International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.675

(05/2015)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

OSI networking and system aspects – Naming, Addressing and Registration

OID-based resolution framework for heterogeneous identifiers and locators

Recommendation ITU-T X.675

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	
Services and facilities	X.1–X.19
Interfaces	X.20–X.49
Transmission, signalling and switching	X.50–X.89
Network aspects	X.90–X.149
Maintenance	X.150–X.179
Administrative arrangements	X.180–X.199
OPEN SYSTEMS INTERCONNECTION	
Model and notation	X.200–X.209
Service definitions	X.210–X.219
Connection-mode protocol specifications	X.220–X.229
Connectionless-mode protocol specifications	X.230–X.239
PICS proformas	X.240–X.259
Protocol Identification	X.260–X.269
Security Protocols	X.270–X.279
Layer Managed Objects	X.280–X.289
Conformance testing	X.290–X.299
INTERWORKING BETWEEN NETWORKS	
General	X.300–X.349
Satellite data transmission systems	X.350–X.369
IP-based networks	X.370–X.379
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	
Networking	X.600–X.629
Efficiency	X.630–X.639
Quality of service	X.640–X.649
Naming, Addressing and Registration	**X.650–X.679**
Abstract Syntax Notation One (ASN.1)	X.680–X.699
OSI MANAGEMENT	
Systems management framework and architecture	X.700–X.709
Management communication service and protocol	X.710–X.719
Structure of management information	X.720–X.729
Management functions and ODMA functions	X.730–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	
Commitment, concurrency and recovery	X.850–X.859
Transaction processing	X.860–X.879
Remote operations	X.880–X.889
Generic applications of ASN.1	X.890–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	X.1000–X.1099
SECURE APPLICATIONS AND SERVICES	X.1100–X.1199
CYBERSPACE SECURITY	X.1200–X.1299
SECURE APPLICATIONS AND SERVICES	X.1300–X.1399
CYBERSECURITY INFORMATION EXCHANGE	X.1500–X.1599
CLOUD COMPUTING SECURITY	X.1600–X.1699

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

Recommendation ITU-T X.675

OID-based resolution framework for heterogeneous identifiers and locators

Summary

In Internet of things (IoT) environments, many different identifiers (IDs) from various resources could be created and used. It could be difficult to unite all the existing IDs, but some systems could provide interoperability among heterogeneous IDs. As an effective solution, an integrated resolution framework for a set of existing IDs is provided. Recommendation ITU-T X.675 analyses requirements, such as ID independence, ID separation, compatibility, uniqueness, tolerance, stability and security. The general architecture for the object identifier (OID)-based resolution framework is specified with several scenarios. These scenarios show how to operate the resolution framework for heterogeneous IDs and locators (LOCs). It should be noted that this is one means of achieving interoperability, and other methods of operation are possible with other IDs and/or resolution systems.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.675	2015-05-29	17	11.1002/1000/12475

Keywords

Heterogeneous identifiers, identification, object identifiers, resolution framework.

[*] 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 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 X.675

OID-based resolution framework for heterogeneous identifiers and locators

1 Scope

This Recommendation includes the following items:

- overview of the object identifier (OID)-based resolution framework for heterogeneous identifiers (IDs)/locators (LOCs);
- requirements for a heterogeneous ID/LOC resolution framework;
- OID-based resolution service scenarios for heterogeneous IDs/LOCs.

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 X.672]	Recommendation ITU-T X.672 (2010) | ISO/IEC 29168-1:2011, *Information technology – Open systems interconnection – Object identifier resolution system (ORS).*
[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 routing locator separation in IPv6-based next generation networks*.
[ITU-T Y.3001]	Recommendation ITU-T Y.3001 (2011), *Future networks: Objectives and design goals*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 identifier (ID) [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).

3.1.2 Internet of things (IoT) [b-ITU-T Y.2060]: A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.

NOTE 1 – Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled.

NOTE 2 – From a broader perspective, the IoT can be perceived as a vision with technological and societal implications.

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.

3.1.4 OID resolution process [ITU-T X.672]: Process which provides information associated with an OID.

3.1.5 OID resolution system (ORS) [ITU-T X.672]: Implementation of the OID resolution process.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 identifier registry (ID registry): An ID registry is a database of identifiers and locators (LOCs), which are assigned to nodes in a local network. ID registry servers return a corresponding LOC when an identifier is given as an input value.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

DNS	Domain Name System
FN	Future Network
ID	Identifier
IoT	Internet of Things
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
LOC	Locator
NGN	Next-Generation Network
OID	Object Identifier
ORS	OID Resolution Server
TCP/IP	Transmission Control Protocol/Internet Protocol

5 Conventions

None.

6 Considerations on a resolution framework between heterogeneous identifiers/locators

In IoT [b-ITU-T Y.2060] environments, many different IDs from various resources could be created and used. It could be difficult to unite all the existing IDs, but some systems could provide interoperability among the heterogeneous IDs. As an effective solution, an integrated resolution framework for a set of existing IDs is provided as shown in Figure 1. Firstly, [ITU-T Y.3001] recommends that future networks (FNs) provide a new identification structure, defining new IDs that would identify communication objects, which efficiently support the new communication paradigms in FNs. The new identification infrastructure can unify the different types of IDs; however, this approach would be costly and time consuming. Secondly, another approach is an integrated resolution framework for all the existing IDs. This approach will be more effective in terms of cost and time because the existing IDs do not have to be modified.

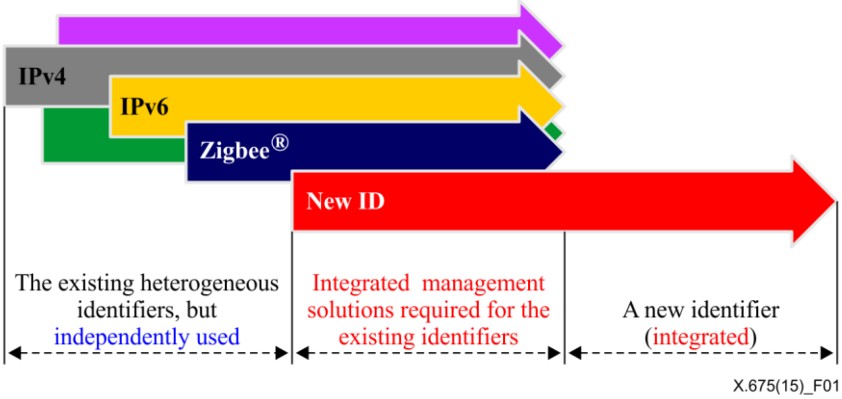
IPv4
IPv6
Zigbee®
New ID
The existing heterogeneous identifiers, but independently used
Integrated management solutions required for the existing identifiers
A new identifier (integrated)
X.675(15)_F01

Figure 1 – Necessity of solutions for heterogeneous ID/LOC resolution framework

Typically, when new IDs are created and used, they are independently managed and used until they are unified into one ID. However, it is recommended to support a uniform resolution service for heterogeneous IDs rather than to unify heterogeneous IDs. This is the reason why the OID-based resolution framework for heterogeneous IDs is necessary.

In addition, currently used Internet protocol version 4 (IPv4) and Internet protocol version 6 (IPv6) addresses actually imply both IDs and LOCs. However, IDs in next-generation networks (NGNs) are separated from LOCs according to [ITU-T Y.2015]. Therefore, the framework should consider ID/LOC separation (see Figure 2).

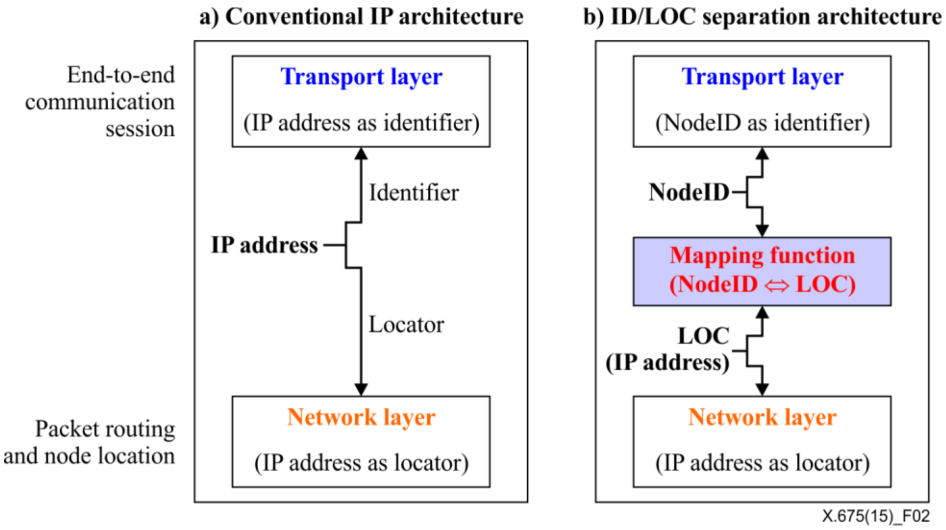

Figure 2 – Comparison between conventional IP architecture and new ID/LOC separation architecture ITU-T Y.2015

Lastly, the framework should consider the problems which could happen when the heterogeneous IDs are integrated into an open network. Even though there are two different identification schemes, both schemes can create the same ID as shown in Figure 3. In this case, there is no way to distinguish between the two nodes even if they have different ID schemes. Thus, the ID commonality problem is the phenomenon that two or more devices have the same ID but identification schemes are all different. For this reason, when the heterogeneous IDs are integrated into an open network, solutions are required to identify them (as shown in Figure 3).

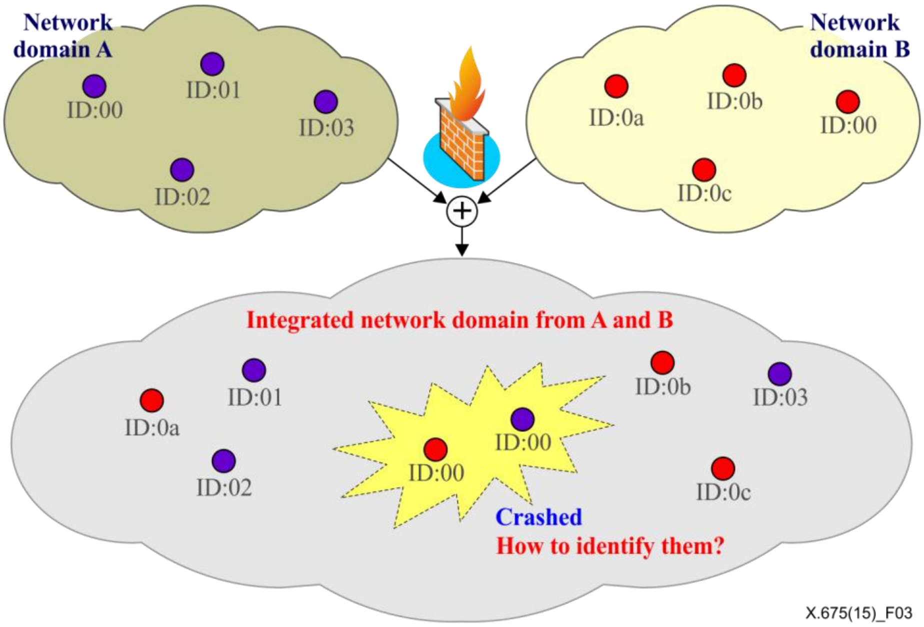

Figure 3 – ID commonality problem

7 Requirements for resolution framework for heterogeneous identifiers/locators

The uniform resolution framework for heterogeneous IDs shall address the following requirements.

7.1 Support of independence from the existing identifiers' operation

The framework should not influence the operation of the existing ID, such as operating procedures, structures, protocols, and so on. Therefore, the use of existing IDs shall not require any modification to the framework to provide resolution services.

7.2 Support of both identifiers and locators separately

[ITU-T Y.2022] and [ITU-T Y.2057] specify ID/LOC split functions in NGNs. Likewise, [ITU-T Y.3001] recommends that IDs in FNs should be separated from LOCs. In the case of the Internet, IPv4 and IPv6 addresses are a kind of ID in the network layer, but they also play the role of LOCs as discussed in [ITU-T Y.2015]. In addition, similarly to IDs of the domain name system (DNS), some existing IDs would play only the role of an ID. Therefore, the resolution framework should guarantee capabilities both of identification and location of IDs.

7.3 Support of the heterogeneous existing identifiers

When there are many IDs, each ID can be based on a different identification scheme from the others. Therefore, it is required that the resolution framework support a part of the heterogeneous existing IDs for interoperability.

7.4 Guarantee uniqueness of the existing identifiers

As mentioned in clause 6, many closed networks have their own polices and schemes for identification, so some of the IDs cannot be unique when the closed networks are integrated into an open network. The resolution framework should be able to support the uniqueness of the existing IDs.

7.5 Support of new identifiers

After the resolution framework service is provided for the existing IDs, brand-new IDs can be created. In other words, new IDs can be created anytime if there is a demand. Therefore, the resolution framework needs to be able to support new IDs.

7.6 Support of fault tolerance and stability

While the resolution framework service is being provided, errors and faults could occur anytime. Therefore, it is required to prevent such errors and faults for stable services.

7.7 Support of end-to-end identification

When a terminal wants to connect to another end node for communications, ID resolution is accomplished between the two end nodes. The resolution framework should support identification for the end nodes even though the end nodes are hidden behind another node, such as a gateway.

7.8 Support of authentication and authorization

When the resolution framework service is provided, third parties' security threats could happen anywhere and anytime. Therefore, to prevent such security threats, authentication and authorization have to be considered.

8 OID-based resolution framework for heterogeneous identifiers/locators

The OID-based resolution framework for heterogeneous IDs/LOCs is defined based on the requirements mentioned in this clause.

8.1 General architecture

Figure 4 presents a general architecture of OID-based resolution framework for heterogeneous IDs. In Figure 4, all nodes have their IDs and LOCs and belong to one of the access networks A, B or C. The access networks are connected to a core network; therefore, all nodes can communicate with each other. Each access network has a different ID scheme from the others. The nodes in network A and B can directly communicate with each other. On the other hand, the nodes in network C are indirectly linked to the core network. The nodes are directly connected with a gateway, and the gateway plays the role of a forwarding agent between the core network and the nodes. Therefore, when all nodes want to connect to outside nodes, the gateway should provide intermediate services.

Each of the networks A, B or C can have its own identification scheme that is different from the other networks. In addition, all of the networks guarantee the uniqueness of IDs of nodes within the each respective network; therefore, the same two IDs can exist across the networks. However, when all the networks are connected to an open network and are connected with each other, ID duplication is a critical problem.

The key components of this framework are the OID resolution server (ORS) and ID registries. An ORS is interconnected with the ID registries to manage the information of the ID registries. In addition, each ID registry manages the information of the nodes' IDs and LOCs in its access network.

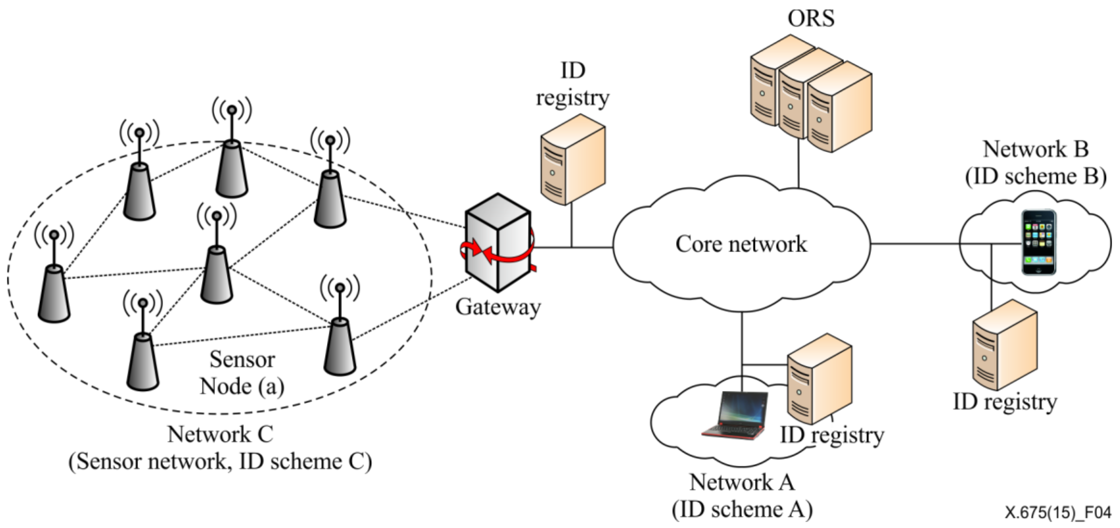

Figure 4 – General architecture of the OID-based resolution framework for heterogeneous IDs/LOCs

8.1.1 ID registry

An ID registry is a local resolution system to support nodes in a local access network. The local networks have one ID registry, and the ID registry manages a database(s) of IDs and LOCs of local nodes (and gateways). This database is used for the ID registry to search for a corresponding LOC and return it.

8.1.2 Object identifier resolution server

An ORS [ITU-T X.672] plays the role of a centralized ORS to identify ID registries. The ORS has a database(s) of OIDs and LOCs of the ID registries. OIDs are utilized as the key values to identify heterogeneous identification schemes. When any node sends an OID value to the ORS, the ORS returns the LOC value of a corresponding ID registry.

8.1.3 OID assignment

OIDs are predefined and have globally unique values, which are respectively assigned to all ID registries. This means that each local access network can be identified by assigned OIDs because the local network has at least one ID registry. OIDs are used as well-known values in public like port numbers of transmission control protocol/Internet protocol (TCP/IP). Therefore, this enables all nodes to be aware of OID values related to the identification scheme used by the destination nodes.

8.2 Registration of object identifiers, identifiers and locators

Above all, the registration of OIDs, IDs, and LOCs is a required process for ORS, and ID registries may have databases to provide a resolution framework service through the registration procedure. The OID-based resolution framework provides a two-level registration approach, such as nodes to the ID registry and ID registry to the ORS as shown in Figure 5, and as detailed in clauses 8.2.1 and 8.2.2.

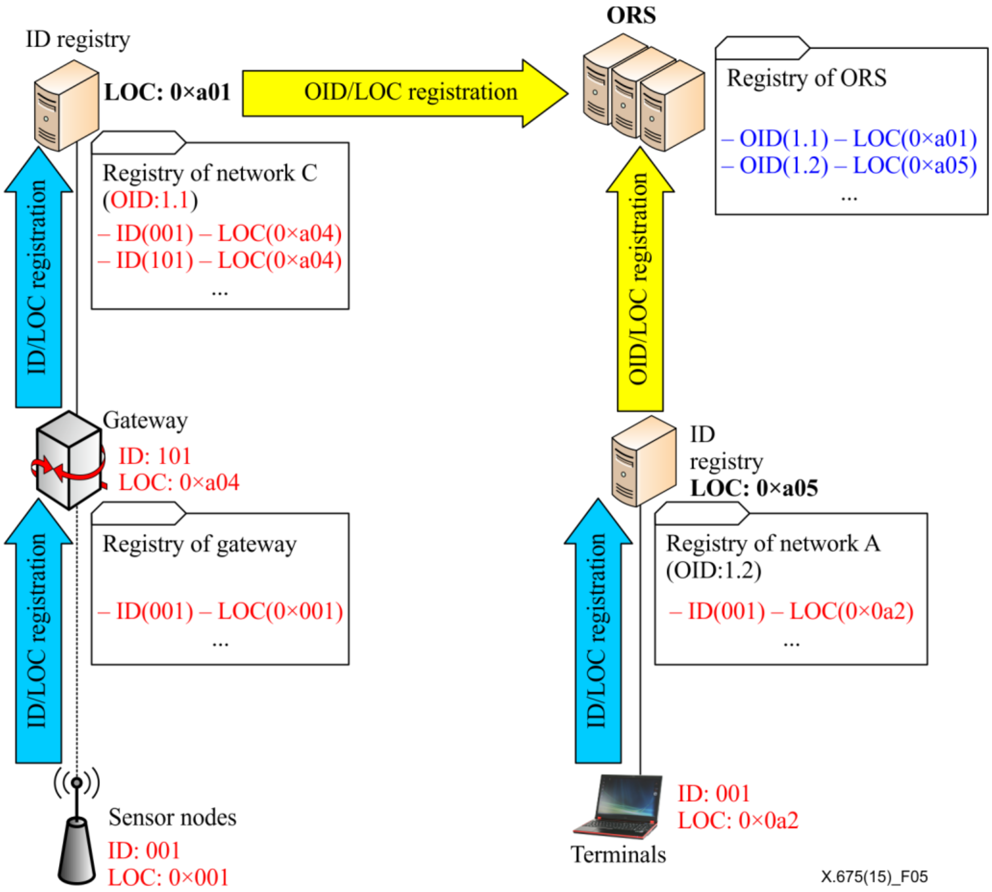

Figure 5 – ID/LOC/OID registration procedure

8.2.1 Registration to an ID registry

At the beginning, IDs and LOCs of all the local nodes including gateways should be registered with their ID registries. This registration process from the nodes to the ID registries is reflected in two different scenarios: the first scenario is where a gateway does not exist; and the second scenario is where a gateway exists. The first case is that local nodes can directly send information of their IDs and LOCs to their ID registry because the ID registry and the local nodes are directly connected to each other. The second case is that local nodes are connected to their ID registry via a gateway, as shown in Figure 5. Therefore, the local nodes send information of their IDs and LOCs to their gateway, and the gateway sends the information to its ID registry.

– **Case where a gateway does not exist**: All local nodes are directly connected to their ID registry; the ID registry manages the information pairs of the IDs and the LOCs of all local nodes in a database.

– **Case where a gateway does exist**: On the other hand, all local nodes are connected to their gateway, and the gateway is connected to its ID registry. The ID registry manages the information pairs of the IDs and the LOCs of the gateway in a database, and the gateway also manages the information pairs of the IDs and the LOCs of the local nodes in a database. The ID registry does not have to worry about whether the information of the IDs and LOCs in its database belongs to the gateway or local nodes.

8.2.2 Registration to ORS

At the next stage, each ID registry registers its LOC with a corresponding OID value to the ORS. Then the ORS can find the LOC of the ID registry to which a destination node belongs.

8.3 Scenarios of resolution framework for heterogeneous IDs and LOCs

This clause presents service scenarios of the OID-based resolution framework in the two cases: where a gateway does not exist; and where a gateway exists. The scenarios have an assumption that there are two different nodes having the same ID (e.g., 001) but their identification schemes are different. Also, registration to the ID registry and ORS is already done according to the procedures in clause 8.2 (as shown in Figure 5).

8.3.1 Scenario I: A gateway exists

Figure 6 shows the case when a destination node has an ID (001) and is connected to the outside network through a gateway. This scenario presents the procedures to retrieve a LOC of the destination node and to deliver data to the destination node.

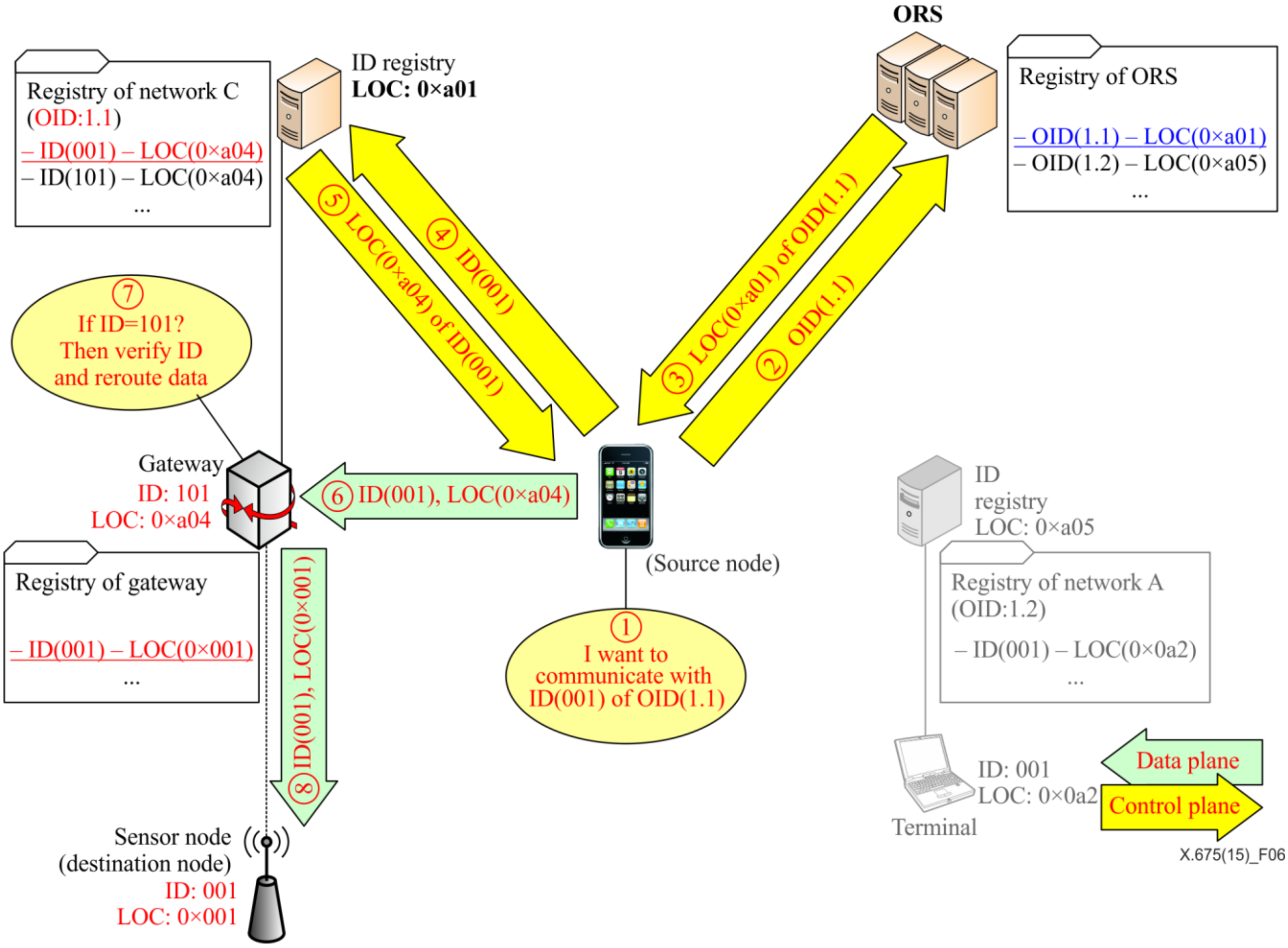

Figure 6 – Scenario I: A gateway exists

1) A source node wants to transfer data to a destination node (ID: 001, "Sensor node" in Figure 5); the node is also aware of OID (1.1) of the ID of the destination node.

2) The source node sends OID (1.1) to the ORS.

3) ORS retrieves a corresponding LOC of ID registry (0xa01) from its database. After that, the LOC of the corresponding ID registry (0xa01) is returned to the source node.

4) The source node is aware of a location of the ID registry of the destination node, and the node sends ID of the destination node (001) to the ID registry.

5) The ID registry retrieves 0xa04, a LOC corresponding to the ID from its database, and then the ID registry returns the retrieved LOC (0xa04) to the source node.

6) The returned LOC (0xa04) is not a LOC of the destination node but is in fact the gateway; however, the source node recognizes that the LOC (0xa04) is a LOC of the destination node. Therefore, data sent by the source node are transferred to the gateway with the ID of the destination node (001).

7) When the gateway receives the data with ID (001), it verifies the received ID. Unless the ID received is one of the IDs already in the database, the gateway discards the data. On the other hand, if the ID is not the same as the ID of the gateway, the gateway re-routes the data to the destination node.

8) The data are then sent again by the gateway to the destination node.

8.3.2 Scenario II: A gateway does not exist

Figure 7 shows the scenario when a destination node has an ID (001) and is directly connected to the outside network.

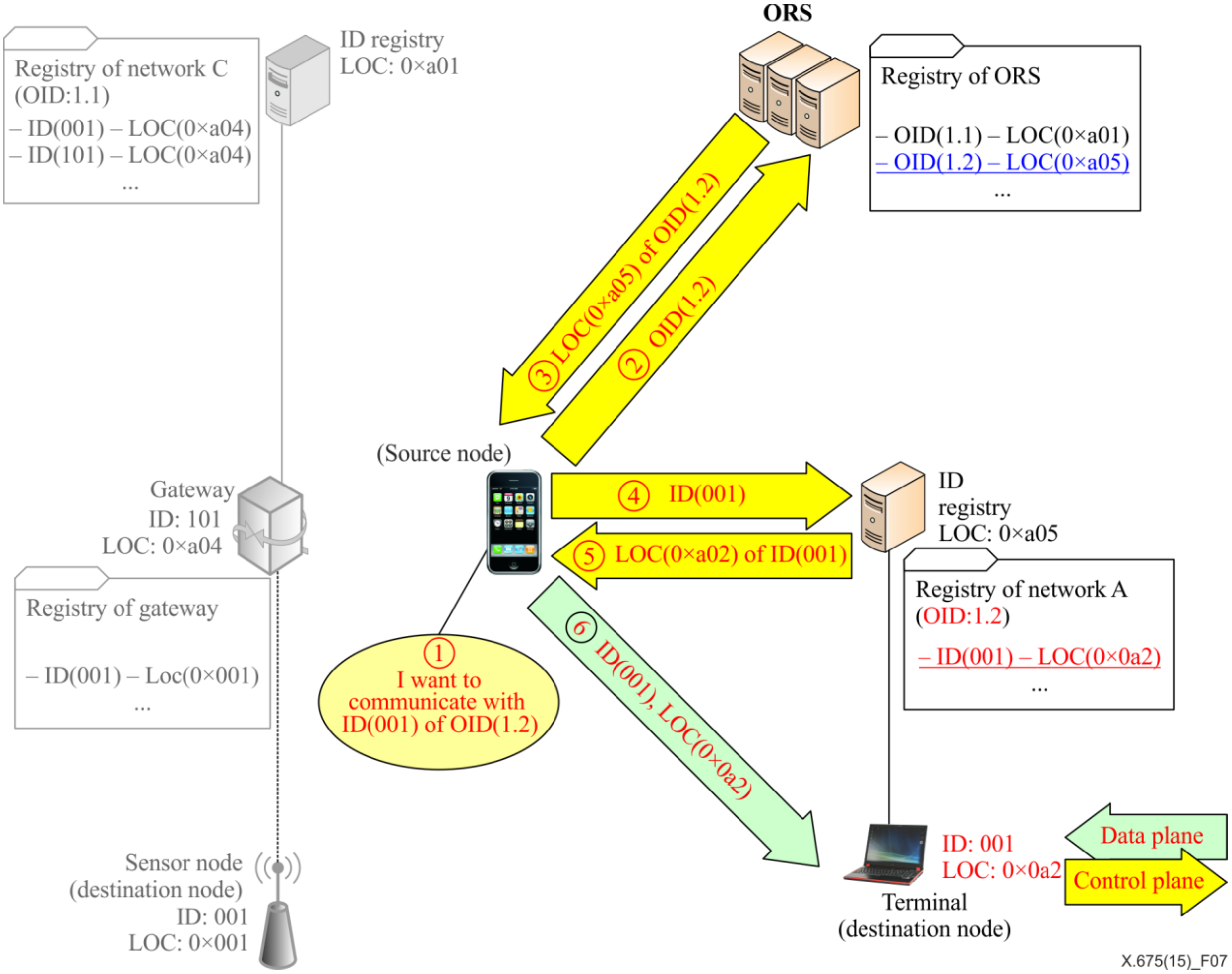

Figure 7 – Scenario II: A gateway does not exist

1) A source node wants to transfer data to a destination node (ID: 001, "Terminal" in Figure 6). Even though ID 001 is the same as the ID of the sensor node in scenario I, the source node can identify them with a different OID (1.2).

2) The source node sends OID (1.2) to ORS.

3) ORS retrieves 0xa05, a corresponding LOC of an ID registry from its database. After that, the LOC of the corresponding ID registry is returned to the source node.

4) The source node is aware of a location of the ID registry of the destination node, and the node sends the ID of the destination node (001) to the ID registry.

5) The ID registry retrieves a LOC (0x0a2) corresponding to the ID value from its database, and then the ID registry returns the retrieved LOC (0x0a2) to the source node.

6) The 0xa02 is a LOC of the destination node, so the source node transfers the data to the destination node.

Appendix I

Scenario of assigning OIDs directly to end devices as IDs

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

It is technically possible that an OID is directly assigned to end devices as an ID. However, the ORS should manage many entries if OIDs are assigned to many end devices. For this reason, this scenario may not be a general use case of the OID-based resolution framework but a special use case. This appendix describes an ID/LOC/OID registration procedure and a resolution scenario when an OID is directly assigned to an end device.

I.1 ID/LOC/OID registration procedure for end devices

Figure I.1 shows the registration procedure for this scenario where OID of the node could be directly registered to ORS.

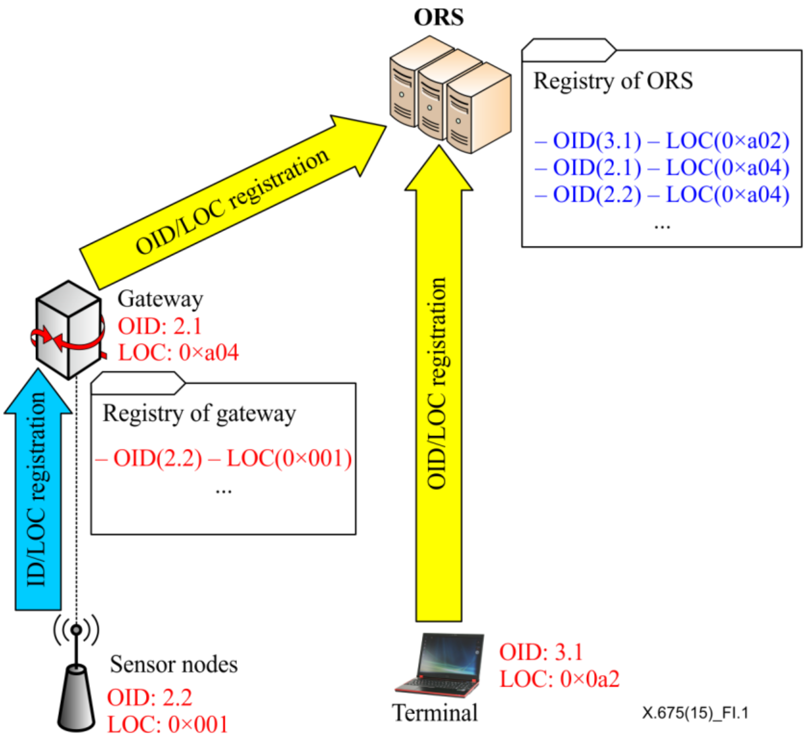

Figure I.1 – ID/LOC/OID registration procedure for end devices

I.2 Scenario where a gateway exists

Figure I.2 shows a use case when a destination node which is identified by OID method has an OID (2.2) and is connected to the outside network through a gateway. This scenario presents procedures to retrieve a LOC of the destination node and to deliver data to the destination node.

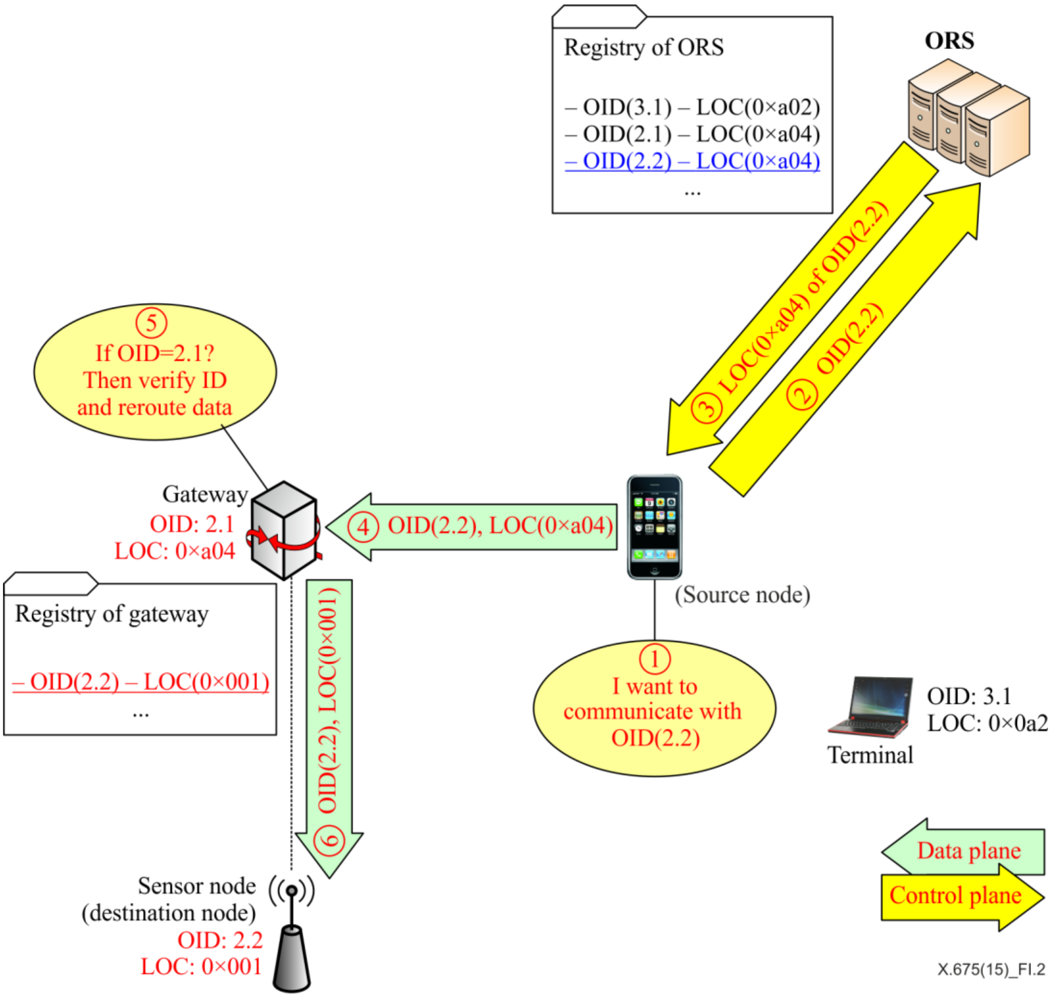

Figure I.2 – Resolution service scenario for end devices

1) A source node wants to transfer data to a destination node (OID: 2.2, "Sensor node" in Figure I.2).

2) The source node sends the OID value (2.2) to ORS.

3) ORS retrieves a corresponding LOC (0xa04) of the gateway by using the given OID value from its database. After that, the LOC of the corresponding gateway is returned to the source node.

4) The source node realizes that the LOC (0xa04) is a value of the destination node. Therefore, the source node sends data to the gateway with OID (2.2) of the destination node.

5) When the gateway receives the data with OID (2.2), it verifies the received ID. Unless the ID received is one of the IDs already in the database, the gateway discards the data. On the other hand, if the ID is not the same as the ID of the gateway, the gateway re-routes the data to the destination node.

6) The destination node receives the data from the gateway.

Bibliography

[b-ITU-T Y.2060] Recommendation ITU-T Y.2060 (2012), *Overview of the Internet of things*.

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

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