International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.3077

(09/2021)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Future networks

Framework for interworking of heterogeneous application domain connected objects through information-centric networking in IMT-2020

Recommendation ITU-T Y.3077

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

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
Computing power networks	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.3599
BIG DATA	Y.3600–Y.3799
QUANTUM KEY DISTRIBUTION NETWORKS	Y.3800–Y.3999
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	
General	Y.4000–Y.4049
Definitions and terminologies	Y.4050–Y.4099
Requirements and use cases	Y.4100–Y.4249
Infrastructure, connectivity and networks	Y.4250–Y.4399
Frameworks, architectures and protocols	Y.4400–Y.4549
Services, applications, computation and data processing	Y.4550–Y.4699
Management, control and performance	Y.4700–Y.4799
Identification and security	Y.4800–Y.4899
Evaluation and assessment	Y.4900–Y.4999

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

Recommendation ITU-T Y.3077

Framework for interworking of heterogeneous application domain connected objects through information-centric networking in IMT-2020

Summary

Recommendation ITU-T Y.3077 specifies the framework, functions, and procedures for information-centric networking (ICN) device registration and discovery in distributed directory system functions collocated in gateways of each application domain and interworking of the directory system functions of various application domains by extending the ICN approach. It also specifies the communication procedure for interworking of devices within and across heterogeneous application domains for device management as well as accessing data and services provided by the devices.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.3077	2021-09-13	13	11.1002/1000/14775

Keywords

Directory service, ICN, information-centric networking, IMT-2020.

---

* 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/software copyrights, 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 appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T Y.3077

Framework for interworking of heterogeneous application domain connected objects through information-centric networking in IMT-2020

1 Scope

The scope of this Recommendation includes the extension of the information-centric networking (ICN) approach to specifying the following framework, functions, and procedures:

- Device registration and discovery in distributed directory system functions collocated in gateways of each application domain and interworking of the directory system functions of various application domains.
- Communication procedure for interworking of devices within and across domains for device management as well as accessing data and services provided by them.

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

[ITU-T Y.3071] Recommendation ITU-T Y.3071 (2017), *Data aware networking (information centric networking) – Requirements and capabilities*.

[ITU-T Y.3074] Recommendation ITU-T Y.3074 (2019), *Framework for directory service for management of huge numbers of heterogeneously named objects in IMT-2020*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 device (ICN) [ITU-T Y.3074]: An entity connected to the network that generates, holds, transmits or consumes data, contents, or information.

3.1.2 directory service [ITU-T Y.3074]: A network entity that stores information about objects as records and provides records to other entities that send look-up queries containing a search key of the requested records. A directory service stores and provides records that can be useful for control and management functions of the network.

3.1.3 information-centric networking (ICN) [b-ITU-T Y-Sup.48]: A new approach to networking where named objects (not only devices) are the principal components for the network. Named data objects can be stored in network nodes (with caching capability) distributed throughout the network. Data objects are transmitted by using names to requesting consumers from any network node that can provide requested data. Locations of the nodes that store data objects in their caches are irrelevant to consumers because they send their requests for data objects by using names (not the data object locations).

NOTE – ICN is an alias to data-aware networking (DAN) [b-ITU-T Y.3033], and content-centric networking (CCN) [b-CCN] and named data networking (NDN) [b-NDN] are the example implementations of ICN.

3.1.4 ICN device [ITU-T Y.3074]: An entity connected to the network that generates, holds, transmits, or consumes ICN data objects.

3.1.5 named device [ITU-T Y.3074]: A device that is assigned with or identified by a name.

3.1.6 named object [ITU-T Y.3074]: An object that is assigned with or identified by a name.

3.1.7 record [ITU-T Y.3074]: Information about an object stored in and provided by directory service function.

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

3.2 Terms defined in this Recommendation

This Recommendation uses the following terms:

3.2.1 application-specific local domain: A local network of devices for a specific application, which may use the domain-specific device naming architecture and communication protocols.

3.2.2 ICN-based common naming domain: A global network consisting of information-centric networking (ICN) routers and directory service functions and communicating by using ICN protocols to interconnect application-specific local domains via gateways.

3.2.3 local directory service function: A directory service function located in an application-specific local domain.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AMQP	Advance Message Queueing Protocol
CCN	Content-Centric Networking
DAN	Data-Aware Networking
DHCP	Dynamic Host Configuration Protocol
DSF	Directory Service Function
DSF-ICN	Directory Service Function in ICN-based common name domain
GW	Gateway
ICN	Information-Centric Networking
ID	Identifier
LDSF	Local Directory Service Function
LDSCF	Local Directory Service and Cache Function
NDN	Named Data Networking
SOAP	Simple Object Access Protocol
XMPP	Extensible Messaging and Presence Protocol
Wi-SUN	Wireless Smart Ubiquitous Network

5 Conventions

In this Recommendation:

The keywords "is required to" indicate a requirement which must be strictly followed and from which no deviation is permitted, if conformance to this Recommendation is to be claimed.

The keywords "is recommended" indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

The keywords "can optionally" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option, and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with this Recommendation.

6 Introduction

New connected devices used in various application domains such as energy management, factory automation, home appliances, and environment sensors usually have their own naming architecture and communication methods, and they may not be able to communicate across domains. The devices used in these silo application domains are usually named heterogeneously by the device manufacturers or application service providers. Because of heterogeneity in names and communication methods, these devices are also not easy to manage by human operators because their names may not be human friendly, such as a random sequence of alphanumeric characters, and not uniform across various application domains. To overcome this situation, this Recommendation proposes to extend the information-centric networking (ICN) approach [ITU-T Y.3071] to specifying the framework, functions and procedures for device registration and discovery in distributed directory service system functions, which can be either collocated in gateways or exist separately, of each application domain and interworking of the directory system functions of various application domains. It describes communication procedures for interworking of devices within and across domains for device management as well as accessing data and services provided by them.

For a reference, Appendix I presents the different types of naming schemes for devices, data and services considered for application-specific domains in various standards.

7 Framework of ICN-based device registration and discovery

Figure 1 shows the framework for interworking of application-specific local domains through the ICN-based common name domain. It contains the local directory service function (LDSF) in each application-specific local domain and directory service function in the ICN-based common name domain (DSF-ICN). As specified in [ITU-T Y.3074], in the IMT-2020 network's control plane, the local directory service exists as the local directory service and cache function (LDSCF) and the directory service exists in the directory service function (DSF). In non IMT-2020 access networks of application-specific local domains, the local directory service function may exist separately. This clause describes the local directory service function of non IMT-2020 local access domains, therefore, the sequences of operations of name record registration and resolution described here are different in various aspects from those described for IMT-2020 access network in [ITU-T Y.3074].

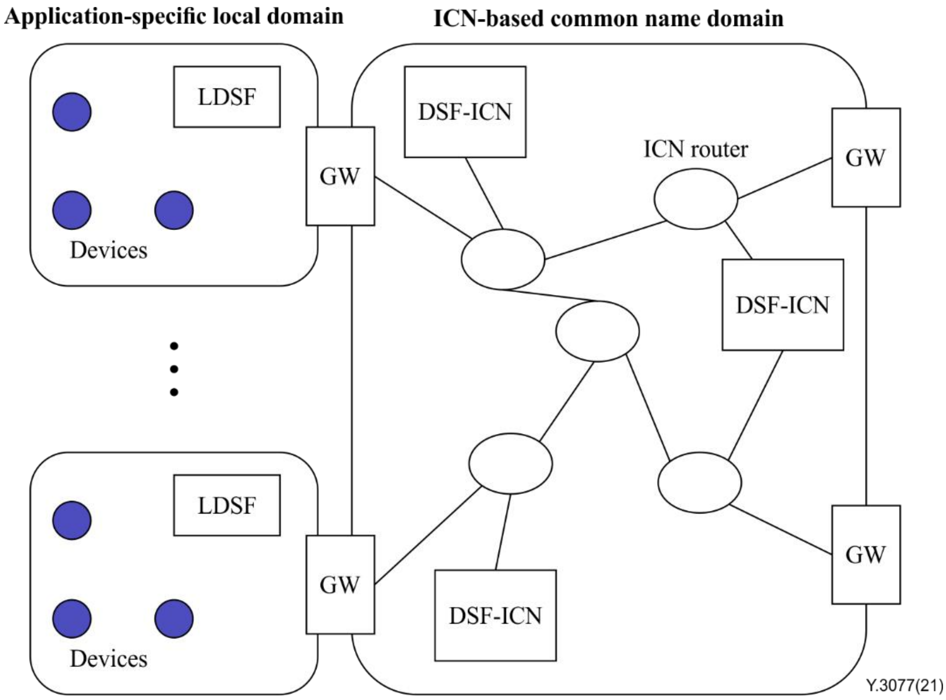

Figure 1 – Components of ICN-based device registration and discovery framework

The other components i

n the application specific local domain are the end devices or objects that provide or consume service or data of the application-specific local domain. The devices in the given application-specific local domain may have their own naming architectures. The device names, together with other parameters of the devices such as their security parameters and types of services or data they provide, are stored in the LDSF. The LDSF interacts with the DSF-ICN through the gateway for the registration of device names and other parameters.

The gateways (GWs) interconnect the application-specific local domains and ICN-based common name domain. To interconnect the application-specific local domains that have heterogeneous types of device naming architectures and enable data plane communication across the ICN-based common name domain, the GWs contain *adaptation functions* in the control plane and a *message translation function* in the data plane. The GW control plane interacts with both the LDSF and DSF-ICN to retrieve name records containing various parameters of devices that are used by the adaptation function for enabling communication across domains.

Inside the ICN-based common name domain there are ICN routers that are provisioned with a name-based routing mechanism. They use device or content names present in a message header to carry out forwarding decisions based on the entries in the routing table. The routers interact with the DSF-ICN to get the name prefix, which are used in route computation. The routes are populated in routing tables, more specifically, in a forwarding information base.

7.1 ICN-based device registration

This clause describes the methods for local directory service configuration, device configuration and device registration.

7.1.1 Local directory service configuration

In each application-specific local domain, an LDSF is configured at the beginning of the procedure for setting up the application-specific domain. LDSF configuration is similar to a domain name system (DNS) [b-DNS] server and resolver that are configured within a local area network connected to the Internet.

7.1.2 Device configuration

The devices that are to be connected to the application-specific domain are supposed to be equipped with functions and necessary parameters (e.g., serial number, ID, authentication keys, and certificates) either hardcoded in the factory or provided by the administrator who connects them to the network. When the devices are connected to the network, they obtain access parameters, such as IDs, names, addresses, and security keys, of the LDSF and the GW either manually supplied by the administrator or automatically provided by a preinstalled function through interacting with the network, like dynamic host configuration protocol (DHCP) [b-DHCP] being used by devices for getting connected to the Internet.

7.1.3 Device registration

After obtaining the access parameters of the LDSF, the device configures a name registration request message containing the device authentication parameters, such as serial number, ID, and certificates, and the message is properly secured through the available security mechanism. The message is transmitted to the LDSF by the available communication method in the given application-specific domain.

After receiving the message, the LDSF verifies the message authenticity and creates a name record with the parameters of the devices. The name record is stored in the local directory database in the format specific to the local domain. The name record contains the name as well as other parameters such as security keys, certificate, device owner's name, and types of data or services the device provides.

Since each domain may have a different naming scheme, the type of names and communication methods they use to register the name and related parameters in the LDSF can optionally be different.

7.2 ICN-based interworking of name directory service functions

This clause describes the LDSF setup, global name configuration, and global name registration and distribution in the ICN-based common name domain.

7.2.1 Local directory service setup

When an LDSF is setup in an application-specific local domain, it is required to setup a secure communication session with the DSF-ICN if the LDSF interworks with the DSF-ICN. The establishment of the secure communication session can be initiated either by the LDSF in the application-specific local domain or by the DSF-ICN.

In the former case, the LDSF is required to be provided with the access information such as name, address, and security keys of a DSF-ICN and with the directory service subscription information such as ID, access key, and authentication parameters. With this information the LDSF becomes capable of initiating a secure communication session with the DSF-ICN.

In the latter case, the DSF-ICN is required to be provided with the access information such as name, address, and security keys of the LDSF and with the local directory service subscription information such as ID, access key, and authentication parameters. With this information the DSF-ICN is capable of initiating a secure communication session with the LDSF of the application-specific local domain.

In either case, the counterpart of the session initiator can derive the subscription information for the session initiator through the established communication session.

Through the interaction with the DSF-ICN, the LDSF may optionally receive one or more names to identify the application-specific local domain in the global name scope.

7.2.2 Global name configuration

By using the global name of the application-specific local domain, the LDSF may optionally configure a global name for each of the devices. The LDSF uses a global name configuration method to produce the global name in the format as specified by the DSF-ICN. The global name of a device contains the global name of the application-specific local domain assigned by the DSF-ICN and a parameter related with the local ID of the device. The node ID configuration method specified in [ITU-T Y.3032] can be used for the global name configuration, which concatenates the global name of the application-specific local domain with the local name or its hash value to generate the global name of a device.

For reference, Appendix II presents a general-purpose name configuration framework.

7.2.3 Global name registration

The LDSF generates a name registration request message containing the global names of one or more devices and related parameters (e.g., security keys and certificates) and types of data and services the device provides. The message is properly secured through available security mechanisms and transmitted to the DSF-ICN through the GW. After receiving the message, the DSF-ICN verifies the message's authenticity, creates a name record for each device and stores in its database in the format specific to the common name domain. If the name in the registration message does not carry the global name of the application-specific local domain, the global name is added to the name record.

The LDSF may store several parameters specific to the application-specific local domain, which cannot be shared outside the domain because of privacy issues or being irrelevant. When performing the global registration, the LDSF filters these parameters according to the privacy policy rules set for the records of each device.

7.2.4 Global name distribution in common name domain

After storing global name records of devices in the DSF-ICN, they are proactively distributed to routers located in the common name domain. The routers update their routing tables in such a way that a service or data request destined to a global name would be forwarded to the GW of the application specific local domain where the device with the global name is located in. Since there exist several copies of DSF-ICNs for reasons of scalability, resiliency and load sharing, the global name records can optionally be distributed from one DSF-ICN to another. In this case, the source DSF-ICN is the authoritative directory service function for the given global name prefix, while the destination DSF-ICNs are the proxy directory service functions. The proxy directory service functions hold the name records temporarily in caches and may delete after a timeout.

7.3 ICN-based device and service discovery

The services provided by the application specific local domain or devices are discovered through the name resolution procedures. This clause describes the procedures for name resolution within a local domain and across domains.

7.3.1 Name resolution within a local domain

The application requesting services or data from devices located in the same application-specific local domain configures a name resolution request message containing the device's or service's local name as the target search key and the list of parameter names whose values are expected to be returned in response. The LDSF searches its database with the target search key and retrieves all requested parameter values. The LDSF then configures a response message containing the requested parameter values and sends the response to the requesting application.

7.3.2 Name resolution across domains

The application requesting services or data from devices that are located in different application-specific local domains must configure a name resolution request message containing the device's global name as the target search key and the list of parameter names whose values need to be returned in a response. The name resolution request message is answered either by a nearby proxy DSF-ICN or routed to the authoritative DSF-ICN. In either of these cases, the DSF-ICN searches its database with the global name as the target search key and retrieves all requested parameter values. The DSF-ICN then configures a response message containing the requested parameter values and sends it to the requesting application. The requesting application can also be a name-based routing protocol in an ICN router of the ICN-based common name domain that does not contain the route information for the global name appearing in messages arriving at the router.

8 ICN-based communication procedure for interworking of devices

An ICN-based interworking system has the functional components as shown in Figure 2. In addition to the LDSF used in each local domain, the ICN-based interworking system maintains a directory service with the functionality of directory service function defined in [ITU-T Y.3074]. The directory service (DSF-ICN) is used to store a variety of attributes including hostnames, locations, local domains, object types and group names among others.

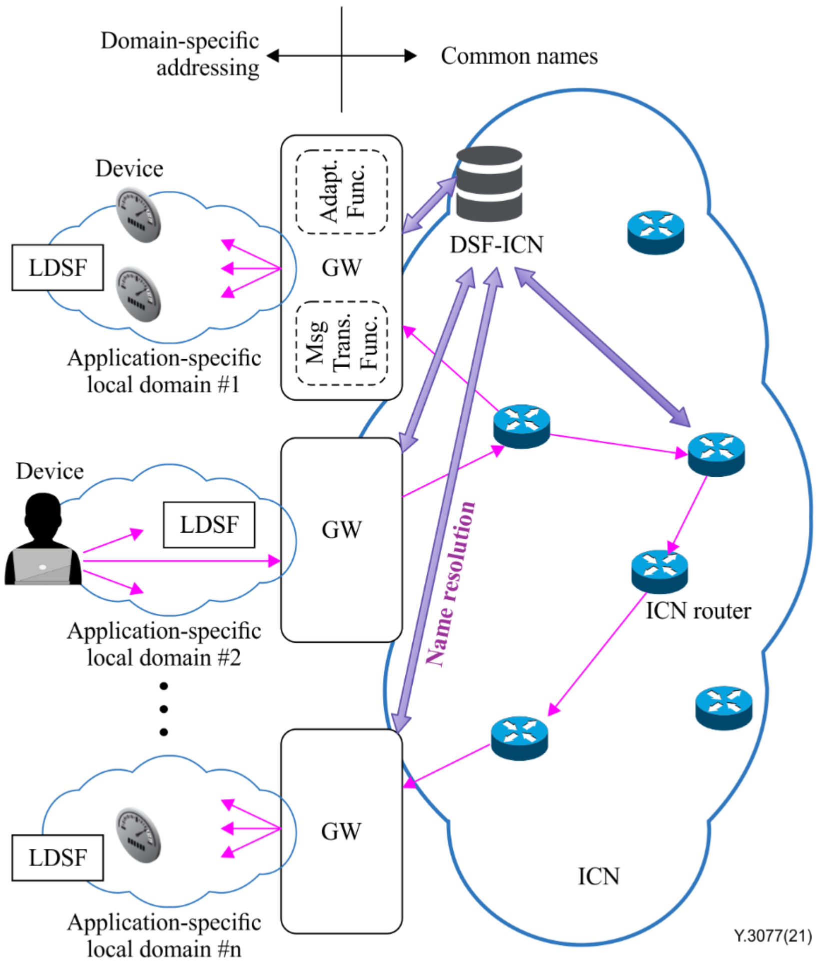

Figure 2 – Functional blocks for interworking of domains

The DSF-ICN is used to store and provide the name mapping records required to convert the domain-specific addresses used in each application-specific domain and the ICN-based common name domain. The adaptation function included in the GW that connects an application-specific domain with the ICN-based common name domain communicates with the DSF-ICN to use and manage name-related mapping records. In addition to the adaptation functions collocated in the GWs, ICN routers may communicate with the DSF-ICN to resolve names to addresses.

The GW contains the message translation function which translate a message header when forwarding the message in the data plane from the application-specific local domain to the ICN-based common name domain and vice-versa.

8.1 Message format

The application message created in one of the application-specific local domains contains an address/name specifying the destination of the message. The message is first forwarded in the ICN-based common name domain, and then through the GW it is further forwarded in the other application-specific local domain using different addressing/naming schemes. The message traverses different networking environments from its originating domain through GWs. At the GW of a different network environment, the destination address/name needs to be resolved to the address/name of the entering domain.

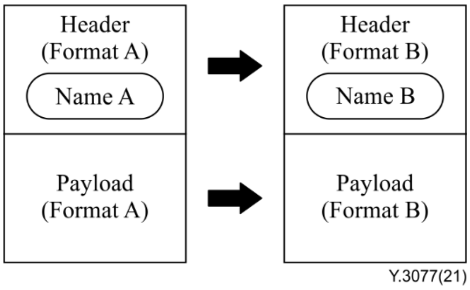

Figure 3 – Message conversion

As shown in Figure 3, messages generally have two parts: header and payload. The header formats are different from one domain to another although a header is required to contain at least a name field. What the name field expresses depends on the domain: the name may express a topic in publish/subscribe networks or a content address/name to be requested in other ICN-based domains. The name is information to specify the destinations of the message in either way. Another name to send response messages to the originator of the message may be included in the header as well. Such a name also needs to be converted if it exists. The name mapping information is required to be supplied by the DSF-ICN. Moreover, the formats of payloads may be different in different domains. The format mapping information can optionally be supplied by the DSF-ICN. Based on the format mapping information, the message translation function of the GW converts messages to the format that fits with the entering domain. Thus, the message format conversion capability can optionally be included in the message translation function.

8.2 Communication sequence

The communication procedure for interworking of different application-specific local domains and an ICN-based common name domain is shown in Figure 4.

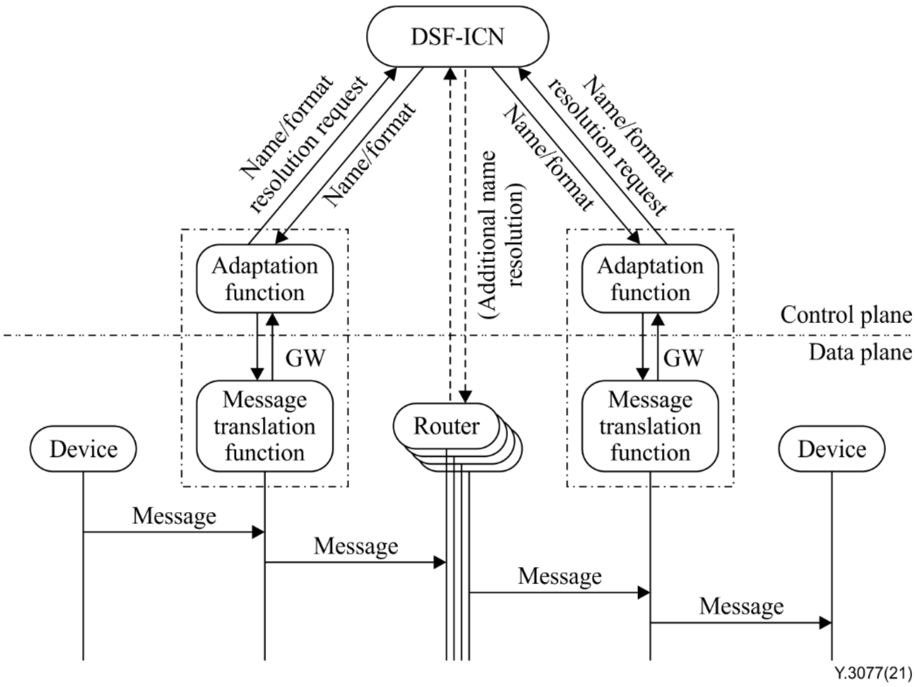

Figure 4 – Interdomain communication sequence

NOTE – Although the figure only shows the message originating from an application-specific local domain, traversing the ICN-based common name domain, and terminating in another application-specific local domain, some communications can originate from or terminate in the ICN-based common name domain.

Since naming schemes used in an application-specific local domain and the ICN-based common name domain are different, name translation is required to be performed at the GW connecting the application-specific local domain and the ICN-based common name domain. The adaptation function inquires the DSF-ICN to obtain name records that are used to translate the name/address used in one domain to the name/domain used in the other domain. In addition, the DSF-ICN may optionally also provide routing information in the ICN-based common name domain.

The message generated at a domain, either an application specific local domain or the ICN-based common name domain, traverses the same domain, and eventually reaches to the adaptation function of its GW. Upon the reception of the message by the GW, the message translation function determines whether the message is to be forwarded to another domain from the destination address field of the message. If the message is to be forwarded to the other domain, the message translation function requests the adaptation function of the GW to find the proper name/address in the domain to be forwarded. The message translation function may optionally request the adaptation function to translate other addresses/names such as the name of the originator of the message. The adaptation function inquires the DSF-ICN to find the addresses/names. The message translation function receives the name/address from the adaptation function, and the name field in the message format shown in Figure 3 is filled with the name/address. Also, the message translation function may translate other names. In addition to the name/address translation, the message translation function may optionally perform payload translation based on the information provided by the adaptation function. After translation of the message, it is forwarded to the next router. The message is received by another GW if the message is addressing another application-specific local domain. Similarly, the adaptation function of the egress GW inquires the DSF-ICN so that it can find the proper address/name to further forward the message in the outgoing domain.

9 Security considerations

A secure communication session is required to be set up between an LDSF and the DSF-ICN as stated in clause 7.2. Using this secure communication session, information of devices registered at the LDSF and determined by the LDSF to be globally accessed is forwarded to the DSF-ICN. The secure communication channel authenticates and authorizes both the LDSF and the DSF-ICN reciprocally. The reliability of the device information stored in the DSF-ICN depends on the trustworthiness of the LDSF and the management of its application-specific domain. When an application-specific domain is connected to the DSF-ICN, the management of the application-specific domain should be carefully reviewed, or vice versa.

Authenticity of communication counterparts can be examined using information stored in LDSFs and the DSF-ICN.

Appendix I

Status of various types of naming schemes in related standards

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

Various approaches to naming devices, data, and services have been discussed in the literature and specified in related standards. This appendix lists some of these activities being carried out in standards development organizations and forums.

Internet Research Task Force (IRTF) Information-Centric Networking Research Group has listed various types of names in [b-ICNRG ICN-IoT]. These are hash-based content names, hierarchical names, and semantic and metadata-based content names. Various approaches to naming devices, content, and services are also discussed. Several characteristics of names such as size, flexibility, trust, scoping, and confidentiality are considered as the influencing factors in naming. For the name resolution services, the characteristics of scalability, deployability, latency, locality, network efficiency, and agility are listed. In terms of security, the name spoofing attack, stale mapping attack, false name announcement attack, and malicious collusion attack are also discussed. However, it does not specify any naming architecture.

ZigBee is considered as a suitable technology for connecting various types of IoT application-specific devices because of its low cost and low power operation. Typical application areas of ZigBee include: home and commercial building automation, wireless sensor networks, industrial control systems, e-health data collection, smoke and intruder warning, smart meters and energy grids. ZigBee specifies three types of devices: ZigBee End Device (ZED), ZigBee Router (ZR), and ZigBee Coordinator (ZC). They use IEEE 802.15.4 in physical and link layers. ZigBee uses destination and source addresses in different layers: IEEE 802.15.4 link layer, ZigBee network layer (NWK), and ZigBee application support (APS). ZigBee applications or cluster library contains control commands, e.g., toggle switch (switch ID 2 bytes). Devices and services are given names in the applications only. The lower layers use one to six bytes addresses (e.g., MAC address) for networking. Match descriptor is a mapping table maintained by ZigBee nodes to translate a node or service name used in applications (e.g., OnOffSwitch) to the addresses used in lower layers.

ZigBee Smart Energy 2.0 specifications define an Internet protocol-based communication protocol to monitor, control, inform, and automate the delivery and use of energy and water.

Similarly, for more lower range communication, especially connect peripheral devices to a hub system or computer, Bluetooth Low Energy has been used. BLE provides higher throughput than ZigBee. As ZigBee, BLE also uses names in applications and MAC addresses in lower communication layers.

For naming resources in the Internet, Universal Resource Identifiers (URIs) [b-URI] are to name services, content, or devices (also known as hosts) in the Web and Internet applications. A URI is generally represented as URI = *scheme: [//authority] path [?query] [#fragment]*, where the authority component constitutes three subcomponents: *[uerinfo@], host, and [:port]*. Popular schemes are *http, https, ftp, mailto, file,* and *data*. Uniform resource locator (URL) is a type of URI that identifies a resource by its primary access mechanism and network location.

The other Internet application protocols that use names are CoAP [b-CoAP], extensible messaging and presence protocol (XMPP) [b-XMPP], MQTT [b-MQTT], and advance message queueing protocol (AMQP) [b-AMQP]. CoAP is a REST based protocol which represents resources by tagging with attributes. These attributes are also used for resource discovery. XMPP protocols is used for instant messaging. It contains functions for message presence notification, session establishment, and data transfer. MQTT is a lightweight publish/subscribe messaging protocol, which is used for enterprise telemetry. Similarly, AMQP is the protocol for message queueing, publish and subscription notification, and data transfer with delivery guarantees. It is used in financial services. All these protocols are run over Internet (TCP/UDP/HTTP).

IEEE1888 ubiquitous green community control network protocol is another application layer protocol developed for application specific domains. It is used for environmental monitoring, smart energy, and facility management applications. It is a simple protocol that supports reading and writing of time-series data using the extended markup language (XML) and the simple object access protocol (SOAP). The devices and data are named by using URIs. It considers heterogeneous networks convergence and scalability, specifies the requirements of network convergence, and extends the system architecture to make it capable of interoperating with heterogeneous access networks and improves the efficiency, flexibility, scalability, and manageability.

Wireless smart ubiquitous network (Wi-SUN) [b-WiSUN] is another application specific domain protocol, which is based on IEEE802.15.4g standard as well as other IEEE 802 and IETF standards. Wi-SUN field area network (FAN) is a mesh network protocol and allows its messages to travel a very long-distance hop-by-hop traversal, unlike the indoor personal area mesh networks (PAN) such as ZigBee and BLE.

Appendix II

General-purpose name configuration framework

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

This appendix describes a general-purpose name configuration framework, which can accommodate different kinds of name generation engines to configure various types of names as per the networking and application scenarios and requirements. Figure II.1 shows the general-purpose name configuration framework, which takes heterogeneous types of names from various groups of objects as input and generates output names suitable for given networking scenarios. The general-purpose naming framework contains various kinds of name generation engines.

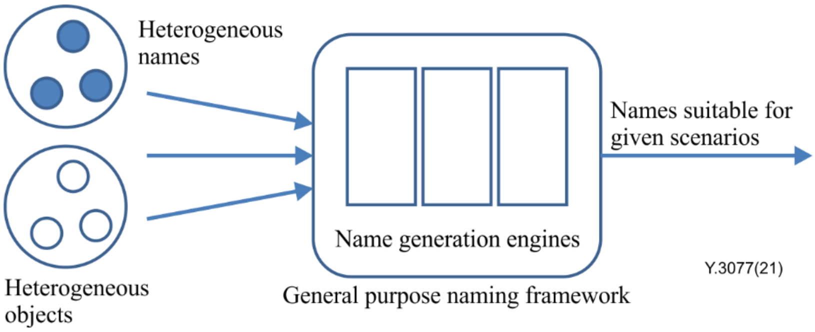

Figure II.1 – General-purpose name generation framework

Figure II.2 shows the layout of a name generation engine. Beside the input name, the name generation engine also takes as input the static parameters and generates an output name by mixing the input name and the static parameters.

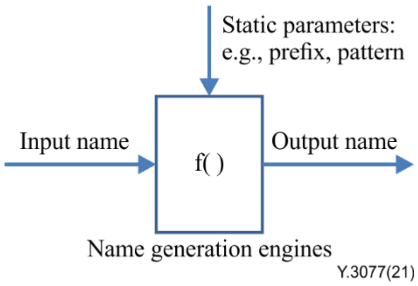

Figure II.2 – Name generation engine

Some example name generation scenarios (hierarchical names with a static prefix and a random suffix) are outlined below.

Table II.1 – Name generation in various schemes

Scheme	Input name	*f ()*	Static parameters	Output name
[b-URI]	Various parameters	URI = *scheme: [//authority] path [?query] [#fragment]*	Authority parameter	URI value
[ITU-T Y.3032]	Device local name	Global hostname = *local_hostname#domain_name* Global ID = *prefix+scope+Hash(global hostname)*	Prefix, scope	Globally unique hostname
[b-MobilityFirst]	Public key	GUID = *Hash (public key)*	None	Global unique identifier (GUID)
[b-HIP]	Public key	HIT = *Hash (public key)*	None	Host identity tag (128 bits)

Table II.1 shows a few name generation example schemes. As described in Appendix I, URI takes the scheme, authority, query and fragment parameters and concatenates these parameters by syntax symbols of slash, colon, question mark and hash tag. To generate a name the authority (i.e., domain name) is the static parameter.

[ITU-T Y.3032] specifies a global hostname and global ID generation scheme which takes a device local name as an input parameter and prefix and scope as static parameters and generates a global hostname and a global host ID. The prefix is unique for the administration that is responsible for the management and administration of the entities (i.e., devices, data and services) that are named, and the scope indicates the validity of a generated ID (e.g., locally or globally scoped).

Similarly, [b-MobilityFirst], a National Science Foundation (NSF) funded project for a future Internet architecture, generates a global unique identifier (GUID) by hashing the public key of an entity. Likewise, host identity protocol (HIP), a secure session establishment protocol specified by IETF, also generates a host identity tag (HIT) by hashing the public key.

In this way, several name generation engines can co-exist inside a general-purpose name configuration framework to generate various kinds of names and identifiers.

Bibliography

[b-ITU-T Y.2091] Recommendation ITU-T Y.2091 (2014), *Terms and definitions for Next Generation Networks.*

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

[b-ITU-T Y-Sup.48]: ITU-T Y-series Recommendations – Supplement 48 (2018), *Proof-of-concept for data service using information centric networking in IMT-2020.*

[b-AMQP] *Advance Message Queueing Protocol*. https://www.amqp.org/

[b-CCN] RFC 8569 (2019), *Content-Centric Networking (CCNx) Semantics*, IETF, July.

[b-CoAP] RFC 7252 (2014), *The Constrained Application Protocol (CoAP)*, IETF, June.

[b-DHCP] RFC 2131 (1997), *Dynamic Host Configuration Protocol*, IETF, March.

[b-DNS] RFC 1034 (1987), *Domain Names – Concepts and Facilities*, IETF, November.

[b-HIP] A. Gurtov (2008), *Host Identity Protocol (HIP), Towards the Secure Mobile Internet*, Wiley.

[b-ICNRG ICN-IoT] *Design Considerations for Applying ICN to IoT* (2019), Internet-Draft, draft-irtf-icnrg-icniot-03, IRTF, May.

[b-MobilityFirst] A. Venkataramani, J.F. Kurose, Dipankar Raychaudhuri, K. Nagaraja, S. Banerjee, and Z. Morley Mao, *MobilityFirst: A Mobility-Centric and Trustworthy Internet Architecture*, ACM SIGCOMM Computer Communication Review, Vol. 44, No. 3, July 2014, pp. 74-80.

[b-MQTT] *MQTT Protocol* (2020), OASIS standard. http://mqtt.org/

[b-NDN] Lixia Zhang, Alexander Afanasyev, Jeffrey Burke, Van Jacobson, kc claffy, Patrick Crowley, Christos Papadopoulos, Lan Wang, and Beichuan Zhang. *Named data networking*. SIGCOMM Comput. Commun. Rev., Vol. 44, No. 3, pp. 66-73, July 2014.

[b-URI] RFC 3986 (2005), *Uniform Resource Identifier (URI): Generic Synta*x, IETF, January.

[b-XMPP] RFC 6120 (2011), *Extensible Messaging and Presence Protocol (XMPP): Core*, IETF, March.

[b-Wi-SUN] *Wi-SUN Alliance* (2020). https://www.wi-sun.org/

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
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	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
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, next-generation networks, Internet of Things and smart cities**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2021