International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

H.643.1

(05/2019)

SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS

Broadband, triple-play and advanced multimedia services – Ubiquitous sensor network applications and Internet of Things

Architecture for the deployment of information-centric networks

Recommendation ITU-T H.643.1

ITU-T H-SERIES RECOMMENDATIONS

AUDIOVISUAL AND MULTIMEDIA SYSTEMS

CHARACTERISTICS OF VISUAL TELEPHONE SYSTEMS	H.100–H.199
INFRASTRUCTURE OF AUDIOVISUAL SERVICES	
General	H.200–H.219
Transmission multiplexing and synchronization	H.220–H.229
Systems aspects	H.230–H.239
Communication procedures	H.240–H.259
Coding of moving video	H.260–H.279
Related systems aspects	H.280–H.299
Systems and terminal equipment for audiovisual services	H.300–H.349
Directory services architecture for audiovisual and multimedia services	H.350–H.359
Quality of service architecture for audiovisual and multimedia services	H.360–H.369
Telepresence, immersive environments, virtual and extended reality	H.420–H.439
Supplementary services for multimedia	H.450–H.499
MOBILITY AND COLLABORATION PROCEDURES	
Overview of Mobility and Collaboration, definitions, protocols and procedures	H.500–H.509
Mobility for H-Series multimedia systems and services	H.510–H.519
Mobile multimedia collaboration applications and services	H.520–H.529
Security for mobile multimedia systems and services	H.530–H.539
Security for mobile multimedia collaboration applications and services	H.540–H.549
VEHICULAR GATEWAYS AND INTELLIGENT TRANSPORTATION SYSTEMS (ITS)	
Architecture for vehicular gateways	H.550–H.559
Vehicular gateway interfaces	H.560–H.569
BROADBAND, TRIPLE-PLAY AND ADVANCED MULTIMEDIA SERVICES	
Broadband multimedia services over VDSL	H.610–H.619
Advanced multimedia services and applications	H.620–H.629
Ubiquitous sensor network applications and Internet of Things	**H.640–H.649**
IPTV MULTIMEDIA SERVICES AND APPLICATIONS FOR IPTV	
General aspects	H.700–H.719
IPTV terminal devices	H.720–H.729
IPTV middleware	H.730–H.739
IPTV application event handling	H.740–H.749
IPTV metadata	H.750–H.759
IPTV multimedia application frameworks	H.760–H.769
IPTV service discovery up to consumption	H.770–H.779
Digital Signage	H.780–H.789
E-HEALTH MULTIMEDIA SYSTEMS, SERVICES AND APPLICATIONS	
Personal health systems	H.810–H.819
Interoperability compliance testing of personal health systems (HRN, PAN, LAN, TAN and WAN)	H.820–H.859
Multimedia e-health data exchange services	H.860–H.869
Safe listening	H.870–H.879

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

Recommendation ITU-T H.643.1

Architecture for the deployment of information-centric networks

Summary

Recommendation ITU-T H.643.1 describes the functional architecture for the deployment of information-centric networks (DICNs), including functional entities, reference points and service control flows. It also describes the required DICN capabilities. This architecture can be used to flexibly support the deployment of any particular information-centric network instance and the coexistence of multiple ICN instances on top of one physical network. It also facilitates the inter-operation between different ICN instances.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T H.643.1	2019-05-14	16	11.1002/1000/13906

Keywords

Architecture, deployment, information-centric networks, inter-operation

---

* 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 H.643.1

Architecture for the deployment of information-centric networks

1 Scope

This Recommendation describes the architecture for the deployment of information-centric networks (DICNs), which satisfies the requirements described in [ITU-T F.746.4].

This Recommendation covers the following:

– functional architecture for DICN;

– functional entities, reference points and service control flows of DICNs.

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 F.746.4] Recommendation ITU-T F.746.4 (2017), *Requirements for deployment of information-centric network*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 functional architecture [b-ITU-T Y.2012]: A set of functional entities, and the reference points between them used to describe the structure of an NGN. These functional entities are separated by reference points, and thus, they define the distribution of functions.

NOTE 1 – The functional entities can be used to describe a set of reference configurations. These reference configurations identify which reference points are visible at the boundaries of equipment implementation and between administrative domains.

NOTE 2 – The definition is not only applicable to NGNs but also to other IP packet-switch-based networks.

3.1.2 functional entity [b-ITU-T Y.2012]: An entity that comprises an indivisible set of specific functions. Functional entities are logical concepts, while groupings of functional entities are used to describe practical, physical implementations.

3.1.3 interface [b-ITU-T Y.101]: A shared boundary between two functional units.

NOTE – An interface is defined by various characteristics pertaining to the functions, physical interconnections, signal exchanges, and other characteristics as appropriate.

3.1.4 reference point [b-ITU-T Y.2012]: A conceptual point at the conjunction of two non-overlapping functional entities that can be used to identify the type of information passing between these functional entities.

NOTE – A reference point may correspond to one or more physical interfaces between pieces of equipment.

3.1.5 service [b-ITU-T Y.101]: A structure set of capabilities intended to support applications.

3.2 Terms defined in this Recommendation

None

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

DICN Deployment of Information-Centric Network

ICN Information-Centric Network

5 Conventions

In this Recommendation:

– The expression "is required to" indicates a requirement which must be strictly followed and from which no deviation is permitted if conformance to this Recommendation is to be claimed.

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

6 Overview

This Recommendation describes the architecture for the deployment of information-centric networks (DICNs), which satisfies the requirements described in [ITU-T F.746.4]. This Recommendation includes the required DICN capabilities and functional architecture for DICNs (including functional entities, reference points and service control flows of DICNs).

Currently, the deployment of information-centric networks (ICNs) has attracted considerable attention. However, there are too many ICN candidates, each of which has its own design principles and technical details in terms of naming, routing, and so on ([b-ITU-T Y.3033], [b-Dannewitz], [b-Jacobson], [b-Sarela], [b-Seskar], [b-Detti]). These ICN candidates have their own pros and cons, each of which is best suited to particular application requirements. Thus, it is highly likely that different ICN service providers will implement their own ICN instants with different ICN candidates to provide specific services to users. However, using dedicated physical resources to deploy each individual ICN instants is a waste of resource. Thus, it is reasonable that various ICN instances will coexist on top of one physical network. What is more, there is a scenario that a client of one ICN instance needs to access the resources provided by the server belongs to another ICN instance. In this case, to provide efficient content delivery services, the inter-operation between different ICN instances is also needed.

The architecture for deployment of information-centric networks (DICNs) aims to enable multiple ICN instances' coexistence to provide efficient content delivery services to users.

7 Required DICN capabilities

This clause describes the required DICN capabilities, i.e., name-based content delivery, in-network cache, coexistence, inter-operation and security.

7.1 Name-based content delivery

The capability of name-based content delivery is responsible for delivering content based on the content name. In an information-centric network a user can directly obtain a content object by its name (or identification), without specifying the location of the content object. For each user's request, the network also needs to find the appropriate holder to provide the content to the user according to the content name.

7.2 In-network cache

The capability of in-network cache is responsible for caching content in routers or switches, and for providing the content to the users from a nearby cache. Routers or switches equipped with caches need to store copies of traversed content objects and respond to subsequent content requests with the cached copies, which will significantly reduce bandwidth consumption and server load.

7.3 Coexistence

The capability of coexistence is responsible for enabling multiple ICN instances, each of which can employ different ICN architecture candidates to coexist in one physical network. The physical resources are virtualized into different slices, each of which is dedicated to a particular ICN instance. The packets for each ICN instance needs to be delivered according to particular protocols and not be affected by other ICN instances.

7.4 Inter-operation

The capability of inter-operation is responsible for enabling an ICN user which adopts one ICN candidate to obtain content from another one which adopts another different ICN candidate. The DICN needs to handle the difference between different ICN protocols, including the difference of packet format, protocol procedure and so on.

7.5 Security

The capability of security is responsible for providing a secure service, including authentication and authorization. The DICN needs to verify whether or not the user can access the content. A DICN client can only access the content that it is permitted to access.

8 Functional architecture for DICN

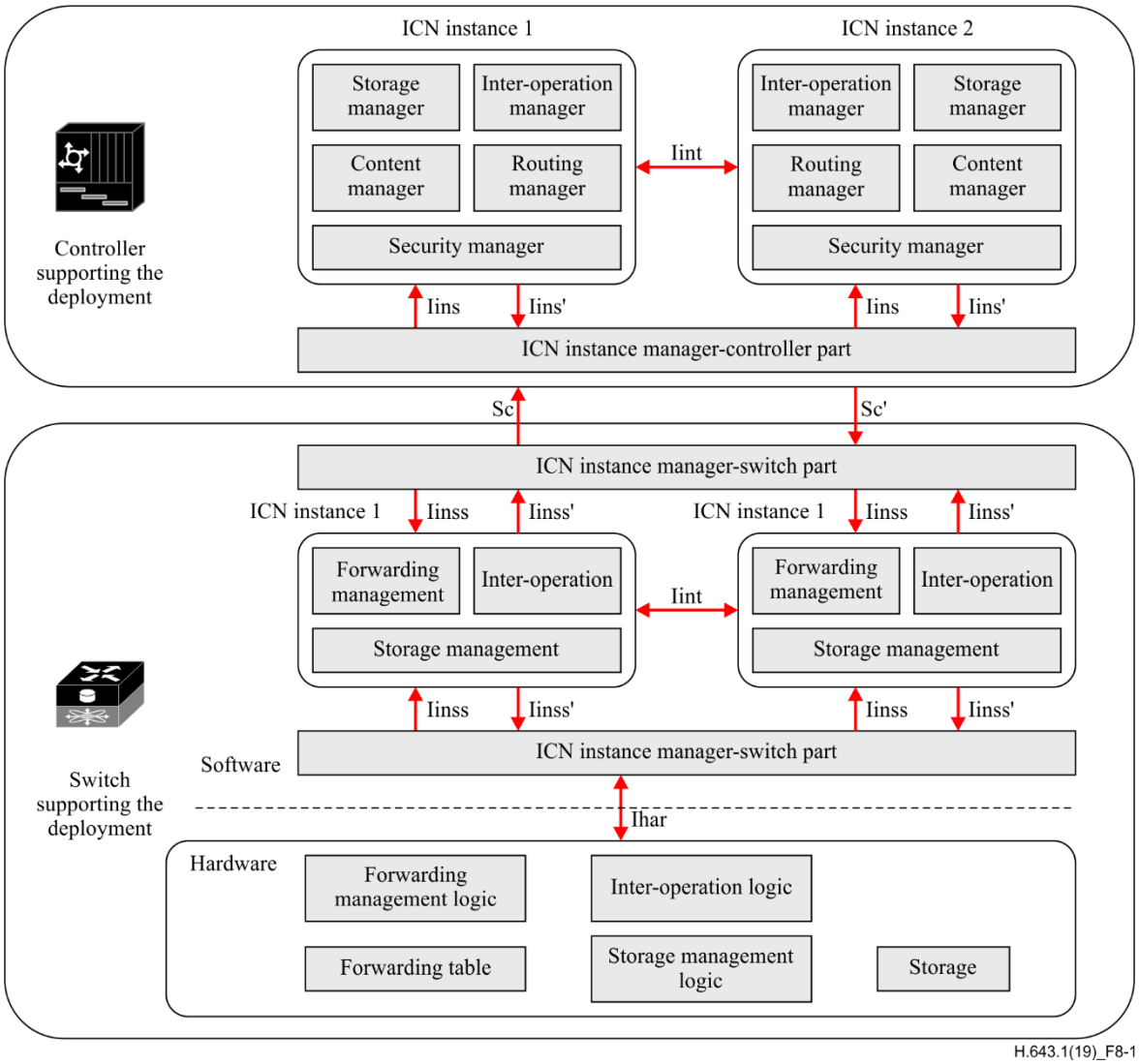

Figure 8-1 – Functional architecture for DICN

This clause describes the DICN functional components which are required to perform DICN functionalities. Figure 8-1 shows the functional architecture with the functional entities and reference points between different functional entities. To illustrate the coexistence of ICN instances and demonstrate the reference points for inter-operation there are two ICN instances shown in Figure 8-1.

8.1 Functional architecture

Figure 8-1 shows the functional architecture for DICNs. The DICN consists of two parts, the DICN controller and DICN switches. The DICN controller consists of the ICN instances manager (controller part) and various ICN instances each of which is created to conform to different ICN protocols. The DICN switch consists of the hardware part which supports the general ICN-related operations and the software part which is used to support the resource virtualization for the implementation and coexistence of multiple ICN instances. The ICN instances manager (switch part) also resides in DICN switches.

8.2 Functional entities in DICN

8.2.1 DICN controller

The DICN controller is designed to manage virtualized physical network resources for each ICN instance. There are five function modules provided to ICN service providers, as shown in Figure 8-1, including content manager, routing manager, storage manager, security manager and inter-operation manager. With these five function modules, each ICN service provider can deploy its own ICN instance according to the specification of a particular ICN architecture candidate by implementing appropriate modules.

The content manager is the key unit for DICNs and is used to maintain information about content sources. If one DICN client hosts content, it should register this information to the content manager module in the DICN controller.

The routing manager is used to maintain the topology of this ICN instance and performs ICN-related routing algorithms. Each ICN service provider can adopt its own routing algorithms to satisfy its own purposes. Then it should configure the DICN switches to perform the routing.

The storage manager is used to set the policies for managing physical content storage. In DICNs, the content can be cached by intermediate node, i.e., routers and switches. ICN service providers can use this module to guide the DICN switches about where and how to cache this content to ensure DICN clients can retrieve the content from a nearby location.

The security manager is responsible for providing secure service. As DICN clients can obtain the requested content from nearby routers or switches rather than the original content providers, to ensure that the content is not accessed by undesired users, the ICN service provider defines its own security policies and uses the security manager to verify the permissions.

The inter-operation manager is used to guide the inter-operation with other ICN instances. Different ICN instances may have different naming schemes and operations. To retrieve content from a node which uses another ICN protocol, the inter-operation manager should establish the mapping between the different names of the same content and guide the DICN switches to deal with the differences of ICN operations.

A typical ICN instance can be implemented in a centralized or distributed way. In the centralized way, the ICN service provider only selects one DICN controller to deploy its ICN instance. In this case all information, including content sources, topology and so on, should be submitted to this selected DICN controller. Otherwise, serval DICN controllers can be used, each of which can hold parts of this information and cooperate to provide the required functions.

To manage these different ICN instances, there is an ICN instances manager (controller part). It is responsible for creating an ICN instance according to the request of the ICN service provider and reserve resources for the ICN instance in the physical network. It is also used to deliver the packets (including configuration messages, user's request and data packets) to the corresponding ICN instance.

8.2.2 DICN switch

The DICN switch, which is responsible for forwarding packets belonging to different ICN instances, consists of the hardware and software parts. There are six hardware elements in the hardware part: switching element, forwarding table, storage, forwarding management logic, storage management logic and inter-operation logic, which are shared by different ICN instances. Such hardware resources are virtualized into different slices, each of which is dedicated to a particular ICN instance. The switch also provides interfaces, including forwarding management, storage management and inter-operation, to ICN instances to manage the resources allocated to them. The ICN instance manager (switch part) is responsible for distinguishing packets (including configuration messages, user's request, and data

packets) belonging to different ICN instance received from controller and hardware, and delivering them to the corresponding ICN instance.

8.3 Reference points

8.3.1 Reference point Sc: DICN switch – DICN controller

The reference point is located between the ICN instance manager of the DICN switch and the ICN instance manager of the DICN controller. It is used to deliver the users' requests and packets from the DICN switch to the DICN controller.

8.3.2 Reference point Sc': DICN Controller – DICN switch

The reference point is located between the ICN instance manager of the DICN controller and the ICN instance manager of the DICN switch. It is used to deliver the configuration messages from the DICN controller to the DICN switch.

8.3.3 Reference point Iins: ICN instance manager (controller part) – ICN instance

The reference point is located between the ICN instance manager (controller part) and the ICN instances. It is used to deliver the users' requests, packets and configuration messages from the ICN instance manager to the corresponding ICN instance. Note that there are several "Iins" points in the DICN.

8.3.4 Reference point Iins': ICN instance – ICN instance manager (controller part)

The reference point is located between the ICN instances and the ICN instance manager (controller part). It is used to deliver the users' requests, packets and configuration messages from the ICN instances to the ICN instance manager. Note that there are several "Iins'" points in the DICN.

8.3.5 Reference point Iinss: ICN instance manager (switch part) – ICN instance

The reference point is located between the ICN instance manager (switch part) and the ICN instances. It is used to deliver the users' requests, packets and configuration messages from the ICN instance manager (switch part) to the corresponding ICN instance. Note that there are several "Iinss" points in the DICN.

8.3.6 Reference point Iinss': ICN instance – ICN instance manager (switch part)

The reference point is located between the ICN instances and the ICN instance manager (switch part). It is used to deliver the users' requests, packets and configuration messages from the ICN instances to the ICN instance manager (switch part). Note that there are several "Iinss'" points in DICN.

8.3.7 Reference point Iint: ICN instance - ICN instance

The reference point is located between different ICN instances. It is used to deliver inter-operation related controller messages. Note that there are several "Iint'" points in the DICN.

8.3.8 Reference point Ihar: ICN instance manager of DICN switch – hardware

The reference point is located between the software part and hardware part of the DICN switch. It is used to deliver the users' requests, packets and configuration messages between the software and hardware part.

8.4 Service control flows

8.4.1 ICN instance initialization

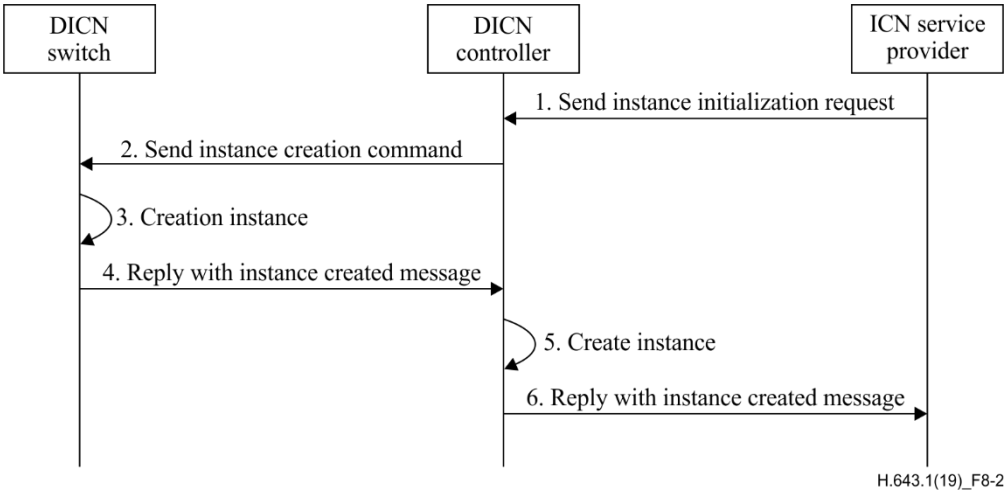

Figure 8-2 – Procedural flows for ICN instance initialization

Figure 8-2 illustrates the steps for ICN instance initialization:

1) First, the ICN service provider sends the ICN instance initialization request to the instance manager in the DICN controller.
2) The controller part of the ICN instances manager will verify the information and check the required resources to determine whether or not to accept this request. If the request is accepted, the controller part of the ICN instance manager will send the create instance command to the DICN switch.
3) The switch part of the ICN instance manager will create a new ICN instance and reserve the required resources in the DICN switches.
4) The switch part of the ICN instance manager replies with the instance created message to the controller part of the ICN instance manager.
5) The controller part of the ICN instance manager receives the response and creates a new ICN instance in the DICN controller.
6) The controller part of the ICN instances manager returns the information of the newly created instance to the ICN service provider.

When the ICN instance is initialized, the ICN service provider sends the configuration information of the ICN instance, which is set based on its own specification, to the ICN instance manager (controller part). Then the ICN instance manager (controller part) configures the ICN instance in the controller which in turn configures the routing and caching polices in the ICN instance resided in the DICN switch.

8.4.2 Registration of topology information

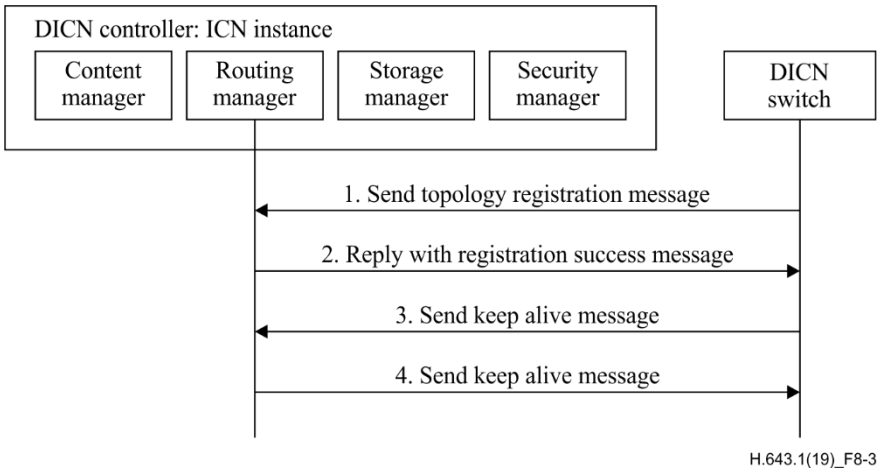

Figure 8-3 – Procedural flows for registration of topology information

Figure 8-3 shows the procedural flows for registration and deregistration of topology information:

1) A DICN switch registers itself and the connection with its neighbours to the routing manager of the ICN instance in the DICN controller.
2) The routing manager replies with a registration success message and saves this topology information.
3) The DICN switch sends a "keep alive" message to the routing manager of the ICN instance periodically. If the routing manager cannot receive the "keep alive" message for a long time (e.g., 10s), it will delete the DICN switch from the topology maintained.
4) The routing manager also sends a "keep alive" message to the DICN switch. If the DICN switch cannot receive the "keep alive" message for a long time it will inform the network administrator.

8.4.3 Registration and deregistration of content

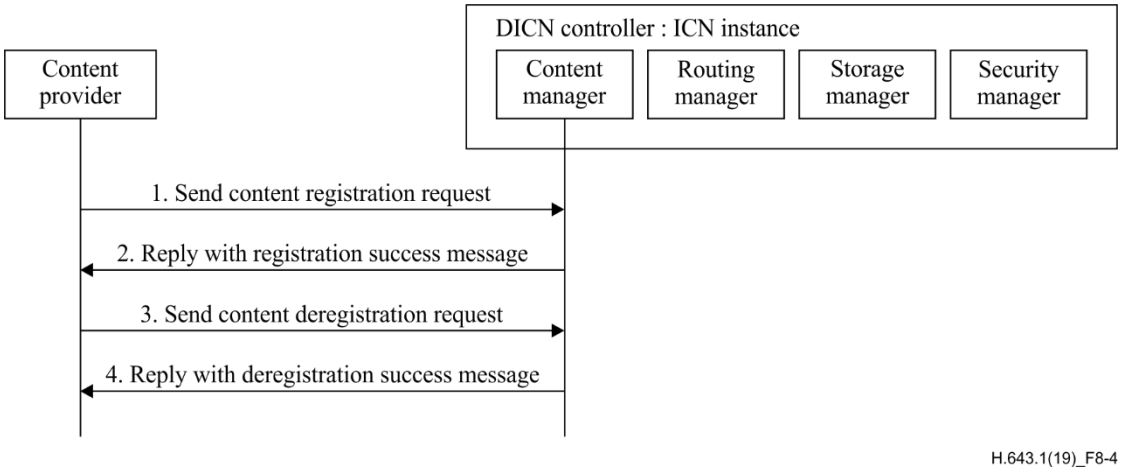

Figure 8-4 – Procedural flows for registration and deregistration of content

Figure 8-4 shows the procedural flows for registration and deregistration of content:

1) The content provider registers the content which it holds to the content manager of the ICN instance in the DICN controller.
2) The content manager replies with the registration success message to the content providers.

3) If the content provider will stop providing some content it can deregister the content by sending the content deregistration request.

4) The content manager of the controller replies with a deregistration success message.

8.4.4 Authentication and authorization

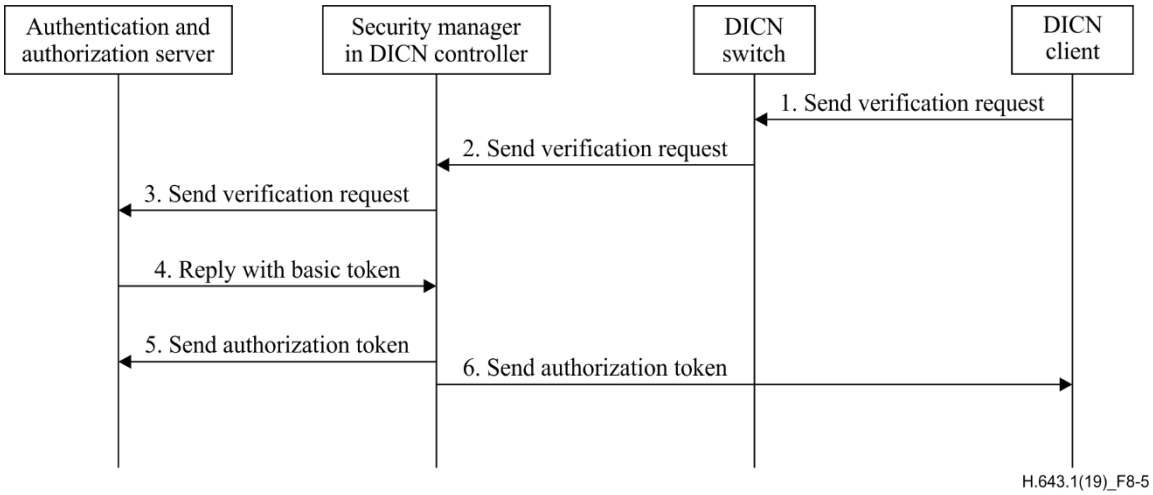

Figure 8-5 – Procedural flows for authentication and authorization

Figure 8-5 shows the procedural flows for authentication and authorization:

1) A new DICN client sends a user verification request to the DICN switch to verify whether the DICN client has the right to access the network and what content it can access. The verification request includes the DICN client's identity which identifies the current network location of the DICN client (such as the IP address, MAC address, etc.).

2) The DICN switch forwards the verification request to the security manager of the corresponding ICN instance in the DICN controller.

3) The security manager of the ICN instance forwards the verification request to the authentication and authorization server.

4) The authentication and authorization server performs user verification on the DICN client according to the verification request. If the DICN client passed verification the authentication and authorization server generates an encryption token (called basic token) according to the DICN client's identity and the content list that the DICN client can access, and it sends this token, which includes the identity and the content list, to the security manager of the ICN instance in the ICN controller.

5) The security manager extracts and saves the DICN client's identity and the content list that the DICN client can access from the received basic token. The security manager then uses its own key to generate a new encrypted token (called authorization token) based on the obtained information. It sends back this new generated encrypted token to the authentication and authorization server.

6) The security manager of the ICN instance also sends the new encrypted token, including the obtained information (i.e., contents list that the DICN client can access), to the DICN client.

8.4.5 Content delivery

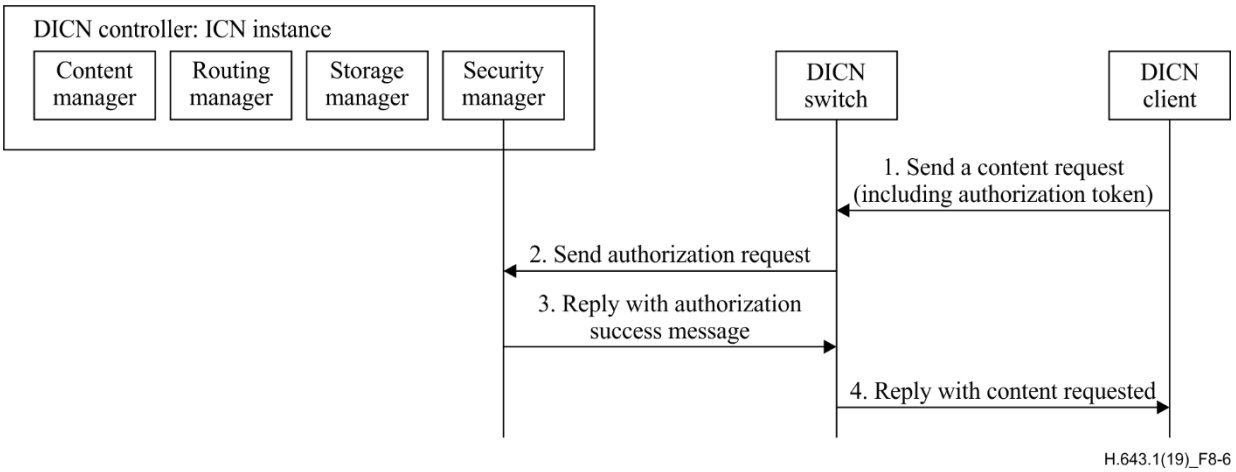

Figure 8-6 – Procedural flows for content delivery with local cache

Figure 8-6 shows the procedural flows for content delivery when the content is cached at the DICN switch:

1) The DICN client requests content and sends this request and its own authorization token to the DICN switch it is connected to.
2) The DICN switch sends the authorization request to the security manager of the corresponding ICN instance in the DICN controller to verify whether or not the user can access the content.
3) The security manager verifies the user's identity and replies with an authorization success message.
4) As the switch has cached the content it sends back the content to the user.

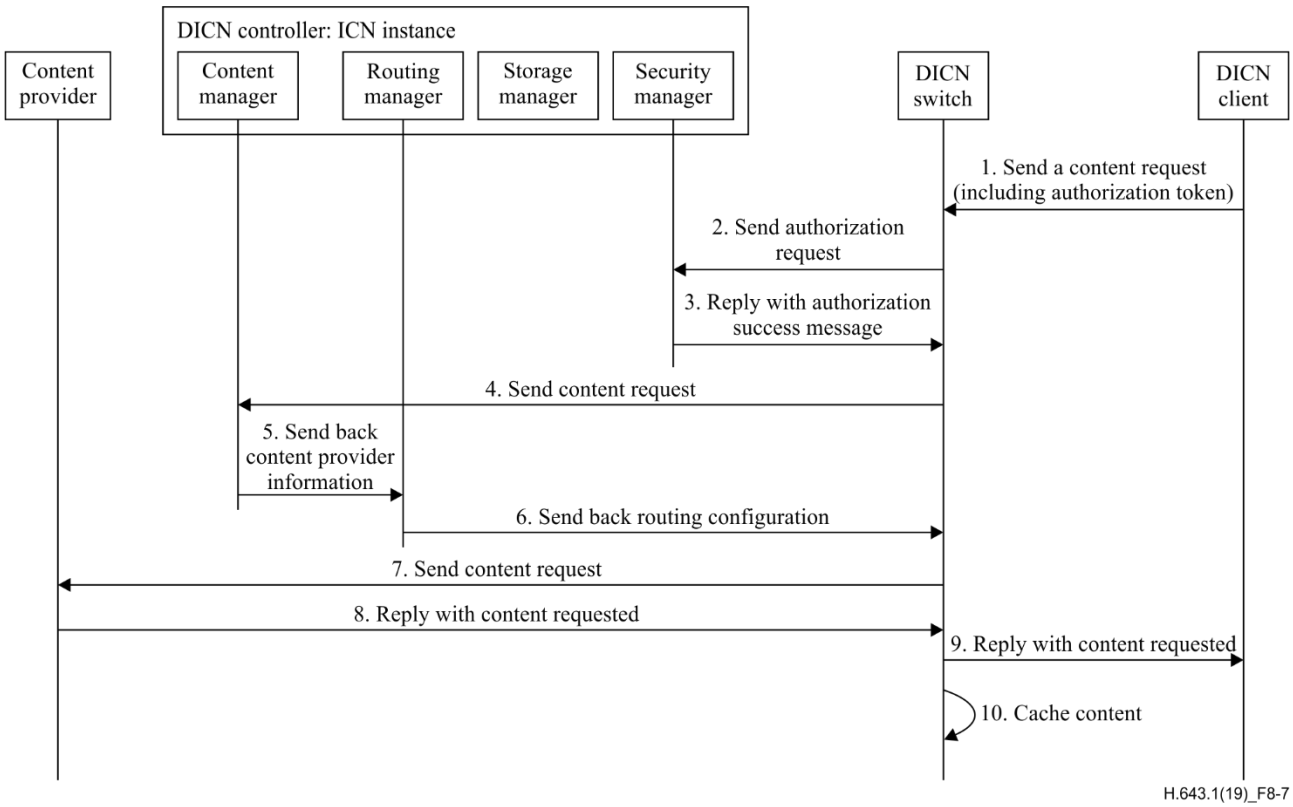

Figure 8-7 – Procedural flows for content delivery without local cache

Figure 8-7 shows the procedural flows for content delivery when the content is not cached at the DICN switch:

1) The DICN client requests some content and sends this request and the authorization token to the DICN switch it is connected to.
2) The DICN switch sends the authorization information to the security manager of the corresponding ICN instance in the DICN controller to verify whether or not the user can access the content.
3) The security manager verifies the user's identity and replies with an authorization success message.
4) As the DICN switch does not cache the content it forwards the request to the content manager of the corresponding ICN instance to look up who can provide this content.
5) The content manager sends the information of the selected content provider to the routing manager, which will find a route for content delivery.
6) The routing manager configures the route for the content delivery.
7) The DICN switch forwards the request to the content provider.
8) When the content provider receives the request it replies with the content requested to the DICN switch near the DICN client.
9) The DICN switch forwards the content to the DICN client.
10) The DICN switch determines whether or not to cache this content based on policies configured by the storage manager.

8.4.6 Inter-operation

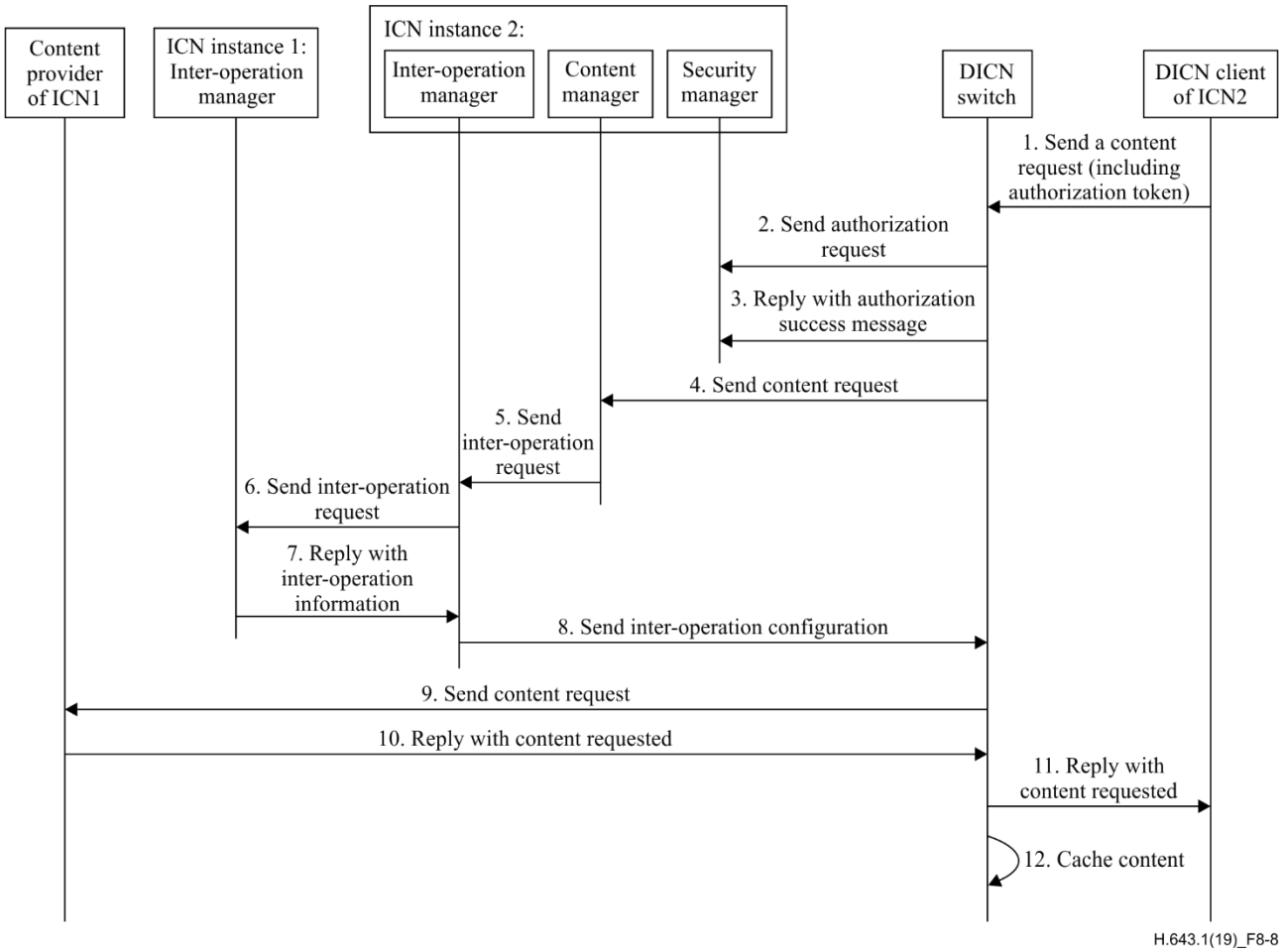

Figure 8-8 – Procedural flows for inter-operation

Figure 8-8 illustrates the procedural flows for inter-operation:

1) A DICN client of ICN instance 2 requests content held by a provider which adopts another ICN protocol, i.e., the ICN instance 1. It sends the content request and authorization token to the DICN switch.
2) The DICN switch sends the authorization request to the security manager of ICN instance 2.
3) The security manager verifies the users' identities and replies with authorization success message;
4) The DICN switch receives the authorization success message and sends the content request to the content manager of the corresponding ICN instance 2 in the DICN controller.
5) The content manager of ICN instance 2 finds that no content provider registers this content. It sends this request to the inter-operation manager of the ICN instance 2 in DICN controller.
6) The inter-operation manager of ICN instance 2 forwards the request to the inter-operation manager of ICN instance 1.
7) The inter-operation manager of ICN instance 1 replies with the inter-operation information, including the inter-operation policy (tunnelling or translation) and the name-mapping of the requested content.
8) Based on the returned policies, the inter-operation manager configures the inter-operation API in the DICN switch to perform the inter-operation.
9) The DICN switch requests the content from the content provider.

10) The content provider of ICN instance 1 replies with the content requested to the DICN switch.
11) The DICN switch sends back the content to the DICN client.
12) The DICN switch caches the content based on the caching policies.

Bibliography

[b-ITU-T Y.101] Recommendation ITU-T Y.101 (2000), *Global Information Infrastructure terminology: Terms and definitions*.

[b-ITU-T Y.2012] Recommendation ITU-T Y.2012 (2010), *Functional requirements and architecture of next generation networks*.

[b-ITU-T Y.2201] Recommendation ITU-T Y.2201 (2009), *Requirements and capabilities for ITU-T NGN*.

[b-ITU-T Y.2701] Recommendation ITU-T Y.2701 (2007), *Security requirements for NGN release 1*.

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

[b-Dannewitz] Dannewitz, C. (2009), *NetInf: An Information-Centric Design for the Future Internet*, In Proc. 3rd GI/ITG KuVS Workshop on The Future Internet, May.

[b-Detti] Detti A, Blefari Melazzi N, Salsano S, et al. (2011), *CONET: a content centric inter-networking architecture*. In Proc. ACM SIGCOMM workshop on Information-Centric Networking, August.

[b-Jacobson] Jacobson, V., et al. (2009), *Networking Named Content*, In Proc. ACM CoNEXT, December.

[b-Sarela] Sarela, M., et al. (2008), *RTFM: Publish/Subscribe Internetworking Architecture*, ICT-Mobile Summit, June.

[b-Seskar] Seskar I, Nagaraja K, Nelson S, et al. (2011), *MobilityFirst future internet architecture project*. In Proc. 7th Asian Internet Engineering Conference, December.

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, 2019