International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.3033

(01/2014)

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

Future networks

Framework of data aware networking for future networks

Recommendation ITU-T Y.3033

ITU-T Y-SERIES RECOMMENDATIONS

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

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Enhancements to NGN	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Packet-based Networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
FUTURE NETWORKS	**Y.3000–Y.3499**
CLOUD COMPUTING	Y.3500–Y.3999

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

Recommendation ITU-T Y.3033

Framework of data aware networking for future networks

Summary

Recommendation ITU-T Y.3033 describes data aware networking pertinent to the data awareness aspect of future networks envisioned in Recommendation ITU-T Y.3001. It provides the overview of data aware networking and describes problem spaces that are addressed by data aware networking. Finally, it describes the design goals for the realization of data aware networking.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.3033	2014-01-13	13	11.1002/1000/12076-en

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

FOREWORD

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

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

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

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

NOTE

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

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

INTELLECTUAL PROPERTY RIGHTS

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

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

Table of Contents

Recommendation ITU-T Y.3033

Framework of data aware networking for future networks

1 Scope

The scope of this Recommendation includes the following items:

- Overview of data aware networking;
- Problem spaces of data aware networking;
- Design goals of data aware networking.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is published regularly. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T Y.2221] Recommendation ITU-T Y.2221 (2010), *Requirements for support of ubiquitous sensor network (USN) applications and services in the NGN environment*.

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

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

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

3.1.2 identifier [b-ITU-T Y.2091]: An identifier is a series of digits, characters and symbols or any other form of data used to identify subscriber(s), user(s), network element(s), function(s), network entity(ies) providing services/applications, or other entities (e.g., physical or logical objects).

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

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 data ID: An identifier used to identify a data object. It has a form of a series of digits, characters and symbols or any of these combinations, which generally do not have any meaning.

3.2.2 data name: A string of alpha-numeric characters that is used to identify the data object. A data name, which may have variable length, is usually configured in such a way that it would be easier to be read and remembered by humans.

NOTE – A data object may have both data name and data ID. In this Recommendation, data name and data ID are used interchangeably.

3.2.3 data object: An individually identifiable unit of information created by individuals, institutions and technology to benefit audiences in contexts that they value.

3.2.4 provider: A network element in data aware networking that stores the original data object in order to provide access to the data object through data aware networking.

3.2.5 publisher: An entity that signs the original data object in order to distribute it through data aware networking.

4 Abbreviation and acronyms

This Recommendation uses the following abbreviations and acronyms:

API Application Programming Interface

DAN Data Aware Networking

FLN Flat Naming

FN Future Network

HN Hierarchical Naming

HR Hybrid Routing

HRN Human-Readable Naming

ICN Information Centric Networking

ICT Information and Communication Technology

ID Identifier

LBNR Lookup-By-Name Routing

N-HRN Non-Human-Readable Naming

P2P Peer-to-Peer

PKI Public Key Infrastructure

RBNR Route-By-Name Routing

URI Uniform Resource Identifier

5 Conventions

This Recommendation uses "is recommended" to indicate the main points to be taken into account in the standardization of data aware networking (DAN). Detailed requirements and their degree ("required", "recommended", or "optional") need further study.

6 Introduction

[ITU-T Y.3001] defines four objectives and twelve design goals which reflect the new emerging requirements for FNs. One of the objectives is data awareness which allows FNs to have mechanisms for promptly retrieving data regardless of their locations. Recently, this concept has been paid much attention in the network R&D community under the name of information centric networking (ICN) [b-Dannewitz] [b-Jacobson] [b-Sarela] because data acquiring would be more

efficient with this technology, and the concept itself would change the current network architectures drastically. This Recommendation therefore specifies the framework of data aware networking (DAN) for FNs.

A major Internet usage today is the retrieval of data whose amount has been changing in an explosive manner. For instance, the sum of all forms of video (TV, video on demand, Internet, and P2P) would continue to be approximately 90% of global consumer traffic by 2015 [b-Cisco]. Social networking services are also creating huge volumes of blog articles instantaneously, ubiquitous sensor networks [ITU-T Y.2221] are generating massive amount of digital data every second, and some applications called "micro-blogs" generate quasi-real-time communication that includes multimedia data [ITU-T Y.3001]. Since this trend is likely to be sustained in the future, FNs should be able to provide users with the means to access appropriate data in an efficient manner.

At the same time, the behaviour of subscribers has been changed from stationary to mobile. Due to the unpredictable behaviour of proliferated mobile devices, the resources of information and communication technology (ICT) are hard to be allocated in advance to accommodate the bursty traffic generated by mobile users called "flash crowd". Thus, FNs should also adaptively react to such environment to provide users with the means to access data without interruption.

DAN is a new network architecture that would have the capabilities to deal with enormous amount of data efficiently in a distributed environment and enables users to access desired data safely, easily, quickly and accurately, regardless of data locations. This technology enables networks to be aware of user requests and to react accordingly to support adaptive data distribution. Therefore, DAN is considered as a key approach to realizing FNs.

7 Overview of data aware networking

DAN enables users to distribute data objects in the network and to retrieve them in an efficient and adaptive manner. The essence of DAN lies in the name based communication that routes a data object in the network by its name or identifier (ID).

The name based communication enables not only end hosts but also intermediate nodes between them to be aware of user requests as well as the corresponding responses in the forms of data name or ID as well as its attributes.

"Data-aware" in the name of DAN means that the intermediate network elements recognize the data name or ID as well as its attributes which are provided for the network, and make a decision based on them. The decisions include:

1) Routing of user requests and the corresponding responses.
2) Responding to user requests directly if the requested data object is available.
3) Processing of user requests and the corresponding responses. The term "processing" includes any optimization process of the user requests and the corresponding responses before transmitting them.

Due to this awareness feature of DAN, a network element such as router can route, respond and process user requests and the corresponding responses to optimize the distribution of data objects. For example, DAN can route user requests to a nearby cached data object, respond to user requests by returning the cached data object, and process the data object based on user requests by modifying the data format, e.g., to fit the capability of the user terminal. By optimizing the data distribution, users can experience higher throughput and lower latency, and network resources can be saved by reducing redundant traffic or localizing bursty traffic caused by "flash crowd".

Moreover, the name based communication enables DAN to locate a data object regardless of its location, which ensures the continuation of communication associated with the names of data objects without being interrupted by its location change. For this reason, DAN can handle mobility in a more native manner than the current IP networks where the data object is located by using the

IP address of the host holding the data object and the communication is based on the location of the data object.

Figure 1 illustrates three general use cases of DAN. In case 1 in the figure, a user request for a data object is routed to the provider of the data object. While the requested data object is downloaded from the provider to the requester, the data object that is being downloaded can be stored on DAN elements along the downloading path, e.g., close to the requester. In case 2, each DAN element can respond to a user request with the data object which is available in its cache or storage so that the user request does not need to be routed to the provider of the original data object which may be distant from the requester. In case 3, DAN elements can process the data object before they respond to the requester so that the format of the data object fits the capability of the user's terminal.

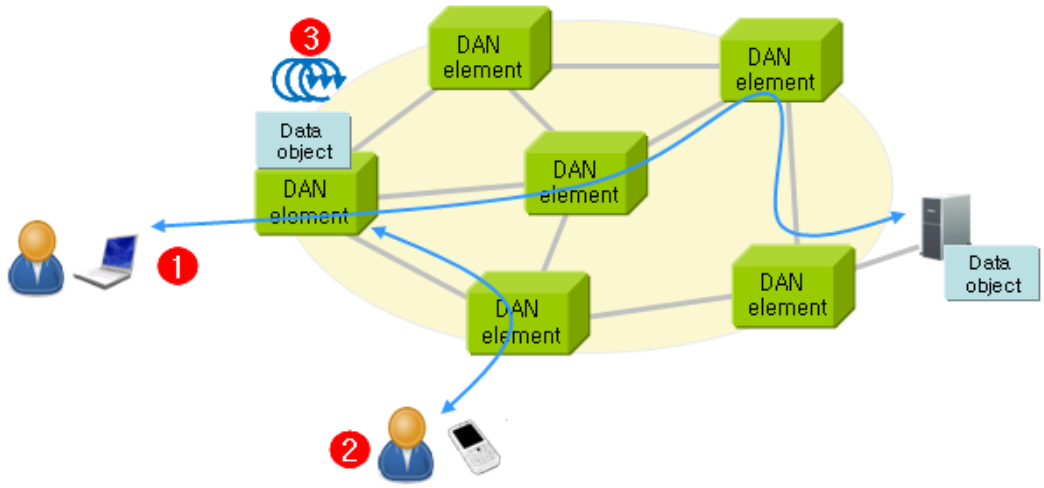

Figure 1 – Use cases of data aware networking

8 Problem spaces

8.1 Scalable and cost-efficient content distribution

Global data traffic has been increasing explosively, especially after various forms of multimedia traffic were introduced to the current networks. To deal with the problem, multiple heterogeneous infrastructures have been built on top of the conventional network architectures to provide data object distribution for users in more scalable and efficient manner. However, the heterogeneity restricts the interoperability of different infrastructures, which prevents scalable data object distribution in a cooperated manner. In addition, the infrastructures for the distribution of the individual data objects are mostly operated as service overlays where the transport network and the infrastructure of data object delivery are separated. For this reason, network resources used in data object distribution are often managed in a suboptimal manner, which makes data object distribution inefficient under the current networks [b-Ahlgren].

8.2 Mobility

The current networks require the communicating end terminals to maintain an end-to-end connection. However, managing end-to-end connections of proliferating mobile terminals is not a trivial task with the current IP networks. The problem originates from the use of IP address which is bound to the terminal's location and thus the change in location of terminal or data object will lead to failure in the end-to-end connection, thus interrupting the application sessions. Various solutions to overcome this problem have been proposed, but they also introduced complexity and processing overhead to the network due to the need for additional network entities such as gateways and network functionalities such as signalling and tunnelling [b-Kutscher]. The complexity and processing overhead will be immense and will become an operational problem, especially when the

number of terminals grows and frequent mobility occurs in a vastly distributed network environment.

8.3 Disruption tolerance

In the current networks, there are various applications which do not require seamless end-to-end communication, but require continuous sub-optimal communication under disruptive network environment where an end-to-end disconnection is common. There are several examples: sensor-based networks making intermittent connectivity, wireless networks experiencing frequent handovers and vehicular networks having moderate delays and frequent interruptions. However, the current IP-based network was initially designed to support an end-to-end communication so that it cannot provide reliable and optimized performance under disrupting network environments.

9 Design goals

This clause investigates the design goals of realizing each architectural components of DAN.

9.1 Naming

DAN is recommended to provide a data object with persistent and unique name.

Rationale: DAN names data objects using a naming scheme to identify each data object uniquely. There are a large number of identical copies of a data object which are distributed in different locations since all DAN elements have caching capability. Thus, the name of a data object should be persistent and unique so that users can access a data object simply based on its unique name regardless of its location. Unique name may represent one single data object, a group of data objects, or a group of identical copies of a data object. Moreover, since DAN elements use the attributes of a data object, e.g., file extension, to process user requests and the corresponding responses, DAN should be able to provide a naming scheme which supports the attributes of the data object.

9.2 Routing

DAN routing scheme is recommended to be scalable to support a large number of data objects. Additionally, it is recommended to support availability and adaptability.

Rationale: Routing in DAN locates a data object based on its name. It can use either a name resolution process which translates the name of requested data object into its locator and forward the user request based on its locator, or simply carry out routing based on the name of the data object without the resolution process. Routing in DAN uses the name of the data object whose number is estimated to be as high as 10^11 [b-Koponen]. Thus, the routing scheme in DAN should be scalable to deal with such a large number of data objects. Also, DAN is recommended to incorporate caching data objects into the routing scheme so that users take advantage of retrieving a data object from a nearby cache, which provides high availability of the data object. Moreover, a copy at cache has volatile behaviour since copies are frequently added, deleted, or replaced in the cache. Thus, a routing scheme in DAN is also recommended to adaptively take into account the volatile behaviour of copies in the cache.

9.3 Caching

Each network element in DAN is recommended to support a caching mechanism and be also able to inspect user requests that pass through it so that it can make a decision on user requests and respond using the cached data objects.

Rationale: To enable DAN elements to respond user requests, caching is a compulsory part of DAN. DAN is recommended to offer a caching mechanism which benefits from the recognition of user requests. For instance, since all DAN elements can cache any data object passing through

them, a caching decision is preferably made by the DAN elements. It is known as on-path caching which provides an implicit mechanism for DAN to distribute more data objects to the places where there are heavy requests with the minimum extra overhead of the caching mechanism.

9.4 Security

DAN is recommended to provide users with a security mechanism to verify the origin and integrity of data objects.

Rationale: The user of DAN retrieves a data object not only from an original copy provider but also from any network elements with the cached data objects. Since data objects can be maliciously modified, every data object in DAN should be signed by its publisher so that a user of the data object can verify the validity of the data object based on the signature. Since the data object is expected to be created by the publisher and is expected to be accessed by an unspecified number of users, an asymmetric cryptography is recommended to be used in the verification. To verify the signature of a data object, individual users should know the publisher's public key so that they can verify the origin and integrity of the data object. Therefore, DAN should support a mechanism which distributes the publisher's public key to the consumers of data objects. For example, an external third party authority such as hierarchical public key infrastructure (PKI) [b-IETF RFC 5280] can be cooperated with DAN to distribute public keys, or the publisher which received a user request provides its public key with the requested data object. This is known as self-certifying, which the user can verify whether the data object actually comes from the publisher simply by hashing the received public key and comparing it with acquainted hashed public key value.

In principle, the data object itself is encrypted so that DAN may allow anonymous users to access it or restrict the access by imposing authentication. The access control to the data object can be decided on the basis of the network operator's or content provider's policy.

9.5 Mobility

DAN is recommended to allow the end hosts to communicate without establishing or managing an end-to-end connection, thus simplifying the mobility aspects of the end terminals.

Rationale: DAN communicates using data name, which eliminates the need for end terminals to use the address of the data object or the address of the host where the data object is located. This realizes simple mobility management for the end hosts, especially when the location of the data object is unclear to the end hosts, or when the data object or the host holding the data object is relocated during the communication and a handover is required. Moreover, DAN allows the data object to be stored in intermediate nodes and be retransmitted by the intermediate node on behalf of the end hosts to adapt to varying network conditions, including fluctuation in data throughput and temporal disconnection during the handover.

9.6 Application programming interface

DAN is recommended to support two types of application programming interfaces (APIs) for data object distribution and retrieval: put/get and publish/subscribe based APIs. Moreover, DAN is recommended to support APIs that enable applications to retrieve the meta information, e.g., attributes of data object, to enable the applications to respond to the request accordingly.

Rationale: Most fundamental APIs of DAN define how data objects are distributed to and retrieved from the network. The put/get APIs allow applications to request and pull a data object from its serving network element, and the publish/subscribe APIs allow applications to specify what data object is wanted by them, and then the data object is delivered to the users as soon as it is published.

9.7 Transport

DAN is recommended to support two types of transport mechanisms, receiver and sender driven transports of data objects.

Rationale: In the receiver driven transport, the receiver sends the requests for specific pieces of a data object to the sender so that the senders respond to the request accordingly. In this case, the receiver is responsible for maintaining reliable data transmission by resending requests for any missing piece of the data object. In the sender driven transport, the sender controls sending rate of the pieces of a data object while performing loss detection and congestion control.

10 Environmental considerations

DAN is able to provide several mechanisms for operators to reduce the network resources and energy consumptions. First, network elements of DAN are able to respond to user requests directly rather than routing them to other end points so that other network elements can save their network resources and energy. Second, adaptive caching function of DAN localizes bursty traffic caused by unpredictable mobile users. For this reason, operators do not need to over-provision the network to handle the unpredictable bursty traffic. Therefore, the installation of unnecessary network resources can be minimized, which also reduces overall energy consumption level.

A possible drawback is that individual network elements of DAN require additional resources (e.g., cache or storage) which increase installation cost initially. Also, processing user requests may consume more energy.

11 Security considerations

Design goal of security for DAN is described in clause 9.4. Since DAN processes the requests and responses, various security issues can be raised. For instance, processing the retrieved data object that contains confidential information in its header may lead to privacy violation.

In addition, the in-network caching function of DAN may cause privacy and ownership issues. As mentioned previously, DAN secures each data object based on the signature of its publisher rather than securing the connection between two end points. Therefore, the distribution of public keys should be also considered while planning and designing DAN.

Appendix I

ICN: naming, routing and caching

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

I.1 Naming

There are two main naming schemes in ICN literature: hierarchical naming (HN) and flat naming (FLN).

HN has a hierarchical naming structure similar to a current web uniform resource identifier (URI) in IP networks. There are two reasons to have such a structure. One is to aggregate the names of data objects under publisher's prefix just as network prefixes are aggregated in IP networks. The other one is to have IP compatibility so that it can be deployed incrementally in the current IP networks. Content centric networking [b-Jacobson] adopted this approach. FLN names a data object as a fixed-length string which is generated by a hash function. This naming scheme can achieve persistence of data names for individual data objects. However, due to its flatness, naming aggregation is relatively less efficient than HN. Network of Information [b-Dannewitz] adopted this naming scheme.

Other than the naming schemes mentioned above, there is another categorical way to distinguish them: human-readable naming (HRN) and non-human-readable naming (N-HRN). HRN enables users, to some extent, to guess the relation between a data object and its name. Since this naming scheme is readable and has a semantic meaning, it could be remembered and reusable once it is exposed to users. HRN is closely related to HN above. N-HRN does not provide the name of a data object with a semantic meaning. It is difficult to be learnt or be reusable even though it is exposed to users previously. Thus, this naming scheme requires a name resolution process which translates the meaningless name into a semantic name, and vice versa. N-HRN is closely related to FLN above.

I.2 Routing

ICN routes user requests based on the name of the requested data object. The routing mechanism is composed of three steps: a name resolution step, a discovery step and a delivery step. The name resolution step translates the name of the requested data object into its locator, e.g., IP address. The discovery step routes user request to the data object. The last delivery step routes the requested data object to the requester. Depending on how the above steps are combined, three routing mechanisms have been introduced in ICN: route-by-name routing (RBNR), lookup-by-name routing (LBNR) and hybrid routing (HR).

RBNR omits the first name resolution step. The name of a data object is directly used, without being translated into a locator, to route user request to the data object. Therefore, ICN network elements need to hold routing information based on the names of data objects. Since the number of data objects is far more than that of hosts, maintaining such routing information causes scalability problem. However, this approach reduces overall latency and simplifies the routing process due to the omission of the resolution process. Regarding the delivery step, RBNR needs another ID of either host or location to route back the requested data object to the requester. Otherwise, an additional routing mechanism, such as bread-crumb approach: a request leaves behind a trail of breadcrumbs along its routing path, and then response can be routed back to the requester consuming the trail, is needed.

LBNR uses the first name resolution step to translate the name of the requested data object into its locator. Then, the second discovery step is carried out based on the translated locator information. Since the locator information includes IP address, the discovery step can depend on the current IP-based infrastructures. One challenge issue of LBNR is to construct a scalable resolution system

which maps the names of data objects to their corresponding locator information. The delivery step can be implemented in the same way as IP networks. The locator of requester is included in the request message, and then the requested data object is delivered to the requester based on the information.

HR combines both RBNR and LBNR to benefit from their advantages. For instance, intra-domain routing where scalability issue is not a serious problem can adopt RBNR to reduce overall latency by omitting the resolution process. Then, inter-domain routing where scalability is a critical issue can be supported by LBNR.

I.3 Caching

ICN supports two main caching mechanisms depending on how and where a data object is cached: on-path caching and off-path caching.

On-path caching selects a caching point(s) among nodes on the downloading path when a data object is being downloaded from its sender to requester. Since the caching decision can be made whenever data objects are downloaded, on-path caching provides an implicit mechanism for ICN to distribute more data objects to the places where there are heavy requests with the minimum extra overhead of caching protocol.

Off-path caching selects an optimal location of the network and caches a data object on the selected locations. Its operation is the same as a traditional surrogate server placement in CDN in the sense that the optimal selection of proper spots over the network yields optimal performance. However, off-path caching may be suitable only for small networks since it becomes impractical for large networks due to the significant increase in signalling traffic overhead caused by coordinated caching among caching nodes.

Bibliography

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

[b-IETF RFC 5280] IETF RFC 5280 (2008), *Internet X.509 Public Key Infrastructure Certificate Revocation List (CRL) Profile*.

[b-Ahlgren] Ahlgren, B., *et al*. (2012), *A Survey of Information-Centric Networking*, IEEE Communication Magazine, Vol. 50, No. 7, July.

[b-Cisco] *Cisco visual networking Index: Global Mobile Data Traffic Forecast Update*, 2011-2016, http://www.cisco.com.

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

[b-Koponen] Koponen, T., *et al*. (2007), *A data-oriented (and beyond) network architecture*, ACM SIGCOMM Computer Communication Review, Vol. 37, No. 4, pp. 181-192, October.

[b-Kutscher] Kutscher, D., *et al.* (2013), *ICN Research Challenges*, ICNRG, draft-kutscher-icnrg-challenges-04, March.

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

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects and next-generation networks**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2014