International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.3080

(09/2022)

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

Future networks

Information-centric networking in networks beyond IMT-2020: Requirements and mechanisms of the transport layer

Recommendation ITU-T Y.3080

ITU-T Y-SERIES RECOMMENDATIONS

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

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Enhancements to NGN	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Computing power networks	Y.2500–Y.2599
Packet-based Networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
FUTURE NETWORKS	**Y.3000–Y.3499**
CLOUD COMPUTING	Y.3500–Y.3599
BIG DATA	Y.3600–Y.3799
QUANTUM KEY DISTRIBUTION NETWORKS	Y.3800–Y.3999
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	
General	Y.4000–Y.4049
Definitions and terminologies	Y.4050–Y.4099
Requirements and use cases	Y.4100–Y.4249
Infrastructure, connectivity and networks	Y.4250–Y.4399
Frameworks, architectures and protocols	Y.4400–Y.4549
Services, applications, computation and data processing	Y.4550–Y.4699
Management, control and performance	Y.4700–Y.4799
Identification and security	Y.4800–Y.4899
Evaluation and assessment	Y.4900–Y.4999

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

Recommendation ITU-T Y.3080

Information-centric networking in networks beyond IMT-2020: Requirements and mechanisms of the transport layer

Summary

Recommendation ITU-T Y.3080 describes the requirements and mechanisms of the transport layer for information-centric networking (ICN) in networks beyond International Mobile Telecommunications 2020 (IMT-2020). 1) It provides an introduction to the transport layer in networks beyond IMT-2020. 2) It describes service and functional requirements of the transport layer. 3) Based on the requirements, it specifies the mechanisms of the transport layer for ICN in networks beyond IMT-2020.

History

Edition	Recommendation	Approval	Study Group	Unique ID[*]
1.0	ITU-T Y.3080	2022-09-29	13	11.1002/1000/15050

Keywords

ICN, IMT-2020, named data chunk, transport layer.

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

FOREWORD

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

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

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

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

NOTE

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

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

INTELLECTUAL PROPERTY RIGHTS

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

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

Table of Contents

Recommendation ITU-T Y.3080

Information-centric networking in networks beyond IMT-2020: Requirements and mechanisms of the transport layer

1 Scope

This Recommendation describes requirements and mechanisms of the transport layer for information-centric networking (ICN) in networks beyond International Mobile Telecommunications 2020 (IMT-2020), which focuses on named data chunk (NDC) retrieval. The scope includes:

– service requirements of the transport layer in ICN;

– functional requirements of the transport layer in ICN;

– mechanisms of the transport layer in ICN.

2 References

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

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

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

[ITU-T Y.3075] Recommendation ITU-T Y.3075 (2020), *Requirements and capabilities of information-centric networking routing and forwarding based on control and user plane separation in IMT-2020*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 caching [b-ITU-T X.525]: The process of creating cache copies.

3.1.2 control plane [b-ITU-T Y.2011]: The set of functions that controls the operation of entities in the stratum or layer under consideration, plus the functions required to support this control.

3.1.3 data plane [b-ITU-T Y.2011]: The set of functions used to transfer data in the stratum or layer under consideration.

3.1.4 identifier (ID): 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).

NOTE – Based on [b-ITU-T Y.2091].

3.1.5 identifier protocol (IDP) [ITU-T Y.3075]: A set of rules and regulations that specifies how the locator(s) of a data packet is/are manipulated based on ID in network layer under the ID/locator separation of information-centric networking (ICN).

3.1.6 IMT-2020 [ITU-T Y.3100]: (Based on [b-ITU-R M.2083-0]) Systems, system components, and related technologies that provide far more enhanced capabilities than those described in [b-ITU-R M.1645].

NOTE – [b-ITU-R M.1645] defines the framework and overall objectives of the future development of IMT-2000 and systems beyond IMT-2000 for the radio access network.

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

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

3.1.9 named data object (NDO) [b-ITU-T Y.Suppl.35]: A data object that is identifiable by a name.

3.1.10 named object (NO) [ITU-T Y.3075]: An object that is identifiable by a name. The object can be a data object, a device, a service, etc.

3.1.11 user plane [b-ITU-T Y.2011]: A synonym for data plane.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 in-network caching: The inherent capability of information-centric networking to allow intermediate network nodes, such as switches and routers with storage resources, to store data for a period.

3.2.2 named data chunk (NDC): A part of data that is uniquely identified by an identifier and the basic data unit to be transmitted in the transport layer of information-centric networking for in-network caching.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ICN	Information-Centric Networking
ID	Identifier
IDP	Identifier Protocol
IMT-2020	International Mobile Telecommunications 2020
I/O	Input/Output
IP	Internet Protocol
LOC	Locator
NA	Network Address
NDC	Named Data Chunk

NDO	Named Data Object
NO	Named Object
QoS	Quality of Service

5 Conventions

In this Recommendation:

The phrase "is required to" indicates a requirement that must be strictly followed and from which no deviation is permitted, if conformity to this Recommendation is to be claimed.

The phrase "is prohibited from" indicates a requirement that must be strictly followed and from which no deviation is permitted if conformity to this Recommendation is to be claimed.

The phrase "is recommended" indicates a requirement that is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformity.

The phrase "is not recommended" indicates a requirement that is not recommended but which is not specifically prohibited. Thus, conformity with this Recommendation can still be claimed even if this requirement is present.

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

6 Introduction

ICN provides a new network paradigm to efficiently deal with enormous amount of data in a distributed environment. ICN benefits IMT-2020 and beyond in challenging scenarios such as enhanced mobile broadband, ultra-reliable and low latency communications and massive machine type communication, enabling users to access desired data safely, easily, quickly and accurately by name/ID, regardless of data locations. In [ITU-T Y.3033], data can be cached and retransmitted by intermediate nodes on behalf of the end hosts to adapt to dynamic network conditions, which enables the new transport strategies, completely different from end-to-end transport in the transmission control protocol. Moreover, ICN is recommended to allow end hosts to communicate without establishing or managing end-to-end connections to simplify their mobility [ITU-T Y.3033]. [ITU-T Y.3031] specifies ID spaces used in ICN. In ID spaces, there are IDs for the user, data or content, service, node and location (network attachment point IDs or locators (LOCs)), some of which are used to identify various objects in transport layers [ITU-T Y.3031]. Actually, the requirements of the transport layer for the transmission of various objects are different. For example, in content ID-based transmission, more attention is paid to the number of content replicas, caching mechanism and transmission reliability; in service ID-based transmission, the workload and location of the service provider may be considered. Therefore, for various transmission purposes, impact factors on the transport layer are different, and some new features should be taken into account in designing the transmission mechanism.

Figure 6-1-a describes the layer view of ICN in IMT-2020 and beyond. There are two major categories for routing and forwarding of packets in the network layer. One is the ID-based routing method, in which addressing is achieved based on ID, such as named data networking. The other is the ID/LOC hybrid routing method in which an ID remains unchanged during a transmission process. Since the Internet protocol (IP) is the most widely used LOC-based addressing mechanism, ID/IP hybrid routing is a reasonable optional mechanism for ICN. The remainder of this Recommendation is based on the IP address, but the mechanisms and methods are also applicable to other methods based on the network address (NA).

In ICN, multiple replicas of the data may be stored in different locations, so one ID may correspond to multiple addresses, such as in the caching and multi-homing scenarios. Therefore, in the transmission process, the data source may be changed if necessary, which means the IP address of the data packet can be dynamically altered during the transmission. For example, when an intermediate network node detects the congestion, it can modify the address of the data packet to avoid the congestion path. An identifier protocol (IDP) is needed at the network layer to determine the rules and regulations that specify how the LOC(s) of a data packet is/are manipulated based on the ID in the network layer under the ID/LOC separation of ICN [ITU-T Y.3075]. Based on the capabilities of the network layer, the transport layer can provide flexible and efficient communication services for application processes.

In content-ID-based transmission, content from applications needs to be segmented into data chunks and assigned unique names/IDs that are called NDCs, which are the basic data units to be efficiently transmitted and cached in the transport layer for ICN (Figure 6-1-b). This Recommendation mainly focuses on the requirements and mechanisms of NDC transmission. Non-NDC transmission, whose ID could be a service, a host or a device [ITU-T Y.3031], lies outside the scope of this Recommendation.

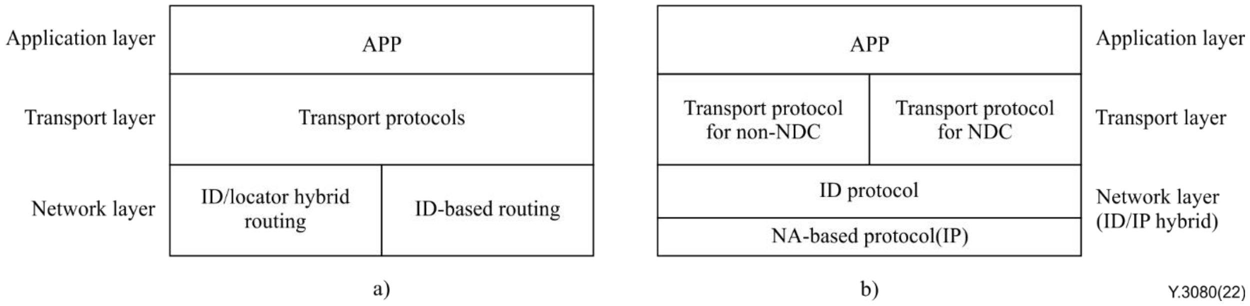

Figure 6-1 – Layer view for transport layer for ICN in IMT-2020 and beyond
a – General; b – Based on ID/IP hybrid routing

7 Requirements of transport layer for ICN in IMT-2020 and beyond

Requirements of transport layer for ICN in IMT-2020 and beyond, including service requirements and functional requirements, are described in clauses 7.1 and 7.2, respectively.

7.1 Service requirements

1. It is required to provide reliable NDC transmission services for applications.
2. It is required to provide NDC transmission services from in-network caching.

   NOTE – Because intermediate network nodes with replicas can provide data services directly, IP addresses of the data packet may be modified to the NA of the proper replica node to avoid the congestion path.
3. It is required that both end nodes provide the transport service and interface for the application layer.
4. It is required to support various transmission preferences from the diversified requirements of the application layer.
5. It is recommended to support the secure transmission requirements of sensitive data.

7.2 Functional requirements

NDC Segmentation

1. It is required to divide the NDC into smaller segments, which will be encapsulated in network layer packets for transmission.
2. It is required to reassemble the NDC correctly from the received packets of the network layer. It is required that an integrity check be executed after the assembly is completed. If verification fails, an incorrect NDC should be dropped and re-fetched.
3. It is recommended that the size of segments be smaller than the maximum transmission unit to avoid the IP fragmentation operation for network efficiency when these pieces are transmitted in network layer packets.

Transmission

1. It is required to use fault recovery functions to ensure the reliability of the transmission and to support integrity detection of the NDC.
2. It is required that nodes for not only the end, but also for the intermediate network, have the capability to respond to NDC requests and transmit NDC packets.
3. It is required to use receiver driven flow control functions to resolve the mismatch problem between data sending and receiving rates.
4. It is required to use receiver driven congestion control functions to alleviate congestion by autonomously selecting a proper data replica to alter the transmission path or adjust the flow rate. ICN native functions of receiver driven congestion control can be used.

   NOTE – In receiver driven transport, the receiver sends requests for specific pieces of a data object to the sender so that it responds accordingly. In this case, the receiver is responsible for maintaining reliable data transmission by resending requests for any missing piece of the data object [ITU-T Y.3033].
5. It is recommended to have the capability to carry the information about establishment of the transmission in the transport layer header, such as port.
6. It is recommended to use multipath transmission function to improve transmission efficiency by retrieving different pieces of NDC from multiple replica sources concurrently.

In-network caching and storage

1. It is required that the intermediate network nodes have the capability to store the NDC.
2. It is required that the intermediate network nodes have the capability to reassemble the data packets to the NDC.
3. It is required that the intermediate network nodes have the capability to elastically manage cached data resources for in-network caching or storage.
4. It is recommended that the intermediate network nodes have the capability simultaneously to support high speed caching and maintain line-speed transmission.

Preference processing

1. It is required that preference fields be encapsulated in the transport layer header to support preference processing. Through the preference fields, network functions and corresponding strategies can be determined by applications, such as whether to allow caching, in-network storage mechanisms and quality of service (QoS) guarantee mechanisms.
2. It is required that intermediate network nodes have the capability to execute actions according to preference fields encapsulated in the transport layer header. The intermediate network nodes can make decisions and execute related actions based on the preference field and the local network status.

For example,

1) In a caching scenario, due to privacy or consistency requirements, some data cannot be cached by intermediate nodes, which can be achieved by indicating whether caching is allowed in the preference field. Also, the location of the replica can be specified in the preference field, such as at the edge of the network and the centre of the network. Network nodes can cache popular replicas at the edge of the network, which usually improve the quality of NDC retrieval services.
2) In a network-storage scenario, the number of replicas stored in the network can be specified in the preference field. Additionally, based on the field, the intermediate network nodes determine whether to store the replica and whether to make a copy and forward it to other appropriate nodes according to local network status.
3) In a low-latency transmission scenario, the transmission priority can be specified in the preference field. Intermediate network nodes preferentially forward high-priority packets. Also, it can be specified in the preference field that multipath transmission function is used to reduce transmission delay.
4) In the sensitive data transmission scenario, the security requirements of transmission can be specified in the preference field, such as encryption hop by hop and transmission on variable paths. Intermediate network nodes can process the data according to the preference field.

3. It is required that the intermediate network nodes have the capability to autonomously make decisions according to the preference fields, such as whether the NDC should be stored or cached.
4. It is required that the intermediate network nodes have the capability to provide collaborative in-network caching or storage to improve utilization according to the preference fields.

8 Mechanisms of transport layer for ICN in IMT-2020 and beyond

8.1 NDC segmentation mechanism

A NDC is the basic data unit to be transmitted at the transport layer of ICN for in-network caching. The size of the NDC is usually larger than that of a network layer packet. Hence the NDC needs to be segmented into a series of smaller pieces to be encapsulated in the packets of the network layer. A data structure should be created to describe the relationship between the NDC and the segmented pieces.

The data structure contains position information about pieces and check information. The position information may contain offset and length, or the sequence number of each piece. The position information of the piece is used to reassemble the NDC. The checking information, such as checksum or digest, is used to detect whether the piece data is wrong. The receiver does not differentiate the arriving orders of the pieces, thereby avoiding head-of-line blocking.

8.2 Transmission mechanisms

8.2.1 ID-based transmission

The transport layer of ICN uses the ID-based interface of a network layer provided by the IDP. Both communication sides are labelled by unique and consistent IDs, which remain unchanged during transmission, even if their addresses change. Therefore, the ID-based transmission is location independent.

8.2.2 Receiver-driven transmission

In ICN, it is essential to consider what is to be retrieved rather than where to retrieve it. Data transmission is labelled by two location-independent IDs, one of which is the ID of the NDC to be retrieved and the other the receiver requesting to retrieve the NDC at either end. The receiver is responsible for initiating, maintaining and controlling the transmission by sending data requests with the ID of the NDC. The host of the NDC responds to the requests and transmits the NDC data according to the requests from the receiver.

Fault recovery

Retransmission is adopted for fault recovery in the transport layer. The receiver deals with NDC reassembly and integrity checking. Accordingly, it is the receiver that detects the lost or damaged data pieces using the segmentation data structure and local timers. The receiver sends a request for a lost data piece using position information from the segmentation data structure. The sender resends the pieces according to the receiver's request. The receiver discards received data that are duplicated.

Congestion control

Congestion control can be performed by autonomously selecting the data replica before NDC transmission and adjusting the request sending rate during it.

In-network caching can provide multiple replicas of the NDC. The appropriate data replica can be selected through the IDP of the network layer to alleviate congestion during transmission. Replica selection may depend on network status including network latency, bandwidth and packet loss rate. Selection of the appropiater data replica can improve transmission performance and load balancing.

The transport layer can provide a congestion control mechanism. The receiver may maintain certain congestion control parameters, including congestion window, round-trip time and request queue, to increase or reduce the request sending rate and data size accordingly. It is recommended that the receiver use the quick start mode when sending data requests. The initial request sending rate and data size may be determined by information such as transmission history.

One of these two situations can switch to the other in some cases. For example, if the congestion of the current NDC transmission is intolerable, the data replica source can be switched during transmission.

Flow control

The receiver should increase or reduce the request sending rate and data size based on the receiver's buffer occupancy to maximize transmission efficiency while avoiding the overflow buffer.

8.3 In-network caching/storage mechanisms

8.3.1 Switch and storage separation

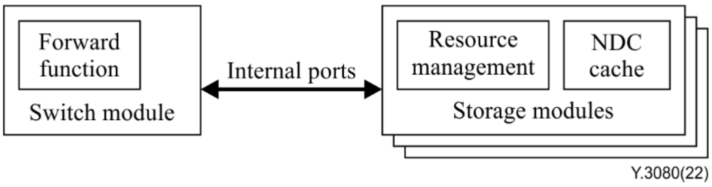

Figure 8-1 – Switch and storage separation structure of intermediate network nodes

The input/output (I/O) speed of a storage device is much lower than the forwarding speed of a switch. In order to avoid the effect on the line-speed forwarding process, the functions of intermediate network nodes are divided into two parts: switch module; and storage module (Figure 8-1).

– The switch module only focuses on the forwarding process to support line-speed forwarding performance.

- The storage module deals with storage resource management and NDC caching, which should not affect the performance of the switch module. Moreover, the storage module should cache the NDC as fast as possible.
- The switch and storage modules are connected by a dedicated internal port that is not exposed to the networks. The dedicated internal port can be a pre-configured network one directly connecting two modules or the interface for inter-processing communication. Thus, the requirement of the caching performance is restricted to the internal port and the port-line-speed caching that it is possible to achieve.
- A switch module may connect multiple storage modules via multiple internal ports to achieve caching scalability of an intermediate network node elastically.

If an in-network caching condition is matched, simultaneously, an NDC packet should be forwarded by the switch module immediately while a copy of the packet is forwarded to the storage module for the caching process via the dedicated internal port. For a packet whose destination address is that of an intermediate network node, it should be forwarded to this node and received by its switch module. Then its switch module forwards the packet to the storage module via the dedicated internal port for further caching operations.

8.4 Preference-processing mechanisms

The preference field, which is related to the transmission and storage capabilities provided by the network, should be encapsulated in the transport layer header to meet the differentiated service requirements from applications. Furthermore, based on the preference field and local information, the intermediate network nodes can make on-site decisions, such as whether to cache the data chunk or forward the data packet. The transport layer preference field is related to: 1) caching strategy; 2) reliability of the cached NDC; 3) storage location; 4) transmission QoS, as shown in Figure 8-2.

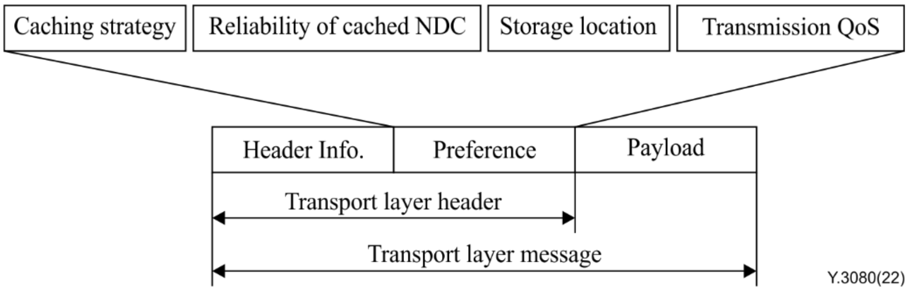

Figure 8-2 – Preference field in transport layer header

8.4.1 Caching strategy

An intermediate network node can make decisions autonomously on whether to cache an NDC based on its caching status. Meanwhile, collaborative caching strategies, which are supported by the IDP, are used to improve in-network storage utilization. Each intermediate network node has an IDP processing module that maintains the status information of nearby nodes. The node status table may record the dynamic status values of nearby nodes, such as storage status, service status and I/O status that are periodically exchanged among network nodes. The nearby node can be used for the autonomous selection of migration nodes. When a node is too busy to provide the caching service, hot replicas in this node are migrated to the appropriate nodes selected from the node status table. The status information is particularly useful for selecting nodes when replica migration occurs. For example, when the storage space of a node is insufficient, the cold replicas in this node may be deleted or migrated to other appropriate nodes. The migration request is sent to the destination node, which initiates the receiver-driven transmission for the NDC.

8.4.2 Reliability of cached NDC

For different preferences from applications, multiple levels of reliability of cached NDC should be provided. The reliability label that is encapsulated in the transport layer header is related to the factors such as the number of replicas, the storage position of replicas and the type of nodes. When a node processes the packet with a specified reliability level, the corresponding node status table and factors previously mentioned should be considered together to autonomously determine the forwarding destinations of packets. When the storage load of a node is too heavy to provide storage service, it should select another appropriate node as the destination to forward the received NDC packets. The nearby node status table can be used for the selection of the storage destination node, while the IDP module in each node can provide information about nearby node status.

8.4.3 Storage location

The storage location preference may be useful for some applications. The storage location can be near the end nodes, at the edge of the network and the centre of the network. The location of an intermediate network node can be characterized by calculating the hops between this node and nearby end nodes. If the hops are less than a certain number, the intermediate network node can be characterized as an edge node; contrarily, this node can be characterized as a centre node. A label reflecting the storage location preference can be encapsulated in the transport layer header. When an intermediate network node processes the packet, the label and the location of this node can be considered together to determine the storage operation.

8.4.4 Transmission QoS

The application may propose different transmission QoS requirements, such as transmission rate and transmission latency. The priority control is used to implement different levels of transmission QoS. To meet the transmission rate requirements, high-priority NDC requests are sent preferentially and the sender/receiver network resources, such as sending/receiving queues, are reserved for high-priority NDC transmissions. To meet the transmission latency requirements, a distance-constrained data replica is selected to realize the nearby data retrieval that can be achieved by the IDP.

9 Security consideration

To support the capabilities of the transport layer, different kinds of security threat should be considered.

Node attack

Intermediate network nodes can be data providers and become the destination of user packets. A direct denial of service attack caused by node address leakage may be the risk. To alleviate this risk, address translation can be executed at the network boundary, and the real addresses of intermediate nodes are shielded for end users. In addition, some mature protection approaches can also be directly used, e.g., a firewall.

Confidentiality of transmission

Encrypted transmission of NDC can be used to ensure its confidentiality. NDC encryption with different security levels can be supported during the transmission based on application-related preference. For example, keys can be negotiated between intermediate nodes and multiple encryption can be performed to meet the needs of high security transmission.

Covert channel for network transmission

Multi-path and variable path transmission of NDCs based on the IDP can be used to make the transmission path unpredictable and changeable, so as to ensure the concealment of NDC transmission and prevent eavesdropping.

Integrity of NDC

Integrity may be achieved through the naming mechanism of NDCs. For example, if the identity/name of an NDC is assigned by the hash of DC, the identity/name can be used to verify its integrity.

Bibliography

[b-ITU-T X.525] Recommendation ITU-T X.525 (2019), *Information technology – Open Systems Interconnection – The directory: Replication*.

[b-ITU-T Y.2011] Recommendation ITU-T Y.2011 (2004), *General principles and general reference model for next generation networks*.

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

[b-ITU-T Y.3100] Recommendation ITU-T Y.3100 (2017), *Terms and definitions for IMT-2020 network*.

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

[b-ITU-T Y.Suppl.35] ITU-T Y-series Recommendations – Supplement 35 (2016), *ITU-T Y.3033 – Data aware networking – Scenarios and use cases*.

[b-ITU-R M.1645] Recommendation ITU-R M.1645 (2003), *Framework and overall objectives of the future development of IMT-2000 and systems beyond IMT-2000*.

[b-ITU-R M.2083] Recommendation ITU-R M.2083 (2015), *IMT vision – Framework and overall objectives of the future development of IMT for 2020 and beyond*.

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, 2022