International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2059

(07/2012)

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

Next Generation Networks – Frameworks and functional architecture models

Functional requirements for accessing IPv6-based next generation networks

Recommendation ITU-T Y.2059

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
IPTV over NGN	Y.1900–Y.1999
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
Packet-based Networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
FUTURE NETWORKS	Y.3000–Y.3499
CLOUD COMPUTING	Y.3500–Y.3999

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

Recommendation ITU-T Y.2059

Functional requirements for accessing IPv6-based next generation networks

Summary

Recommendation ITU-T Y.2059 provides the impact study, scenario analysis and functional requirements for the networks which are connected to the IPv6-based NGN. It involves both the access network side and the core network side of NGN.

All the analysis is basically divided into two aspects, which are IPv6 connectivity and IPv4-compatible connectivity. IPv6 connectivity focuses on IPv6-only network provision which contains prefix and address allocation, configuration, etc. IPv4-compatible connectivity focuses on IPv4-to-IPv6 transition technologies that continue to provide IPv4 services to users.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T Y.2059	2012-07-29	13

Keywords

IPv6, IPv6 network access, 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/.

Table of Contents

Page

Recommendation ITU-T Y.2059

Functional requirements for accessing IPv6-based next generation networks

1 Scope

The objective of this Recommendation is to identify impacts on networks which are connected to the IPv6-based NGN, and to describe the relevant scenarios/models in order to identify the functional requirements.

NGN transport stratum functions provide a series of transport and transport control functions that support the service stratum features. In IPv6, some mechanisms have been already introduced to support both transport and transport control functions in order to perform the access to the IPv6-based NGN. Along with IPv6, the devices in network also have relevant functional requirements. This Recommendation covers:

– identification of the impact on networks which are connected to IPv6-based NGNs;

– network access scenarios specific to the NGN, including parameter configurations such as prefix, address and server configurations;

– scenarios of access network level registration in IPv6-based NGNs;

– functional requirements for networks which are connected to IPv6-based NGNs.

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

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

[ITU-T Y.2053] Recommendation ITU-T Y.2053 (2008), *Functional requirements for IPv6 migration in NGN.*

[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 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.

3.1.2 NAT64 [b-IETF RFC 6146]: A mechanism for IPv4-IPv6 transition and IPv4-IPv6 coexistence. Together with DNS64, these two mechanisms allow an IPv6-only client to initiate communications to an IPv4-only server.

3.1.3 next generation network [ITU-T Y.2001]: A packet-based network able to provide telecommunication services and to make use of multiple broadband, (QoS)-enabled transport technologies and in which service-related functions are independent from underlying transport-related technologies. It enables unfettered access for users to networks and to competing service providers and/or services of their choice. It supports generalized mobility which will allow consistent and ubiquitous provision of services to users.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 DNS64 (based on [b-IETF RFC 6147]): A mechanism for synthesizing IPv6 DNS [b-IETF RFC 1035] records from IPv4 DNS records. DNS64 is used with an IPv6/IPv4 translator to enable client-server communication between an IPv6-only client and an IPv4-only server, without requiring any changes to either the IPv6 or the IPv4 node for the class of applications that work through NATs.

3.2.2 tunnel concentrator: A function/device that terminates multiple tunnels from a user side, concentrates traffic carried by the tunnels, and forwards the traffic to a new tunnel towards a network side, so that the number of tunnels to be handled by the network is reduced.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AAAA	Authentication, Authorization, Accounting and Auditing
CGA	Cryptographically Generated Address
CPE	Customer Premises Equipment
DHCPv6	Dynamic Host Configuration Protocol version 6
DNS	Domain Name Service
DUID	DHCP Unique Identifier
FE	Functional Entity
ID	Identifier
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISP	Internet Service Provider
LAN	Local Area Network
MAC	Media Access Control
NACF	Network Attachment Control Function
NAT	Network Address Translation
ND	Network Discovery
NGN	Next Generation Network
OAM	Operation and Maintenance
PD	Prefix Delegation

PPP	Point-to-Point Protocol
RA	Router Advertisement
RACF	Resource and Admission Control Function
RS	Router Solicitation
UE	User Equipment
VLAN	Virtual Local Area Network
WAN	Wide Area Network

5 Conventions

None.

6 Impact on network functions for accessing the IPv6-based NGN

IPv6 is different from IPv4 in various aspects. To access the IPv6-based NGN, the basic approach is to provide IPv6 connectivity, which includes mainly prefix/address provisioning and allocation. An IPv6 address is composed of prefix and interface ID. Existing mechanisms provide different methods to configure the prefixes and addresses. Besides the IPv6 connectivity, the network also needs to support the old IPv4 users to access the IPv6-based NGN. Further, IPv6 security requirements are also different from the security requirements of IPv4. This clause identifies these mechanisms and describes how they impact network access.

6.1 IPv6 connectivity provision

6.1.1 Prefix and address space

The IPv6 address is 128 bits long. The most common addressing architecture is 64 bits for the network number (prefix) and 64 bits for the host number (interface ID). IPv6 has a more complex addressing architecture than IPv4. With a huge IPv6 address space and a complex prefix structure, the following impact on network access the IPv6-based NGN should be considered.

- Address availability and reachability: A user can have one or more globally unique IPv6 addresses. The problems caused by a limited IPv4 address space would not exist any longer. It should be technically easy and efficient for every user who wants to obtain a globally unique IPv6 address. Users can be considered globally reachable via the obtained IPv6 address. The adoption of IPv6 addresses impacts network address translation techniques, which may be reduced or even abandoned in IPv6 networks.

  In IPv6, the scope of the address is embedded in part of the address structure. Unicast addresses have three defined scopes, including link-local, unique link-local and global. Default address selection for both source and destination takes scope into account. The address scope impacts address acquisition by the user terminal, the bootstrapping sequence of customer premises equipment (CPE) interfaces, etc.

- Prefix structure: The address mask is used in IPv4 to distinguish the network portion from the host portion. The address mask is not used in IPv6; instead, address prefix is used to distinguish the sub-network prefix of an address. IPv6 has its own way of performing the prefix advertisement and delegation in order to organize the prefix in a manageable way for service providers or customers. User equipment should be able to easily get the prefix.

6.1.2 Prefix and address allocation mechanism

IPv6 supports both stateful and stateless address configuration. The relevant mechanisms have already been standardized in IETF, including DHCPv6 [b-IETF RCF 3315], neighbour discovery for IPv6 [b-IETF RFC 4861], IPv6 stateless address auto configuration [b-IETF RFC 4862], IPv6 prefix options for DHCPv6 [b-IETF RFC 3633] and a number of other RFCs and Recommendations. Prefix and address allocation mechanisms in IPv6 are different from those in IPv4. They impact the following aspects:

- CPE side: The CPE is a connection point between the home network and the access/aggregation network. It may employ different prefix and address allocation mechanisms on LAN and WAN interfaces. A user's network access depends greatly on the functions and features provided by the CPE.
- Network side: The operators can have their own way for advertising prefixes and configuring addresses. In some cases, both stateful and stateless address configuration may be used simultaneously. Some network nodes should be aware of the IPv6 signalling in order to help and monitor the IPv6 data transport.

6.1.3 Multiple addresses

One of the important features of IPv6 is that it allows multiple addresses to be assigned to an interface. The feature could be utilized in many scenarios such as mobile IPv6 and multi-homing. Besides, IPv6 addresses also have different scopes such as link-local and global. These features are included in the IPv6 standard protocols. So, it may be very common to have multiple addresses in one node in the IPv6-based NGN.

Multiple addresses with different scopes will bring new requirements to the access network for node configuration.

6.2 IPv4-compatible connectivity provision

There is consensus in industry that IPv4-IPv6 transition will take a long time. While IPv6 is incrementally deployed, IPv4 services must continue for a while. So the impact on the access network can be considered in light of the following aspects:

- Dual-stack: Some devices (such as hosts, CPE and edge routers) may need to be upgraded to support both IPv4 and IPv6 protocols based on the transition solution selected by the ISP.
- Tunnels: Set-up of tunnels, such as IPv6-in-IPv4, may be needed.
- Address/protocol translation: IPv4-IPv6 interaction has to involve address/protocol translation mechanisms such as NAT64 [b-IETF RFC 6146] and DNS64 [b-IETF RFC 6147].

6.3 Security

6.3.1 Access network level registration

Access network level registration involves the identification, authentication and authorization procedures between the CPE and the network attachment control function (NACF) in the NGN to control access. It basically includes the implicit authentication and explicit authentication.

- Implicit authentication: A node connects to a network through a physical wired-link, and it can obtain some information only through the link (for example, the telephone signalling or the IP addresses), so the link establishment itself can be considered as an implicit authentication.

  IPv6 has both stateful and stateless configurations. It may impact the ways of obtaining the link information and how nodes or functions deal with the information.

- Explicit authentication: Explicit identifiers and/or credentials are used for authentication. IPv6 may have different methods for presenting those identifiers and/or credentials. It may impact the flow of explicit authentication in various access scenarios, e.g., PPP, IP access, etc.

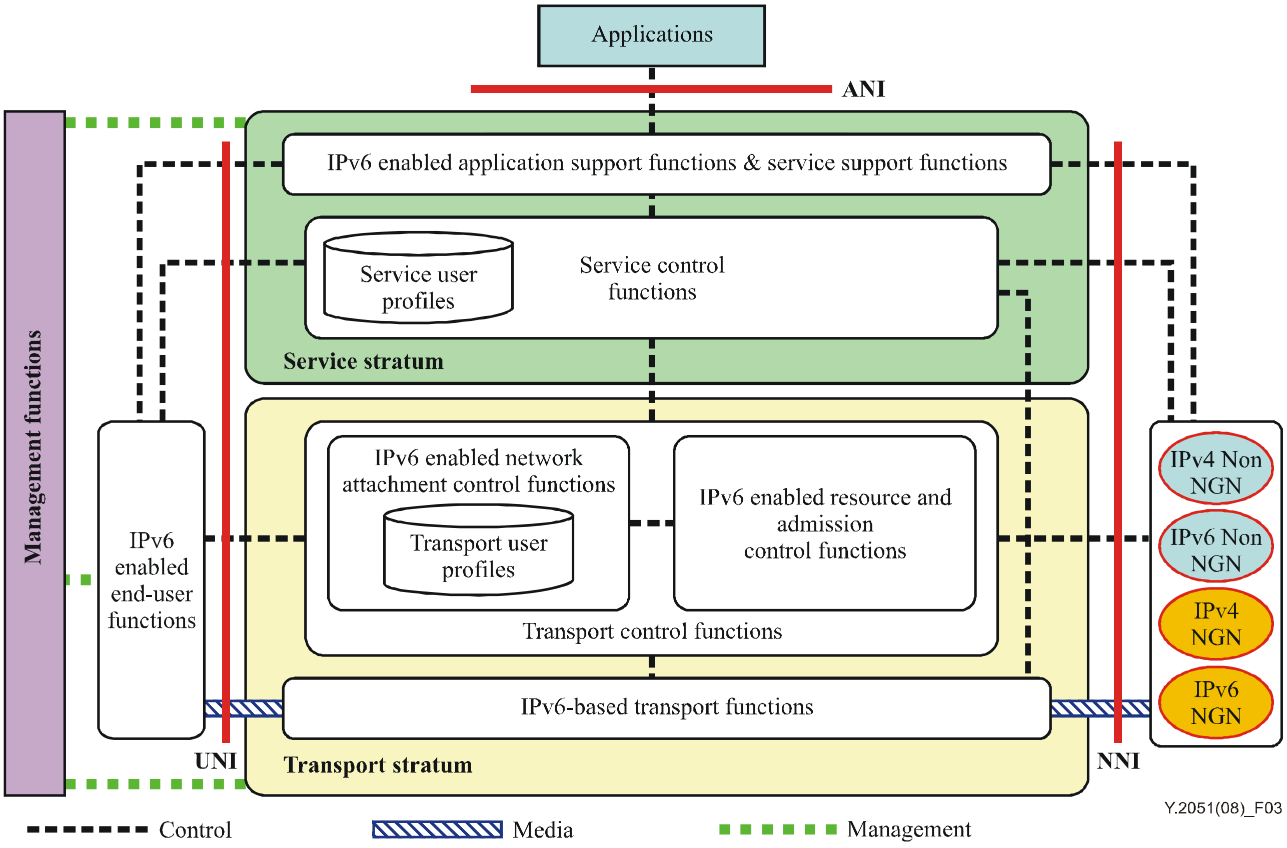
6.3.2 Source address validation and filtering

The access network should usually perform source address validation and filtering for user data transport. In an IPv4 access network, source address validation and filtering is normally based on the IP address/MAC/VLAN/port binding information. IPv6 has separate mechanisms for prefix and address allocation and has different scoped addresses. It adds complexity to the source address validation and impacts user access.

7 Scenarios and parameter configurations for accessing the IPv6-based NGN

There are various scenarios and parameter configurations possible in the IPv6-based NGN, e.g., stateless IPv6 prefix/address provisioning, stateful IPv6 prefix/address provisioning and prefix delegation combined with stateful or stateless address configuration. Various scenarios are explained in this clause.

Figure 1 shows the functional architecture of the IPv6-based NGN in [ITU-T Y.2051].



Applications
ANI
Management functions
IPv6 enabled application support functions & service support functions
Service user profiles
Service control functions
Service stratum
IPv6 enabled end-user functions
IPv6 enabled network attachment control functions
Transport user profiles
IPv6 enabled resource and admission control functions
Transport control functions
IPv6-based transport functions
Transport stratum
UNI
NNI
IPv4 Non NGN
IPv6 Non NGN
IPv4 NGN
IPv6 NGN
Y.2051(08)_F03
Control
Media
Management

Figure 1 – Functional architecture of the IPv6-based NGN

IPv6-based transport functions can be further decomposed as access network functions, edge functions, core transport functions, gateway functions and media handling functions, which are all IPv6 compatible. For users connecting to the networks, it is highly related to access network functions and edge functions; at the same time, other functions may be involved depending on the scenarios. Considering that transport control functions interact with transport functions, IPv6 enabled network attachment control functions should work closely with the relevant transport functions. IPv6 enabled end-user functions include a series of CPE and terminal functions, which closely cooperate with transport function and transport control functions. The service stratum is at the higher level and is not directly related to network access. Figure 2 shows the network architecture for network access and Figure 3 gives the logical presentation of the architecture.

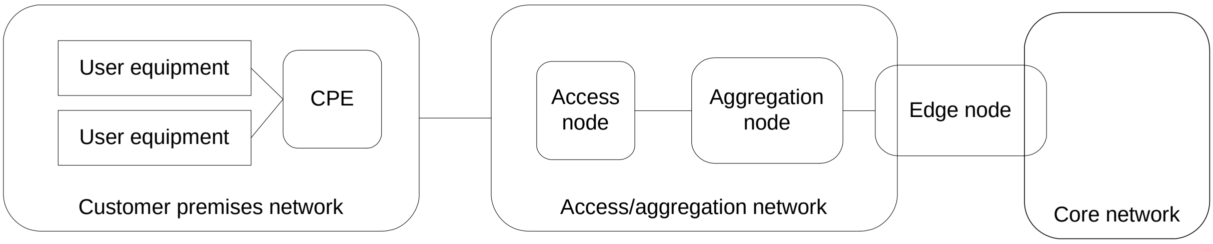


Figure 2 – Network architecture of network access

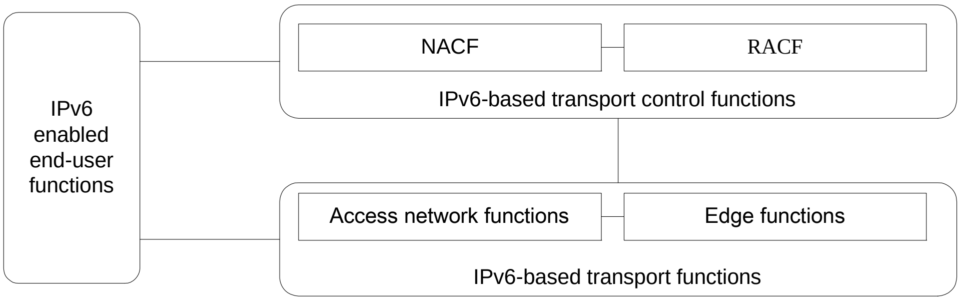

IPv6 enabled end-user functions
NACF
RACF
IPv6-based transport control functions
Access network functions
Edge functions
IPv6-based transport functions

Figure 3 – Logical architecture of network access

7.1 IPv6 connectivity provisioning

7.1.1 Prefix/address configuration

In most access networks, the prefix should be configured in a structured manner. The configuration can be either static or dynamic. There are two major dynamic ways to advertise the prefix: via router advertisement and via DHCPv6 prefix delegation. The purpose of prefix/address configuration in network access, as shown in Figure 4, is to make sure every CPE can be uniquely identified and be assigned a proper prefix value. It helps in maintaining the IPv6-user profiles in a structured manner and making OAM easier.

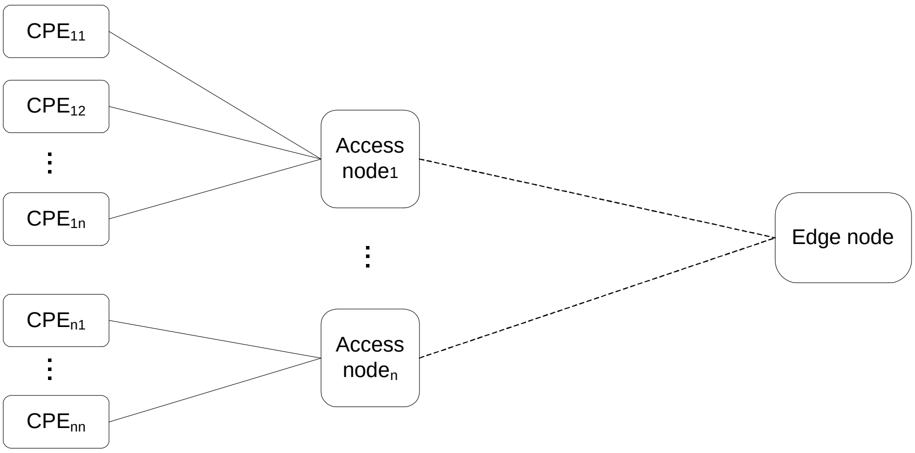


Figure 4 – Network element structure for network access

7.1.1.1 Static provisioning

In static provisioning, access nodes are statically configured with some information (e.g., delegation configuration) for helping subsequent prefix and address configuration. For easy maintenance, access nodes usually need to advertise a specific sub-network prefix per downstream interface. Hence, the configuration information should be provisioned based on the mapping relationship between the prefix received from the upstream interface and the prefix which should be advertised on each downstream interface. An access node receives the router advertisements from the edge node with the prefix information, determines the prefix to be advertised on the downstream interface based on the provisioned information, and then sends the router advertisements with that prefix to the downstream interface.

There are different methods to provide the network access services which include OAM methods and access node configuration protocol. According to the method used to present configuration information, different objectives or effects can be achieved, such as provisioning sub-network prefix based on services or always provisioning a CPE with a relatively static prefix. Static provisioning can fulfil different provisioning requirements in various scenarios. Figure 5 gives an example of the static provisioning scenario.

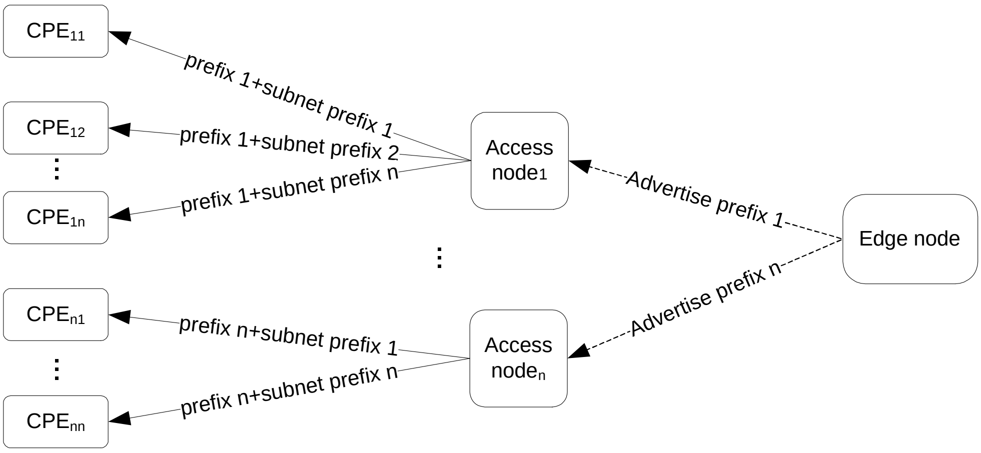


Figure 5 – Example of static provisioning scenario

7.1.1.2 Dynamic advertising

In some scenarios, an edge node may want to control the prefix/address configuration and advertisement for individual CPEs regardless of the structure or hierarchy of the access network. In such a scenario, the edge node should advertise the proper prefix to the different CPEs. In order to do that, the access node needs to inform the edge node about its identification information when forwarding the prefix request from the CPE to the edge node. The identification information may include the downstream port number of the access node, access node ID and/or other parameters. When the edge node receives the prefix request with the CPE identification information, it performs the authentication, authorization and accounting procedures for the prefix of the CPE, which should be advertised to the CPE.

Figure 6 shows an example of the dynamic advertising scenarios. The edge node dynamically provides prefix information based on the hint given by the access nodes.

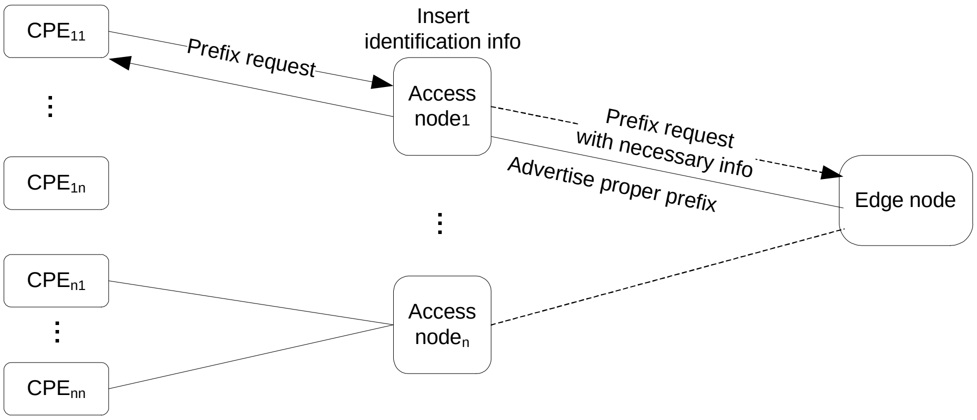


Figure 6 – Example of dynamic advertising scenario

7.1.1.3 Cascading delegation

As the IPv6 global address has high availability, it can be expected that a more complicated home network structure will be supported. Cascading prefix delegation is one of the possible examples in home networks as shown in Figure 7. The edge node or dynamic host configuration protocol (DHCPv6) server embedded in the edge node sends a delegated prefix to a CPE. With the existence of the cascaded router, multiple sub-networks may coexist in the home network behind the CPE. Thus, the CPE should send the cascaded prefix further down.

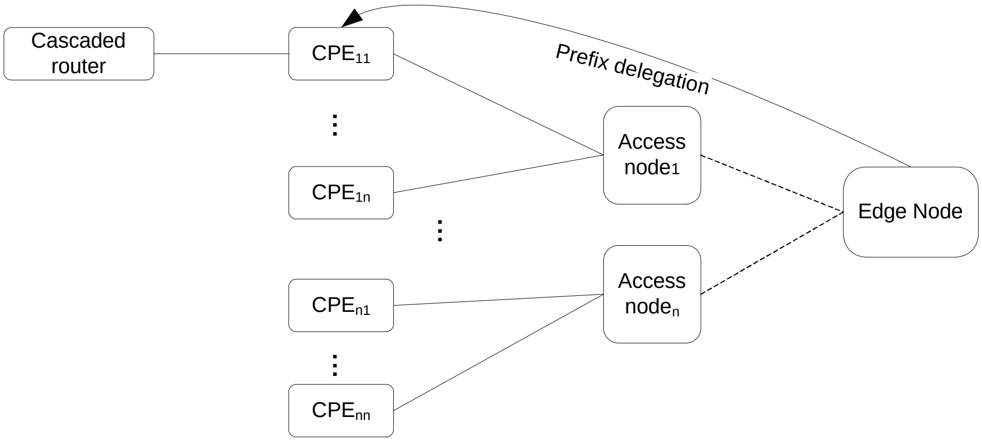


Figure 7 – Example of cascading prefix delegation

With proper prefix delegation management, the CPE gets the delegated prefix and the rule or policy indications for the cascaded delegation in the home network. Different mechanisms can be employed including DHCPv6, terminal management protocol and PPP. The rule or policy indication maps to the cascaded prefix extension. The CPE extends the prefix based on the cascaded prefix extension value and delegates that prefix to the cascaded router.

With the cascading delegation scenario, prefixes can be delegated down several levels under the control of the operator.

7.1.1.4 Prefix renumbering

Sometimes the prefix needs to be renumbered for various reasons, such as an address allocation change made by the operator, the changes of internal network topology or an authorization method change made by a policy server. In the case of renumbering, the CPE should update both the delegated prefix and its WAN interface prefix.

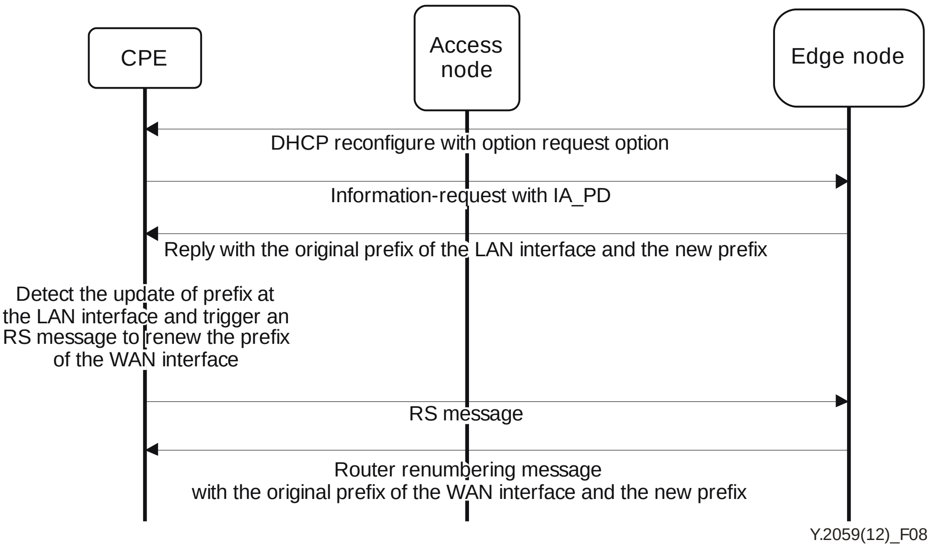

CPE
Access node
Edge node
DHCP reconfigure with option request option
Information-request with IA_PD
Reply with the original prefix of the LAN interface and the new prefix
Detect the update of prefix at the LAN interface and trigger an RS message to renew the prefix of the WAN interface
RS message
Router renumbering message with the original prefix of the WAN interface and the new prefix
Y.2059(12)_F08

Figure 8 – DHCPv6-triggered prefix renumbering

In the example of prefix renumbering shown in Figure 8, the edge node initiates the prefix renumbering by sending a DHCPv6 reconfiguration message to announce the change of the delegated prefix to the CPE. After proper prefix delegation management, the CPE updates the delegated prefix and triggers an RS message to renew the prefix of its WAN interface.

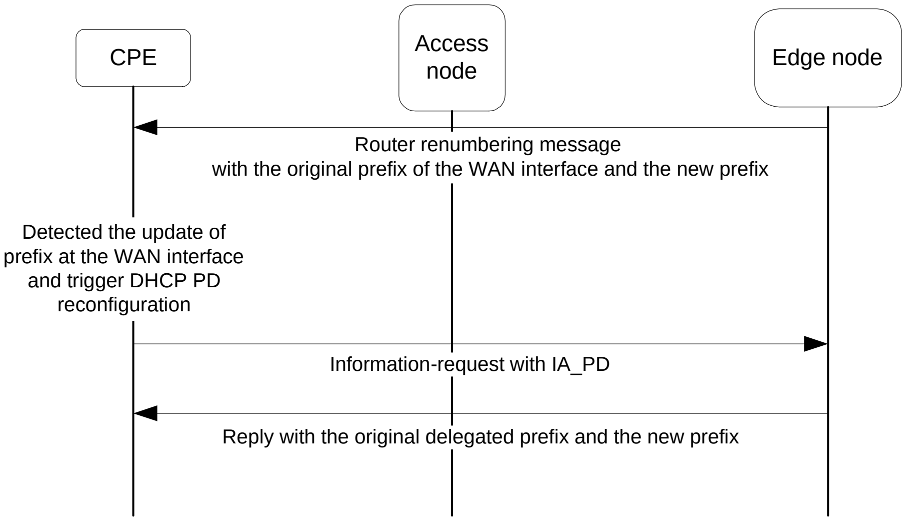

CPE
Access node
Edge node
Router renumbering message with the original prefix of the WAN interface and the new prefix
Detected the update of prefix at the WAN interface and trigger DHCP PD reconfiguration
Information-request with IA_PD
Reply with the original delegated prefix and the new prefix

Figure 9 – Router renumbering triggered prefix renumbering

As shown in Figure 9, in some cases, the edge node may initiate the prefix renumbering by sending a router-renumbering message [b-IETF RFC 2894] to the WAN interface of the CPE. Then, the CPE detects the update of the prefix at the WAN interface and triggers the DHCPv6 PD reconfiguration.

Figure 8 illustrates the renumbering cases initiated by DHCPv6 and ND. Note that in some cases, DHCPv6 and ND may be used simultaneously to initiate renumbering on one interface. This may cause potential conflict of address configuration policies. For example, the prefixes in DHCPv6 and ND messages are different due to the network administrator's mistake; or DHCPv6-managed hosts receive RA address configuration messages, which may cause unpredictable host behaviour because neither DHCPv6 nor ND has defined the host behaviour in this situation. If during the renumbering process the hosts receive address configuration messages (either through the ND or DHCPv6), and if there is a conflict with the address configuration policy, the host should report the conflict to the network. Then the hosts accept the address configuration indication from the network.

7.1.1.5 Dynamic address allocation

The DHCPv6 protocol enables network management to dynamically allocate IPv6 addresses to user equipment and configure the related network parameters, as shown in Figure 10. The user equipment sends address and configuration requests to the DHCPv6 server, which may be embedded in the access node, edge node, or running independently through the CPE relay. After a DHCPv6 server receives the request, it allocates an IPv6 address to the user equipment and propagates other configuration parameters towards the user equipment by DHCPv6 reply messages.

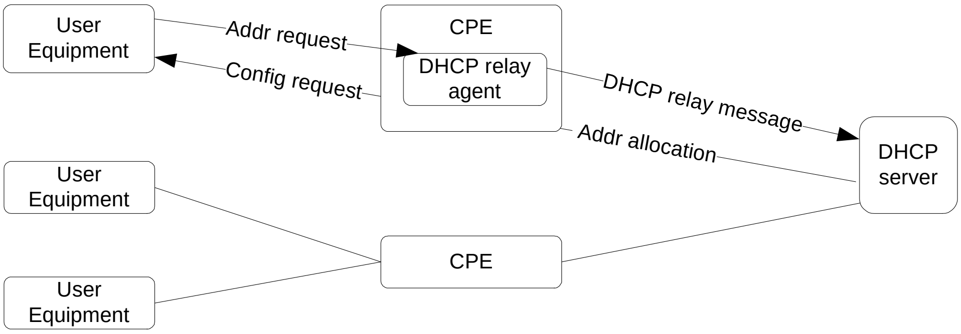


Figure 10 – Example of DHCPv6 address allocation

The DHCPv6 server should also manage the IPv6 addresses even when they are generated by user equipment, such as a cryptographically generated address (CGA) [b-IETF RFC 3971]. The client generates a CGA, sends the CGA to the DHCPv6 server and requests the DHCPv6 server to determine whether the generated CGA satisfies the requirements of the network configuration (comprising a CGA security level set by the DHCPv6 server). If the CGA does not satisfy the requirements of the network configuration, the DHCPv6 server then sends back the proper network configuration to the node. The node then generates a new CGA according to the configuration (comprising a client public key and a CGA security level designated by the client) sent from the DHCPv6 server, and re-sends the CGA to the DHCPv6 server for request again.

The DHCPv6 can also help user equipment to generate a CGA with the right network configuration parameters. User equipment sends a request to a DHCPv6 server to generate a CGA, which satisfies the requirements of network configuration. The DHCPv6 server receives client configuration information (comprising a client public key and a CGA security level designated by the client) sent from the client, and generates a CGA according to the configuration with a higher priority from the client configuration and the network configuration (comprising a CGA security level set by the DHCPv6 server). It then delivers the CGA to the client.

7.1.2 Multiple addresses

Among various address configuration scenarios mentioned in clause 6.3, multi-homing [b-ITU-T Y.2052] is the most explicit and definite requirement in the IPv6-based NGN.

Figure 11 illustrates a typical multi-homing scenario in IPv6 access to the NGN.

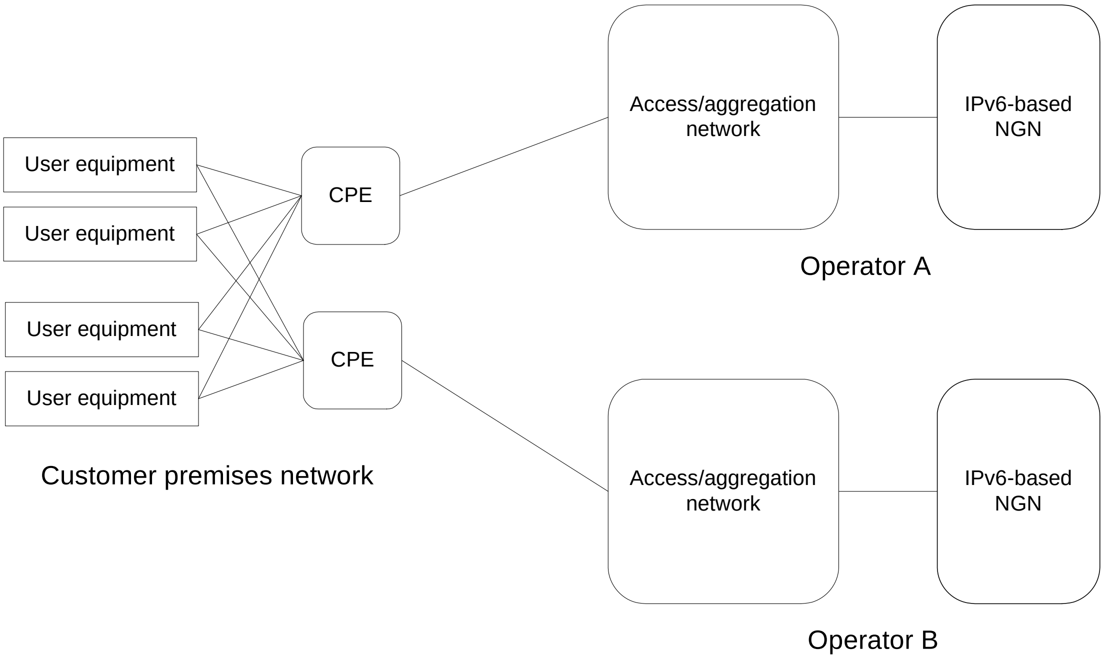


Figure 11 – Typical scenario of multi-homing in IPv6 access to the NGN

There is a case where the access/aggregation networks may deploy IPv6 transition mechanisms which involve processing IP packets differently (for example, tunnelling and translation mentioned in clauses 7.2.1 and 7.2.2). So for a specific type of IP packet (either IPv4 or IPv6), the transmission efficiency across different access/aggregation networks may vary. It is one case of the network selection problem that was defined in [b-IETF RFC 5113]. To deal with network selection problem, a method is needed for selecting the proper route for the UE in a multi-homed site. The UE sends transition information request messages to the CPE. Upon receiving the transition information from the CPE, the UE correlates the transition information with the IP address of the CPE. The correlation information will be recorded in a table in the UE, and then the UE makes a routing selection according to the correlation information. The transition information can be pre-configured in the CPE, or generated by the CPE according to the received network messages.

7.2 IPv4-compatible connectivity provision

7.2.1 Accessing IPv4 nodes through a dual-stack and tunnelling combination

In this scenario, users act as IPv4 nodes to access the IPv4 nodes. Set up of IPv4-over-IPv6 tunnels across the IPv6-based NGN is then needed.

The impact on the access network is explicit that user equipment and CPE need to support dual-stack IPv4 and IPv6 protocols. CPE encapsulate the IPv4 packets into IPv6 packets and forward them to the tunnel concentrator across the IPv6-based NGN. The tunnel concentrator relays the IPv4 packets between the IPv4 network and the CPE.

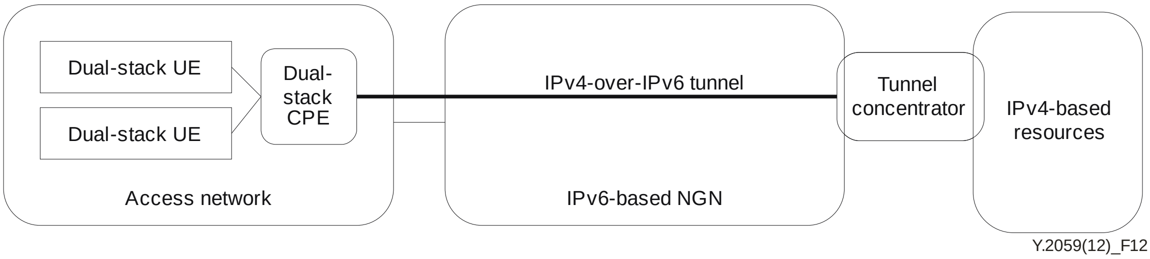


Figure 12 – Accessing IPv4 nodes through a dual-stack and tunnelling combination

7.2.2 Accessing IPv4 nodes through an IPv6-IPv4 translator

In this scenario, users are IPv6 nodes that access the IPv4 nodes. An IPv6-IPv4 translator is required.

Some translation mechanisms need specific address space which may impact the address allocation and management of the access network.

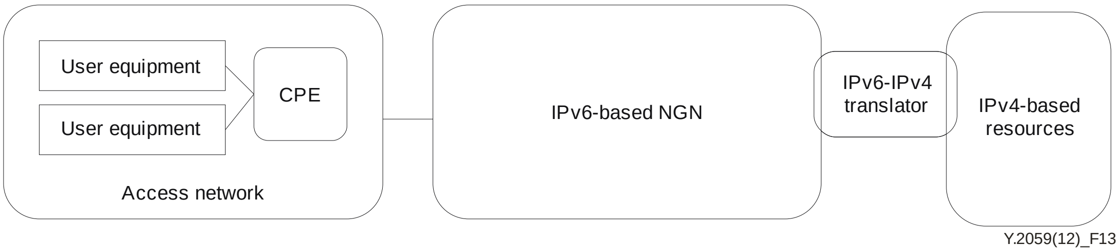


Figure 13 – Accessing IPv4 nodes through an IPv6-IPv4 translator

7.3 Security

7.3.1 Access network level registration

7.3.1.1 Stateless configured address registration

Clause 6.3.1 mentioned the implicit line authentication. When a node gets an IPv6 address from the network, it can be considered as having passed line authentication.

IPv6 has both stateful and stateless address configuration modes. In stateless mode, the node can configure its address by itself without notifying the network. IPv6 stateless address auto-configuration is a big improvement from IPv4, but it conflicts conceptually with the network managed address architecture. For example, in a DHCPv6-managed network or a network with an access control list, the addresses are assigned and managed by the network. Especially from the line authentication viewpoint, auto-configuration is a lack of registration.

The DHCPv6 and router advertisement may be extended to propagate the address registration request from the network manager to the user equipment. A DHCPv6 server may act as the address registration server with newly defined DHCPv6 options. The general procedures of address registration can be illustrated as shown in Figure 14.

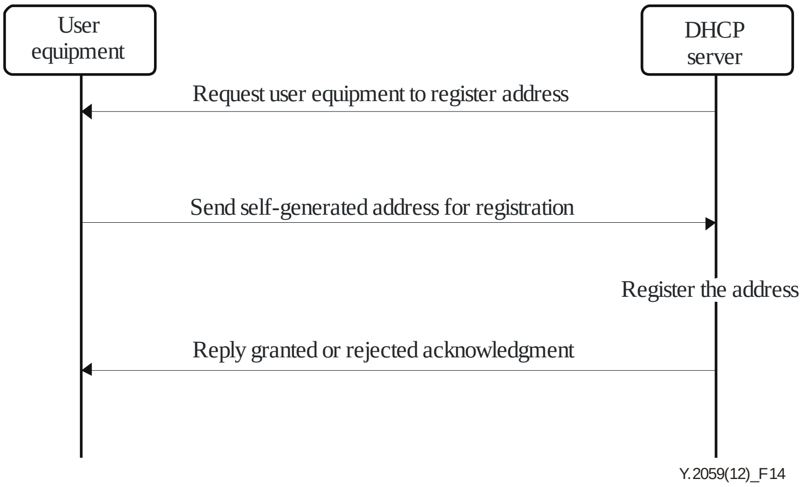

User equipment
DHCP server
Request user equipment to register address
Send self-generated address for registration
Register the address
Reply granted or rejected acknowledgment
Y.2059(12)_F14

Figure 14 – Address registration procedure

7.3.1.2 PPP authentication scenarios

PPP has been widely deployed for network access. It is a link layer protocol suite containing authentication functions. The PPP interface for IPv6 had been defined in [b-IETF RFC 5072] and [b-IETF RFC 5172]. So it is proper to use the PPP as IPv6 access authentication. According to the CPE working mode, the PPP authentication scenarios can be either of the following two types.

- CPE working in router mode: The CPE initially sends an access request, which should be authenticated by the operator. After authentication, the operator will normally assign an IPv6 prefix to the CPE through the DHCPv6-PD. User equipment will be assigned addresses by the CPE through the DHCPv6 or ND protocol and will not be directly managed by the operator.

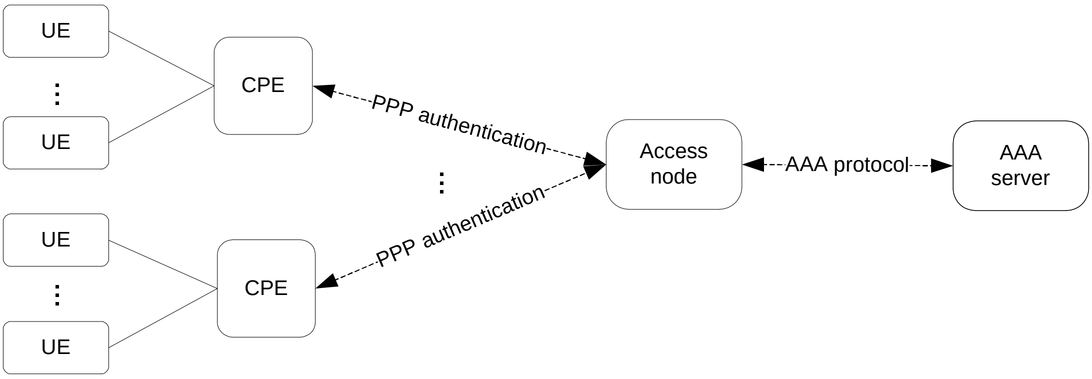


Figure 15 – PPP authentication when the CPE works in router mode

- CPE working in bridge mode: In the CPE bridge mode, the user equipment directly interacts with the access node to perform PPP authentication and address configuration. When UE only supports stateless address configuration, the access node normally acts as a DHCPv6-PD proxy to request an IPv6 prefix from the DHCPv6 server and delivers the prefix to the UE through the ND protocol. When UE supports DHCPv6, the access node normally acts as a DHCPv6 relay agent to relay messages between the UE and the DHCPv6 server.

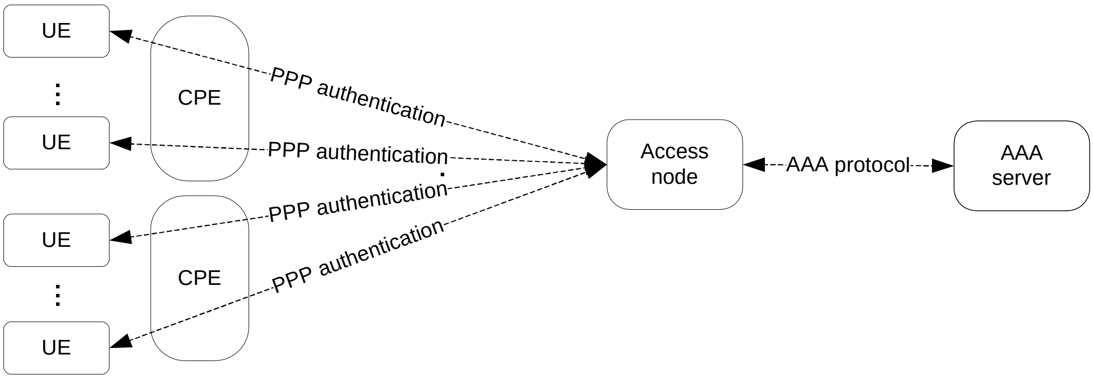


Figure 16 – PPP authentication when the CPE works in bridge mode

7.3.2 Source address validation and filtering

The source address validation function is important for network access. It is useful for access control and authorization, filtering traffic from customer interfaces implemented as ports in a layer 3-aware bridge or a router, general improvements in filtering accuracy in enterprise networks, etc.

The source address validation function can be applied to various protocols relevant to network access.

7.3.2.1 Source address validation in the DHCPv6 scenario

When DHCPv6 servers and user equipment use the CGA, they are able to perform source address validation.

A DHCPv6 node (either a server, a relay agent or a client) receives a DHCPv6 message, wherein the source of the DHCPv6 message is a CGA, and the DHCPv6 message carries a signature of the sender of the DHCPv6 message. The DHCPv6 node verifies both the CGA and the signature and then handles the payload of the DHCPv6 message. The CGA parameter included in the DHCPv6 message is carried in the CGA parameter option, while the signature is carried in the signature option. The receiver, the DHCPv6 server, can find the sender's source CGA in the peer-address field for CGA verification. In the server-relay-client scenarios, a DHCPv6 server knows a client is behind relay(s) when it receives a relay-forward DHCPv6 message. Then it replies with a relay-reply message containing the server's source CGA being carried in the server's DHCP unique identifier (DUID), which is in the payload. In this way the receiver, a DHCPv6 client, can get the server's source CGA for source address verification.

7.3.2.2 Source address validation in the access control scenario

A common mechanism of source address validation in access control scenarios is binding of IP addresses and MAC addresses. When the network validates a device's identity, it not only checks the source address, but also the MAC address embedded in the Ethernet frame.

8 Functional requirements for access to the IPv6-based NGN

Some functional entities (FEs) in the NGN structure need to extend their existing functions to support the scenarios described in clause 7. In this clause, relevant functional requirements are described.

8.1 Transport stratum functions

Access network functions and edge functions in the transport functions are highly related to user network access.

8.1.1 Functions to support IPv6 connectivity provision

- In the access network, edge functions are recommended to provide prefix information to the CPE to help them obtain proper prefix and address configuration through static or dynamic mechanisms.
- Edge functions are recommended to support prefix-renumbering operation according to the changes of network topology or authorization policy. With particular protocol messages, such as DHCPv6 reconfigure and RS messages, prefix renumbering on the LAN and WAN interfaces of the CPE are completed.
- Access network functions and edge functions are recommended to interact with some prefix-related information to cooperate to complete prefix and/or address allocation. Access network functions handle the prefix and configuration parameters received from edge functions, and allocate appropriate downstream port prefixes based on these parameters.
- Access network functions are recommended to interact with edge functions to inform the access node's identification information when necessary, such as when the edge node wants to control the prefixes/addresses configuration directly. With this identification information, edge functions determine a prefix to be advertised to the particular CPE.

8.1.2 Functions to support IPv4-compatible connectivity provision

- Edge nodes are recommended to support dual-stack functions.
- Edge nodes are recommended to support IPv4-over-IPv6 tunnelling functions.
- In translation scenarios, edge nodes should support IPv6/IPv4 protocol translation functions.

8.1.3 Functions to support security mechanisms

- Transport functions allow user equipment to generate its address with its own parameters. For the address generated by the user equipment, such as a CGA, edge functions are recommended to support the management operation which can register the user self-generated addresses to the network side (e.g., DHCPv6 server).
- According to whether the CGA matches the network configuration or not, edge functions grant the use of it or inform the user equipment to generate another one.
- When the edge node or access node includes DHCPv6, and uses CGA, edge functions or access network functions are recommended to support the relevant address validation function.

8.2 End-user functions

As closely cooperating with transport functions and transport control functions, IPv6 enabled end-user functions (such as CPE and terminal functions) shall meet the following requirements.

8.2.1 Functions to support IPv6 connectivity provision

- In the cascading delegation situation, end-user functions are recommended to apply the delegated prefix and related policy or rules to the home network where a cascaded router exists and supports sending the cascaded prefix further down.
- In the prefix renumbering situation, the CPE is recommended to check the new LAN interface prefix carried in the DHCPv6 reconfigure message received from the edge node, and trigger an RS message to update its WAN interface prefix.
- When the edge node initiates router renumbering, after receiving this message on the WAN interface, a CPE is recommended to be able to detect the updated prefix at its WAN interface and trigger the DHCPv6 PD reconfiguration.

- End-user functions should support the DHCPv6 client role, interact with transport functions with parameters and send an address configure request to the DHCPv6 server, which is embedded in the access node/edge node or independently.

8.2.2 Functions to support IPv4-compatible connectivity provision

- User equipment is recommended to support dual-stack protocols.
- If the operator deploys an IPv4 address sharing mechanism, the user equipment may need to support an IPv4 network address translation function.

8.2.3 Functions to support security mechanisms

End-user functions are recommended to support the source address validation when the end-user functions use a CGA as the source address.

9 Security considerations

This Recommendation generally aligns with the security requirements in [ITU-T Y.2701]. Address filtering is particularly noticed as the following:

As described in clause 6, multiple addresses may be common in IPv6 nodes. Especially in multi-homed sites, nodes may use multiple prefixes. Packets may be discarded according to the filter policy given by an ISP when they are passing through the uplink gateway with the address prefixes assigned by another ISP. The normal ingress filtering is also more complex than that in IPv4 due to the multiple addresses of an IPv6 node.

Bibliography

[b-ITU-T Y.2052] Recommendation ITU-T Y.2052 (2008), *Framework of multi-homing in IPv6-based NGN*.

[b-IETF RFC 1035] IETF RFC 1035 (1987), *Domain Names – Implementation and Specification*.

[b-IETF RFC 2894] IETF RFC 2894 (2000), *Router Renumbering for IPv6*.

[b-IETF RFC 3315] IETF RFC 3315 (2003), *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*.

[b-IETF RFC 3633] IETF RFC 3633 (2003), *IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6*.

[b-IETF RFC 3971] IETF RFC 3971 (2005), *Secure Neighbour Discovery (SEND)*.

[b-IETF RFC 4861] IETF RFC 4861 (2007), *Neighbour discovery for IP version 6 (IPv6)*.

[b-IETF RFC 4862] IETF RFC 4862 (2007), *IPv6 Stateless Address Autoconfiguration.*

[b-IETF RFC 5072] IETF RFC 5072 (2007), *IP Version 6 over PPP*.

[b-IETF RFC 5113] IETF RFC 5113 (2008), *Network Discovery and Selection Problem*.

[b-IETF RFC 5172] IETF RFC 5172 (2008), *Negotiation for IPv6 Datagram Compression Using IPv6 Control Protocol*.

[b-IETF RFC 6146] IETF RFC 6146 (2011), *Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers*.

[b-IETF RFC 6147] IETF RFC 6147 (2011), *DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers*.

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	Terminals and subjective and objective assessment methods
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, 2013