International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

H.644.3

(08/2020)

SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS

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

Functional architecture of multimedia content delivery networks

Recommendation ITU-T H.644.3

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.644.3

Functional architecture of multimedia content delivery networks

Summary

Recommendation ITU-T H.644.3 specifies the common functional architecture for multimedia content delivery networks. The functions and functional blocks within this common functional architecture and the related reference points are specified in this Recommendation for matching the requirements of various kinds of content ingestion, content distribution and content delivery within different networks and platforms. In addition, this Recommendation also provides some examples of the related service features, workflows, an implementation guide, and the security aspects in appendices.

This Recommendation is intended to provide the references for multimedia content delivery network (MCDN) providers to help them to build the common infrastructures of a multimedia content delivery network. This Recommendation is of benefit for multimedia content providers who wish to dispatch their content to different types of end-users by taking advantage of a common MCDN capability.

History

Edition	Recommendation	Approval	Study Group	Unique ID[*]
1.0	ITU-T H.644.3	2020-08-13	16	11.1002/1000/14340

Keywords

Architecture, multimedia content delivery network, reference point.

[*] 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.644.3

Functional architecture of multimedia content delivery networks

1 Scope

This Recommendation specifies the common functional architecture for multimedia content delivery networks (MCDNs). The functions and functional blocks within that functional architecture and the related reference points are specified in this Recommendation for matching the requirements of various kinds of content ingestion, content distribution and content delivery within different networks and platforms. In addition, this Recommendation also provides some examples of the related service features, workflows, an implementation guide and the security aspects in the Appendices.

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.2019] Recommendation ITU-T Y.2019 (2010), *Content delivery functional architecture in NGN.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 content [b-ITU-T H.780]: A combination of audio, still image, graphic, video, or data.

3.1.2 content delivery network (CDN) [b-ITU-T Y.2084]: A content delivery network (CDN) is a system of distributed servers that deliver content (e.g., web pages, files, videos and audios) to users based on pre-defined criteria such as the geographic locations of users, the status of the content delivery server and the IP network connection.

3.1.3 content delivery [b-ITU-T Y.2080]: In the context of the distributed service networking (DSN) functional architecture, the operation of sending and receiving content between the requested peer and the requesting peer or client.

NOTE – A client is a service consumer external to DSN. A peer is a node within DSN.

3.1.4 content distribution [b-ITU-T Y.2080]: In the context of the distributed service networking (DSN) functional architecture, the whole process of content sending from one or more content sources, and sharing among DSN nodes.

NOTE – During the content distribution process, content is often sent to appropriate intermediate nodes to enable subsequent delivery.

3.1.5 data encryption [b-ITU-T J.191]: Data encryption prevents the unauthorized disclosure/access of data. Data encryption does an excellent job at providing data confidentiality and protection against theft of service. Encryption prevents making data unable to read without the correct decryption key; however, it does not validate the source/receiving entities and it does not provide copy protection after the data have been decrypted. It also does not prevent denial of service (DoS) attacks.

3.1.6 delivery [b-ITU-T X.609]: The procedures and means employed to provide a user with the required archived material for reuse.

3.1.7 distributed service networking (DSN) [b-ITU-T Y.2206]: An overlay networking which provides distributed and manageable capabilities to support various multimedia services and applications.

3.1.8 metadata [b-ITU-T X.1255]: Structured information that pertains to the identity of users, systems, services, processes, resources, information or other entities.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 content distribution service: The service provided by content/service providers (CP/SPs) or content delivery network (CDN) venders/providers with the capability of distributing and delivering the content from content source to the destination by using CDN facilities.

3.2.2 distribution: The unidirectional flow of information from a given point in the network to other (multiple) locations.

3.2.3 dynamic content: Content created on demand when a user uses a web application dynamically.

3.2.4 static content: Content that seldom changes and that does not change with the requests from the users.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AES	Advanced Encryption Standard
AF	Aggregation Functions
A/S-MBF	Application/Service Business Management Functions
CBR	Constant Bitrate
CD&DF	Content Distribution and Delivery Functions
CL&DF	Content Location and Distribution Functions
CDF	Content Delivery Functions
CDN	Content Delivery Network
CMS	Content Management System
CNAME	Canonical NAME
CPF	Content Provider Functions
CRF	Content Routing/Redirecting Functions
DNS	Domain Name System
DoS	Denial of Service
EPG	Electronic Programme Guide
EUF	End-user Functions
FTP	File Transfer Protocol

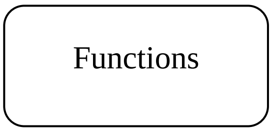
GSLB	Global Service Load Balance
HLS	HTTP Live Streaming
HPD	HTTP Progress Download
HTTP	Hypertext Transfer Protocol
IPTV	Internet Protocol Television
MCDN	Multimedia Content Delivery Network
NF	Network Functions
NFV	Network Functions Virtualization
NFVO	NFV Orchestrator
NGN	Next Generation Network
OTT	Over The Top
QoS	Quality of Service
RR	Request Routing
RTSP	Real-Time Streaming Protocol
SDN	Software Defined Network
SLB	Service Load Balance
SOAP	Simple Object Access Protocol
STB	Set Top Box
URL	Uniform Resource Locator
VBR	Variable Bitrate
VOD	Video On Demand
VR	Virtual Reality
XML	Extensible Markup language

5 Conventions

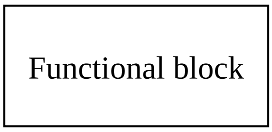
In this Recommendation:

- The keywords "is required to" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.
- The keywords "is prohibited from" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.
- The keywords "is recommended" indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.
- The keywords "is not recommended" indicate a requirement which is not recommended but which is not specifically prohibited. Thus, conformance with this specification can still be claimed even if this requirement is present.
- The keywords "can optionally" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

Functions: In the context of MCDN architecture, "functions" are defined as a collection of functionalities. It is represented by the following symbol:



Functional block: In the context of MCDN architecture, a "functional block" is defined as a group of functionalities that has not been further subdivided at the level of detail described in this Recommendation. It is represented by the following symbol:



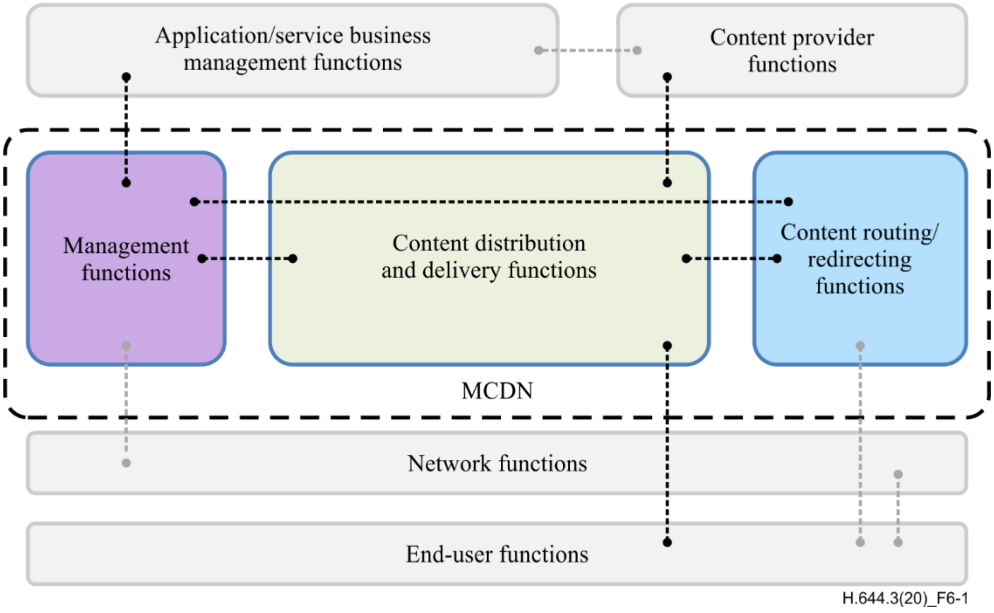
NOTE – In the future, other groups or other Recommendations may possibly further subdivide these functional blocks.

6 Introduction

The current [ITU-T Y.2019] has defined the functional architecture of content delivery functions in next generation network (NGN). It is a general functional architecture but was built based on the Internet protocol television (IPTV) service. Currently, many additional services such as over the top (OTT) may also apply this functional architecture, but some functional blocks may need to be enhanced to support the various types of service. In order to support those services, some reference points and protocols may also need to be updated accordingly. Moreover, to provide an end-to-end content delivery service, a management and content routing system are also need to be included. Therefore, the current context in [ITU-T Y.2019] may not be sufficient to satisfy those new requirements.

A multimedia content delivery network (MCDN) as defined in this Recommendation is an integrated networking structure which is able to provide a common multimedia content distribution service to the various end-users by ignoring the difference of content type (e.g., static content, dynamic content), network and service platform, etc. Basically, the functional architecture for MCDN consists of the conventional content delivery network (CDN) functions in common, i.e., the basic functions that all types of CDN service are required to implement, e.g., content ingestion, storage and distribution, etc. However, there are many service feature differences between different types of CDN. For example, for the video service provided by streaming media CDN, a variety of streaming protocols (e.g., RTSP, HLS and Dash) should be supported but it is not required for web CDN which merely supports download protocols (e.g., HTTP and FTP). These differences can be eliminated by adopting the enhanced capability provided by MCDN functions.

Figure 6-1 provides an overview of the MCDN functional architecture.



Application/service business management functions
Content provider functions
Management functions
Content distribution and delivery functions
Content routing/ redirecting functions
MCDN
Network functions
End-user functions
H.644.3(20)_F6-1

Figure 6-1 – An overview of the MCDN functional architecture

NOTE – The functions and reference points represented by the blocks and dotted lines in grey are only introduced as the associated background information in this Recommendation.

6.1 An overview of the MCDN functional architecture

This clause provides descriptions of each of the functional components in MCDN functional architecture. The related functions and the functional blocks in each function are further broken down in clause 7.

6.1.1 Content distribution and delivery functions

The content distribution and delivery functions (CD&DF) provide the core functionality of content ingestion, processing and storage. This also provides the content service for the end-user by distributing the content to the MCDN edge node.

Considering the actual implementation of CD&DF, a nodes deployment with 2-layer-networking or 3-layer-networking are typically used and different types of MCDN node are deployed in each layer. These node types are described as follows:

Centre node

The centre node receives content from the content provider, stores and pre-processes and distributes it to the downstream nodes using the network functions, under the control of the application/service system management functions.

Relay/middle node

The relay/middle node acts as the buffer function between centre node and edge node, which is able to provide content service when the content is not in edge nodes.

NOTE – In some special circumstances, e.g., when the MCDN service coverage is restricted, the relay/middle node may not be applied.

Edge node

The major function of edge node is to deliver the related content to end-users based on users' requests, the adapted transport protocols, and the server nodes' status. Edge nodes can be designed for different architectures according to the service that a service provider wants to provide.

6.1.2 Content routing/redirecting functions

The content routing/redirecting functions (CRF) are responsible for selecting the requested content resource for users. The content resource may be the URL of content or the media server address.

NOTE – By considering the real implementation of this function with various network situations, e.g., fixed or mobile networks, there may be many approaches for accessing the content routing/redirecting server, e.g., by using DNS recursion/application level redirecting. These approaches are out of scope in this Recommendation but will be specified in the other MCDN related Recommendations.

6.1.3 Management functions

The management functions (MF) perform overall system management (e.g., content management, node management, access/ingestion management, network management, distribution policy management, and routing/redirection policy management). The major role of this function is to manage the content, policy and node server to guarantee the CDN running in a highly efficient and secure environment.

6.2 Functional groups of the external system

6.2.1 Content provider functions

The content provider functions (CPF) are provided by the entity that owns or is licensed to provide (e.g., sell, rent or give free usage permission) content or content assets (e.g., owner of the source content, metadata and usage rights). The function of content provider is used to edit, review, release and broadcast control (including advertisement insertion, content switching, content monitoring, etc.) of content injected by content provider. Content provider functions are also responsible for maintaining the customer authorized domain name system (DNS) functions.

6.2.2 Application/service business management functions

The application/service business management functions (A/S-MBF) are responsible for business configuration, including user's life cycle management (account opening, account cancellation, account authentication and account change), business ordering information management and billing, and arrangement of the browsing interface for users.

6.2.3 Network functions

The network Functions (NF) provide the network resources for data transmission and processing for those functions that are the infrastructure functions and contribute to the provision of the quality of service (QoS) required by the multimedia services.

6.2.4 End-user functions

The end-user functions (EUF) perform mediation between the end user and the media service node.

7 The high-levelled MCDN functional architecture

This clause describes the functions and functional blocks by considering the multimedia services usage including the content/service provider access, the content ingestion and the content distribution and delivery. Functions and functional blocks described in this clause are common to functional components as detailed in clause 6.1.

Figure 7-1 provides the high-levelled MCDN functional architecture with detailed information.

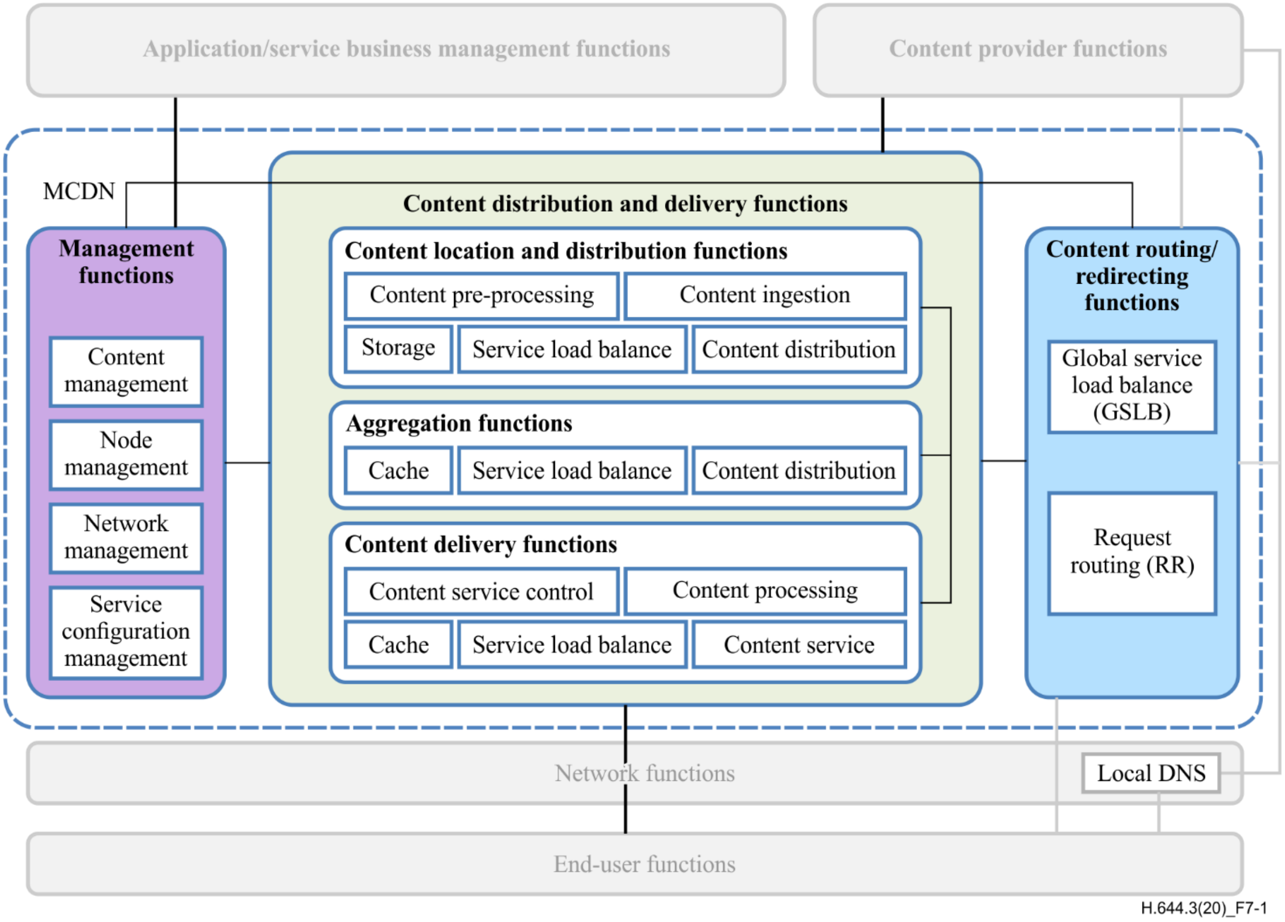


Figure 7-1 – The high-levelled MCDN functional architecture

NOTE – The definition of functions and the line in grey are outside of the scope of this Recommendation.

7.1 Content distribution and delivery functions

7.1.1 Content location and distribution functions (centre node)

Content location and distribution functions (CL&DF), acting as a centre node, is mainly responsible for docking with the application/service management system functions to achieve content ingestion, management, storage and active distribution to various media service nodes in MCDN, which includes the function blocks presented in clauses 7.1.1.1 to 7.1.1.5.

7.1.1.1 Content ingestion

According to the content ingestion instruction of the content management system (CMS) which may be provided by the content provider, the content ingestion functional block acquires the specified content, ingested into the content storage and registered in the content management functional block. Alternatively, instead of ingesting content through the CMS, the content and metadata sources are accessed by the way of back-to-source.

7.1.1.2 Content pre-processing

The content pre-processing functional block allows the ingested content processing, such as content slicing, transcoding, and encapsulation, etc.

7.1.1.3 Service load balance

The service load balance (SLB) functional block receives the content location and/or content request from the downstream nodes, and selects the most appropriate media server to provide services based on the load balance strategy inside the centre node.

7.1.1.4 Content storage

The content storage functional block provides the storage resources for online media content according to the strategy in the content management functional block, and updates media content according to the caching strategy.

7.1.1.5 Content distribution

The content distribution functional block is used for content distribution and transmission based on the scheduling strategy in the content management functional block.

7.1.2 Content delivery functions (edge node)

Content delivery functions (CDF), acting as an edge node in MCDN service, is responsible for receiving end-user requests, authenticating and then serving cached content to users. If there is a cache miss, the edge node will pull content from the upstream node and cache it, or redirect the request to the upstream node, to serve the content. Edge node includes the functional blocks presented in clauses 7.1.2.1 to 7.1.2.5:

7.1.2.1 Content service control

The content service control functional block locates the node that can serve desired contents, based on the content ID.

7.1.2.2 Content processing

The content processing functional block allows the ingested content to be processed, such as slicing, transcoding, and encapsulation, etc.

7.1.2.3 Content service

The content service functional block supports a variety of multimedia services, such as e-business, web portal service, video on demand, live-streaming, and downloading files including game installation packages, audios/videos, and firmware.

7.1.2.4 Service load balance

The service load balance (SLB) functional block receives the content location and/or content request from the end-user via content routing/redirecting functions, and selects the most appropriate media server to provide services based on the load balance strategy inside each edge node.

7.1.2.5 Cache

The cache functional block provides the capability of temporary storage of the content locally in the Edge node. The content may be added, removed and replaced automatically according to a pre-defined cache policy. Normally, the most popular/hottest content will be cached in the Edge node.

7.1.3 Aggregation functions (relay/middle node)

Aggregation functions (AF), acting as a relay/middle node, is an optional function within the functional architecture in this Recommendation. However it is recommended to be implemented as a functional entity in the real MCDN deployment. It is very useful for delivering multimedia service especially within a wide geographical area that covered by the MCDN service.

The aggregation functions stores and updates multimedia content based on caching strategy.

7.1.3.1 Service load balance

The service load balance (SLB) functional block receives the content location and/or content request from the downstream nodes, and selects the most appropriate media server to provide services based on the load balance strategy inside the relay/middle node.

7.1.3.2 Cache

The cache functional block provides the capability of temporary storage of the content locally in the relay/middle node. The content may be added, removed and replaced automatically according to a pre-defined cache policy.

7.1.3.3 Content distribution

The content distribution functional block is used for content distribution and transmission based on the routing strategy in the content management block.

7.2 Management functions

7.2.1 Content management

The content management functional block registers and manages the attributes of contents in the MCDN, including the content ID, media metadata information, life cycle, content status, and content update policy.

7.2.2 Node management

The node management functional block manages all nodes in the MCDN, including node information maintenance, device adding and deleting within the node, the content and service policy maintenance within the node.

7.2.3 Network management

The network management functional block manages MCDN network performance, alarms, and topology information.

NOTE – By considering the applying of the evolved network technology, such as NFV, SDN, the network management functional block can also optionally manage the underlay network, including network performance, alarms and topology information, by co-operating with the other network functions, such as SDN controller, NFVO, etc.

7.2.4 Service configuration management

The service configuration management functional block provides the unified management of MCDN service configuration, for example, the management of content injection, content service, the policy of content distribution, routing and dispatching.

7.3 Content routing/redirecting functions

The content routing/redirecting functions are further composed of the following two functional blocks.

7.3.1 Global service load balance

The global service load balance (GSLB) functional block provides the unified entrance of MCDN service for the user requests and dispatches those requests among MCDN service nodes in the different areas.

7.3.2 Request routing

The request routing (RR) functional block provides the entrance of MCDN service within a specific area for the user requests and dispatches those requests among the MCDN service nodes within the same area.

8 Reference points

This clause describes the general definitions of reference points and the related protocols that are applied on the reference points. The MCDN reference points, based on the system they are interacting with, are classified into external reference points and internal reference points.

Figure 8-1 shows the reference points among the functions and functional blocks within MCDN functional architecture.

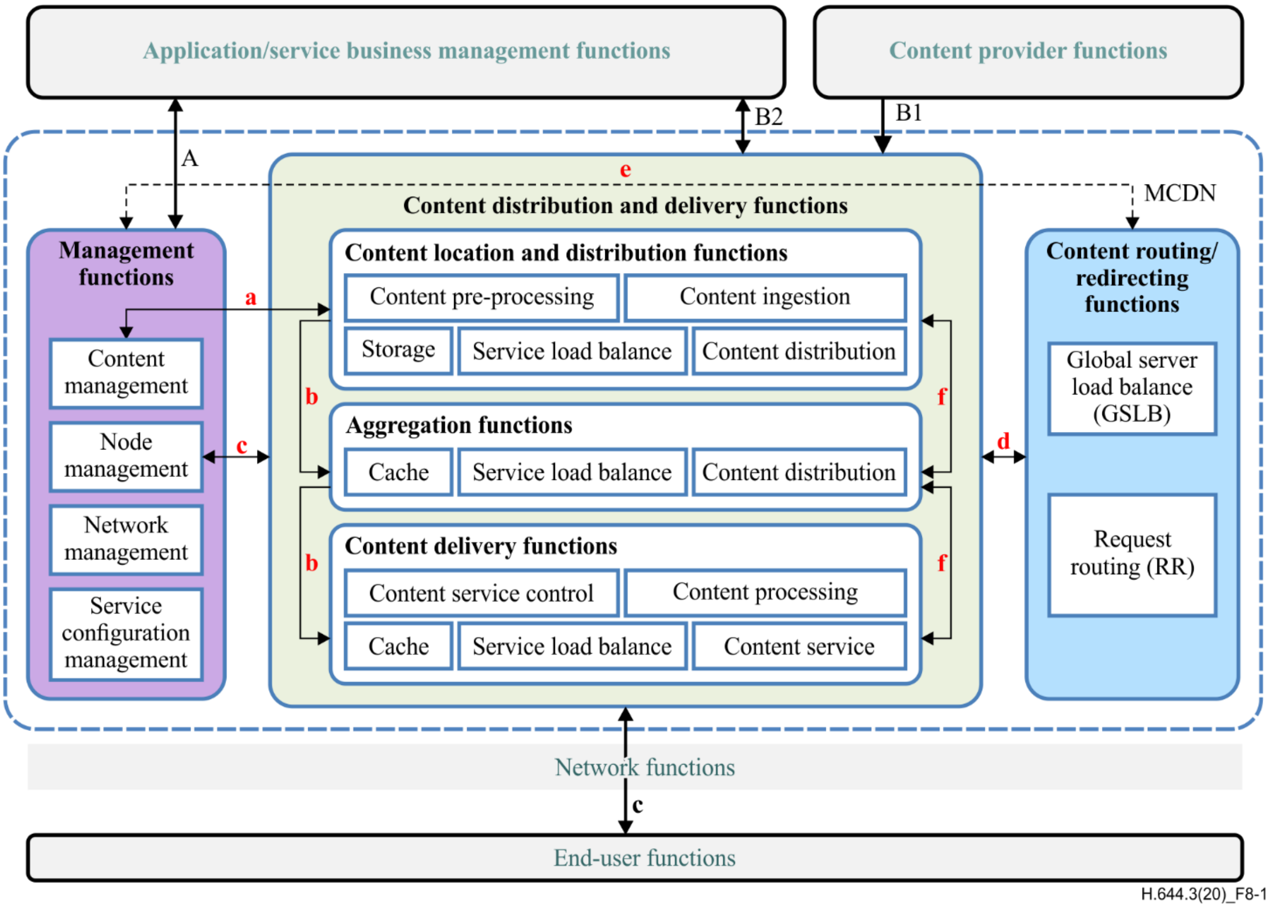


Figure 8-1 – Reference points within MCDN functional architecture

8.1 External reference points

According to the system and network architecture, MCDN external reference points are defined as indicated in Table 8-1.

NOTE – There may be other reference points that need to be defined, such as the reference point between the content routing/redirecting system and content provider or end-user. Those reference points are outside the scope of this Recommendation.

Table 8-1 – External reference points

Reference point	Definition	Protocol	Notes
A	Reference point between A/S-BMF and MF	HTTP, FTP	This reference point A for MCDN management system is to receive the management and configuration instruction from the external management platform.

Table 8-1 – External reference points

Reference point	Definition	Protocol	Notes
B1	Reference point between CPF and CD & DF (mostly implemented by centre node)	SOAP+XML	The content provider informs the centre node of MCDN to obtain the information of external content source and metadata into MCDN via the reference point B1. After receiving the ingestion message instruction from the reference point B1, the centre node of MCDN is able to obtain the content and keep it locally through the reference point B2.
B2	Reference point between CPF and CD & DF (mostly implemented by centre node).	HTTP, FTP	When the content requested from the end-user is not cached in any MCDN node, the MCDN centre node will obtain the requested content from the external content source through the reference point B2.
C	Reference point between EUF and CDF (edge node).	RTSP, HTTP	This reference point C is used for the MCDN edge node to deliver the content service information and media stream to the end-user. This referent point is also used for redirecting the content request while the content is not cached in the edge node. RTSP protocol is used for RTSP content transmission; HTTP protocol is used for HTTP live streaming (HLS), picture and download content transmission.

8.2 Internal reference points

According to the system and network architecture, MCDN internal reference points are defined as indicated in Table 8-2.

Table 8-2 – Internal reference points

Reference point	Definition	Protocol	Notes
a	Reference point between content management functional block in MF and CL&DF	HTTP	The reference point is responsible for the management of content transcoding, slicing, storage injection and deletion.
b	Reference point between CL&DF and CDF/AF (if AF is deployed)	SOAP+XML	The upstream MCDN node informs the downstream MCDN node(s) to obtain the content distribution/ ingest information through the reference point b. After receiving the

Table 8-2 – Internal reference points

Reference point	Definition	Protocol	Notes
			distribution/ingest message instruction, the centre node(s) of MCDN is able to obtain the content and keep it locally through the reference point f.
c	Reference point between CD&DF and node management functional block in MF	HTTP	The reference point includes functions for managing all the MCDN nodes by performing adding, deleting, upgrading operations.
d	Reference point between CRF and CD&DF	HTTP	The reference point is for MCDN routing/redirecting functions to select the most appropriate MCDN node for the end-user, based on the user's content request.
f	Reference point between CL&DF and CDF/AF (if AF is deployed)	HTTP, RTSP, FTP	The reference point is used for the downstream node to locate and retrieve content from the upstream node. It may have two content retrieving modes: Passively: The downstream node only retrieves the content from the upstream node when the content requested from the end-user is not cached in any the downstream node. Actively: When the upstream node count of the requests of downstream node(s) exceeds a certain statistic threshold, it actively sends the content distribution request to the downstream node through the reference point b and the downstream node retrieves the content from the upstream node through the reference point f.
e (optional)	Reference point between CRF and MF	HTTP	The reference point e is an optional interface which is used for content routing/redirecting functions to obtain management information from MCDN management function, e.g., the routing/redirecting policy, network management information, etc.

Appendix I

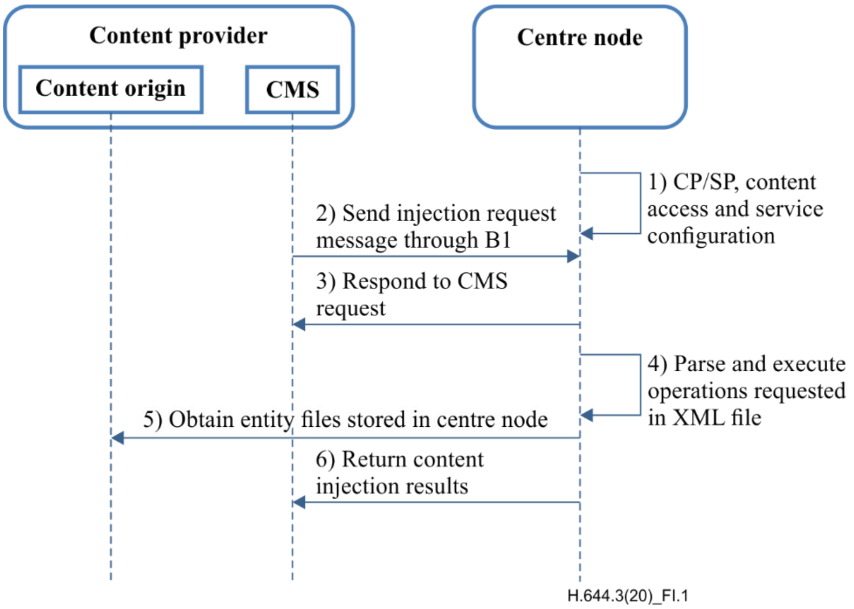
Examples of media transmission and service procedures

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

I.1 Content access

I.1.1 Content ingestion

The process of content access by content ingestion is as indicated in Figure I.1.



Content provider
Content origin
CMS
Centre node
1) CP/SP, content access and service configuration
2) Send injection request message through B1
3) Respond to CMS request
4) Parse and execute operations requested in XML file
5) Obtain entity files stored in centre node
6) Return content injection results
H.644.3(20)_FI.1

Figure I.1 – The service procedure of content ingestion

In the content ingestion method, the CMS will actively send ingestion request messages to the centre node of MCDN. Then the centre node parses and executes the XML file sent by CMS. Finally, the centre node obtains and stores contents from the content origin. Therefore, MCDN can directly serve contents to end-users upon requests, elevating the end-user experience of the service. Content injected by content ingestion method will be stored in MCDN permanently until being removed by instruction.

I.1.2 Content pre-ingestion

The process of content access by content pre-ingestion is as indicated in Figure I.2.

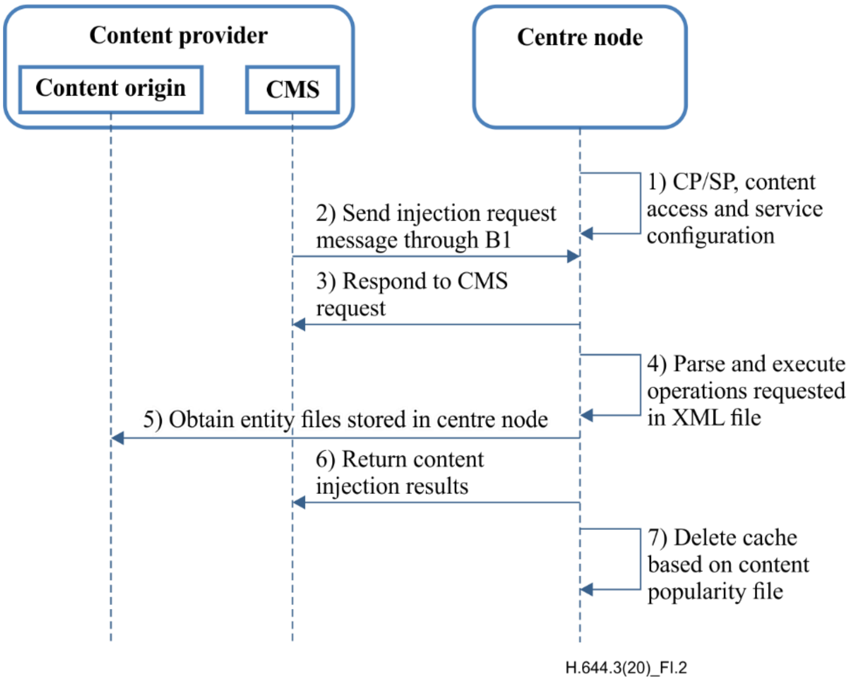
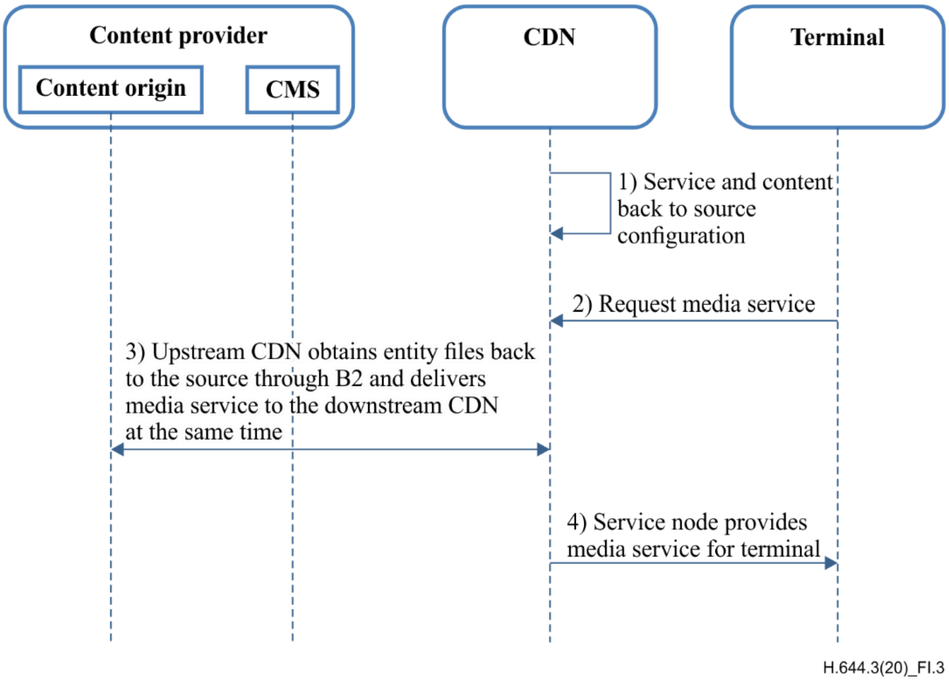

Content provider
Content origin
CMS
Centre node
1) CP/SP, content access and service configuration
2) Send injection request message through B1
3) Respond to CMS request
4) Parse and execute operations requested in XML file
5) Obtain entity files stored in centre node
6) Return content injection results
7) Delete cache based on content popularity file
H.644.3(20)_FI.2

Figure I.2 – The service procedure of content pre-ingestion

In the content pre-ingestion method, the CMS will actively send ingestion request messages to the centre node of MCDN which parses and executes the XML files sent by CMS to obtain and store contents from the content origin as in the content ingestion method. However, content obtained through pre-ingestion will be deleted based on popularity instead of being permanently stored in MCDN. Pre-ingestion content can have a protection duration to prevent it from being deleted.

I.1.3 Back-to-source

The process of back to source is as indicated in Figure I.3.



Content provider
Content origin
CMS
CDN
Terminal
1) Service and content back to source configuration
2) Request media service
3) Upstream CDN obtains entity files back to the source through B2 and delivers media service to the downstream CDN at the same time
4) Service node provides media service for terminal
H.644.3(20)_FI.3

Figure I.3 – The service procedure of back-to-source

The back-to-source method does not require injecting content into MCDN in advance. Instead, it needs to be configured to access the configuration tables of content providers. Upon receiving a request from an end-user, the centre node of MCDN obtains content from the content origin immediately and distributes media files to the downstream node at the same time to provide media service for end-users.

I.2 Content distribution

The process of content distribution is as indicated in Figure I.4.

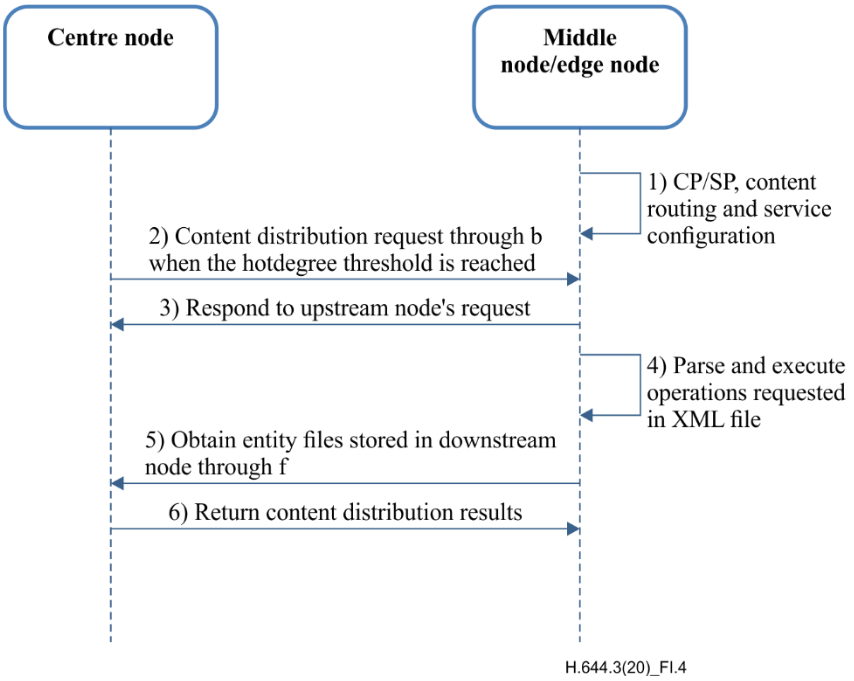

Centre node
Middle node/edge node
1) CP/SP, content routing and service configuration
2) Content distribution request through b when the hotdegree threshold is reached
3) Respond to upstream node's request
4) Parse and execute operations requested in XML file
5) Obtain entity files stored in downstream node through f
6) Return content distribution results
H.644.3(20)_FI.4

Figure I.4 – The service procedure of content distribution

When the hot degree threshold is reached, the centre node will actively send a distribution request message to the downstream node of MCDN. Then the downstream node parses and executes the XML file sent by the centre node. Finally, the downstream node obtains and stores contents from the centre node.

I.3 Content delivery

The process of content delivery is illustrated in Figure I.5.

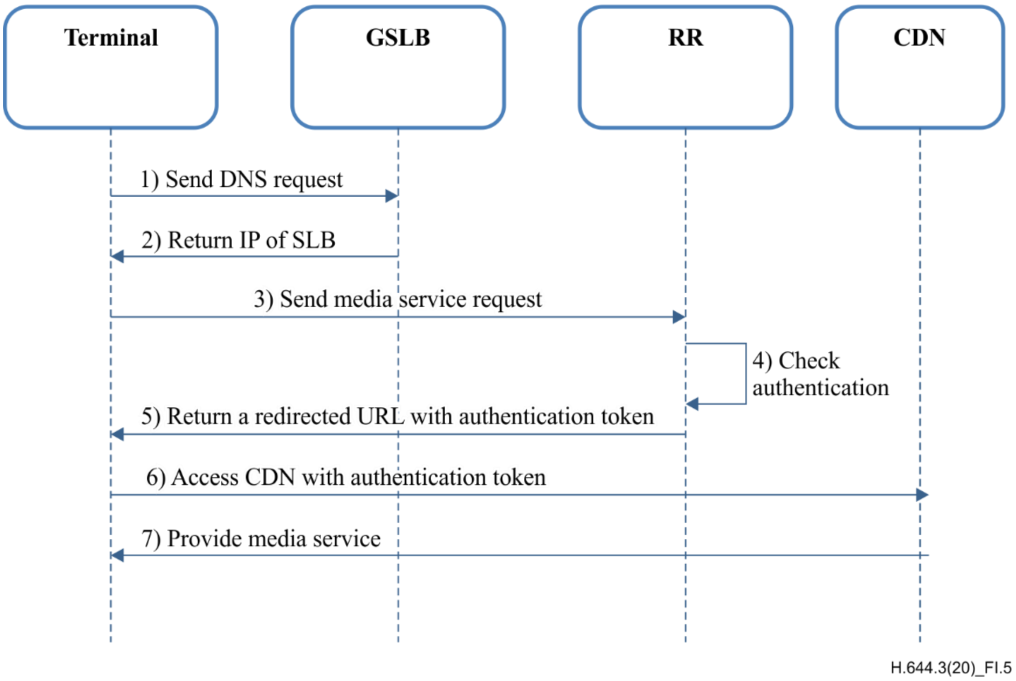

Terminal
GSLB
RR
CDN
1) Send DNS request
2) Return IP of SLB
3) Send media service request
4) Check authentication
5) Return a redirected URL with authentication token
6) Access CDN with authentication token
7) Provide media service
H.644.3(20)_FI.5

Figure I.5 – The service procedure of content delivery

When the terminal requests media service, it requests a domain name resolution from GSLB, and GSLB returns the IP address of RR to the terminal. Then, the terminal sends the media service request to RR, and RR returns to the terminal to select the optimal node to serve the terminal. Finally, the terminal establishes a connection with the streaming service node and starts the media service process.

Appendix II

Implementation mechanisms related to the functions

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

This appendix describes possible implementation guidelines for realizing the MCDN functions. It gives the essential procedurals in order to understand how the MCDN works. The detailed solutions and the relationship with the reference points are for future study and are to be specified in the future ITU-T Recommendations.

Content access is the first step for MCDN to provide services for users. It is the process of content injection from the source server into MCDN, so that the content of the source server can be obtained by the MCDN system. When the user requests the content, the MCDN content routing system optimises the content selection process to the MCDN node closest to the user with the best performance, and finally the node provides services to the user. The following clauses describe the implementation mechanisms of content access, content distribution, content routing and content service.

II.1 Content access mechanism

Content access means the process of ingesting content into MCDN. This clause will introduce three methods for MCDN to access contents, which are content ingestion, content pre-ingestion, and back-to-source method to access content of arbitrary content formats. When MCDN receives a content ingestion request from CMS, or a service request from an end-user while MCDN does not have the required content, it will access referred content from a content and metadata source and store it in MCDN.

II.1.1 Content access methods

II.1.1.1 Content ingestion

In the content ingestion method, the application/service management system will actively send instructions to centre nodes of MCDN which will acquire and store contents according to the instruction. Therefore, MCDN can directly serve contents to end-users upon requests, elevating the end-user experience of the service. Content ingested using the content ingestion method will be stored in MCDN permanently until removed by instruction.

MCDN supports different content ingestion methods and strategies for different content providers. It also supports ingested content management, including content addition, deletion, and update.

II.1.1.2 Content pre-ingestion

The application/service management system can send instructions to MCDN, directing it to acquire content from the content and metadata source, so that MCDN can later directly offer services to end-users nearby for content acquired through pre-ingestion, which will be deleted based on popularity instead of being permanently stored in MCDN. Pre-ingestion content can have a protection duration to prevent it from being deleted. After a content is deleted, MCDN can still serve that content through the back-to-source method.

II.1.1.3 Back-to-source

The back-to-source method does not require ingesting content into MCDN in advance. Instead, upon receiving a request from an end-user, MCDN acquires content from the content and metadata source in real time, and serves it to the end-user through nearby nodes. To use the back-to-source method, MCDN needs to be configured to access a configuration table of content providers.

MCDN should support different back-to-source methods and strategies for different content providers. It should support back-to-source requests aggregation inside a node, which means that MCDN will deliver content to all requesting users after retrieving it. MCDN should support a back-to-source method using a service URL or specific back-to-source URL, as well as supporting back-to-source methods for both static and dynamic content.

II.1.1.4 Unique identification method

Considering that MCDN should support multiple content ingestion methods, content ingestion for different application/service management systems, and multiple content ingestion requests in one application/service, it is required to introduce the UniContentID to identify different contents from different content providers.

II.2 Content distribution mechanism

II.2.1 Content distribution methods

Content distribution refers to the process of content distribution in MCDN network based on a user request or active content management strategy. MCDN content distribution is mainly based on active distribution (PUSH) mode, while passive distribution (PULL) mode is optional.

II.2.1.1 Active distribution (Push mode)

Smart PUSH distribution is necessary for the MCDN. The MCDN can actively adjust the distribution of hot content in the content distribution system and push hot content to the edge nodes according to the current status of content services in the MCDN.

For PUSH distribution mode, it is necessary to support single or batch manual distribution and automatic distribution. At least, it should support the immediate and regular distribution strategy of new content; support content distribution according to the attribute policy of the content domain of the node; expand support for distribution strategies such as setting distribution threshold according to the amount of visits; support classified and hierarchical content distribution strategy; expand support for distribution priority, and update the frequency and distribution threshold of content.

II.2.1.2 Passive distribution (Pull mode)

For the smart PULL distribution mode, when the content is not hit locally by the request, it is necessary to support real-time access to the upstream MCDN to download content while providing services for users, and the service delay must be bound by service requirements. The edge node should support updating its own storage based on the hotspot to improve the hit rate.

II.3 Content routing mechanism

MCDN content routing chooses the appropriate MCDN according to the user content routing strategy to schedule end user's requests, and dispatches the end user's requests to the appropriate MCDN nodes.

MCDN content routing mainly includes DNS and IP application layer scheduling, which can be deployed separately or in combination.

II.3.1 DNS routing (GSLB)

The MCDN routing server (GSLB) needs to register the domain name and assign a secondary domain name to each business platform that uses a canonical name (CNAME) record to invoke GSLB capabilities. MCDN GSLB can be interpreted by DNS for selecting MCDN edge nodes or MCDN RR for users. GSLB should support the following routing strategies:

The user content routing strategy based on proximity should be supported, and the user requests should be scheduled to the MCDN near the user's physical location according to IP or IP segment.

The content routing strategy based on weight should be supported, and user requests should be scheduled to the MCDN with low weight according to node weight strategy.

IP blacklisting strategy should be supported, which means that a request from any specific IP in the list will be scheduled to a designated MCDN or will be denied of service.

Partition routing strategy should be supported, which can be scheduled to a designated MCDN node or node groups based on a specific city code.

Special routing strategy should be supported, meaning applying a specific scheduling strategy request or characteristics of user's request.

Any combination of the above content routing strategies should be supported. Their priorities in descending order are: IP blacklisting – > content type – > special strategy – > proximity – > partition scheduling – > weight – > load.

Default strategy should be supported, which means that if a request comes from a terminal IP or LDNS IP outside of any service IP segment, by default it will be scheduled to a designated service node to provide services.

In order to improve the reliability of the system, the dispatching control subsystem supports the deployment mode of dual-plane network. The two nodes can work based on the main standby mode or load sharing mode.

1) Resolving the whole network request to the main dispatching centre, and the terminal actively switching to the standby dispatching centre in abnormal circumstances.

2) Based on the IP address segment, area or service, the terminal uses different dispatching centres according to the URL.

II.3.2 IP application layer routing (RR)

The main function of MCDN routing server (RR) is to schedule service requests from terminals to appropriate MCDN nodes. After receiving the user's terminal service request, RR chooses the appropriate MCDN node (RR node or media service node) for the user according to the user's content routing strategy. RR should support the following routing strategies:

The user content routing strategy based on proximity should be supported, and the user requests should be scheduled to the node near the user's physical location according to IP or IP segment.

User content routing strategy based on node load should be supported. User requests should be scheduled to MCDN nodes with good network conditions and light loads (configurable threshold) according to node load (such as node traffic, number of connections, health status, etc.).

The content routing strategy based on node weight should be supported, and user requests should be scheduled to the node with low weight according to node weight strategy.

Scheduling based on content domain should be supported. RR supports querying the MCDN service configuration table to obtain the protocol type attribute of the content domain based on the URL from the user's request, and the MCDN node whose content domain attribute is a subset of the protocol type is selected for scheduling.

IP blacklisting strategy should be supported, which means that requests from any specific IP in the list will be scheduled to a designated MCDN or will be denied of service.

Partition routing strategy should be supported, which can be scheduled to a designated node or node groups based on a specific city code.

Special routing strategy should be supported, meaning applying specific scheduling strategy according to URL or characteristics of user's request.

Any combination of the above content routing strategies should be supported. Their priorities in descending order are: IP blacklisting – > content type – > special strategy – > proximity – > partition scheduling – > weight – > load.

Default strategy should be supported, which means that if a request comes from a terminal IP or LDNS IP outside of any service IP segment, by default it will be scheduled to a designated service node to provide services.

Optionally, content-based scheduling can be supported to schedule user service requests to the node with requested content.

In order to improve the reliability of the system, the dispatching control subsystem supports the deployment mode of dual-plane network. The two nodes can work based on the main standby or load sharing mode.

1) Resolving the whole network request to the main dispatching centre, and terminal actively switching to the standby dispatching centre in abnormal circumstances.

2) Based on IP address segment, area or service, the terminal uses different dispatching centres according to the URL.

In order to improve system security, it is necessary to protect the system from DoS attack by limiting the number of connections from the same IP and some other methods, and to support the configuration of turning on anti-DoS characteristics.

II.4 Multimedia content location and streaming service mechanism

Multimedia service refers to the process in which MCDN provides high quality content service to the end user after the end user's request is authenticated according to the reference points protocol, request command and service strategy of the user's requests. If the MCDN does not find the content, it can obtain the content through the content distribution mechanism and provide media services to the user.

Multimedia services in MCDN must support audio and video streaming services for PC, PAD, mobile devices and other terminals; support video on demand (VOD) and live broadcasting services based on HLS, HTTP progress download (HPD) and other protocols; support virtual reality (VR), 8K, 4K, Blu-ray, HD, SD and other streams; support H.264, H.265, AVS2, CBR, VBR and other coding methods to provide services; and support different media service strategies for different domain content providers.

Appendix III

Authentication mechanisms

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

III.1 Authentication mechanism in the edge node

In the edge node, authentication adopts an open-loop encryption and decryption mechanism, which supports authentication based on service authentication digest with algorithm and key, and is verified by the MCDN edge service node. It supports a variety of encryption and decryption algorithms and verification strategies, and can flexibly configure and expand new encryption and decryption algorithms and verification strategies.

A typical authentication mechanism in edge nodes allows a portal (EPG, PC Portal, etc.) and MCDN to share a key, and uses a symmetric algorithm such as advanced encryption standard (AES) to encrypt and decrypt. The portal adds the encrypted service authentication digest (such as authentication key "authInfo" to prevent third-party redirection) to the URL which is then returned to the user. The user uses the URL containing the service authentication information to request content playback from the MCDN. The MCDN decrypts and checks the URL to ensure the legitimacy of the user's service. The key used for the open-loop encryption and decryption mechanism needs to be updated regularly and be synchronized when updating. The specific process is as indicated in Figure III.1.

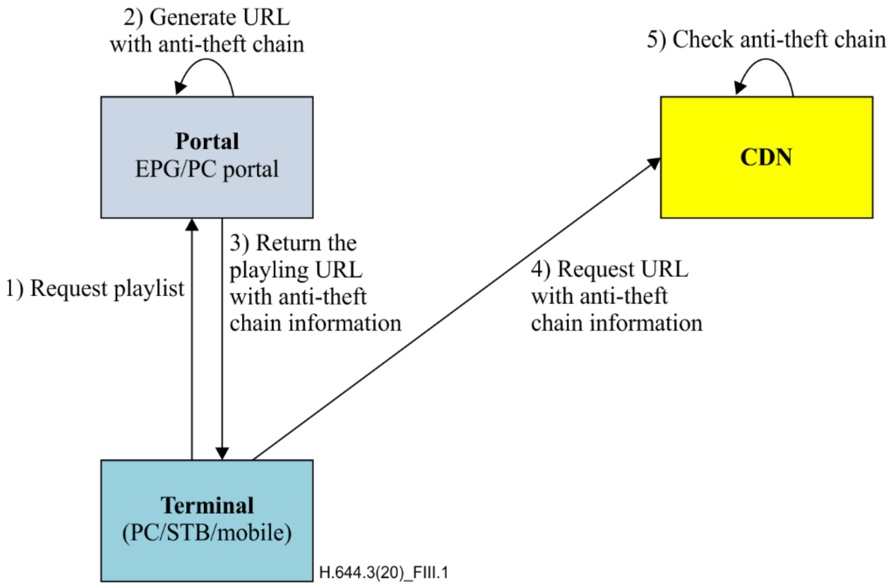

2) Generate URL with anti-theft chain
5) Check anti-theft chain
Portal
EPG/PC portal
CDN
1) Request playlist
3) Return the playing URL with anti-theft chain information
4) Request URL with anti-theft chain information
Terminal
(PC/STB/mobile)
H.644.3(20)_FIII.1

Figure III.1 – Authentication mechanism

III.2 Double authentication mechanism in centre and edge node

In order to further reduce the complexity of the edge node and the difficulty of configuration and maintenance, MCDN can adopt a double authentication mechanism in the centre and edge nodes.

This authentication is checked twice by the MCDN centre node (such as RR) to verify the authentication information brought by the portal. After checking, the centre node replaces the authentication information with a token, and the terminal carries the token information shared by the centre and edge nodes to the edge node for service. See Figure III.2.

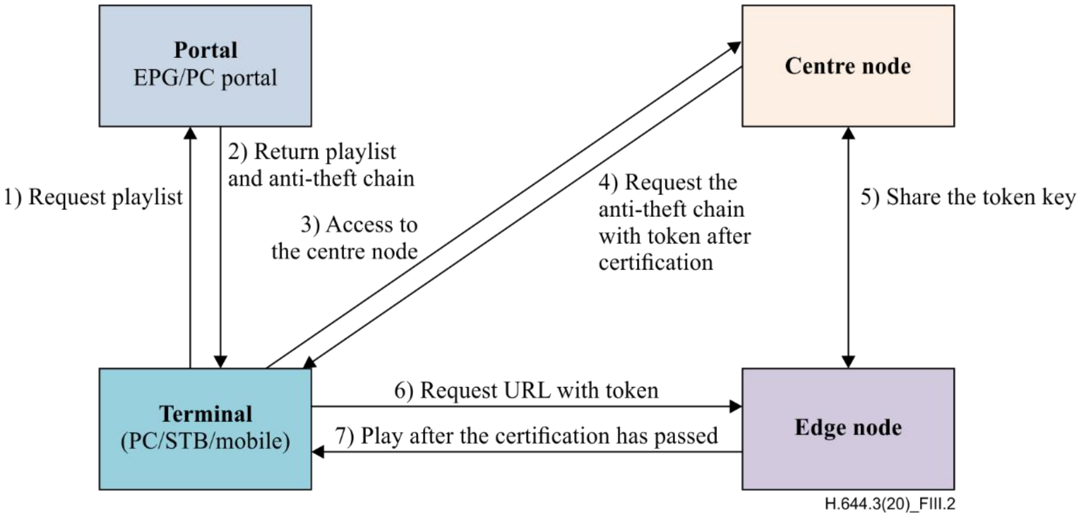

Portal
EPG/PC portal
Centre node
1) Request playlist
2) Return playlist and anti-theft chain
3) Access to the centre node
4) Request the anti-theft chain with token after certification
5) Share the token key
Terminal
(PC/STB/mobile)
6) Request URL with token
7) Play after the certification has passed
Edge node
H.644.3(20)_FIII.2

Figure III.2 – Double authentication mechanism

Bibliography

[b-ITU-T H.780] Recommendation ITU-T H.780 (2012), *Digital signage: Service requirements and IPTV-based architecture*.

[b-ITU-T J.191] Recommendation ITU-T J.191 (2004), *IP feature package to enhance cable modems.*

[b-ITU-T X.609] Recommendation ITU-T X.609 (2015), *Managed peer-to-peer (P2P) communications: Functional architecture*.

[b-ITU-T X.1255] Recommendation ITU-T X.1255 (2013), *Framework for discovery of identity management information.*

[b-ITU-T Y.2080] Recommendation ITU-T Y.2080 (2012), *Functional architecture for distributed service networking.*

[b-ITU-T Y.2084] Recommendation ITU-T Y.2084 (2015), *Distributed service networking content distribution functions.*

[b-ITU-T Y.2206] Recommendation ITU-T X.2206 (2010), *Requirements for distributed service networking capabilities.*

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, 2020