NGN transport stratum are classified into access transport processing FEs and core transport processing FEs. In the figure, the FEs associated with multi-homing in IPv6-based NGN are marked as the shaded boxes.

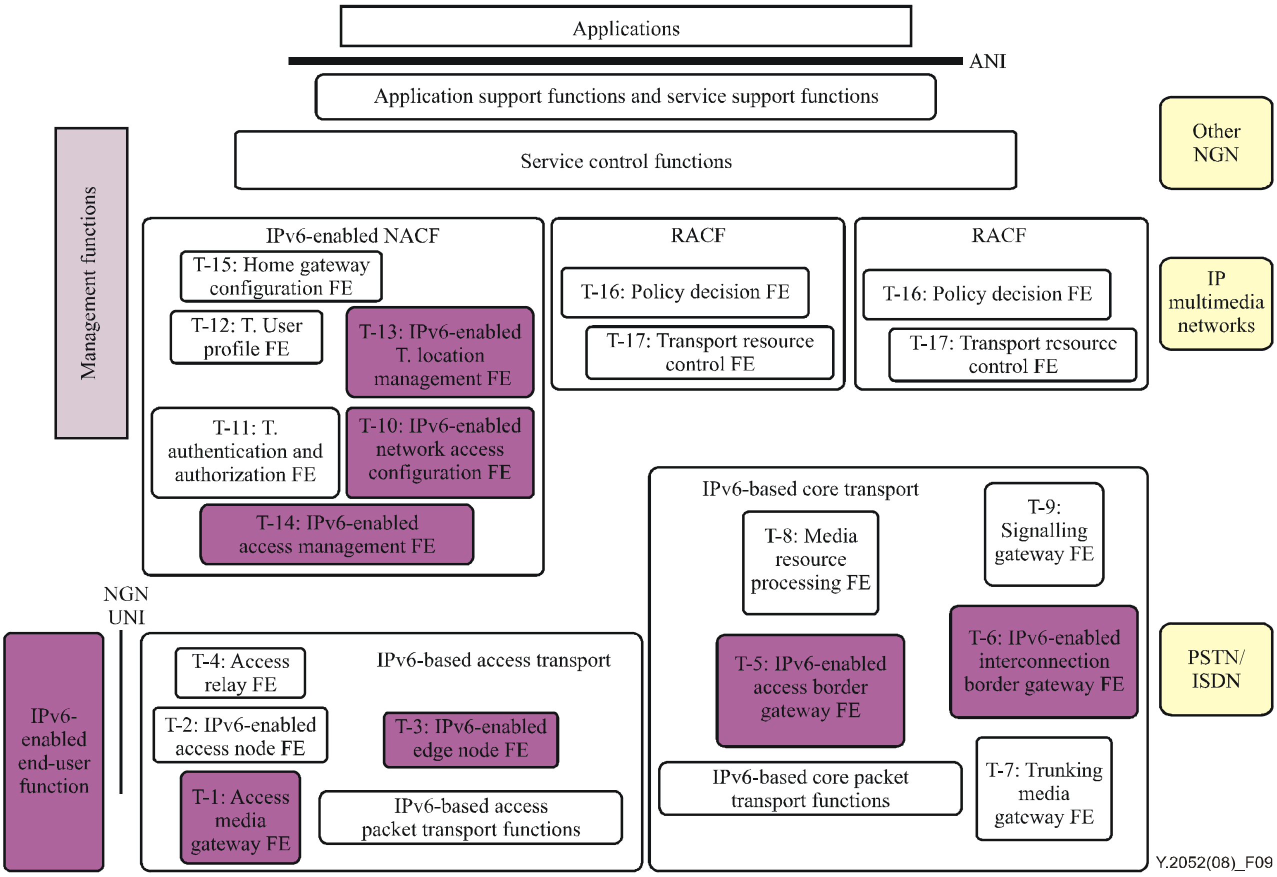

Figure 9 – NGN functional architecture related to multi-homing

T-2 access node FE in IP access network directly connects to end user functions and terminates the first/last mile link signals at the network side. The multiple network connections between access network and end user functions might be established by using the multi-homing features. For this purpose, multi-homing capability shall be supported in the T-2 access node FE.

T-3 edge node FE in the access packet transport functions is a layer 3 device with IP forwarding capabilities. Similarly to the T-2 access node FE, multiple network connections might be established between the access packet transport functions and core packet transport functions. Accordingly, multi-homing in IPv6-based NGN shall be supported in the T-3 edge node FE.

T-5 access border gateway FE is a packet gateway located between an access network and a core network. If T-3 edge node FE is responsible for packet processing at an access network side, T-5 access border gateway FE is responsible for packet processing at a core network side. In cooperation with T-3 edge node FE, access border gateway FE shall support multi-homing features.

T-6 interconnection border gateway FE is a packet gateway used to interconnect an operator's core transport network with another operator's core transport network. If there is an agreement between those different operators, multi-homing in IPv6-based NGN shall be supported in T-6 interconnection border gateway FE.

On the other hand, the FEs in the transport control processing FE are divided into NACF and resource and admission control functions (RACFs). The NACF includes T-10 network access configuration FE, T-13 transport location management FE, and T-14 access management FE. In particular, the NACF is associated with multi-homing in IPv6-based NGN. The relationship between multi-homing in IPv6-based NGN and RACF is for further study.

T-10 network access configuration FE is used to manage IPv6 address allocation and other network configuration parameters to terminals. For the terminals with multiple network interfaces, this FE might allocate multiple IPv6 addresses. For this purpose, multi-homing capability shall be supported by the T-10 network access configuration FE.

T-13 transport location management FE is used to manage the location information of the user equipment such as IPv6 addresses. To support the users with multiple IPv6 addresses, multi-homing capability shall be supported by this FE.

T-14 access management FE is used to handle the network access request issued by the user equipment. It forwards the request for allocation of an IPv6 address and possibly additional network configuration parameters. To support the users with multiple IPv6 addresses, multi-homing capability shall be supported by this FE.

10 Applications of multi-homing in IPv6-based NGN

This clause describes some examples of applications of multi-homing in IPv6-based NGN.

10.1 Always-on connectivity

In IPv6-based NGN, a user terminal might have the ability to always connect to networks (always-connect service). With this service feature, the NGN user could get more enhanced services. One access network cannot serve all service areas. If one typical wireless access technology is used in some access networks, the service coverage area of the access network is limited by the characteristics of wireless technology and the policy of operators. Access networks may be located in a distributable form. Some access networks may overlap with other access networks but others may not overlap with each other.

While providing the always-connect service in the NGN environment, a NGN user terminal could move from one access network to another access network with continuing ongoing service. In this case, a NGN user terminal might change network interfaces to choose the optimal network interface which can be used in each access network. In particular, more than two network interfaces can be used simultaneously.

Figure 10 shows a NGN user terminal moving across heterogeneous access networks using multiple network interfaces. (In this figure, we assume that each access network uses different access technologies.)

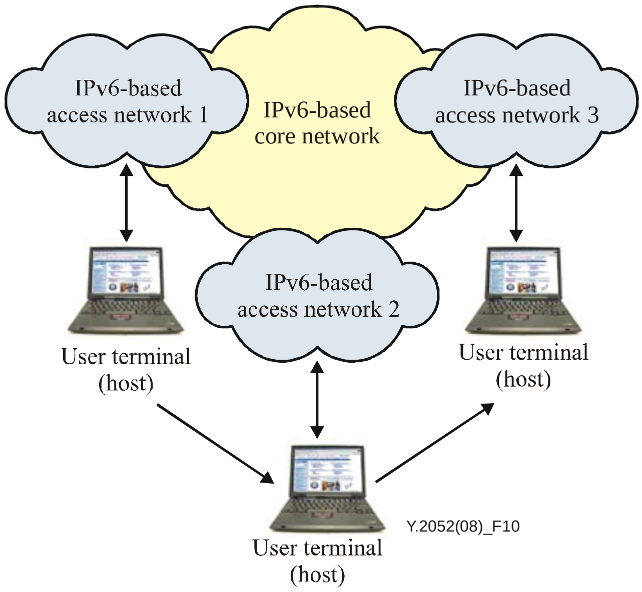

Figure 10 – User terminal moving across heterogeneous access networks with multiple network interfaces

In Figure 10, a NGN user terminal could move across heterogeneous access networks with continuing ongoing service. During the movement of a user terminal, not only IPv6 addresses but also network interfaces are changed because heterogeneous access technologies are used in each access network. Due to the multiple network interfaces of a user terminal and the multiple access networks, the NGN user terminal could be provided with the always-connect service.

Although broadband capabilities with end-to-end QoS are supported in NGN environments, it is difficult to eliminate the possibility of premature disconnection of network path. Even though advanced transport technology and efficient routing protocol may decrease the possibility of communication failure, protection against premature disconnection needs to be considered.

With multi-homing features, a NGN user terminal can have multiple IPv6 addresses and these IPv6 addresses can be routed via different paths. When a NGN user terminal is moving or a network path has some problems, multi-homing features could be used. Figure 11 shows a NGN user terminal which has multiple network connections with multiple IPv6 addresses.

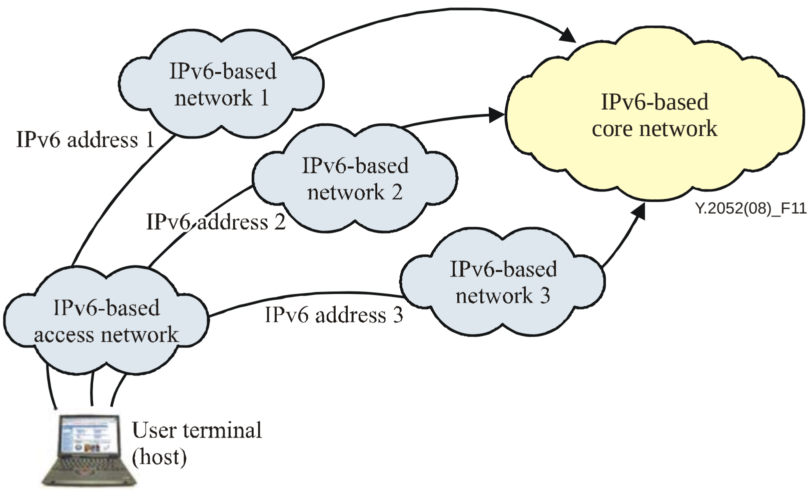

Figure 11 – User terminal using multiple IPv6 addresses

In Figure 11, the NGN user terminal uses three network addresses: IPv6 address 1, IPv6 address 2, IPv6 address 3. IPv6 address 1 is used to route through IPv6-based network 1; IPv6 address 2 is used to route through IPv6-based network 2 and IPv6 address 3 is used to route through IPv6-based network 3. At some point, the NGN user terminal uses IPv6 address 1 and, after some time, a user terminal uses IPv6 address 2 or IPv6 address 3. In this case, a user terminal might have the ability to always connect to the core network with multiple IPv6 addresses irrespective of network problems, such as network failure or traffic congestion.

10.2 Load sharing

In general, the 'traffic load-sharing' scheme could be used to effectively utilize the network or link bandwidth. In the scheme, the overall traffic might be delivered in a balanced way towards each of the multiple connections.

More specifically, load sharing could be implemented using the following multi-homing features:

– host multi-homing in the network layer;

– site multi-homing in the network layer.

Figure 12 shows a scenario of load sharing using host multi-homing in a network layer.

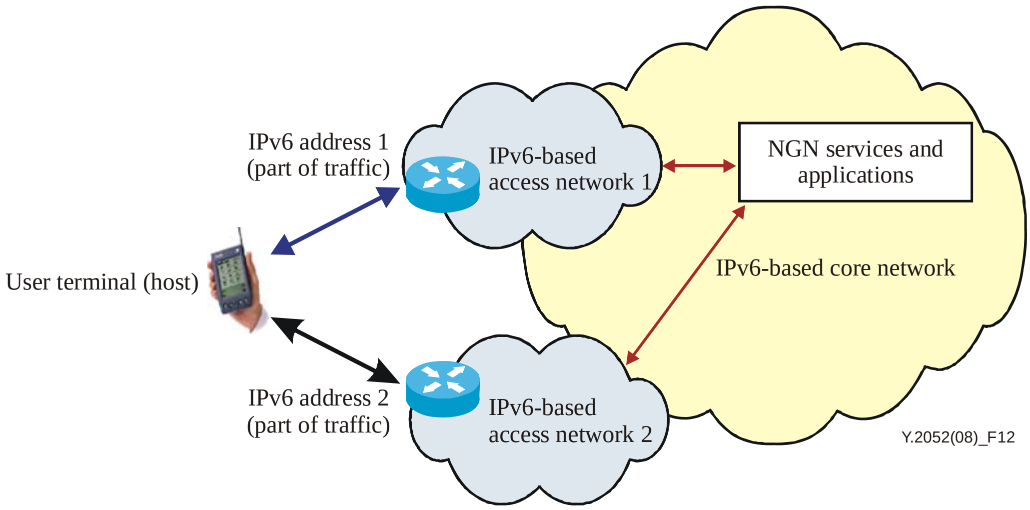

Figure 12 – Load sharing using host multi-homing

In Figure 12, the user terminal transmits its traffic over both IPv6 address 1 and IPv6 address 2. For the purpose of load sharing, a part of the traffic emitted from the user terminal will be forwarded to IPv6-based access network 1 via IPv6 address 1, whereas the remaining traffic will be delivered to IPv6-based access network 2 via IPv6 address 2. In this way, the overall traffic could be balanced and shared by the two network links attached to the user terminal.

This load-sharing scheme could also be applied using site multi-homing in the network layer. In this scenario, the aggregated traffic from the site will be forwarded to the different access networks via the aggregate router (or gateway) of the site network.

10.3 Traffic engineering

In general, the 'traffic engineering' scheme could be used to efficiently route the traffic based on the current status of the network. For example, if one transit network is overwhelmingly loaded or congested at a specific moment, the traffic will be forwarded to the other transit network so as to alleviate the network load of the congested network and to optimize the routing path. More specifically, traffic engineering could be implemented using the site multi-homing in the network layer.

Figure 13 shows a scenario of the traffic engineering using site multi-homing in a network layer.

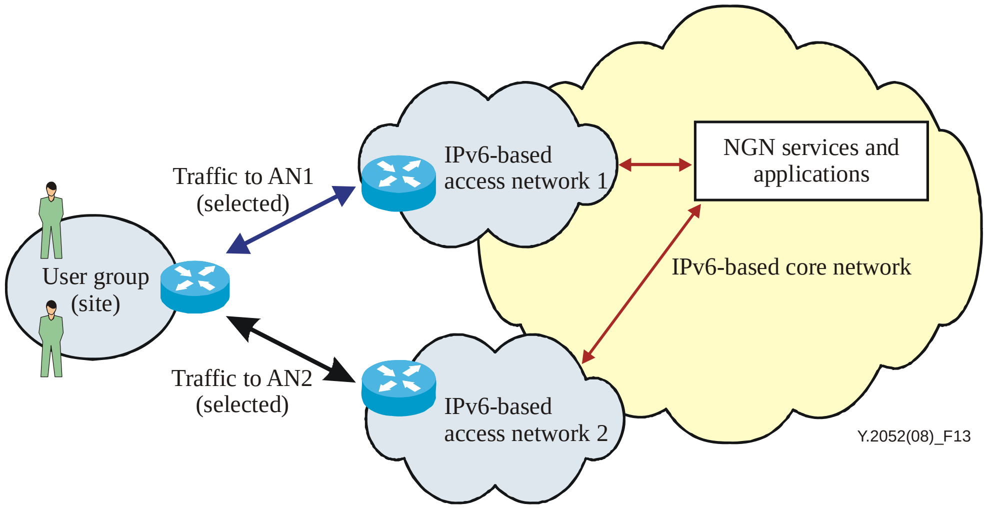

Figure 13 – Traffic engineering using site multi-homing

In Figure 13, the gateway (router) of the site network would transmit the outgoing traffic to IPv6-based core network by using IPv6-based access network 1 or IPv6-based access network 2, which will be selected on the current status of the concerned access networks. For the purpose of traffic engineering, the gateway (router) of the site might have its own policy (or rules) for traffic routing. In this manner, the overall traffic could be routed in an optimized way to one of the two access network links attached to the site.

10.4 Fault tolerance with redundancy

In general, the 'fault tolerance' scheme could be used to recover traffic from failure in the network (e.g., a critical error in the transmission, collapse of the network devices, etc.). To provide fault tolerance, the session between two end-to-end hosts will require redundancy (e.g., a backup path).

For the purpose of this fault tolerance, multi-homing capability could be used. The associated redundancy could be provided by establishing two different end-to-end paths: the primary and backup paths. In the scheme, the backup path will be used between two end hosts when a network fault occurs.

More specifically, the fault tolerance with redundancy could be implemented using the following multi-homing features:

– host multi-homing in the network layer;

– end-to-end multi-homing in the transport layer.

It is noted that to utilize the fault tolerance with redundancy, each user terminal needs to use a transport protocol that is aware of transport-layer multi-homing (e.g., SCTP or DCCP).

Figure 14 shows a scenario of fault tolerance with redundancy using host multi-homing in the network layer.

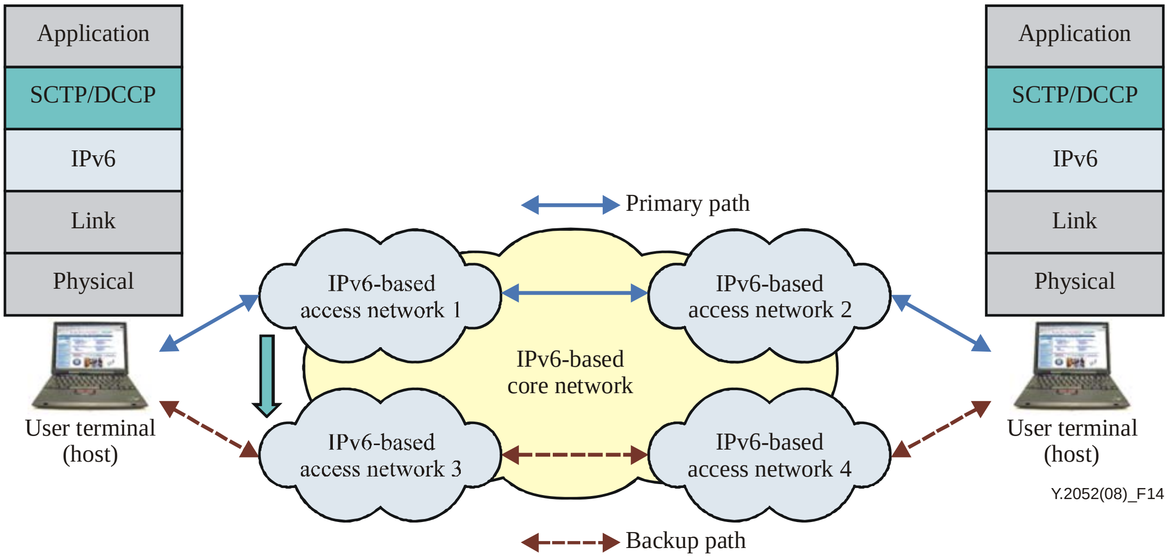

Figure 14 – Fault tolerance with redundancy using host multi-homing

In Figure 14, the user terminal initially transmits its traffic over the IPv6 primary address (path). When a network failure is detected, the IPv6 host will use the IPv6 backup address (path). For the purpose of fault tolerance, the concerned user terminal should be multi-homed to the network in the network and transport layer.

10.5 Session continuity across access networks

In IPv6-based NGN environment, the network consists of an IPv6-based core network and a variety of IPv6-based access networks using the different wireline and wireless access technologies. In the NGN, one of the primary goals is to provide the session continuity for a NGN user terminal that is moving across the heterogeneous access networks.

Multi-homing features could be used to provide this session continuity across the different access networks for the NGN user terminal. More specifically, the session continuity across access networks could be implemented using end-to-end multi-homing in the transport layer. It is noted that to provide the session continuity for the moving NGN user terminal, each user terminal needs to use a transport protocol that is aware of transport-layer multi-homing (e.g., SCTP).

The SCTP, as defined in [b-IETF RFC 2960], is the third transport layer protocol following TCP and UDP. SCTP is featured by having multi-streaming and multi-homing, differently from TCP. It is noted that the multi-homing feature of SCTP enables the SCTP to support the session continuity for the moving user terminal.

In particular, the recent works of SCTP include the dynamic 'Address Configuration' extension, which enables the SCTP/IPv6 host to dynamically add or delete the IPv6 addresses during the session. This feature of SCTP can be used to provide session continuity for the NGN user terminal that is moving across different IPv6 network regions during the active session.

Table 1 summarizes multi-homing features and their promising applications in IPv6-based NGN. The table describes how multi-homing features can be used preferably in the respective application areas. In the table, transport-layer multi-homing will be exploited together with the underlying host multi-homing in the network layer.

Table 1 – Multi-homing features and applications

Layer	Multi-homing features	Applications				
		Always-on connectivity	Load sharing	Traffic engineering	Fault tolerance	Session continuity
Network	Site	Not applicable	More applicable	More applicable	Could be applied	Not applicable
Network	Host	More applicable	Applicable	Applicable	Applicable	Applicable
Transport	Host	Could be applicable	Not applicable	Not applicable	More applicable	More applicable

11 Security considerations

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

Appendix I

Session continuity using multi-homing

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

This appendix describes one typical session continuity mechanism using multi-homing.

Let us consider a mobile client that initiates an SCTP association with a fixed server in IPv6-based NGN networks. After initiation of an SCTP association, the mobile client moves from location A (access router A) to location B (access router B).

Figure I.1 illustrates an example of the use of SCTP for session continuity in multi-homing networks.

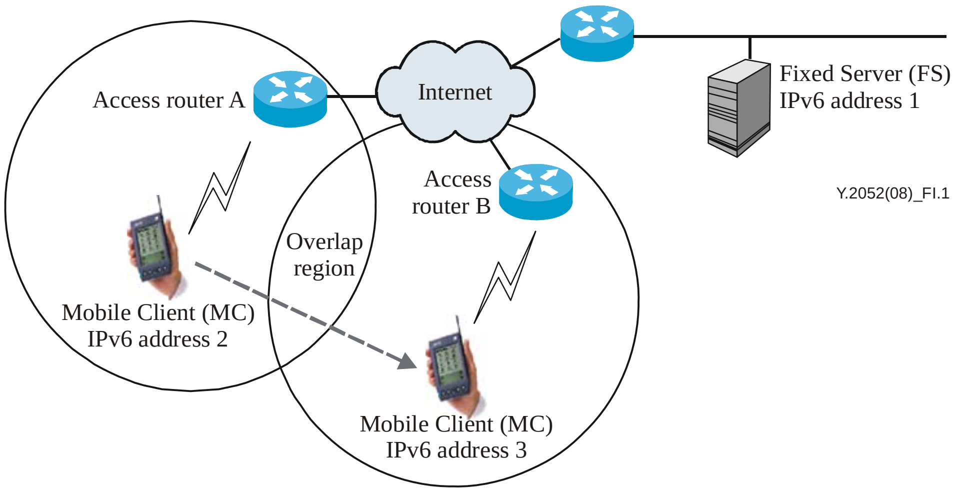

Figure I.1 – Session continuity using transport layer multi-homing

The scheme for the session continuity can be summarized as follows:

a) *Session initiation by mobile client*

We assume that a mobile client initiates an SCTP association with a fixed server. The resulting SCTP association has the set of IPv6 addresses with IPv6 address 2 for mobile client and IPv6 address 1 for fixed server. It is also assumed that the mobile client gets an IPv6 address from access router A, with help of IPv6 stateless address autoconfiguration or dynamic host configuration protocol for IPv6 (DHCPv6)

Note that in this phase the fixed server is in single homing with IPv6 address 1. The mobile client is also in single homing in the initial state, in which IPv6 address 2 is set to its primary IPv6 address in the SCTP initiation process.

b) *Obtaining an IPv6 address for a new location*

Let us assume that the mobile client moves from access router A to access router B and thus it is now in the overlapping region. In this phase, we also need to assume that the mobile client can obtain a new IPv6 address 3 from access router B by using DHCPv6 or IPv6 stateless address autoconfiguration.

By SCTP implementations, the newly obtained IPv6 address 3 must be signalled or informed to the SCTP in the transport layer, and then the SCTP will bind the new IPv6 address to its address list managed by the SCTP association.

c) *Adding the new IPv6 address to the SCTP association*

After obtaining a new IPv6 address, the mobile client's SCTP informs the fixed server that it will use a new IPv6 address. This is done by sending a SCTP address configuration chunk to the fixed server. The mobile client may receive the responding address configuration-acknowledgement chunk from the fixed server.

The mobile client is now in the dual homing state. The old IPv6 address (IPv6 address 2) is still used as the primary address, until the new IPv6 address 3 will be set to be the "Primary Address" by the mobile client. Before the primary address is newly set, IPv6 address 3 will be used as a backup path.

d) *Changing the primary IPv6 address*

While the mobile client further continues to move toward access router B, it needs to change the new IPv6 address into its primary IPv6 address according to the appropriate rule. Actually, the configuration of a specific rule to trigger this "primary address change" is a challenging issue for the mobile SCTP.

Once the primary address is changed, the fixed server will send the incoming data over the new primary IPv6 address, whereas the backup (old) IPv6 address may be used to recover the lost data chunks.

e) *Deleting the old IPv6 address from the SCTP association*

As the mobile client progresses to move towards access router B, if the old IPv6 address becomes inactive, the mobile client must delete it from the address list. The rule for determining if the IPv6 address is inactive may also be implemented by using additional information from the underlying network or physical layer.

The procedural steps described above (step a through e) will be repeated whenever the mobile client moves to a new location, until the SCTP association is released.

Bibliography

[b-ITU-T E.800] Recommendation ITU-T E.800 (1994), *Terms and definitions related to quality of service and network performance including dependability*.

[b-ITU-T Q.1702] Recommendation ITU-T Q.1702 (2002), *Long-term vision of network aspects for systems beyond IMT-2000*.

[b-ITU-T Y.2001] Recommendation ITU-T Y.2001 (2004), *General overview of NGN*.

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

[b-IETF RFC 2260] IETF RFC 2260 (1998), *Scalable Support for Multi-homed Multi-provider Connectivity*. <http://www.ietf.org/rfc/rfc2260.txt?number=2260>

[b-IETF RFC 2772] IETF RFC 2772 (2000), *6Bone Backbone Routing Guidelines*. <http://www.ietf.org/rfc/rfc2772.txt?number=2772>

[b-IETF RFC 2894] IETF RFC 2894 (2000), *Router Renumbering for IPv6*. <http://www.ietf.org/rfc/rfc2894.txt?number=2894>

[b-IETF RFC 2960] IETF RFC 2960 (2000), *Stream Control Transmission Protocol*. <http://www.ietf.org/rfc/rfc2960.txt?number=2960>

[b-IETF RFC 3582] IETF RFC 3582 (2003), *Goals for IPv6 Site-Multihoming Architectures*. <http://www.ietf.org/rfc/rfc3582.txt?number=3582>

[b-IETF RFC 4116] IETF RFC 4116 (2005), *IPv4 Multihoming Practices and Limitations*. <http://www.ietf.org/rfc/rfc4116.txt?number=4116>

[b-IETF RFC 4177] IETF RFC 4177 (2005), *Architectural Approaches to Multi-homing for IPv6*. <http://www.ietf.org/rfc/rfc4177.txt?number=4177>

[b-IETF RFC 4218] IETF RFC 4218 (2005), *Threats relating to IPv6 Multihoming Solutions*. <http://www.ietf.org/rfc/rfc4218.txt?number=4218>

[b-IETF RFC 4219] IETF RFC 4219 (2005), *Things Multihoming in IPv6 (MULTI6) Developers Should Think About*. <http://www.ietf.org/rfc/rfc4219.txt?number=4219>

[b-IETF RFC 4340] IETF RFC 4340 (2006), *Datagram Congestion Control Protocol (DCCP)*. <http://www.ietf.org/rfc/rfc4340.txt?number=4340>

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