International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.3032

(01/2014)

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

Future networks

Configurations of node identifiers and their mapping with locators in future networks

Recommendation ITU-T Y.3032

ITU-T
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.3032

Configurations of node identifiers and their mapping with locators in future networks

Summary

Recommendation ITU-T Y.3032 specifies the formats of node names and IDs, as well as their configuration method. It then specifies the node names to IDs and locators mapping records storage and resolution mechanisms.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.3032	2014-01-13	13	11.1002/1000/12075-en

Keywords

Future networks, ID/locator mapping, ID/locator split, locators, node ID.

* 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.3032

Configurations of node identifiers and their mapping with locators in future networks

1 Scope

The scope of this Recommendation includes the following items:

- overview of node names, node IDs and locators for future networks
- consideration of node name and node ID configuration
- specification of node name to node ID and locator mapping storage and resolution methods.

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.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 (2012), *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.3021] Recommendation ITU-T Y.3021 (2012), *Framework of energy saving for future networks*.

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

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 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.

3.1.2 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).

3.1.3 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 – In this Recommendation, locators are also referred to as location IDs.

3.1.4 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 – This Recommendation specifies a node ID structure.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 node: A node is a connection point that may be a network device, a user terminal or a process where data can be transmitted, received or forwarded. A node is identified by the node name or node ID.

3.2.2 node name: 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.

4 Abbreviation and acronyms

This Recommendation uses the following abbreviations and acronyms:

DHCP Dynamic Host Configuration Protocol

DNR Domain Name Registry

DNS Domain Name System

FN Future Network

HNR Host Name Registry

ID Identifier

NGN Next Generation Network

5 Conventions

None.

6 Overview

The base document for future networks (FNs), Recommendation ITU-T Y.3001, recommends that FNs provide a new identification structure to effectively support mobility and data access in a scalable manner. For mobility support, the node ID and node locator should not be embedded in the same number or value (see [ITU-T Y.2015]). That is, the node IDs and locators should be derived from different namespaces. A node should be able to change its locator without changing its ID. That is, the node ID to locator mapping should be able to be updated dynamically. Similarly for scalable data access, FNs should facilitate the storing or caching of data closer to a user and they should optimize data access by avoiding the same piece of data traversing the same link in the network multiple times. For this purpose, data need to be uniquely identified using a new identification scheme so that the network can use data identifiers for discovering, caching and routing. In addition to node IDs and data IDs, other IDs such as service IDs and user IDs would also be important for FNs. [ITU-T Y.3031] has been accordingly developed recently for specifying the identification framework and generic requirements for new identifiers in future networks. However, [ITU-T Y.3031] does not recommend any specific ID structure or ID configuration and mapping mechanisms. Therefore, to complement [ITU-T Y.3031], this Recommendation specifies node names, node IDs, and their configuration methods and mapping with locators. Data ID formats and ID configuration methods will be specified by future Recommendations.

The detailed specification of node names and node IDs is essential as future network research is highlighting the importance of the ID/locator split-based design approach. In this approach, communication devices are assigned with their IDs and locators from different namespaces in order to overcome the limitations of the current Internet, which uses IP addresses as both IDs and locators, in supporting mobility, multi-homing, security and scalable routing. For introducing ID/locator split functions in NGN, ITU-T has already developed Recommendations [ITU-T Y.2015], [ITU-T Y.2022] and [ITU-T Y.2057]. Although these Recommendations mention the requirements of node IDs and locators and the functional architecture for using them in NGN, they do not mention the format of node IDs and their configuration method. This Recommendation fills that gap.

Moreover, this Recommendation also specifies a method for binding node IDs with locators. [ITU-T Y.2022] and [ITU-T Y.2057] mention the use of ID/locator binding or the mapping storage function for storing and providing the node ID to locator mappings, but they lack the detailed architecture of the mapping storage system. This Recommendation fills this gap as well by introducing two types of mapping registries: host name registry (HNR) and domain name registry (DNR).

The relationship between the node ID and locator may be either temporary or persistent or both, depending on the type of locator and the communication environment. For example, in a mobile network, a node has a temporary locator which changes as the mobile node moves and attaches to a different network. Similarly, one node ID may relate to two or more locators at the same time, e.g., a node ID can be mapped to different locators if the node is multi-homed.

7 Node names and identifiers

This clause presents a method for the configuration of node names and IDs. A node name and a node ID play similar roles in that they both identify the node. The differences lie in their structures and usage. Node names are usually denoted by a variable-length string of alphanumeric characters and symbols, which may have some semantics so that they can be easily read and remembered by humans. Node IDs are usually denoted by strings of bits or alphanumeric characters that may not be easily memorized by humans. Node names are used during a communication initialization process to find node IDs and locators. On the other hand, node IDs are used as control information in communication protocols and packet headers to identify sessions, packets, or communication endpoints.

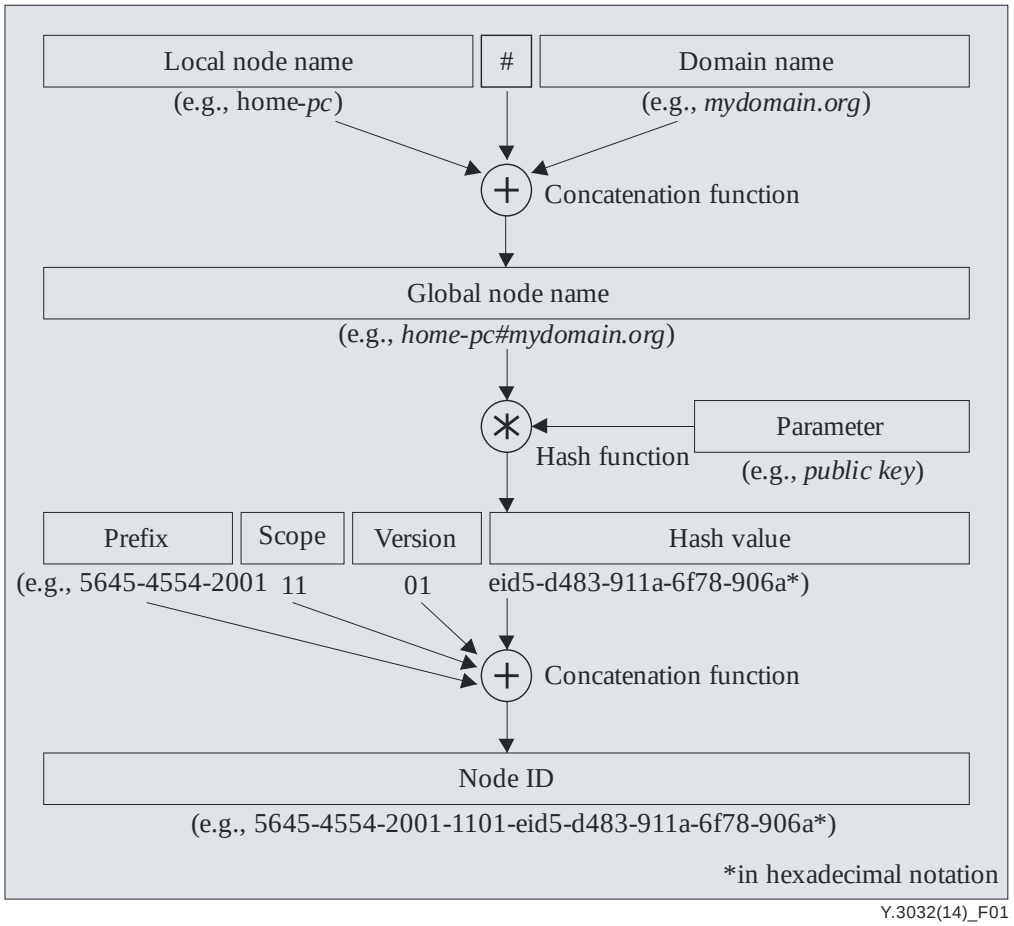

Figure 1 – Possible node name and ID configuration

Figure 1 shows a possible configuration of node names and IDs. A global node name is formed by concatenating a local-scoped node name and global-scoped domain name by using the symbol "#". The local node name is generated from a combination of the node's attributes, such as usage, owner, location, serial number, and installation date and time. Examples of a local node name are *home-pc*, *my-pc-20090731* or *sensor-temp-room-5-202*. The local node name is unique in the administrative domain with which the node is logically associated. The administrative domain is represented by its globally-unique domain name. The global node name is in a format similar to *home-pc#mydomain.org* or *sensor-temp-room-5-202#yourdomain.com*.

A node ID is generated by concatenating prefix, scope and version fields with the cryptographic hash value of the global node name and a parameter. The parameter can be a public key of the node so that the node ID would be the cryptographic binding of the node name and the public key. Such binding is helpful for verifying that the node ID belongs to the given node name. The prefix is used to aggregate node IDs that refer to a specific context and simplify their administration and resolution process. Having a globally-unique prefix helps an organization to generate a bunch of globally-unique node IDs by the organization itself, i.e., without requiring verification of each node ID from an external governing body. A node can optionally derive different versions of node IDs from a single global node name by using different values of the parameter in the hash function, such as SHA-1 [b-NIST-SHS-4]. The scope field indicates the validity and scope of the node ID. It indicates whether the node ID is private, public, local or global. The public IDs are stored in public registries, whereas private IDs that are used for private communications are kept private by the node.

Node IDs find their application in ID/locator split architecture where the node names and node IDs are used in the application and transport layers to identify the endpoints of a communication session [ITU-T Y.2015]. A node ID can simultaneously be mapped to different locators used in network layer protocols. This feature is helpful for mobility and multi-homing because the sessions remain intact even when the network layer changes locators due to mobility or switching the session to a better link in the case of multi-homing. Thus the introduction of node IDs into FNs helps to make the network architecture mobility and multi-homing friendly.

8 Locators

The formats or types of location IDs or locators are dependent on the network layer protocols used in the network. These are the addresses of nodes in the network topology seen by the routing protocols. These protocols define their own locator spaces from which individual nodes obtain/derive their locators. For example, an IPv4 node obtains its locator from the 32-bit long IPv4 address space while an IPv6 node gets its locator from the 128-bit long IPv6 address space.

The other requirements for locators are specified in [ITU-T Y.2015]. A node configures its locator by itself by using an autoconfiguration scheme such as the IPv6 stateless address autoconfiguration protocol specified in [b-IETF RFC 2462]. In order to make the locator globally unique or associate the locator with a network domain, the locator autoconfiguration process uses additional information (such as locator prefix) provided through network advertisements. Alternatively, the node gets a locator from a locator-assigning entity, such as a dynamic host configuration protocol (DHCP) server, by using the DHCP protocol specified in [b-IETF RFC 3315].

9 Node name to node ID and locator mapping storage and name resolution method

Node ID to locator binding methods are essential for dynamically relating a node ID with different locators. The node ID relates to multiple locators simultaneously if the node contains several interfaces (each interface having a unique locator) attached to the network. Similarly, the node ID relates to different locators at different instances of time when the node is moving from one network to another. Thus, a multi-homed node is required to have two or more bindings between its node ID and locators simultaneously, while a mobile node is required to have a changeable binding which is updated easily when the node moves and changes its locator.

The node name to node ID and locator mappings are stored in the mapping storage function, which is updated as the mapping changes due to mobility, multi-homing or locator renumbering (see [ITU-T Y.2015]). To make the mapping storage function scalable, the mapping records are stored in two layers of registries, domain name registries (DNR) and host name registries (HNR) [b-ITU-T Kaleidoscope2009], as shown in Figure 2. The DNR stores the mapping between a domain name and the node ID and the locator of the HNR, while the HNR stores the node name to node ID and locator mappings of all nodes that contain the domain name (managed by the HNR) in their global node names.

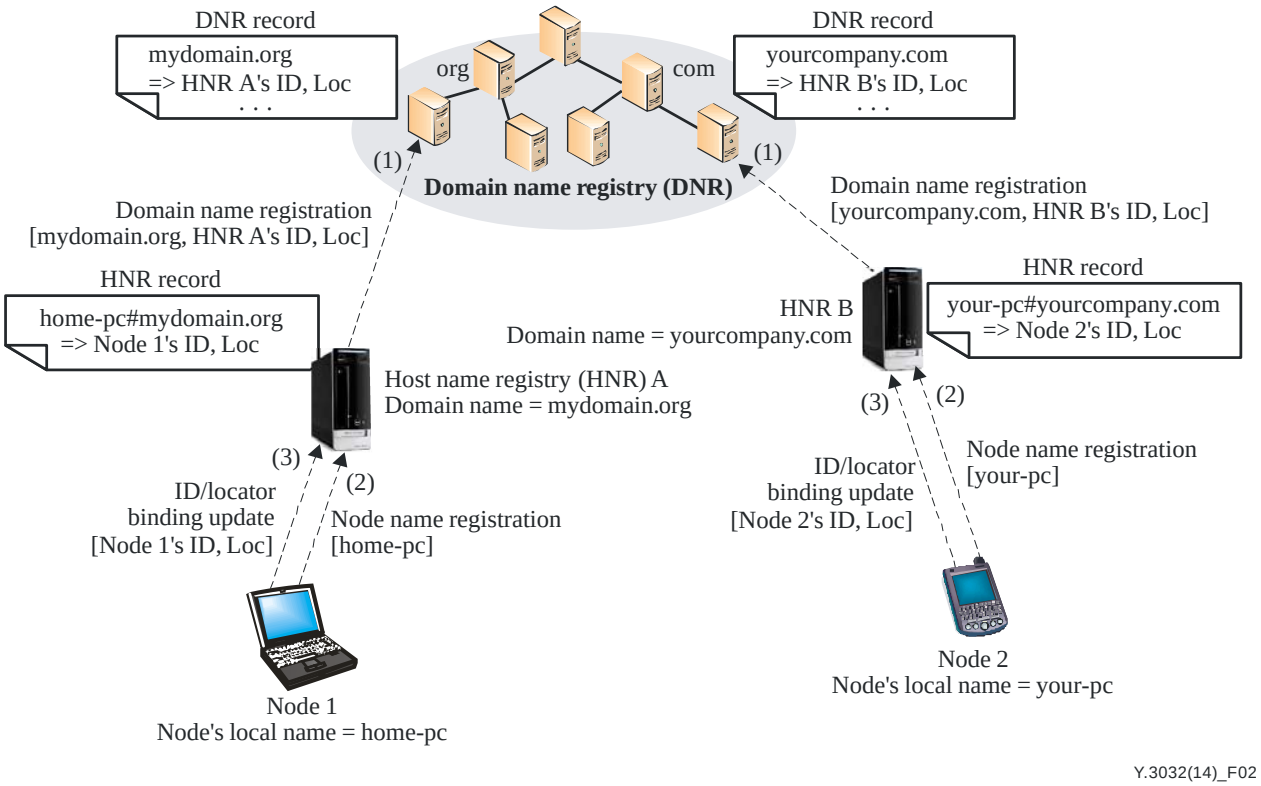

Figure 2 – DNR and HNR records and domain name and node name registration procedures

In Figure 2, each of the domain name registration, node name registration, and ID/locator binding update procedures is shown by a single arrow indicating which node sends the request message and which receives it. Although not shown in the figure, each of these requests is followed by a response in the reverse direction.

The mappings between the domain names and the HNR's IDs and locators that are stored in the DNR (known as DNR records) do not change frequently because the HNRs do not change their ID/locator bindings as the HNRs are assumed to be fixed nodes. The DNRs are organized in a hierarchical structure similar to that of the present-day Internet's DNS because the DNS structure is suitable for storing and retrieving static mapping information. However, unlike the DNS, DNRs are required to store only the domain names assigned to HNRs, and but not the global names of all nodes. Thus, the DNR record size does not grow as fast as the number of nodes. The smaller the size of the DNR record table, the faster the search and retrieval of DNR records.

Since the HNR stores the node name to node ID and locator mapping records and the nodes can change their locators at any time due to mobility, the HNR records are likely to change frequently. So, the HNRs are required to be structured in such a way that their dynamic records can be updated securely at any time by the mobile nodes. In order to ensure consistency in its dynamic records distributed in the network, the HNR does not permit caching of its records by other HNRs. The record is cached only by a peer node which is currently involved in direct communication with the mobile node whose record has been cached. In this case, any update in the mobile node's ID to locator binding is transmitted to the peer node by an explicit binding update signalling message from the mobile node.

9.1 DNR and HNR records registration and update procedure

When an organization wants to set up its network, it decides on its domain name and gets a node ID prefix from an international node ID prefix assigning body. It then builds an HNR to manage the node name to node ID and locator mappings of the nodes belonging to the network. Having received the domain name and other information (such as DNR's ID and locator) from the network

administrator during its set-up, the HNR sends a domain name registration request to the DNR (as shown by arrow (1) in Figure 2). The registration request message includes the binding between the domain name and the HNR's ID and locator, which the DNR saves in its record.

After having its domain name registered in the DNR record, the HNR becomes ready to accept node name registration requests from the nodes belonging to the network. The node sends a node name registration request to the HNR (as shown by arrow (2) in Figure 2) when the node first connects to the edge network or when the user of the node subscribes to the network service. The node name registration request message includes a local name (that is generated by the node itself or entered by the user) of the node and some security content required for authentication. On receiving the registration request the HNR checks if the local name is unique in the domain. If it is not unique (i.e., already stored in the HNR record as another node's name), the HNR requests the node to generate a new name and re-register it. The node name registration process can optionally include an additional negotiation process for deciding on a security function to be used to authenticate the subsequent messages exchanged between the node and the HNR. After registering the node's name the HNR replies with the node and the global node name (i.e., including both local name and domain name). The node then generates a node ID for itself and registers the ID and locator binding in the HNR by sending a node ID to locator binding update message (shown by arrow (3) in Figure 2).

Every time the node changes its locator due to mobility or by connecting through a new link, it is required to send the node ID to locator binding update message to the HNR so that the HNR records always remain up-to-date. The updates in HNR records do not trigger any updates in the DNR records.

The node ID to locator binding update procedure is as follows. When the node changes its locator due to mobility or adds a new locator due to multi-homing, the node configures and sends a binding update message to the HNR. The message includes the node name, node ID, one or more new locators, and their priority levels. The message is secured by using a pre-existing security context (e.g., shared key cryptography). On receiving the binding update message, the HNR first verifies the security, and updates its record based on the message content. After completing the update, the HNR sends an acknowledgement to the node (not shown in Figure 2). In this way, the HNR always stores and provides the node's up-to-date ID to locator mapping records.

9.2 Node name to node ID and locator mapping record retrieval procedure

When a node wants to start communication with another node, these nodes must obtain each other's ID to locator mappings through a name resolution process as shown in Figure 3. To explain the resolution process, assume that Node 1 with node name *home-pc#mydomain.org* wants to communicate with Node 2 with name *your-pc#yourcompany.com*. The resolution process consists of two steps: domain name look-up and node name look-up. For the domain name look-up, Node 1 sends a domain name resolution request containing Node 2's domain name to the DNR and receives HNR B's ID and locator in the response message. Node 1 then performs the node name look-up by querying HNR B. HNR B searches its record for Node 2's name and responds to Node 1 by a node name resolution response containing Node 2's name to node ID and locator mapping record.

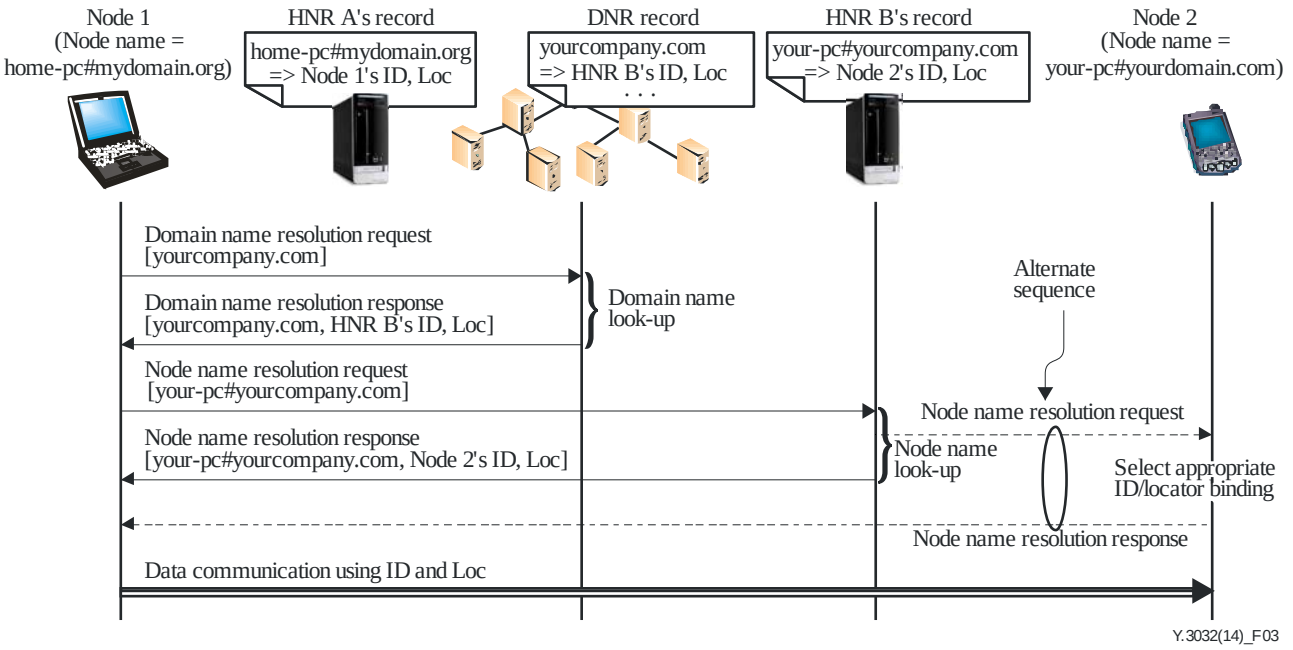

Figure 3 – Node name to node ID and locator mapping retrieval procedure

Through the above procedure Node 1 receives Node 2' name to ID and locator mapping. However, Node 2 has not yet obtained Node 1's name, ID and locator. Node 2 is informed of Node 1's name to ID and locator binding by one of the following two methods. In the first method, after receiving Node 2's name to ID and locator binding in the node name resolution response message from HNR B, Node 1 directly informs of its name to ID and locator binding by inserting the binding in the first data packet or signalling packet sent to Node 2. In the second method, Node 1 inserts its name to ID and locator binding in the node name resolution request. When getting the request, HNR B, instead of replying to Node 1 with the name resolution response message, forwards the request message to Node 2. In this way, Node 2 knows about Node 1's name to ID and locator binding and stores it in its ID table, and then replies to Node 1 by a node name resolution response message containing its node name to ID and locator binding (as shown by the alternate sequence of dotted arrows in Figure 3). The second method has advantages that both nodes can select their appropriate IDs and locators for the given service during the name resolution process, without requiring additional signalling messages exchange for the negotiation.

10 Environmental considerations

The introduction of node ID and locator separation into FNs has both positive and negative impacts on the environment in terms of energy consumption. On the positive side, it helps routers in the core network to save energy consumption by reducing the routing table size and update frequencies even when the edge network configuration changes. On the negative side, the node ID configuration, locator configuration and ID to locator mapping mechanisms consume additional energy.

The node name and node ID configuration method does not have these impacts because it does not take place frequently, as the node configures its name and ID when it is connected to the network for the first time. The locator configuration method can have some impact as it takes place often, when the node moves from one access network to another. Node ID to locator mapping storage and resolution, which takes place frequently when a node looks for another node's name to ID and locator mapping when the former initiates communication with the latter or when the node moves from one network to another, would have a significant impact on the environment. Future Recommendations or the use of existing Recommendations (such as [ITU-T Y.3021]) can optionally be applied to reduce the negative impacts.

11 Security considerations

Both information and infrastructure security concerns are relevant to this Recommendation. Information security concerns exist with the node name and node ID configuration, locator configuration and node name to node ID and locator mapping resolution methods. To configure a node name, node ID or locator, the node needs configuration parameters from the network. Without a proper information and infrastructure security mechanism in place, the node cannot be able to acquire proper values of these parameters. The mapping records can be compromised in the storage servers or on the way when they are being provided to querying nodes. Similarly, the mapping storage infrastructure can be compromised by denial of service (DoS) attacks.

Additional security considerations could be relevant from the regulatory point of view. Future Recommendations or the use of existing Recommendations (specifying encryption, authentication, data or infrastructure protection mechanisms, etc.) could resolve these security issues.

Bibliography

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

[b-ITU-T-Kaleidosocope2009] Kafle, V.P. *et al.* (2009), *An ID/locator split architecture of future networks*, ITU-T Kaleidoscope event, Mar del Plata, Argentina.

[b-IETF RFC 2462] IETF RFC 2462 (1998), *IPv6 Stateless Address Autoconfiguration*.

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

[b-NIST-SHS-4] National Institute of Standards and Technology (2012), *Secure Hash Standard (SHS)*, FIPS PUB 180-4.

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, 2014