International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.3034

(06/2015)

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

Future networks

Architecture for interworking of heterogeneous component networks in ID/locator split-based future networks

Recommendation ITU-T Y.3034

International Telecommunication Union

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
Enhancements to NGN	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.3034

Architecture for interworking of heterogeneous component networks in ID/locator split-based future networks

Summary

Recommendation ITU-T Y.3034 specifies the architecture for interworking of heterogeneous component networks in ID/locator split-based future networks. It describes the functions of the different architectural components such as the host, gateway and ID/locator mapping server. It also lists the advantages and challenges of the architecture.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.3034	2015-06-13	13	11.1002/1000/12521

Keywords

Heterogeneous network, ID/locator split-based future networks, interworking.

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

FOREWORD

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

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

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

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

NOTE

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

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

INTELLECTUAL PROPERTY RIGHTS

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

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

Table of Contents

Recommendation ITU-T Y.3034

Architecture for interworking of heterogeneous component networks in ID/locator split-based future networks

1 Scope

The scope of this Recommendation includes the following items:

- Overview of the functional components of the ID/locator split-based future network architecture relevant to interworking of heterogeneous component networks;
- Architecture for interworking of heterogeneous component networks in ID/locator split-based future networks.

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, 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 published regularly. 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.2015] Recommendation ITU-T Y.2015 (2009), *General requirements for ID/locator separation in NGN*.

[ITU-T Y.2022] Recommendation ITU-T Y.2022 (2011), *Functional architecture for the support of host-based separation of node identifiers and routing locators in next generation networks*.

[ITU-T Y.2057] Recommendation ITU-T Y.2057 (2011), *Framework of node identifier and locator separation in IPv6-based next generation networks*.

[ITU-T Y.3001] Recommendation ITU-T Y.3001 (2011), *Future networks: Objectives and design goals*.

[ITU-T Y.3011] Recommendation ITU-T Y.3011 (2012), *Framework of network virtualization for future networks*.

[ITU-T Y.3031] Recommendation ITU-T Y.3031 (2012), *Identification framework in future networks*.

[ITU-T Y.3032] Recommendation ITU-T Y.3032 (2014), *Configurations of node identifiers and their mapping with locators in future networks*.

[ITU-T Y.3033] Recommendation ITU-T Y.3033 (2014), *Framework of data aware networking for future networks*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 access border gateway [b-ITU-T Y.2091]: A packet gateway between an access network and a core network.

3.1.2 address [b-ITU-T Y.2091]: An address is the identifier for a specific termination point and is used for routing to this termination point.

3.1.3 component network [ITU-T Y.3001]: A single homogeneous network which, by itself, may not provide a single end-to-end global telecommunication infrastructure.

3.1.4 future network (FN) [ITU-T Y.3001]: A network able to provide services, capabilities, and facilities difficult to provide using existing network technologies. A future network is either:

a) A new component network or an enhanced version of an existing one, or

b) A heterogeneous collection of new component networks or of new and existing component networks that is operated as a single network.

3.1.5 gateway [b-ITU-T Y.2261]: A unit that interconnects different networks and performs the necessary translation between the protocols used in these networks.

3.1.6 identifier [b-ITU-T Y.2091]: An identifier is a series of digits, characters and symbols or any other form of data used to identify subscriber(s), user(s), network element(s), function(s), network entity(ies) providing services/applications, or other entities (e.g., physical or logical objects). Identifiers can be used for registration or authorization. They can be either public to all networks, shared between a limited number of networks or private to a specific network (private IDs are normally not disclosed to third parties).

3.1.7 ID/locator mapping [ITU-T Y.2015]: ID/LOC mapping is an association between a node ID and one or more LOCs.

NOTE 1 – A single node ID or several node IDs can be associated with many LOCs associated with a single terminal. The node ID to LOC mapping can have the one-to-one, one-to-many, or many-to-one relationship.

NOTE 2 – ID/LOC mapping is also called ID/LOC binding.

3.1.8 ID/locator mapping function [ITU-T Y.2015]: An ID/LOC mapping function gets mapping information from an ID/LOC mapping storage function and uses the corresponding node ID and/or LOC in packet headers. The ID/LOC mapping function works in a close correlation with the transport user profile associated with the transport control function.

3.1.9 ID/locator mapping storage function [ITU-T Y.2015]: An ID/LOC mapping storage function stores the mapping of NGN identifiers, node IDs and LOCs. This function also updates mapping information, as well as provides mapping information to other functions on request. The mapping storage function can be physically located in an NGN terminal or with other NGN components.

3.1.10 ID/locator separation [ITU-T Y.2015]: ID/LOC separation is decoupling the semantic of IP address into the semantics of node IDs and LOCs. Distinct namespaces are used for node IDs and LOCs so that they can evolve independently. LOCs are associated with the IP layer whereas node IDs are associated with upper layers in such a way that ongoing communication sessions or services shall not be broken by changing LOCs due to mobility and multi-homing.

NOTE – In this Recommendation, ID/locator separation and ID/locator split are used interchangeably.

3.1.11 interworking [b-ITU-T Y.1401]: The term "interworking" is used to express interactions between networks, between end systems, or between parts thereof, with the aim of providing a functional entity capable of supporting an end-to-end communication. The interactions required to provide a functional entity rely on functions and on the means to select these functions.

3.1.12 locator (LOC) [ITU-T Y.2015]: A locator is the network-layer topological name for an interface or a set of interfaces. LOCs are carried in the IP address fields as packets traverse the network.

NOTE – IP addresses can gradually become pure LOCs. However, on the contrary, it cannot be said that a LOC is an IP address. An IP address may associate with the IP layer as well as upper layer protocols (such as TCP and HTTP), whereas a LOC will associate with only the IP layer and be used in IP address fields.

3.1.13 name [b-ITU-T Y.2091]: A name is the identifier of an entity (e.g., subscriber, network element) that may be resolved/translated into an address.

3.1.14 network address translation [b-ITU-T Y.2111]: The operation by which IP addresses are translated (mapped) from one address domain to another address domain.

3.1.15 network address port translation (NAPT) [b-ITU-T Y.2111]: The operation by which IP addresses and transport or port identifiers such as TCP and UDP port numbers are translated (i.e., mapped) from one address domain to another address domain.

3.1.16 node ID [ITU-T Y.2015]: A node ID is an identifier used at the transport and higher layers to identify the node as well as the endpoint of a communication session. A node ID is independent of the node location as well as the network to which the node is attached so that the node ID is not required to change even when the node changes its network connectivity by physically moving or simply activating another interface. The node IDs should be used at the transport and higher layers for replacing the conventional use of IP addresses at these layers. A node may have more than one node ID in use.

NOTE – Unless otherwise specified, the term "ID" used in this Recommendation represents a node ID.

3.1.17 node name [ITU-T Y.3032]: A node name is a string of alphanumeric characters and symbols that is used to uniquely identify the node. A node name, which may have variable length, is usually configured in such a way that it would be easier to be read and remembered by humans.

NOTE – Node names may also consist of human non-readable bit strings.

3.1.18 session [b-ITU-T Y.2091]: A temporary telecommunications relationship among a group of objects in the service stratum that is assigned to collectively fulfil a task for a period of time. A session has a state that may change during its lifetime. Session-based telecommunications may, but need not be, assisted by intermediaries (see mediated services). Session-based telecommunications can be one-to-one, one-to-many, many-to-one, or many-to-many.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 access component network: A component network that provides connectivity to user terminals is called an access component network. The access component network collects data traffic generated from the user terminals connected to it or delivers data traffic destined to the user terminals connected to it.

3.2.2 heterogeneous component networks: Heterogeneous component networks are composed of two or more component networks, each of which may use a different network-layer protocol and locator namespace, and possibly a different routing mechanism. The component networks are connected to one another through one or more gateways, which perform network protocol translation. The computers or user terminals connected to the heterogeneous component networks communicate with one another by using names or IDs in the upper layers and locators in the network layer.

3.2.3 ID/locator split-based future networks: The future networks designed on the basis of the ID/locator split concept where the IDs and locators are derived from distinct namespaces. Generally, only IDs are used by the applications to identity communication entities, e.g., host, session, data or service. The locators are used by the routing system to locate the position of the entity possessing the locator in the network. IDs have relatively longer life than locators and do not change during the lifetime of the entity, such as a session, data or service instance. The locators do change at any time when a change in the network configuration occurs such as due to mobility. The relationship or binding between IDs and locators belonging to an entity is transient, i.e., can change at any time.

3.2.4 transit component network: A component network that connects one access component network to other access component networks is called a transit component network. There may be one or more transit component networks between two access component networks. A transit component network passes data traffic originated from one access component network to another access component network or transit component network.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

FN	Future Network
GW	Gateway
ID	Identifier
LINP	Logically Isolated Network Partition
LOC	Locator
NAT	Network Address Translation
NAPT	Network Address Port Translation
NGN	Next Generation Network
TCP	Transmission Control Protocol

5 Conventions

None.

6 Overview of interworking heterogeneous networks in future networks

[ITU-T Y.3001], which specifies the objectives and design goals of future networks (FNs), mentions in the definition that FNs would be "a heterogeneous collection of new component networks or of new and existing component networks." A component network is "a single homogeneous network which, by itself, may not provide a single end-to-end global telecommunication infrastructure." Therefore, from the definition itself, it is clear that FNs would be a harmonious collection of heterogeneous networks and FN architectures have been recommended to promote this feature. Moreover, many of the objectives and design goals specified in [ITU-T Y.3001] directly or indirectly refer to an effective collection of heterogeneous networks in FNs. Three objectives, viz. service awareness, data awareness, and social economic awareness, are related to heterogeneous networks. Similarly, several design goals, such as service diversity, functional flexibility, data access, energy consumption, service universalization, economic incentives, mobility, and identification demand heterogeneous network support.

The heterogeneity occurs not only be in the access technologies, but also in the network-layer functions and protocols. The exiting Internet Protocol version 4 (IPv4) will continue for some years (decades), while Internet Protocol version 6 (IPv6) picks up deployment. Not only IPv4 and IPv6, but also new protocols being considered for data aware networking [ITU-T Y.3033] or information-centric networking have to coexist harmoniously in the network layer of FNs. The data-aware networking paradigm has been introducing named data searching and delivering functions in the network layer. Moreover, FNs may also need to internetwork not only with the physically separated heterogeneous component networks, but also with logically isolated network partitions (LINPs) [ITU-T Y.3011], where each partition may use a different network-layer protocol. This Recommendation specifies an architecture based on the identifier/locator (ID/locator) split concept for interworking of component networks using heterogeneous network protocols in FNs.

In order to facilitate interworking among the heterogeneous component networks that use different network-layer protocols, the network applications should not be tightly coupled with a particular network-layer protocol. The current Internet does not follow this design guideline, as its applications are tightly bound to the network layer through IP addresses. The applications use IP addresses, which are related to the network-layer protocol, to identify the sockets or endpoints of the communication session. The applications' dependency on the network-layer protocol also imposes limitations on the Internet's capability to natively support mobility and multihoming. However, specifications for mobility and multihoming support are outside the scope of this Recommendation.

In order to overcome this design limitation of the conventional Internet in supporting heterogeneous network-layer protocols in the component networks, FN is being designed on the basis of the ID/locator split concept, where the IDs and locators are derived from distinct namespaces [ITU-T Y.3031]. In the ID/locator split-based FN, the network layer uses locators to locate a node and forward packets, while the upper layers (i.e., transport and application layers) use IDs to identify the nodes, endpoints, sockets, sessions or services. The ID configuration method, as well as the ID to locator mapping storage, update, and resolution methods are specified in [ITU-T Y.3032].

A node can possess multiple network-layer locators if it is simultaneously associated with multiple access networks through a single or multiple interfaces. In this case, the node's single ID can be mapped to various locators. The node can relinquish a locator when the node dissociates with the access network or it can change its locator when it moves from one access network to another. Thus the ID-to-locator mapping relationships are transient, i.e., can change at any time, e.g., due to mobility or multihoming.

The ID/locator split concept and architectures have already been studied in ITU-T for next generation networks (NGNs) and have been documented in [ITU-T Y.2015], [ITU-T Y.2022] and [ITU-T Y.2057]. While these related Recommendations specify framework, general requirements, and architecture for introducing ID/locator splits into the NGN functional architecture, this Recommendation specifies the architecture for interworking heterogeneous networks in FNs.

The following clauses first specify the functional components of the ID/locator split-based FN relevant to the architecture for interworking of heterogeneous component networks and then specify the interworking architecture.

7 Heterogeneous component network environment

Figure 1 shows the network environment with heterogeneous component networks where IPv4, IPv6, and other network-layer protocols can be used. These heterogeneous component networks are connected to one another through gateways (GWs). One component network can be connected to another component network through one or more GWs. Similarly, one component network can be connected to two or more adjacent component networks through two or more GWs. The component network can be an access component network or a transit component network, depending on whether it is transporting data traffic originated from or destined to a user terminal connected to itself or to other component networks. The user terminals can exist in a multitude of forms, such as mobile terminals, fixed terminals, sensors, and servers. In Figure 1, component networks A and F are the access component networks for the mobile terminal and server, respectively, while component networks B and C are transit component networks. The access and transit nature of a component network is relative to the user terminal's location. For example, component network D is an access component network for the fixed terminal, while it is a transit component network for the communication between the mobile terminal connected to component network A and the sensor connected to component network E.

User terminals contain the communication protocols and applications, and are collectively called hosts. A host can have connectivity to one or more component networks. The latter case is called host

multihoming. A multihomed host supporting two or more network-layer protocols can get connected to heterogeneous component networks.

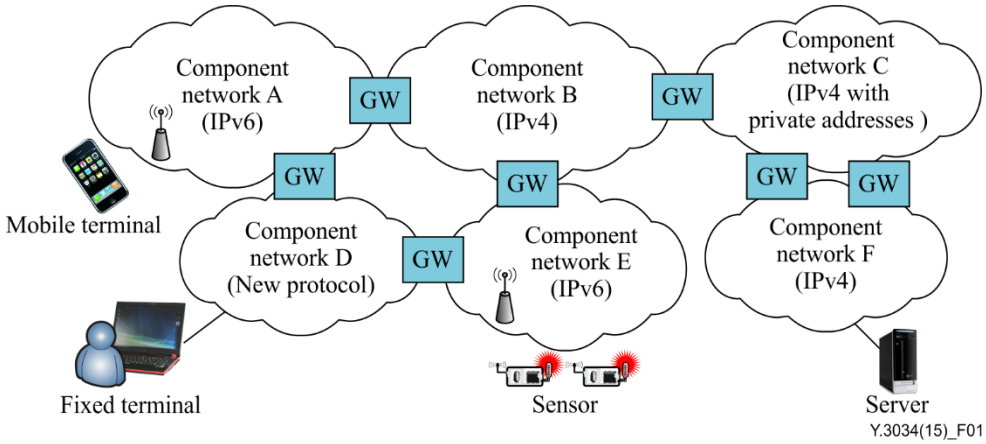

Figure 1 – Network environment with heterogeneous component networks

The GW provides protocol translation when the adjacent component networks use dissimilar network-layer protocols. For example, in Figure 1 the GW connecting component networks A and B translates IPv6 to IPv4 for data packets entering into component network B from component network A, and translates IPv4 to IPv6 for data packets travelling in the reverse direction. The network-layer protocol information is contained in the network-layer header of data packets. Thus, the GW performs translation of the network-layer header.

In the current Internet protocol stack, some values of the network-layer header are also embedded in the fields of the transport layer header, e.g., source and destination addresses of the network header are used in the computation of checksum included in the TCP header. Thus, the translation of the network header also requires translation of the transport header fields, which incurs additional overhead.

The network-layer header translation is required even when two adjacent component networks use the same network protocol, but differently scoped network address spaces, e.g., when one component network uses private IPv4 addresses and the other employs global IPv4 addresses. The GWs connecting these component networks perform network address translation (NAT) in the packet header. If multiple private addresses are mapped to a single global address, some parameters from the upper layer header, e.g., port numbers of the transport header, also need to be translated into some unique values so that the combination of the global source IP address and the translated port number is a unique reference value in the data packets entering from the component network using private IP addresses into the component network using global IP addresses. Similarly, for the data packets travelling in the reverse direction, the combination of the destination port number and the destination IP address is a unique reference value and is used to find and translate into the appropriate private IP address and port number. This can be achieved by using a network address port translation (NAPT) mechanism.

The conventional NAT or NAPT uses IP addresses and port numbers present in the packet headers as the reference values to translate the network header. However, because of limitation in the port number size, these conventional mechanisms pose limitations on the number of sessions a host can have for communications at a given time. This problem is overcome by an ID/locator split-based protocol stack, where the IDs present in the packet's identity header are used as unique reference values to compute the TCP checksum and to translate the network header in data packets.

The data packets containing a different network protocol header can also be transmitted through the component network by using a tunnelling mechanism if both the entry- and exit-side component networks use the same network protocol. The tunnelling mechanism consists of encapsulation of the

data packets by adding a new network header containing information about the network protocol of the component network through which the packets traverse at the entry GW and removing the newly added header from the packets at the exit GW. For example, in Figure 1 when data packets travel from component networks A to E through component network B, the GWs can tunnel the packets through component network B.

The header translation is applicable to interworking of heterogeneous component networks deployed in any configuration, while the tunnelling is applicable only to the transit component network between two component networks using the same network protocol and having the IP addresses derived from the global IP address space. For example, in Figure 1 component network B can perform translation only for the communication between component networks A and C because the IPv6 global addresses used in component network A cannot be understood or is not useable for routing and forwarding in component network C, and vice versa. For these reasons, tunnelling is not good enough for interworking between heterogeneous network protocols in the FN, although it is helpful for traffic engineering. Therefore, in this Recommendation, only the translation mechanism is specified for interworking between heterogeneous network protocols.

8 Configuration of ID/locator split-based future networks

Figure 2 shows the network components of the ID/locator split-based FN architecture. The ID/locator mapping servers are the new functional components, which store ID/locator mapping records, update these records, and provide these records to a querying host or GW.

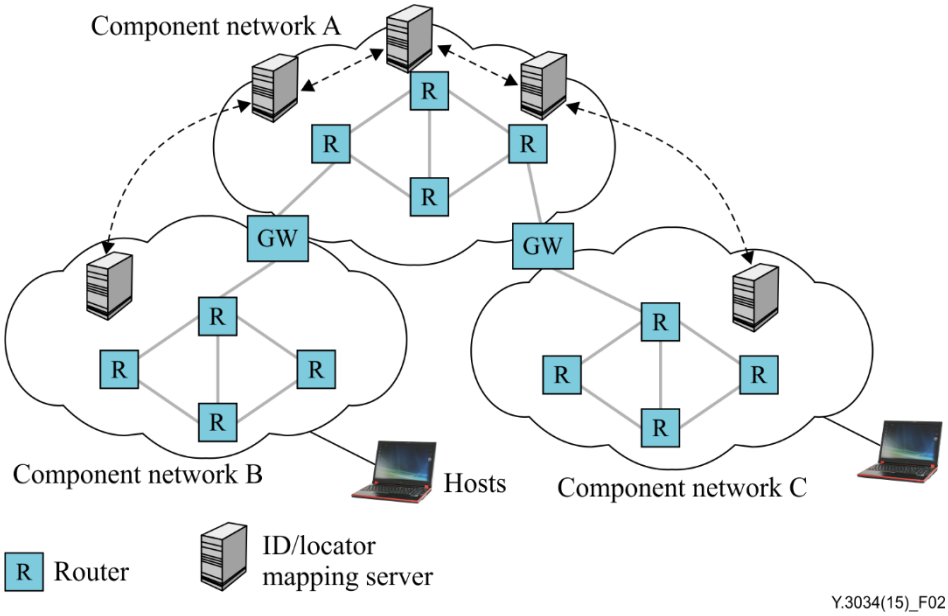

Figure 2 – Components of ID/locator split-based future network

Figure 3 shows the protocol layers of the ID/locator split-based FN architecture. The new identity layer has been introduced in the host and GW protocol stacks. The identity layer protocol has the end-to-end scope, i.e., the major fields of the identity header usually do not change in transit when the data packets traverse the component networks. IDs derived from a newly created namespace, as specified in [ITU-T Y.3032] or borrowed from unused portions of network address space, are used in the transport and upper layers. The IDs are used to identify the host, as well as the transport and application sessions. The identity layer relates an ID with multiple locators belonging to different types of network-layer protocols. Thus, the identity layer functions support multiple or heterogeneous network-layer protocols (e.g., IPv4, IPv6 or future new protocols), while hiding the heterogeneity of the network-layer protocols of the component networks from the transport and application layers.

Namely, the identity layer is the key functional component for interworking of heterogeneous network-layer protocols.

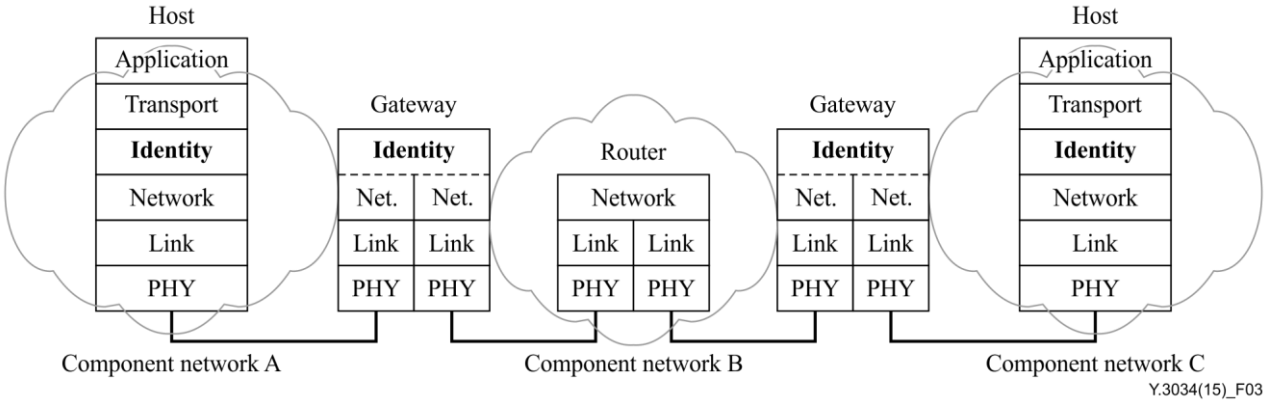

Figure 3 – Protocol layers in ID/locator split-based future networks

The detail format of the identity header is not specified in this Recommendation, and left for future study. This Recommendation simply assumes the existence of the identity header that contains both the source and destination IDs, among other parameters.

In the protocol stack, the network layer and lower layer functions are similar to current networks. The network layer in the source host and the GW protocol stacks configures a network header by including the source and destination locators provided by the identity layer. The network layer in the GWs and routers participates in routing protocols and performs forwarding of data packets based on the forwarding table generated by the routing protocol.

The functions of the identity layer in the host and GW protocol stacks and those of ID/locator mapping servers are described in the following clauses.

8.1 Host function

The identity layer makes the host protocol stack favourable to supporting communication over heterogeneous network protocols. The identity layer prepends in each data packet an identity header containing the source and destination hosts' IDs, finds the related source and destination locators by searching an ID/locator mapping table, and provides source and destination locators to the network layer. The identity layer also includes functions for host or session identification, network-layer protocol selection, mobility and multihoming management, and network access and data session security.

The identity layer also favours host multihoming, as it makes the host capable of being simultaneously connected to two or more component networks of heterogeneous network-layer protocols. The different network protocols may be associated with different interfaces (physically separated component networks) or with a single interface (logically separated component networks). Figure 4 shows the host-multihoming scenario, where the host has two different interfaces, 1 and 2, connected with heterogeneous component networks, A and B. The host gets two locators belonging to each component network's locator namespace. In this way, the host ID can be mapped to two different locators, and the identity layer can select the most appropriate network-layer protocol and locator from the available ones for an outgoing packet and provides the selected locator value to the corresponding network-layer protocol. The network layer configures a network header including the selected source and destination locators, adds the header to the packet received from the identity layer, and sends out the packet to the component network. The identity layer may have functions to select the optimal source and destination locators after matching the application service requirements with the capabilities of the available component networks. The identity layer makes the transport layer

functions independent of the network layer, so that the same transport layer protocol implementation works with various network-layer protocols.

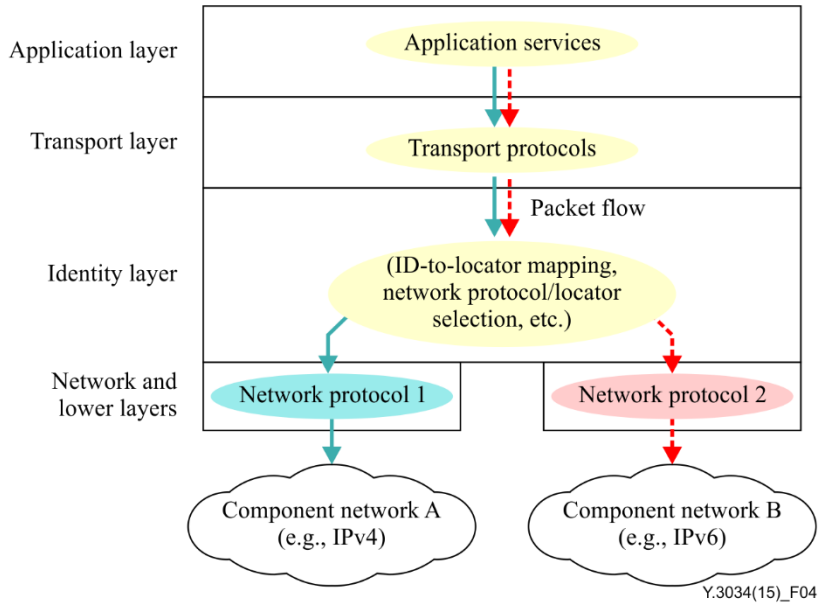

Figure 4 – Multihomed host protocol stack supporting heterogeneous network protocols

8.2 Gateway function

The identity layer in the GW protocol stack provides necessary information to translate the network-layer header of packets from the network layer before the packets are forwarded to heterogeneous component networks. As shown in Figure 5, the packet entering the GW from component network A goes up to the identity layer, which reads the IDs from the identity header and finds the corresponding source and destination locators (and network-layer protocol) either from a locator list supplied by the source host in the identity header or from the ID/locator mapping table cached in the GW. Then the identity layer passes the packet, along with the source and destination locators, to the network-layer protocol. The network layer configures a new network protocol header containing the locators, attaches it to the packet, and forwards the packet to component network B. The packet is routed within the component network using the destination locator present in the packet header. If the destination host is not within the component network, the packet reaches another GW where the network-layer protocol translation process is repeated. Thus, IDs present in the identity header are used as reference values for translating the network-layer header in the GWs, as the packets traverse through heterogeneous component networks.

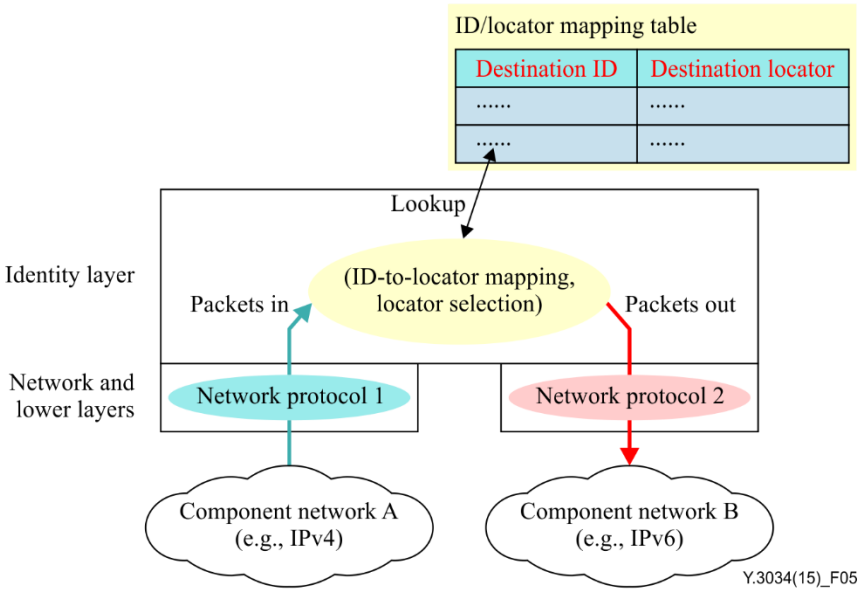

Figure 5 – Gateway protocols stack and functional blocks

8.3 Router function

As shown in Figure 6, the router's main job is to forward packets within the component network by using the destination locators present in the packet header. They execute routing protocols to gather, update, and distribute routing information required to create routing and forwarding tables. They use the table to determine the direction of the packet forwarding. The routers of an access component network forward packets originated from a host to a GW or vice versa, while the routers of a transit component network forward packets sent from a GW to another GW. The identity layer protocol, thus the processing of the identity header, is not required in the routers as they forward packets within the component network domain using the same locator namespace.

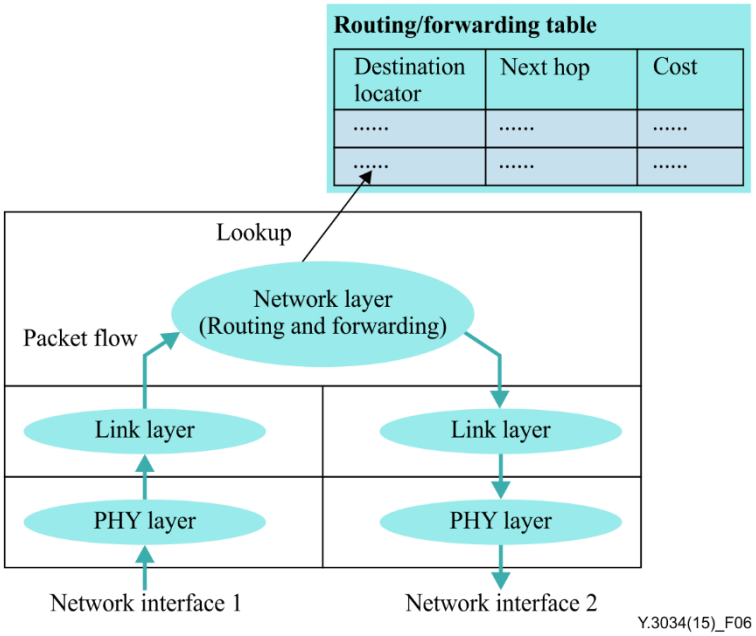

Figure 6 – Router protocols stack and functional blocks

8.4 ID/locator mapping server function

ID/locator mapping server function is the new and major component of the ID/locator split-based FN. It stores and updates ID/locator mapping records in the servers, as well as providing those records to the hosts and GWs. The architecture of the ID/locator mapping servers is specified in [ITU-T Y.3032]. To make the ID/locator mapping storage and update functions scalable, the servers can be organized in a two-layered hierarchical system where the ID/locator mapping records that are less likely to get updated (such as those of fixed hosts) are stored in the servers located in the upper level and the ID/locator mapping records that are more likely to get updated frequently (such as those of mobile terminals) are stored in the servers located in the lower level of the hierarchy. If the mobile host changes its locator when moving from one component network to another, the ID/locator mapping record stored in the server located in the lower level of the hierarchy gets updated.

9 Architecture for interworking of heterogeneous network protocols

The architecture for interworking of heterogeneous network-layer protocols in the FN can be described by the GW operation flow depicted in Figure 7. The GW interconnects two component networks of dissimilar network-layer protocols (protocol A and protocol B). Data packets from component network A entering the GW have source and destination locators (Loc_A1 and Loc_A2) belonging to the locator space of the network protocol used in component network A. The network layer receives the packet and extracts the values of some fields of the network header that are to be used in the new translated header. It then removes the network header from the packet and gives the packet containing the identity header to the identity layer along with the additional information extracted from the previous network header. The identity layer function reads the source and destination IDs from the packet header and performs the ID/locator mapping lookup at the ID/locator mapping table to retrieve the ID-to-locator mapping records associated with component network B. Then, the identity layer provides the source and destination locators (Loc_B1 and Loc_B2), other relevant parameters, and the data packet to the network layer. The network layer constructs a new network header containing the new source and destination locators (Loc_B1 and Loc_B2) and attaches the header to the packet. The network layer then sends out the packet to component network B.

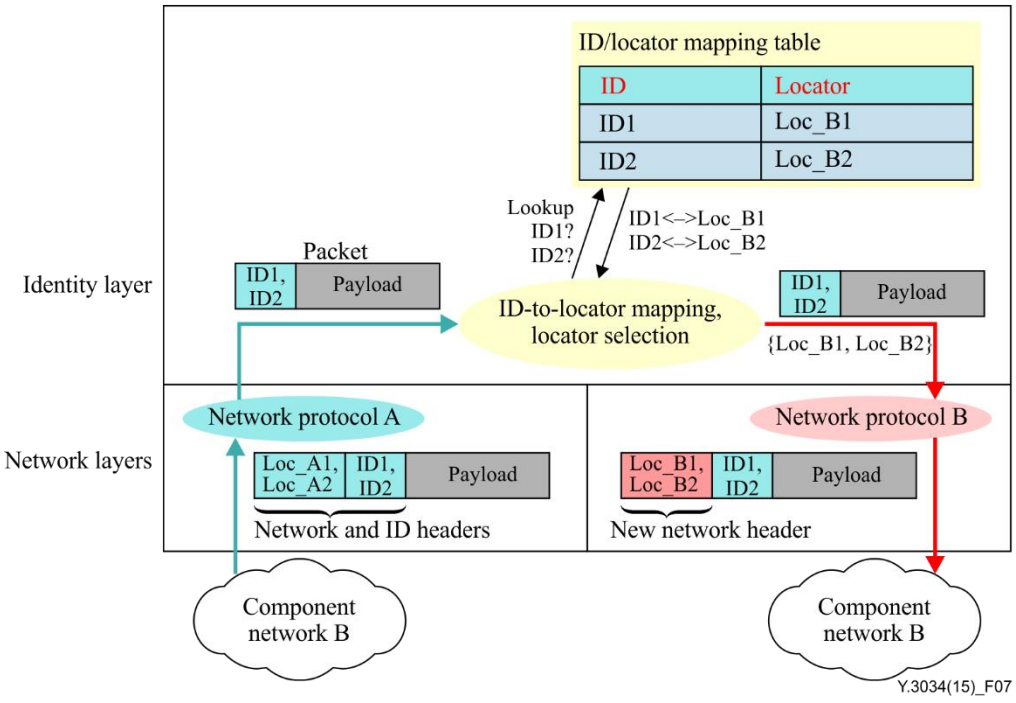

Figure 7 – Gateway operation flow for interworking of heterogeneous network-layer protocols

Thus, the ID-to-locator mapping function of the identity layer of the GW is the key component of the interworking architecture. It uses the ID/locator mapping records cached in the ID/locator mapping table. The ID/locator mapping record can be provided to the GW by different means, which can mainly be classified into two categories depending on whether the hosts are involved in providing the mapping to the GW or not.

a) In the host-based approach, the host provides its ID/locator mapping record to the GW when the host attaches to the component network. To provide the destination host's ID/locator mapping record, the source host first retrieves the destination's ID/locator mapping record from ID/locator mapping servers by performing the name resolution process as specified in [ITU-T Y.3032]. Then, it can provide the destination's ID/locator mapping record to its GW either by sending an explicit signalling message or by including the ID/locator mapping record in the identity header of the first data packet.

b) In the network-based approach, the ID/locator mapping records can be provided to the GW by other means in which the host's involvement is not required. For example, there may exist an ID/locator mapping control plane that can provide the ID/locator mapping records to the relevant GWs when a communication request is sent by the host through the control plane. This approach conceptually matches software-defined networking (SDN) approaches currently under study in ITU-T.

10 Advantages and challenges

10.1 Advantages

The major advantages brought about by the internetworking architecture are the coexistence of heterogeneous component networks, promotion of innovation in new network protocols, open competition in network business, multihoming, mobility, scalability, and security. These advantages are described below.

1) Coexistence of heterogeneous component networks: The interworking architecture specified in this Recommendation enables coexistence of component networks of heterogeneous protocols. Thanks to the protocol translation functions of the GWs interconnecting the heterogeneous component networks, end-to-end communications between user terminals located in component networks of dissimilar protocols become possible.

2) Promotion of innovation in new network protocols: Because of the interworking architecture, component networks are free to develop and use their own network-layer protocol that optimally suits their network capabilities as well as requirements. For example, lightweight network protocols can be developed for resource-constraint terminals, such as sensors, while highly reliable protocols can be developed for mission-control networks and applications.

3) Open competition in network business: The interworking architecture can eliminate or avoid the dominance of a single network protocol in the global business of network service providers. New network service providers can easily enter into the market by introducing a new network protocol that is more efficient than existing ones. Thus, it promotes open competition in network business.

4) Multihoming: The interworking architecture also allows user terminals to be multi-stack and connectable to two or more component networks simultaneously. The user can choose the better network for accessing a higher quality service or can switch the networks dynamically for accessing a better quality network service at a given time and location.

5) Mobility: The multi-stack user terminal can continuously access the network service while changing its point of attachment to various component networks. The mobility capability enables the user terminal to maintain the continuity of its communication session when moving from one component network to another, while enjoying universal connectivity.

6) Scalability: The interworking architecture allows the component networks, especially access component networks, to confine their network configuration details within their component networks. This hiding of the access component network's routing and other internal domain configuration details from the transit component networks facilitates routing state management in the transit network, thus enabling the transit network to perform equally well even if a large number of new access component networks come into existence.

7) Security: Hiding internal configuration details of a component network from other component networks assists in keeping the component networks secure from each other.

10.2 Challenges

The challenges are due to the complexity associated with the user terminals, as well as with the networks. Network complexity can further be divided into signalling plane complexity and data plane complexity. These challenges are described below.

1) Terminal complexity: Enabling user terminals to get universal connectivity with heterogeneous component networks increases user terminal complexity. The user terminal needs to maintain the ID/locator mapping cache as well as perform optimal locator selection for a given communication session and component network type. Maintaining simultaneous connections to various component networks and performing session handover smoothly from one component network to another also requires the user terminal to be more intelligent.

2) Signalling plane complexity: Signalling plane complexity is related to the maintenance and provisioning of ID/locator mapping records required for the interworking architecture. The control plane should be able to provide up-to-date ID/locator mapping records to the user terminals and GWs. Due to the existence of heterogeneous component networks, the same ID should be able to be mapped to different types of locators in different GWs located along the end-to-end path. The challenge is to provide only the most relevant ID/locator mapping of the destination host to the source host and GWs. Moreover, due to the mobile nature of hosts, the mapping keeps on changing and the updating of the control plane to reflect the change in a timely fashion is more challenging. [ITU-T Y.3032] can be helpful in addressing this limitation.

3) Data plane complexity: Data plane complexity is related to the translation function for network protocol information or network header in the data packets as they traverse through the GWs interconnecting heterogeneous component networks. The protocol translation function first selects the most appropriate locators from the relevant ID/locator mapping records provided by the control plane and then translates the network-layer header of the packet before forwarding the packet to the next component network.

Therefore, in order to realize the coexistence of heterogeneous component networks through the interworking architecture specified in this Recommendation, new approaches to address these challenges should also be studied.

11 Environmental considerations

The interworking architecture specified in this Recommendation may have some environmental issues, as it requires additional energy in the both data and signalling planes for the network-layer protocol translation. The data plane requires energy to perform the network header translation of packets in gateways. The signalling plane also requires energy to retrieve ID/locator mapping records from the ID/locator mapping registry system and to store them in the ID/locator mapping tables in the terminals and gateways. The protocol translation function as well as the ID/locator mapping retrieval and update functions should be implemented in an optimal way, so that their environmental impact is negligible.

12 Security considerations

The internetworking architecture specified in this Recommendation has some security issues, which can mostly be resolved by leveraging security measures specified in related Recommendations. The internetworking architecture is based on the translation of network protocol-dependent locators of communication devices included in the packet headers in the intermediated gateways as well as in end-user terminals. The translation architecture relies heavily on ID/locator mapping records obtained from the mapping registry system specified in [ITU-T Y.3032], which also specifies the necessary security measures for protecting the mapping records while they are being retrieved from the mapping registry by the terminals and gateways or while they are being updated in the mapping registries by sending update requests from the terminals whose locators have changed. However, new security measures or extension of existing security measures may be needed to protect the ID/locator mapping records stored in the ID/locator mapping tables of the gateways and terminals from being corrupted or stolen by a malicious piece of software or by other network entities.

The interworking architecture specified in this Recommendation is fundamentally more favourable to end-to-end data security than the NAT/NAPT based interworking architecture, because it uses network-layer protocol independent IDs in packet headers for sessions or services identification in the transport and application layers. The IDs are also used to identify or index the end-to-end security states maintained in the terminals. These security states remain valid even when terminals switch the network-layer protocols to transmit different data packets associated with the same communication session or when the locators present in the packet header get translated on the way while passing through heterogeneous networks.

Bibliography

[b-ITU-T Y.1401] Recommendation ITU-T Y.1401 (2000), *General requirements for interworking with Internet protocol (IP)-based networks*.

[b-ITU-T Y.2091] Recommendation ITU-T Y.2091 (2011), *Terms and definitions for next generation networks*.

[b-ITU-T Y.2111] Recommendation ITU-T Y.2111 (2011), *Resource and admission control functions in next generation networks*.

[b-ITU-T Y.2261] Recommendation ITU-T Y.2261 (2006), *PSTN/ISDN evolution to NGN*.

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	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	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, 2015