ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Recommendation

ITU-T H.644.5 (12/2022)

SERIES H: Audiovisual and multimedia systems

Broadband, triple-play and advanced multimedia services – Content delivery and ubiquitous sensor network applications

Functional architecture of content request routing service in multimedia content delivery networks

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
Content delivery and ubiquitous sensor network applications	**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.644.5

Functional architecture of content request routing service in multimedia content delivery networks

Summary

Recommendation ITU-T H.644.5 specifies the functional architecture and related functional components of content request routing/redirecting service (CRRS), and the reference points of a CRRS within a multimedia content delivery network (MCDN). With consideration for different network environments, content/service types and user/terminal device profiles, this Recommendation also presents potential solutions with the procedures for CRRS to complete the end-user-to-MCDN node attachment in the case of Internet protocol television (IPTV) service (dedicated network), over the top (OTT) media service (public/open Internet) and mobile media streaming service such as 5G network with mobile/multi-access edge computing (MEC) enabled service.

Using Recommendation ITU-T H.644.5, a MCDN service provider and manufacturer can deploy their MCDN node, especially the edge node, deeper into a network edge. The CRRS provides a comprehensive solution to guide users to find the nearest MCDN node for accessing the request content by ignoring the differentiation of network, service type and terminal device and user's location.

History

Edition	Recommendation	Approval	Study Group	Unique ID[*]
1.0	ITU-T H.644.5	2022-12-14	16	11.1002/1000/15205

Keywords

5G, architecture, CDN, content/user request, MEC, MEC enabled CDN reference point, routing/redirection.

[*] 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.

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 H.644.5

Functional architecture of content request routing service in multimedia content delivery networks

1 Scope

This Recommendation specifies the functional architecture with related functional components, reference points and comprehensive solutions for the multimedia content delivery network (MCDN) content/user request routing/redirecting service, with consideration of the variety of service/content types, networking environments, terminal devices and so on.

The scope of this Recommendation comprises:

1) The functional architecture and the related components of content request routing/redirecting service (CRRS) and the related networking architecture.

2) The potential reference points and the protocols between CRRS and other function entities, e.g., content distribution and delivery system, service platform including mobile/multi-access edge computing (MEC) enabled platform, Local DNS terminal device, etc.

3) The candidate content request routing/redirecting mechanism by considering the location of user and MCDN node (including virtualized CDN node and MEC-CDN node), e.g., in the dedicated network & internet, fixed & mobile (IMT-2020) network environment or other possible networking conditions.

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 H.644.3] Recommendation ITU-T H.644.3 (2020), *Functional architecture of multimedia content delivery networks*.

[ITU-T H.644.4] Recommendation ITU-T H.644.4 (2021), *Architecture for mobile/multi-access edge computing enabled content delivery networks*.

[IETF RFC 6891] IETF RFC 6891 (2013), *Extension Mechanisms for DNS (EDNS(0))*.

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

3.1.6 Internet Protocol Television (IPTV) [b-ITU-T Y.1901]: Multimedia services such as television/video/audio/text/graphics/data delivered over IP-based networks managed to support the required level of QoS/QoE, security, interactivity and reliability.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 back-to-source service: A service that is used for relocating the original content request to a content source where the actual media file is hosted.

3.2.2 sourcing multimedia content delivery network (MCDN) node: A multimedia content delivery network (MCDN) node that can provide back-to-source service for the original content requestor.

3.2.3 sourcing domain name system (DNS) resolver: A particular domain name system (DNS) server that provides back-to-source service for the sourcing multimedia content delivery network (MCDN) node.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

5GC	5G Core
APP	Application
CDF	Content Delivery Function
CDN	Content Delivery Network
CNAME	Canonical NAME
CP	Content Provider
CRRF	Content Request Routing/redirecting Functions
CRRS	Content Request Routing/redirecting Service
DNS	Domain Name System
ECS	EDNS-Client-Subnet
EDNS	Extension Mechanisms for DNS
FQDN	Fully Qualified Domain Name
GSLB	Global Service Load Balance
HLS	HTTP Live Streaming

HTTP	Hypertext Transfer Protocol
IPTV	Internet Protocol Television
LAN	Local Area Network
LDNS	Local Domain Name System
MAN	Metropolitan Area Network
MCDN	Multimedia Content Delivery Network
MEC	Mobile/Multi-access Edge Computing
MEP	Mobile/Multi-access Edge Platform
NAT	Network Address Translation
OTT	Over The Top
RR	Request Routing
RTSP	Real-Time Streaming Protocol
RTT	Round-Trip Time
SLB	Service Load Balance
SOAP	Simple Object Access Protocol
SP	Service Provider
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TTL	Time To Live
UPF	User Plane Function
URI	Uniform Resource Identifier

5 Conventions

The following conventions are used 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 Recommendation is to be claimed.

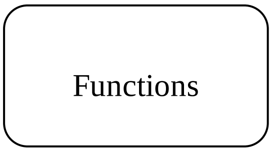
– The keywords "is prohibited from" indicate a requirement which must be strictly followed and from which no deviation is permitted, if conformance to this Recommendation is to be claimed.

– 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.

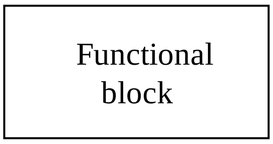
– The keywords "is not recommended" indicate a requirement which is not recommended but which is not specifically prohibited. Thus, conformance with this Recommendation can still be claimed even if this requirement is present.

– 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 this Recommendation.

– The keyword "functions" is defined as a collection of functionalities. It is represented by the following symbol in the context of MCDN/CRRS architecture:



– The keyword "functional block" is defined as a group of functionalities that have not been further subdivided at the level of detail described in this Recommendation. It is represented by the following symbol in the context of MCDN/CRRS architecture:



6 Introduction

6.1 Overview of content request routing service within MCDN architecture

Content request routing/redirecting service (CRRS), sometimes also called user request routing/redirecting service, is one of the essential services provided by MCDN, which is based on the implementation of the content routing/redirecting functions (CRFs) defined in clause 7.3 of [ITU-T H.644.3]. It provides the service entrance for accessing multimedia content for end-users. It guides users to find the desired content and attaches to the nearest MCDN server node according to the user profile of or the service load status. However, the profiles will be very different depending on the content type, network environment, user terminal device type, media service platform, MCDN node deployment and loading status. Therefore, a CRRS should provide a unified functionality to address these issues.

Figure 6-1 shows the CRRS related functions defined in the MCDN functional architecture, which can be found in [ITU-T H.644.3].

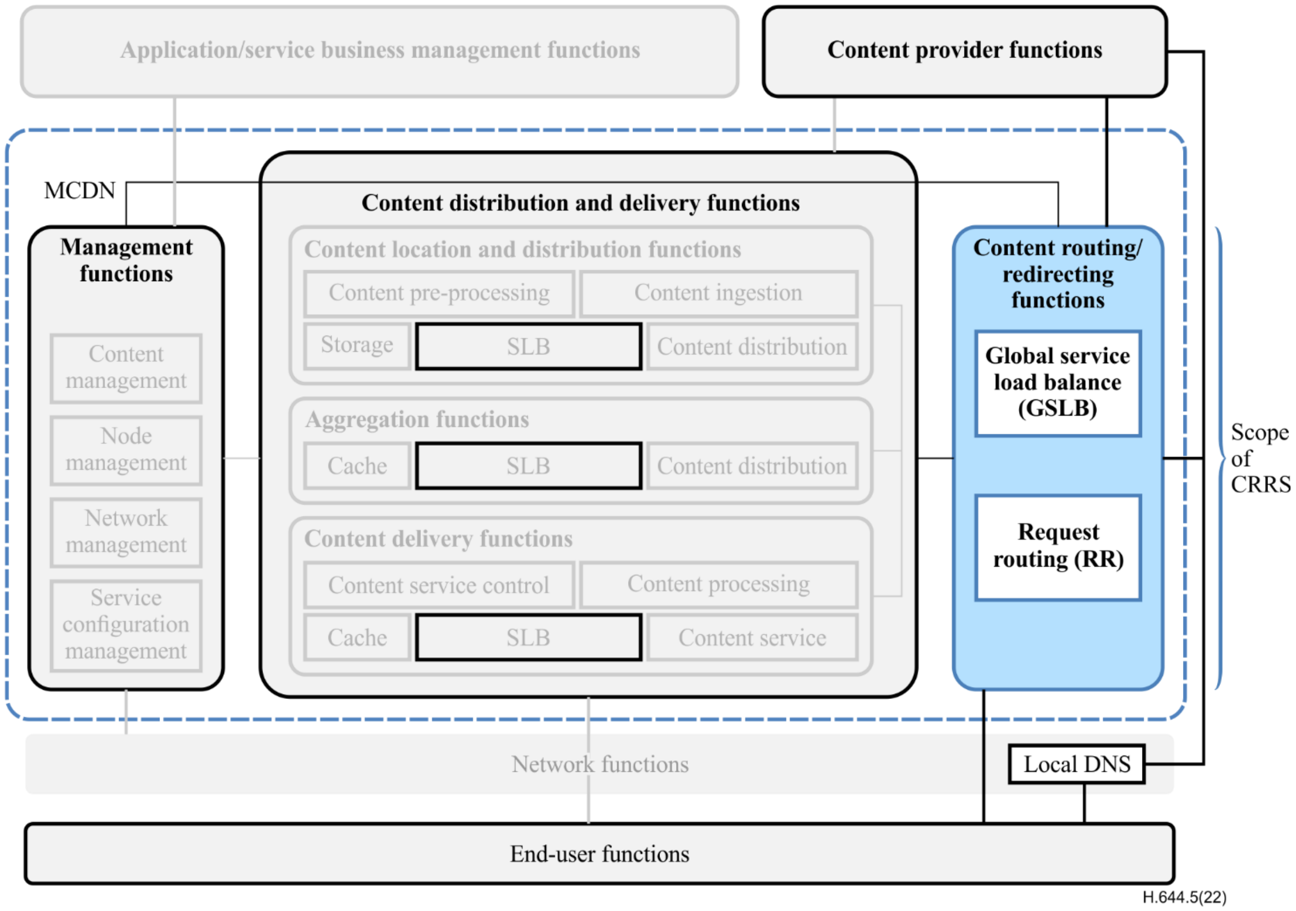


Figure 6-1 – CRS functional components within MCDN functional architecture (based on Figure 7-1 of [ITU-T H.644.3])

NOTE – The detailed definition of functions and reference points in grey can be found in [ITU-T H.644.3]. This Recommendation only addresses the part with a coloured background.

The CRRS is composed of two essential functional entities: a unified content delivery network (CDN) service entrance called global service load balance (GSLB) functions, and the (user/content) request routing (redirecting) functions (RR).

The definition of GSLB and RR can be found in [ITU-T H.644.3]. The functions or functional blocks resident in the GSLB and RR are described in detail in clause 7.

6.2 The relationship of content request routing functions with other MCDN functions

The major design goal of CRRS is to assist an end-user to connect to an appropriate media content server node within MCDN by providing the corresponding node IP address, which is recursively queried by DNS request based on the end-user location and the uniform resource identifier (URI) of content. This can be achieved by the collaboration of the global server load balancing (GLB) and the requesting routing (RR) functional entities. It is noted that RR may not be deployed if there are only a few MCDN server nodes in a small area.

The CRRS entry point information, usually the GSLB server domain name, will be pre-configured in the content provider's/service provider's (CP/SP)'s AUTHORITY DNS by adding a canonical name (*CNAME*) record. By using the common DNS querying, the end-user (local domain name system (LDNS)) is able to obtain the real IP address of RR or MCDN server node (SLB) from GSLB. Then the end-user can request the media streaming from the dispatched MCDN server node.

Figure 6-2 shows the relationship between CRRS and other functional components:

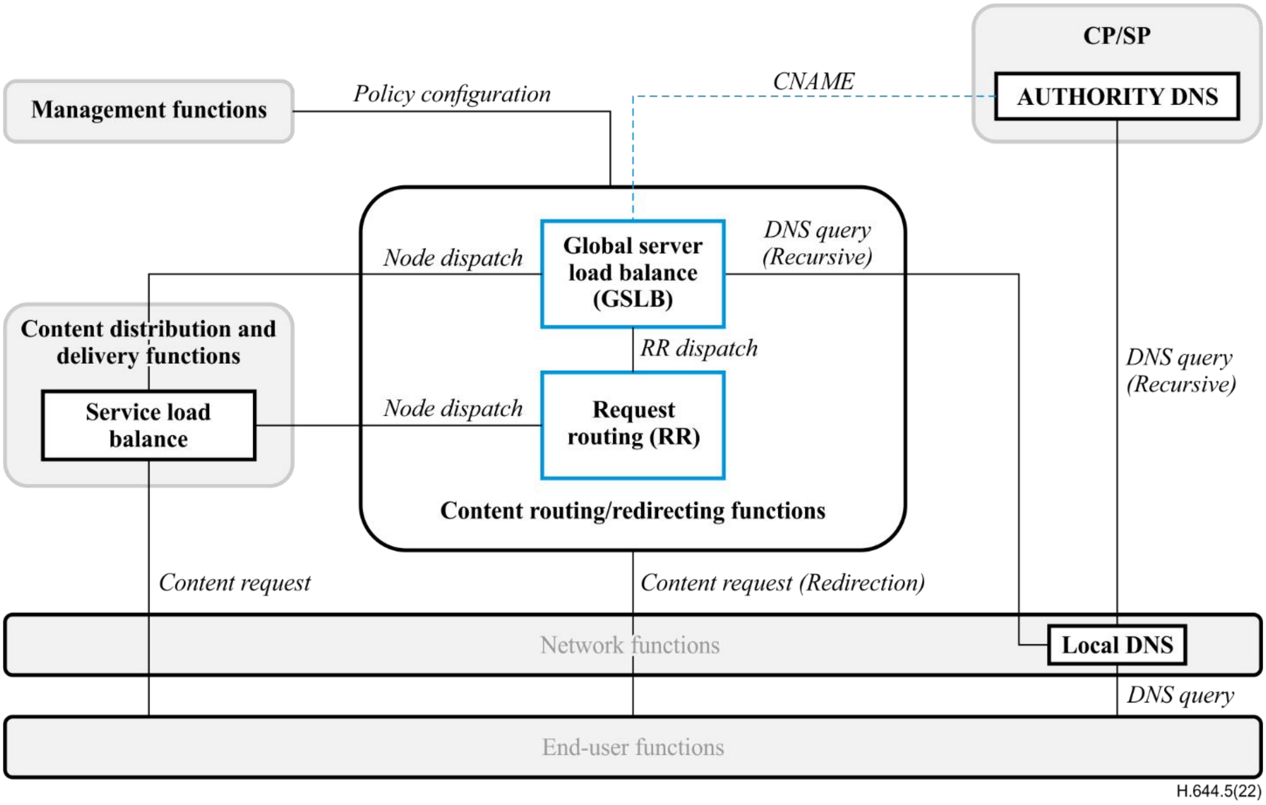


Figure 6-2 – Relationship between CRRS and other functional components

In this figure, GLSB returns an appropriate RR IP address to the LDNS according to the DNS query. RR selects an MCDN node nearest to the end-user terminal and redirects its content request to that MCDN node. When the MCDN node receives the content request, the service load balance (SLB) functions selects an available media server from a media server cluster to answer the content request.

6.3 The challenge of CRRS implementation with MEC-enabled CDN user case

The conventional CDN service is usually deployed on the physical facilities. Typically, once deployed, the CDN node will have a stable location and unique IP address. Usually, network operators are responsible for managing the relationship between IP address and location. With DNS query, the traditional CDN CRRS can return an IP address of the CDN node that is closest to the end-user.

However, this mechanism may not be suitable for the MEC-enabled CDN use cases. While the MEC-CDN is built on the virtualized infrastructure, the MEC-CDN edge node may not have a unique IP address. For example, several MEC-CDN edge nodes (containers) may share one private IP address, or multiple public IP addresses that will be mapped to many MEC-CDN instances. Therefore, the conventional CDN scheduling mechanism cannot be simply reused.

The CRRS issues related to the MEC-enabled CDN scenarios are described in clause 7.3.

7 Functional architecture of the content request routing service

7.1 Functions and functional blocks within the content request routing service

As for the content routing/redirecting functions (CRFs) defined in [ITU-T H.644.3], the main functional components of CRRS are composed of two main functions: GSLB and RR. Those two functions can be further decomposed into several functional blocks, as shown in Figure 7-1.

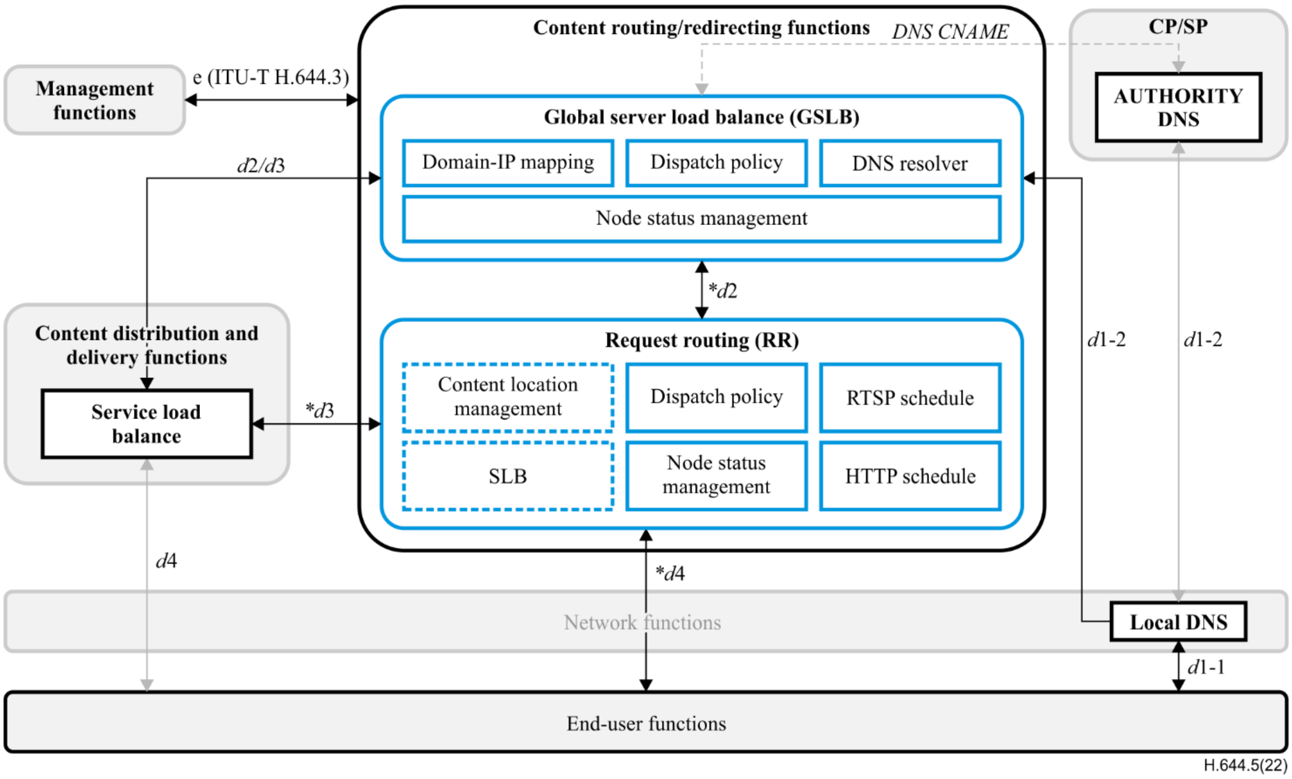


Figure 7-1 – Functional architecture of CRRS

NOTE 1 –Reference Point "d4" may be implemented with different application-level protocols. It depends on the protocol that the end-user used to request the content.

NOTE 2 –Reference points "*d2" and "*d3" might not be used if the RR is not actually used.

NOTE 3 – the functional block with a dash-line boundary refers to the optional functions that might not be implemented in some cases.

CRRF will interact with other functions such as content delivery function (CDF), CP and local DNS. In this Recommendation, only the functionalities in CRRF and the reference points between CRRF and other functions are specified.

The general definition of content request routing/redirection functions can be found in clause 7.3 of [ITU-T H.644.3]. Clauses 7.1.1 and 7.2.2 specify the recommended functional blocks that support the functionalities of GSLB and RR.

7.1.1 Global service load balance

The general definition of GSLB can be found in clause 7.3.1 of [ITU-T H.644.3].

The function of GSLB is to realize the global traffic control and dispatch over all the MCDN service nodes. Usually, GSLB adopts a group of methods such as DNS CNAME, domain-IP mapping and dispatch policy to find the most appropriate server node for the end-users based on their profiles, e.g., user's IP address in most cases. The server node could be an RR or an MCDN edge server node, it depends on the actual implementation.

The functions of GSLB are composed of the following functional blocks:

- DNS resolver: it receives the DNS query from local DNS and returns the selected node IP address back to the local DNS.
- Domain-IP mapping: it maintains the relationship between the domain and its related IP address or IP address list.
- Dispatch policy: it manages the dispatch policy, which may include RR/MCDN load status, distance, round-trip time (RTT), etc.
- Node status management: it monitors the RR or MCDN node running status. It is the basic input information for the dispatch policy.

7.1.2 Request routing

The general definition of RR can be found in clause 7.3.2 of [ITU-T H.644.3].

RR is responsible for the selection of a suitable MCDN node and redirecting the user content request to that node, according to the user's content request. The result of the selection depends on many factors such as MCDN topology, network traffic loading status, the distribution of MCDN nodes, etc.

The functions of RR are composed of the following functional blocks:

- Dispatch policy: it manages the dispatch policy, similar to GSLB, which may include content location, MCDN node load status, distance, RTT, etc.
- Node status management: it monitors the downstream RR or MCDN node running status as the basic dispatch policy.
- HTTP/RTSP schedule: it replies to the HTTP/RTSP based content request and redirects the request to the downstream RR node or MCDN node (SLB).
- SLB: it is an optional function. When it exists, it is responsible for the inner load balance if RR is cascaded or acted as the MCDN node SLB.
- Content location management: it is an optional function when the SLB function is merged into RR. It manages the content distribution status over all the MCDN nodes in a certain region.

7.2 Functional entities deployment of content request routing service

7.2.1 The networking of functional entities in CRRS

Generally, GSLB and RR will be hierarchically deployed in a wide geographical range. GSLB manages all RR status and scheduling methods in a national or state area. RR manages all MCDN nodes in an urban area or among the different types of networks. If there are multiple RR entities, these can be cascaded, as shown in Figure 7-2.

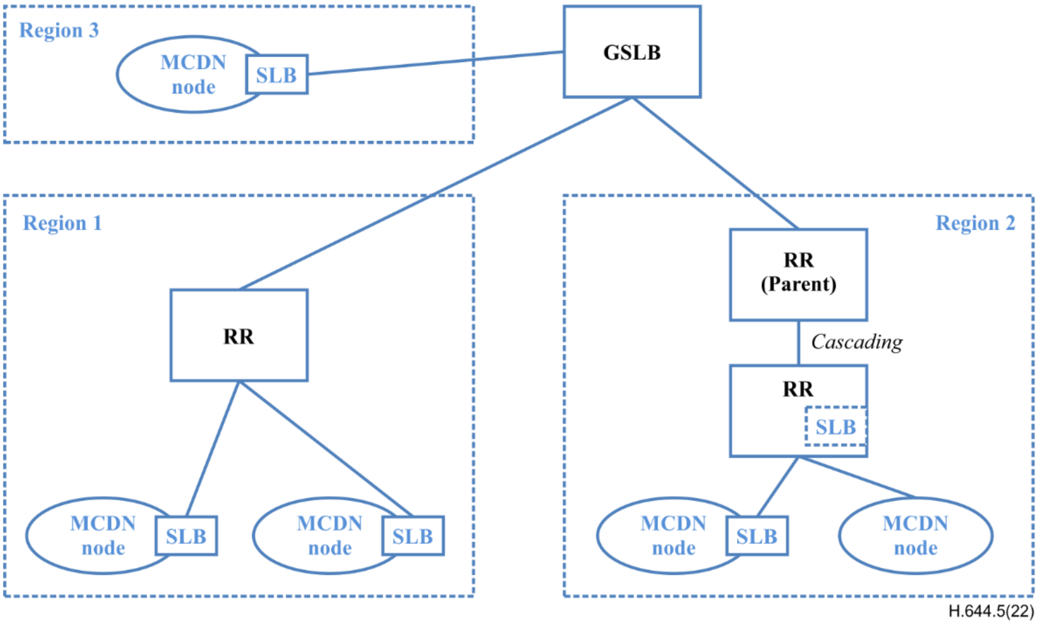


Figure 7-2 – GSLB and RR hierarchically deployment scenario

NOTE – For some special cases, RR may act as the SLB if there is no SLB implemented in the MCDN node.

Actually, GSLB can locate the target MCDN node directly. It depends on where the GSLB is deployed. If there are only a few MCDN nodes in a limited region, the GSLB dedicated to this region will return the MCDN node IP address directly from the DNS resolution, without an intermediate RR.

7.2.2 Basic content request routing procedure for the common scenario

Generally, in content delivery service the content request procedure for an end-user can be divided into two phases:

- Phase 1: DNS query – to obtain an appropriate MCDN edge node IP address. More precisely, a virtual IP address associated with SLB.
- Phase 2: content location – to request the media stream from the MCDN edge node by using media transmission protocols.

7.2.2.1 Phase 1: MCDN edge node selecting based on DNS resolution

DNS query and resolution are the key procedures within the content request routing mechanism. Typically, in the conventional Internet protocol television (IPTV) and over the top (OTT) services, DNS resolution-based solution is a mechanism commonly used in Phase 1. As Figure 7-3 shows, if MCDN service is applied, CRRS is responsible for terminating the DNS query and responding with the MCDN edge node IP address that can finally provide service.

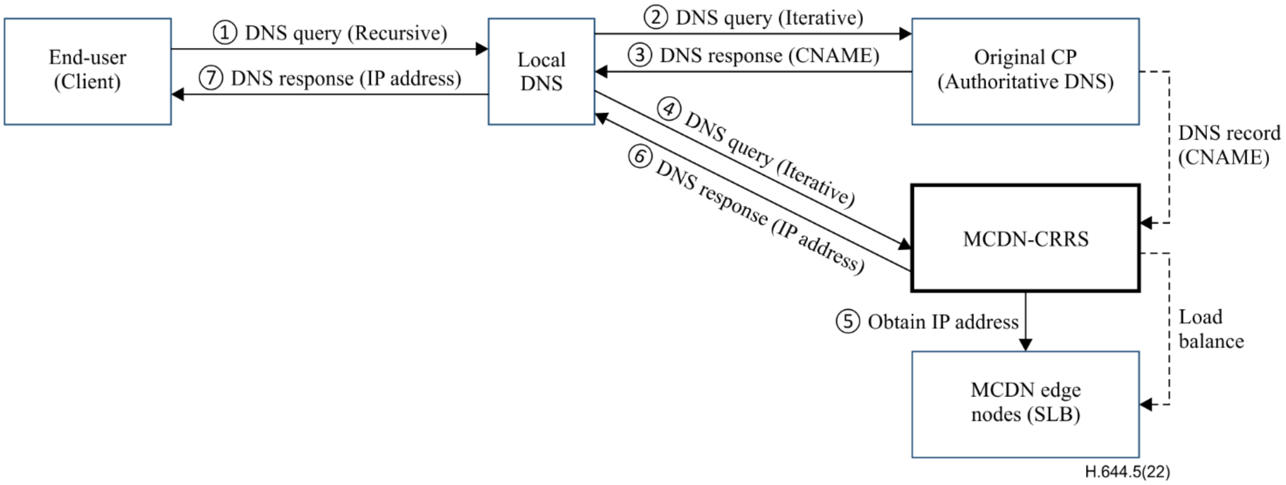


Figure 7-3 – Phase 1: DNS query procedure

During the DNS query, the edge node selection is commonly handled by CRRS based on the end-user's IP address. Network operators may allocate a set of specific prefixes of IP address for a certain geographic area. Therefore, with the mechanism of load balance, CRRS will select the edge node whose IP prefix maximally matches the user IP address (prefix), which means that the selected edge node is geographically closest to the user.

Besides the IP address, the edge node selection policy can be affected by some factors such as node status, server load status, RTT measurement and the traffic status.

7.2.2.2 Phase 2: Content request routing and redirection

During Phase 2, the end-user sends the content request to the MCDN edge node to request the real media files by using various transmission protocols, such as Real-Time Streaming Protocol (RTSP) or DASH/HLS, with the edge node IP. But usually that IP is a virtual IP for the MCDN edge service, and in fact, the cache function is the actual server providing the media streaming service to the end-user.

According to the load balance policy, SLB is responsible for processing the user's content request and selecting an appropriate cache server to provide media service, if the content has already been cached.

When the content does not exist in any cache on the edge node, the content request is recommended to be re-routed or redirected to the other MCDN node. Figure 7-4 lists some approaches.

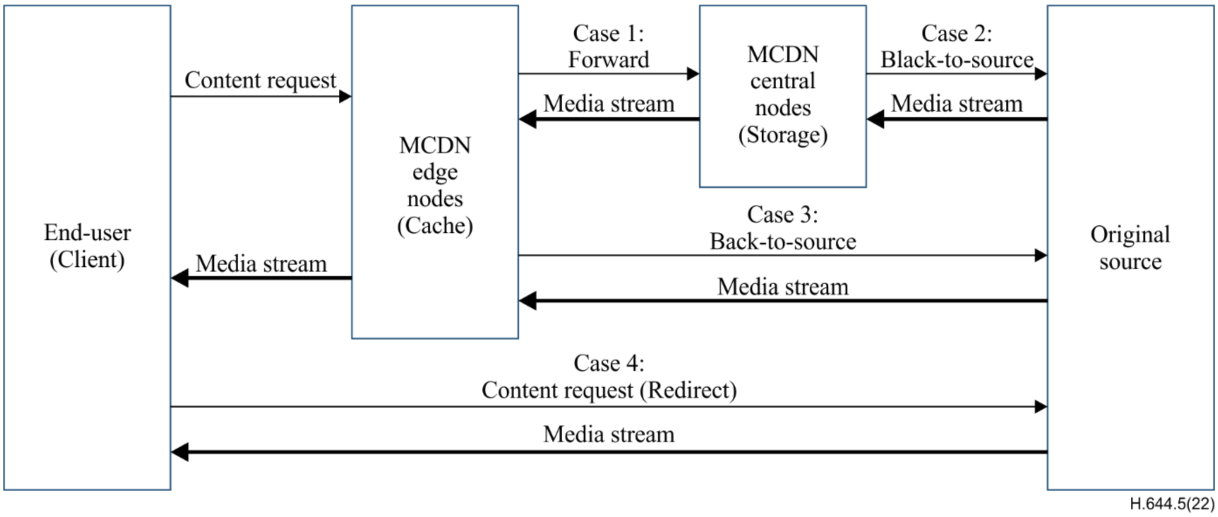


Figure 7-4 – Phase 2: Media content request routing

Once the content request triggers a cache miss on the current MCDN edge node, the back-to-source policy will be applied. The following cases can be referenced:

1) Case 1: The content request will be forwarded to the upstream node, e.g., the central node. If the content is in the central node storage, the media file will be transmitted to the edge node by pull or push mode and then be provided to the end-user.

2) Case 2: If the content does not exist in the upstream node either, the content request will be forwarded to the original content source, e.g., a third-party video service website for requiring the media file. Then the content will subsequently be cached within MCDN node.

3) Case 3: It is possible for the edge node to forward the content request directly to the original content source and subsequently cache the received media file.

4) Case 4: If there is no cached content in any MCDN node, the content request will be redirected to the original content source by returning the source IP address or URL to the end-user. MCDN will not provide delivery or cache service in this case.

The procedure described in clause 7.2.2 provides the basic measure of content request routing and is commonly adopted by many conventional video/audio delivery services such as IPTV. However, as the MCDN edge nodes and video/audio services are deployed closer to the edge of the network, e.g., aggregation network or access network, the accuracy of traditional content request routing schemes is greatly affected.

Clause 7.3 describes a more accurate and enhanced content request routing mechanism based on the concern above.

7.3 Enhanced content request routing procedure based on MEC scenario

As with the legacy content delivery service, the service node of MCDN and the DNS resolution service are usually deployed in the public network area, e.g., with a metropolitan area network (MAN) coverage. However, with the support of MEC technology, the service node can be virtualized and deployed closer to the end-user for a specific network coverage, such as a residential local network, industrial local area network (LAN), the private network of stadium, etc. More background information can be found in [b-ITU-T F.743.10] and [ITU-T H.644.4].

One of the most important features of current network capability, by considering MEC deployment, is traffic steering, which means that the application traffic can be offloaded at a local service node and the response will be returned to the end-user without going through Internet. That requires the end-users to be able to discover and connect to the local service node. However, for the conventional DNS-based discovery mechanism, the local DNS resolver is typically deployed in the edge of Internet where it is higher than the MEC node in the networking topological structure. Moreover, the IP addresses allocated to the MEC applications may be configured according to a special policy, e.g., a shared IP for many containerized applications (APPs) located in the different MEC hosts or a private IP address for each service node. Therefore, the conventional DNS-based content request routing mechanism is no longer suitable for MCDN node discovery in the MEC scenario.

In this Recommendation, it is recommended to adopt an enhanced content request routing mechanism specifically used for MEC-CDN use case. The following clauses introduce the approaches in detail.

7.3.1 MEC-CDN node discovery based on enhanced DNS resolution

In fact, in the traditional DNS query, the IP address used for the CRRS, as an authoritative nameserver, to determine the user's location is actually not the real IP of end-user's terminal device, but the IP of the local DNS resolver. Since the local DNS resolver (recursive resolver) is usually considered as the one topologically closest to the end-user, it could be represented as the location of a group of end-users who are in the same local area, typically the MAN area. But in the MEC scenario, the IP of Local DNS is not accurate enough for determining which MEC-CDN node can be selected. So, the extra information about the end-user is strongly recommended to be attached in the DNS query, together with a MEC-dedicated CRRS.

The MEC-dedicated CRRS (MEC-CRRS) is a special function that is particularly aware of the status of MEC-CDN nodes. It can be implemented in an independent equipment or integrated with the conventional MCDN CRRS functions.

7.3.1.1 Extension mechanisms for DNS (EDNS) query with MEC-CRRS

[IETF RFC 6891] has defined an extension mechanism for DNS (EDNS(0)). Based on that specification, the additional information can be carried by the "RDATA" in OPT RR (option resource record), which is added into additional data section in request. Further, [b-IETF RFC 7871] defined an edns-client-subnet (ECS) protocol, which introduced an informational purpose of carrying the information of the network that originates the DNS query and the network for which the subsequent response can be cached, by extending the EDNS(0) option.

The above two specifications provide an opportunity for MEC-CRRS to select the most appropriate MEC-CDN edge node for a particular end-user according to the additional information carried in the EDNS request. It is noted that the IP address is the most used information for binding the user's location but not the accurate and unique one. In practice, other information can also be used in an EDNS query, such as device ID, service ID, etc.

NOTE 1 – If ECS is used in the EDNS query, only IPv4 address and IPv6 address can currently be used in real implementations. In addition, ECS is an optional format can be used in this Recommendation.

Figure 7-5 shows the example of fundamental information flows of EDNS query (with ECS OPT enabled).

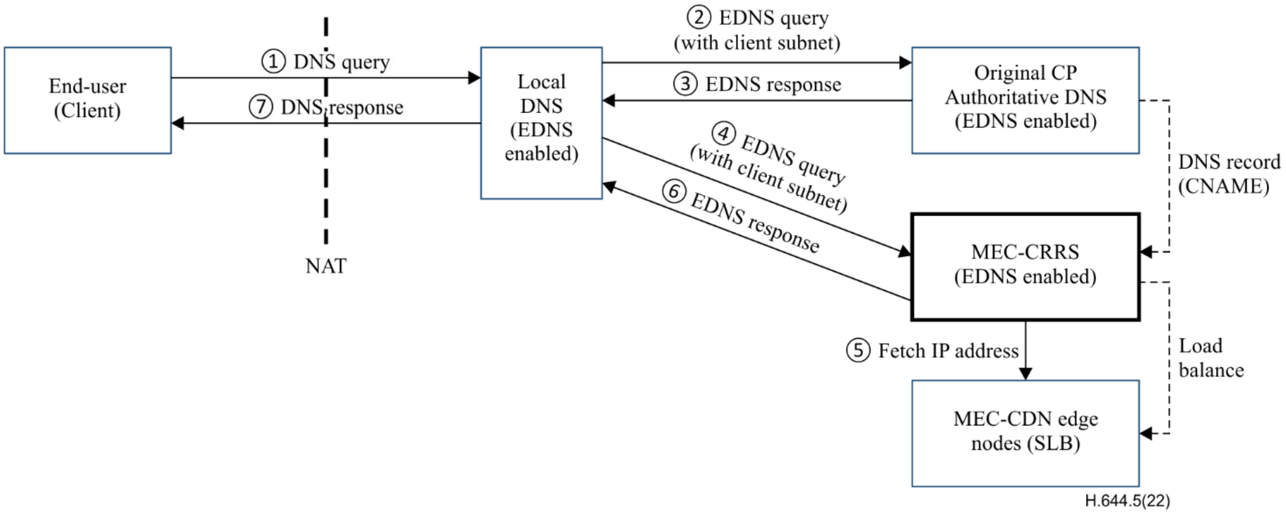


Figure 7-5 – Example of EDNS query flows with MEC-CRRS

If the EDNS mechanism is applied, implementers should be aware of the following principles:

– The local DNS may start an EDNS query if it receives a normal DNS query originated from the end-user (which means that the client may not support the EDNS protocol).

– In this example, all the DNS resolvers, including local DNS (recursive DNS), forwarding DNS and authoritative nameserver are supported by both the EDNS protocol and ECS. Otherwise, the EDNS query may be dropped at one of the DNS resolvers which is not EDNS enabled, and a REFUSE response should be returned. A normal DNS query without OPT data should be subsequently restarted from the original DNS requestor.

NOTE 2 – In this Recommendation, CRRS is considered an authoritative nameserver.

– A customized DNS response may be applied. For example, CRRS may create a tailored response based on the information carried within the ECS option. More issues about the tailored response can be referenced from [b-IETF RFC 7871].

– In many cases, the client IP will be replaced by a network address translation (NAT) device and the NAT device IP will be used in the future EDNS query.

7.3.1.2 DNS/EDNS query with DNS resolver deployed locally in MEC node

A MEC host may provide the DNS handling function in mobile/multi-access edge platform (MEP), probably as a virtualized network function. It is noted that the DNS function in MEP may be accessed as a nameserver or a proxy/cache server. Deploying DNS in a local service area will be beneficial for the end-user to discover the edge application service via the address inquiry service. If a MEC application is activated in the same MEP with the DNS function embedded, the mapping between IP address and its domain name or fully qualified domain name (FQDN) will be configured into DNS rules by MEP or by the request of MEC application.

Figure 7-6 shows the fundamental flows of an EDNS query with a local DNS resolver in the MEC service area.

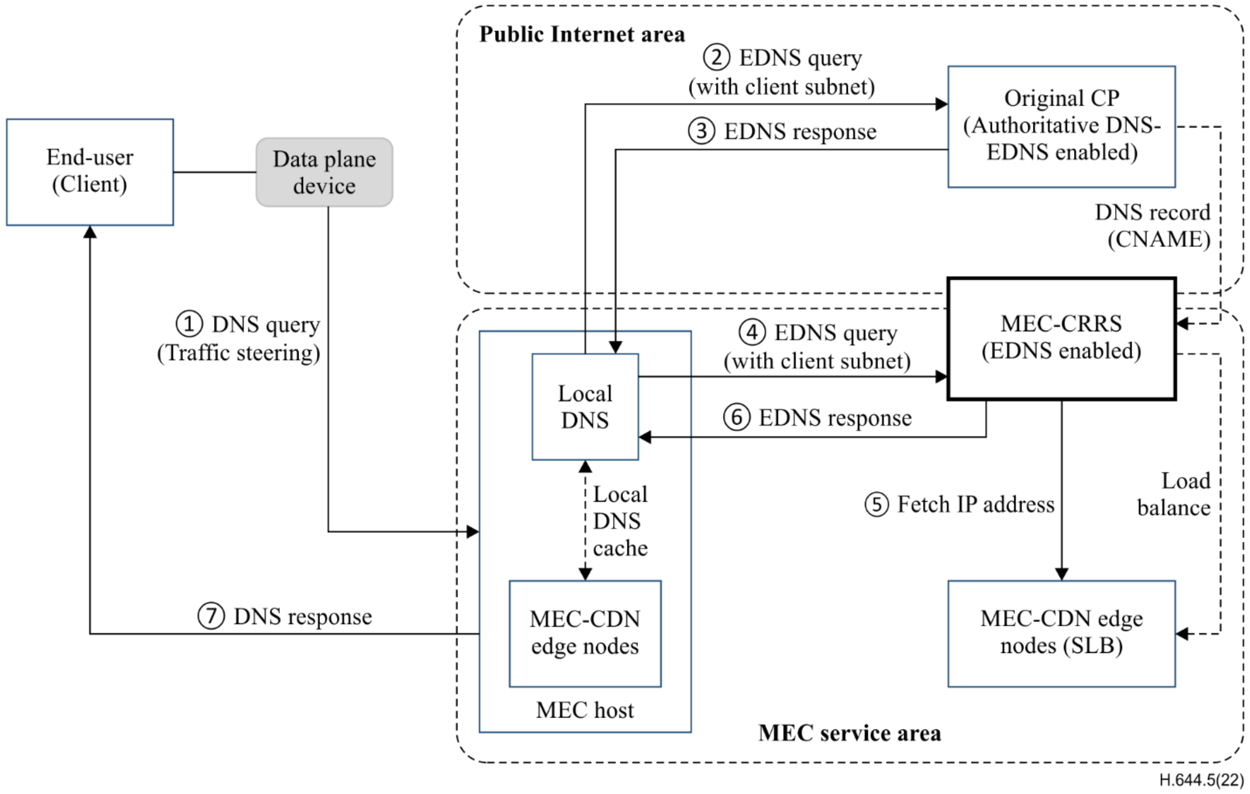


Figure 7-6 – Example of deploying local DNS in a MEC node

NOTE 1 – The data plane device is the routing device that can control the way of traffic forwarding. For example, user plane function (UPF) in a 3GPP 5G network.

NOTE 2 – MEC-CRRS can be an integrated MCDN CRRS located in the public Internet area, or it can be a dedicated MEC-CDN CRRS is in the private MEC service area. Finding the MEC-CRRS depends on the DNS resolution in the authoritative DNS of the original CP, e.g., a different CNAME configuration.

If the MEC-based DNS function is applied in the MEC-CDN scenario, implementers should be aware of the following principles:

- Both the DNS and the EDNS queries can be used in this scenario. Similar to the traditional process, the IP address of local DNS resolver will be used to replace the original DNS requestor.
- The entry point information of MEC based DNS resolver, e.g., an IP address, should be provided to the end-user/client during the network provisioning stage.
- The EDNS query started from the local DNS in MEP is recommended to include the MEC node information in addition to the client IP address.
- If there is no local MEC-CDN edge application running on the MEP or no cached DNS record, the local DNS will forward the DNS/EDNS query to the central DNS resolver/MEC-CRRS, which is in the public Internet area, for inquiring the IP address of a target MEC-CDN edge node, probably via a dedicated connection channel.

7.3.1.3 Considerations on the impact on CRRS using EDNS

The CRRS is able to provide more accurate results of DNS query to the requestor based on the additional information carried in the EDNS message, especially with ECS. But extra overhead may also be required to facilitate CRRS. For example:

- It may need more cache space for maintaining the EDNS record corresponding to the specific end-user request.
- It may need more computing power to process the tailored DNS response.

– If all the DNS queries are off-loaded to the local DNS in MEP, the local DNS may become the "bottleneck" for traffic handling.

– CRRS may need to design or update a traffic steering policy and be capable of interworking with the network control plane, e.g., 5G core (5GC) in mobile networks. Then its policy can be implemented in the data plane device.

– Local DNS resolver's database view should be more fine-grained than MEC CRRS's view in order to satisfy the granularity requirement of CRRS.

– Due to the increasing granularity of the local DNS resolver's database view, it is recommended to be equipped with programmable acceleration circuit (such as a smart network interface card) to improve the performance of the query. Such circuit should have the following functionalities if ECS is enabled:

  - According to pre-defined DNS recursive query rules, attach ECS label information into DNS recursive query.
  - Leverage ECS label information to filter out ECS recursive queries from all DNS queries received.
  - For filtered ECS recursive queries, match client subnet in ECS label to subnet in registered rules and handle them correspondingly.

An EDNS enabled Local DNS resolver in this Recommendation is recommended to satisfy the following requirements:

– To avoid unnecessarily divulging the client subnet to the original CP, the local DNS resolver should store an EDNS query filter, and only attach client subnet information to an EDNS query if such DNS query is sent to a specific MEC-CRRS that is registered on the filter, as Figure 7-7 shows.

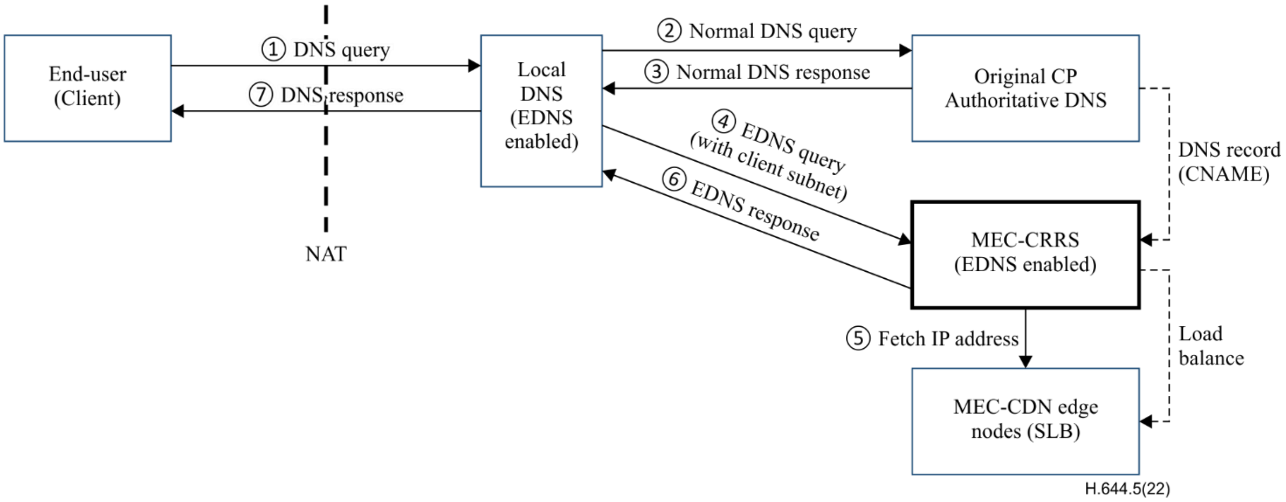


Figure 7-7 – example of local DNS security and privacy enhanced

– The local DNS resolver can establish a map between the client subnet group and the resolver's virtual IP addresses, so, the local DNS resolver can send normal DNS queries using one of its virtual source IP addresses, which represents the query's client subnet group to the MEC-CRRS, as Figure 7-8 shows.

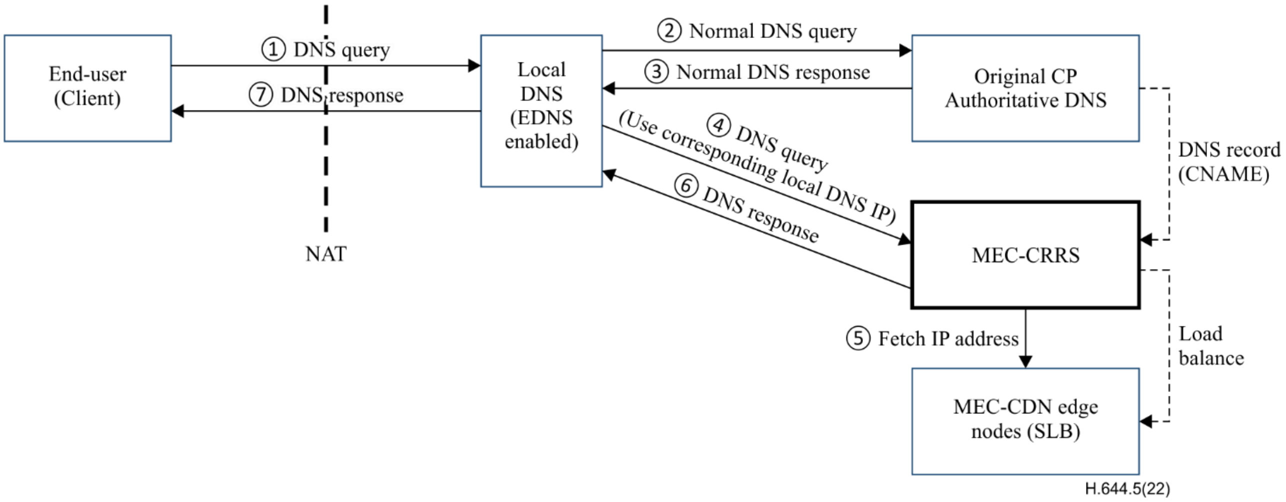


Figure 7-8 – Example of local DNS with DNS query (client subnet)

7.4 Content request routing procedure based on application-layer solution

The legacy DNS solution can only provide a coarse-grained result if no additional information is included. The other defect of the traditional DNS solution is that the scheduling policy cannot be valid immediately, due to the time to live (TTL) configuration in each DNS node. But an application-level scheduling solution can deal with that problem by real-time IP address fetching, i.e., the IP address selecting of CDN edge node is under real-time computing based on each request.

Figure 7-9 shows the example of overview flow of an HTTP based request routing.

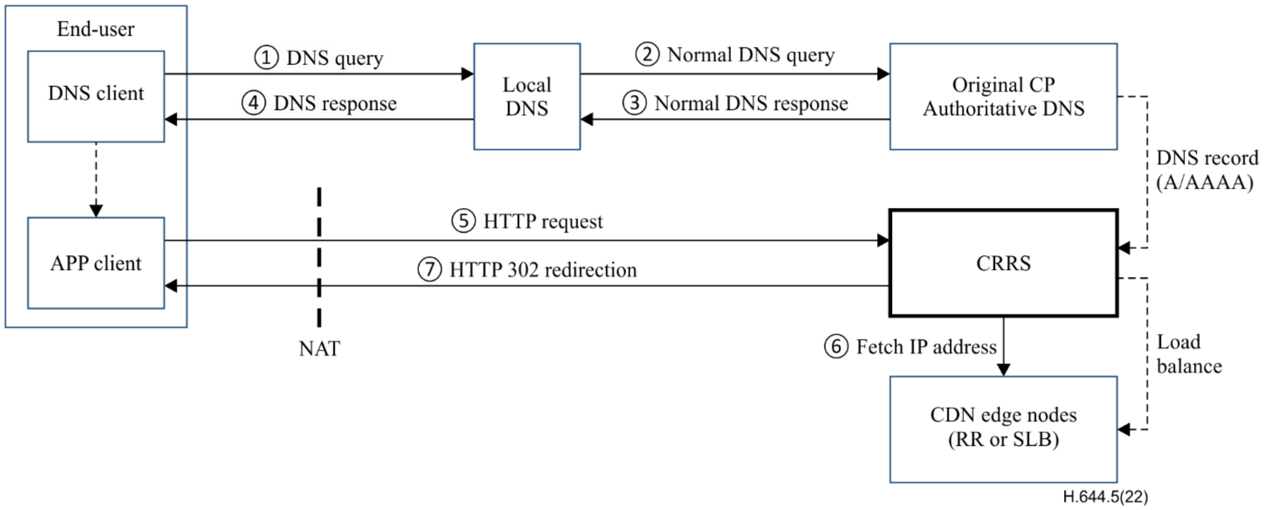


Figure 7-9 – Content request routing based on HTTP request

Typically, for a CRRS with a large-scale service area (see Figure 7-2, Region 2), its central scheduling system, such as GSLB or RR, is usually composed of a cluster of servers and it could be the entry point of the application-level request, e.g., HTTP(s) request, if the HTTP(s) server function is enabled.

In this case, users can obtain the IP address of the central scheduling server cluster in CRRS first, by using a standard DSN query (The IP address can be set as A/AAAA record in the parent DNS nameserver or pre-configured in application client). Then an application (APP) client in the user's terminal device, such as a web browser, will launch a HTTP(s) request to CRRS to request the media content. Different from DNS query, the IP of original HTTP requestor will be carried with HTTP message, and it can be used for scheduling decisions. According to the different implementations of CRRS, the IP address of the CDN edge node can be returned with HTTP 302 (a cascaded RR) as a real-time computing result.

NOTE – If NAT is enabled, the HTTP requestor's IP address is probably replaced by NAT IP.

As to the MEC scenario, it is very similar to the DNS-based solution. If the MEC-CDN is enabled, the HTTP request would be possibly offloaded onto the MEC node due to the traffic steering policy. Therefore, the information related to the MEC node would be carried additionally with the HTTP request while it passes through the data plane device, and that information could be used to select the MEC-CDN node precisely rather than the normal CDN edge node.

An application-level solution can provide a fine-grained content request routing result for the end-user, which is more precise than the DNS-based solution. But the performance of this method may be constrained by the following factors:

– The application client should support HTTP 302 redirection.

– It is not suitable for the latency sensitive service. For example, if the request content contains a lot of small file fragments, such as small web static images, the service loading time may increase due to the additional HTTP 302 redirection for each of the requests.

The detailed information about the method and procedure flow of the application-level request routing can be found in clause 9.1.2.

7.5 Considerations on security and privacy issues

In this Recommendation, the DNS-based domain-IP address resolution is recommended to be applied on the CRRS functional entities. But the conventional DNS-based mechanism exposes many vulnerabilities due to its design of transmission DNS packets in plaintext. Those factors may bring the risks to CRRS such as forged DNS response and private data disclosure.

GSLB takes the responsibility of DNS service in MCDN-CRRS as an authoritative name server, where the security and privacy protection mechanism can be applied. In this Recommendation, the requirements addressed in the following clauses are recommended to be considered as the principles once the related functionalities are enabled on GSLB.

To support applying the valid security and privacy features in MCDN-CRRS, some requirements are also expected to be satisfied by the local DNS, as one kind of recursive DNS resolver.

7.5.1 Requirements of applying authenticity and integrity mechanism

The security mechanism is used to guarantee a trustable DNS resolution result to the DNS requestor, for example, DNSSEC [b-IETF-RFC 4033]. This method requires the DNS records to be kept safe and to be verified by the DNS resolver. The security mechanism should be supported by each entity within the DNS system, including the recursive DNS resolver, the root DNS server and the sub-zone authoritative name server.

Figure 7-10 shows an example of applying the security mechanism in CRRS.

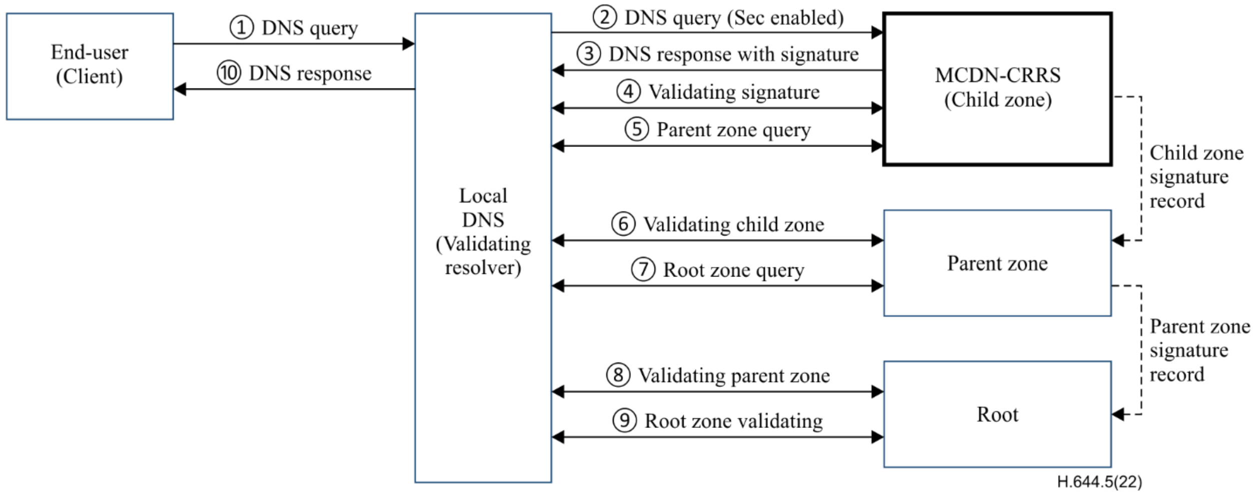


Figure 7-10 – CRRS with security mechanism applied

[Pre-condition]: Once the security mechanism is applied, both the local DNS and the authoritative name server should enable the same security mechanism.

Local DNS, as a recursive DNS resolver, can retrieve the DNS response message which may have an extra DNS record signature attached from the authoritative name server, if the security mechanism is enabled. The DNS record signature is verified afterwards, by traversing the entire DNS name server.

Therefore, the following requirements related to the security protection are recommended to be satisfied:

– MCDN-CRRS is recommended to enable and disable the security mechanism based on the management request.

– MCDN-CRRS is recommended to be able to ignore the DNS request with the additional security query, if there is no security mechanism enabled in CRRS.

– MCDN-CRRS is recommended to encrypt the valid DNS records and create an encryption transcript, for example, to use an encryption key to generate a digital signature.

– When MCDN-CRRS is part the trust chain, it is recommended to enable its DNS encryption transcript to be verified by the parent authoritative name server.

7.5.2 Requirements of applying a privacy mechanism

The enhanced DNS method, such as EDNS, introduced in clause 7.3 will be used more and more in the current MCDN service. Since some private data, such as the end-user information or operator network information carried in the additional EDNS option in plaintext will be transmitted by passing each intermediate DNS resolver, it may cause illegal access to private information during the transmission. Therefore, MCDN-CRRS is recommended to adopt a privacy protection mechanism to avoid unintentional disclosure of user data.

Different from security features, the privacy protection mechanism provides a secured communication between DNS resolver and authoritative name server. Figure 7-11 shows an example of a DNS query with a privacy protection mechanism applied.

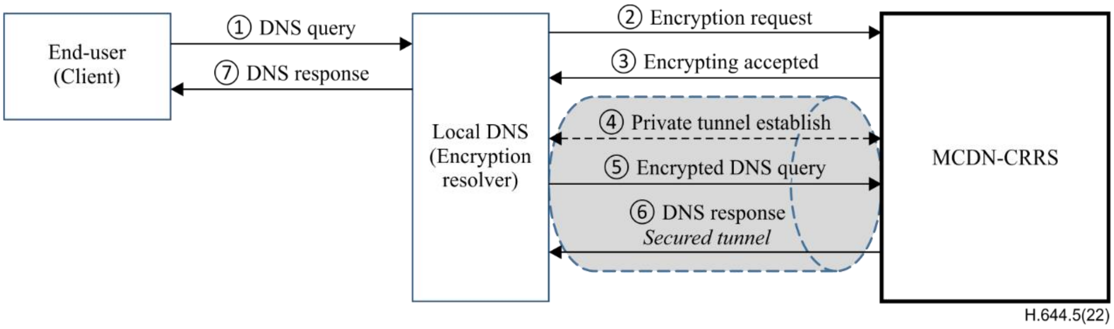


Figure 7-11 – CRRS with privacy protection mechanism applied

When privacy protection is applied, the agreed privacy mechanisms, one or more, should be activated in both recursive DNS resolver (local DNS) and authoritative name server (CRRS). As Figure 7-11 shows, a secured communication tunnel should be established before the DNS query is sent, and the encrypted DNS messages will be subsequently exchanged. There are two types of private communication modes that can be realized:

– Secured-connection oriented method

This method is a typical way of providing an encryption connection between the recursive DNS resolver and authoritative name server, which is very similar to the transport layer security (TLS) in a Transmission Control Protocol (TCP) connection, e.g., DNSCurve [b-DNSCurve]. Before the real DNS query starts, a key pair will be negotiated to be used in the future encryption and verification. As messages can be exchanged in a secured tunnel, it is difficult for the attackers to understand the true information contained in the DNS query and response.

Comparing with other modes, this method provides the top level of security by encrypting all the information contained in the DNS message. Meanwhile, the extra RTT and computing resource maybe required for the secured communication.

– Masked-privacy method

Different from the above method, the masked-privacy method does not need to build a secured connection between the recursive DNS resolver and authoritative name server. Instead, the recursive DNS resolver receives the DNS query from the end-user client, and the private information contained in the query will be sheltered with a pre-configured or pre-negotiated masking algorithm. Then a new DNS query will be created by encapsulating the masked private information and a masking indicator into the query message. Subsequently, the new DNS query is sent to the authoritative name server, in plaintext or not, for the normal DNS response process. Because the masking indicator implies that the private information contained in the DNS query has been masked, the authoritative name server is required to process (such as restoring, de-capsulating, and, etc.) the private information according to the masking indicator.

This method does not need a stable connection between requestor and name server. Instead, an agreement of adopting the paired pre-configured masked-privacy algorithm, e.g., encryption algorithm, mask key, etc., should be negotiated between the recursive DNS resolver and authoritative name server in advance.

Therefore, the following requirements related to the privacy protection are recommended to be satisfied:

– MCDN-CRRS is recommended to be able to enable and disable the privacy protection mechanism based on the management request.

– MCDN-CRRS can optionally interact with network expose function configured by the network provider to access the permitted information.

- MCDN-CRRS is recommended to process an encrypted DNS query by using the agreed encryption/decryption mechanism.
- MCDN-CRRS is recommended to ignore or refuse an encrypted DNS query if corresponding privacy protection mechanism is not enabled.
- MCDN-CRRS is recommended to recognize a masked private information in the DNS query if a corresponding privacy protection mechanism is enabled.
- MCDN-CRRS can optionally process a masked private information in the DNS query by returning a normal DNS response or an error response.
- MCDN-CRRS is recommended to establish a secured tunnel between DNS resolver and the authoritative name server.
- MCDN-CRRS, as an Authoritative Name Server, is recommended to negotiate the agreed privacy protection methods with the DNS resolver and enable it subsequently.

NOTE – The implementation of a security and privacy protection mechanism may cost more computing resource and an extra RTT, which may cause an inefficient DNS resolution process.

8 Reference points

Clause 8 of [ITU-T H.644.3] briefly defines the reference points between the CRRF and other MCDN functions. Specifically, Table 8-2 of [ITU-T H.644.3] defines RP-e and RP-d. In this Recommendation, those reference points are described in detail according to the implementation of CRRS.

Figure 6-2 and Figure 7-1 show the functional architecture of the CRRS and the relationship with the other functions. Figure 8-1 presents the reference points between MCDN CRRS functions and the other functions used in multimedia service, e.g., IPTV, based on the CRRS functional architecture specified in this Recommendation.

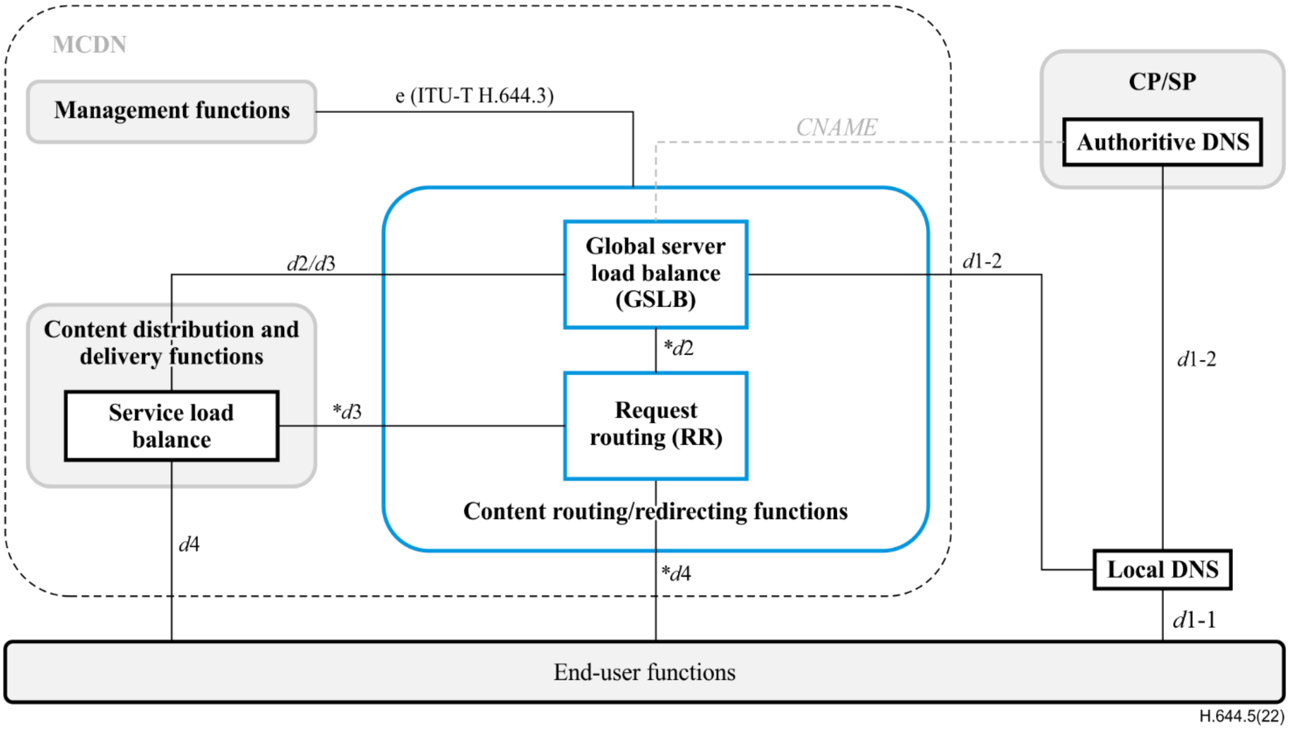


Figure 8-1 – Reference points between CRRS and other multimedia service functions

According to the functional architecture and funtions defined in previous clauses, the reference points in this architecture will be used as followins:

1) To exchange information between end-user, as a DNS requestor, and authoritative DNS to fetch the most appropriate service node information.

2) To select the most appropriate service node by inquiring the available service nodes status.

3) To process the end-user's media stream acquiring request and to redirect the request to the application server that actually provides the media streaming service.

4) To configure the content request routing policy between CRRF and Management functions, e.g., to enable the back-to-source mechanism or content dispatch policy.

Table 8-1 and Table 8-2 describe the detailed functionalities of the reference points.

Table 8-1 shows the main reference points used between CRRS and other service functions outside of the MCDN service scope.

Table 8-1 – Reference points between CRRS and external service functions

Reference Point		Definition	Protocol	Notes
d1	d1-1	DNS query (recursive) reference point between end-user functions and public DNS resolver (local DNS)	DNS/EDNS over UDP	This RP is used for an end-user/client to send the DNS query to the public DNS resolver and get feedback. The IP address of public DNS resolver is allocated during the network provision stage or be configured manually. ECS option can be optionally used in EDNS query.
	d1-2	DNS query (iterative) reference point between public DNS resolver and Authoritative DNS/CRRS (GSLB)	DNS/EDNS over UDP	This RP is used to forward the DNS query to the authoritative nameserver and then fetch the final DNS response. ECS option can be optionally used in EDNS query.
d4/*d4		Reference point between end-user functions and CRRS (RR) or CD&DF (SLB)	RTSP, HTTP	This RP is used for end-user/client to request the media stream from the MCDN edge node. The request will be processed by SLB, and a media streaming server inside of the MCDN edge node will be selected to provide the actual streaming service. The media stream request may be redirected multiple times between different edge nodes.

NOTE 1 – d4 may have a different implementation in practice, depending on whether RR is deployed separately or not. For example, if RR function may be merged into GSLB, *d4 in Figure 8-1 may not be used.

Table 8-2 shows the main reference points that are used between CRRS and other service functions inside the scope of the MCDN service.

Table 8-2 – Reference points between CRRS and other MCDN functions

Reference Point	Definition	Protocol	Notes
d2/*d2	Internal reference point between CRRS (GSLB) and CRRS (RR)	SOAP	This RP is used for GSLB to acquire the performance status of RR or SLB (in heartbeat mode).
d3/*d3	Reference point between CRRS (GSLB/RR) and CD&DF (SLB)	SOAP/HTTP/DNS	This RP is used for GSLB/RR to inquire the load status of MCDN edge nodes. If the back-to-source service is enabled, this RP is also used for requesting the source content URL by using DNS/HTTP redirection method.
e (optional) (defined in [ITU-T H.644.3])	Reference point between CRF and MF	HTTP	The reference point e is an optional interface that is used for content request routing/redirecting functions to obtain management information from MCDN management function, e.g., the routing/redirecting policy, network management information, etc.

NOTE 2 – d2 and d3 may have a different implementation in practice, depending on whether RR is deployed separately or not. For example, if RR function may be merged into GSLB, the *d2 and *d3 in Figure 8-1 may not be used.

9 Mechanism of content request routing/redirection

In this clause, several key mechanisms of content request routing/redirection commonly used in the traditional multimedia service are addressed. Most of them can be applied in the MCDN-CRRS directly and are elaborated in the following clauses.

9.1 Mechanism of content request scheduling

One of the most important mechanisms in CRRS is content request scheduling. For GSLB, its key function is to select the most appropriate MCDN server node for the end-users based on their various types of content requests. Clause 7.1 describes the basic function of GSLB and RR and clause 7.2 shows the networking scenario. Typically, the CRRS should support the content request scheduling by following the policies such as the location of users, the workload of server nodes, the priority of the nodes, the traffic status, etc.

Clause 7.2.2 introduced the basic procedure of content request routing. According to the different types of multimedia service such as IPTV, OTT TV or mobile cache, the CRRS is recommended to support DNS-based scheduling, the application-level redirection scheduling mechanism, or both. Clause 9.1.1 describes the requirements and the basic procedures of those two mechanisms.

9.1.1 DNS-based scheduling

According to the content mention in clause 7.2.2.1, the request scheduling by using DNS resolver major depends on the requestor's IP address (or IP prefix). That may cause a coarse-granularity query result. This method is suitable for those scenarios which CRRS may cover a large geographic area or a minimum networking structure of CRRS.

Before the GSLB returns the final result of DNS query, the selection of MCDN sever node should be processed by following the pre-configured scheduling policy which can be listed, but not exhaustively, as:

– Geographic proximity: GSLB can schedule the request to a server node which is closest to the requestor based on its IP address or IP prefix.

– Workload of server node: GSLB can schedule the request to a server node based on its workload such as node traffic, number of connections and node health status, etc.

– Node priority: GSLB can select a MCDN server node based on its pre-configured node priority.

– IP filter: If the requestor IP is from a specific zone, GSLB can select a dedicated server node for special processing.

Figure 9-1 shows the basic procedure of DNS-based scheduling.

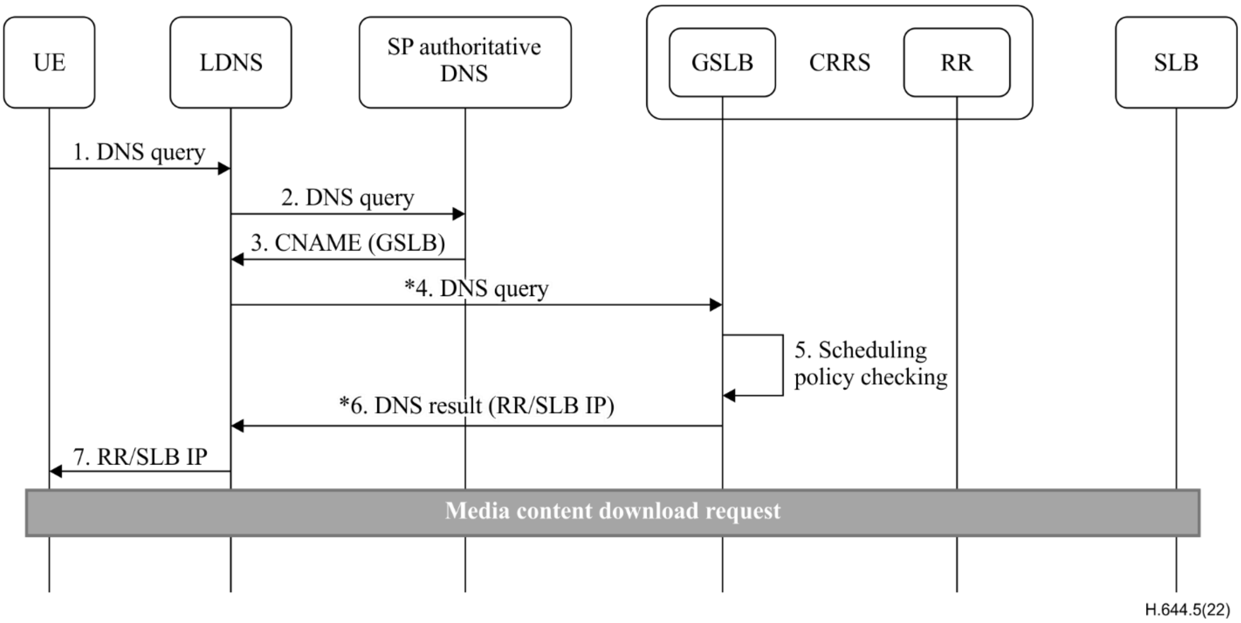


Figure 9-1 – DNS-based scheduling procedure

The steps of the procedure are:

1) An end-user (DNS client) sends a DNS query with the service domain name to the local DNS (recursive DNS resolver)

2) Local DNS forwards this DNS query to the SP authoritative DNS server.

3) If MCDN service is applied, the SP authoritative DNS server returns a DNS record containing a CNAME of MCDN GSLB.

4) Local DNS forwards the DNS query to the GSLB.

NOTE 1 – Before this step, it is noted that possibly only a domain name of GSLB might be returned in Step 3. To obtain the IP address of GSLB finally, the local DNS needs to query with the DNS root server recursively.

5) GSLB selects a MCDN server node by checking the scheduling policy.

6) A MCDN server node IP address is returned to the local DNS.

NOTE 2 – The MCDN server node IP address could be the IP address of node SLB or a public Internet IP address that the media streaming server configured previously. But if RR is deployed, the IP address of RR should be returned instead of MCDN server node IP. Which result should be returned depends on the real implementation of the networking structure shown in Figure 7-2. In the special case, a fixed IP address of

RR may be pre-configured in the UE while UE is rebooting in the previous stage. Thus, it is possible for the end-user to send the application-layer content request directly to that RR by ignoring the domain name resolution.

7) Local DNS returns the final DNS response with server node IP to the end-user.

When the DNS query is completed, the user client can initiate the application-layer request to the MCDN server node for downloading the target media file.

9.1.2 Application-layer-based scheduling

DNS-based scheduling tries to select a MCDN server node that is geographically closest to an end-user, according to its IP address. However, application layer-based scheduling will redirect the user's content request to the actual media content server based on an URL contained in the application layer request, such as HTTP or RTSP request. That may cause a fine-granularity query result and is suitable for those scenarios in which CRRS may be aware of the exact location of the request content.

The following principles are recommended to be applied in application-layer-based scheduling:

– The application-layer-based scheduling method is recommended to be used for RR, SLB or media streaming server. It is optionally used in GSLB if GSLB supports both DNS-based scheduling and application-layer-based scheduling.

– The application-layer-based scheduling policy can be referenced from DNS-based scheduling policy. For SLB, it can optionally schedule the content request preferentially to the server where the content has already stored or cached, based on the location of the content.

– The application-layer-based scheduling is recommended to support the request redirection by reconstruct the original content request message, such as the URL of content file.

An end-user can obtain an IP address of RR or a MCDN server node first, following the procedure shown in Figure 9-1. Figure 9-2 shows the basic procedure of application-layer-based scheduling.

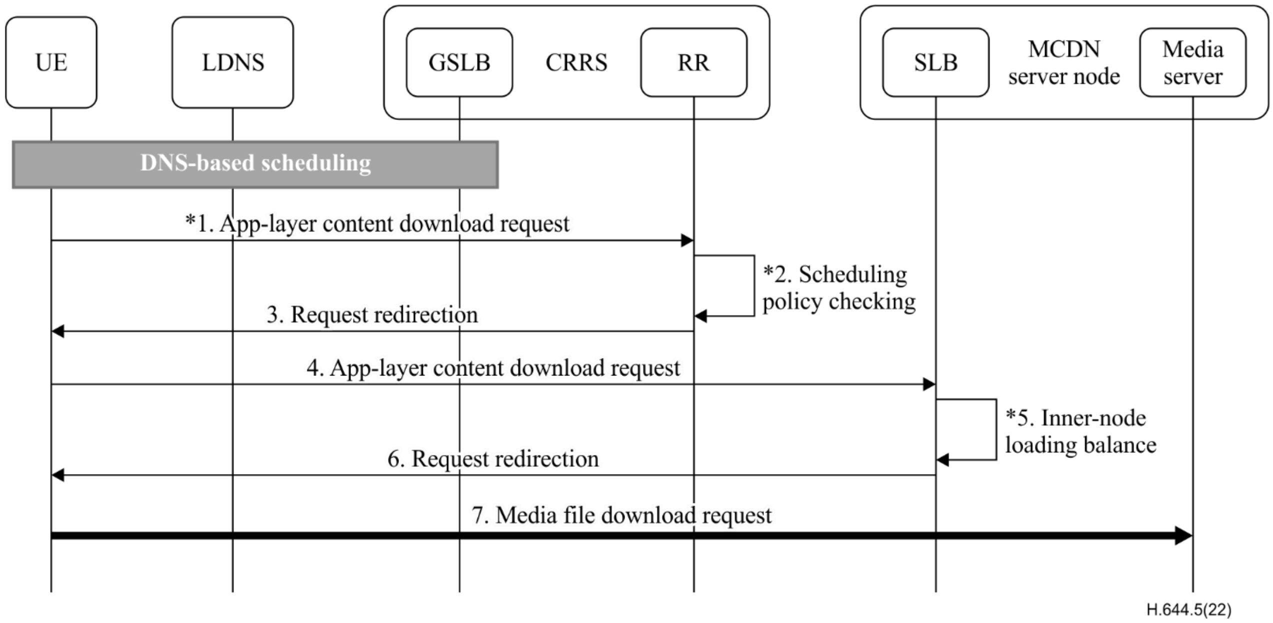

UE
LDNS
GSLB
CRRS
RR
SLB
MCDN server node
Media server
DNS-based scheduling
*1. App-layer content download request
*2. Scheduling policy checking
3. Request redirection
4. App-layer content download request
*5. Inner-node loading balance
6. Request redirection
7. Media file download request
H.644.5(22)

Figure 9-2 – Application layer-based scheduling procedure

The steps of the procedure are:

1) An UE sends an application-layer content request, i.e., a content URL, to RR.

NOTE 1 – If no RR is deployed, Steps 2 and 3 can be omitted, and step 4 should be initiated in this stage.

2) By checking the scheduling policy, RR can select a MCDN server node and reconstruct the content request. For example, to replace the *hostname* in the URL with the target MCDN server node IP address.

NOTE 2 – If a cascaded RR is deployed, a downstream RR should be selected for the next redirection till the final MCDN server node is determined.

3) The redirect request message is returned to the UE by an application-layer protocol. For example, HTTP 302 or RTSP 302 can be used.

4) The UE (re-)sends an application-layer content request to the MCDN server node.

5) If SLB is applied within the MCDN server node, it will select a media streaming server by checking the inner-node load balance policy and the content request is reconstructed.

NOTE 3 – If no SLB is deployed, the media streaming server should be configured with the public Internet IP address and be used as in Figure 9-1, Step 5. Step 6 can be omitted.

6) The redirect request message is returned to the UE by an application-layer protocol.

7) The UE sends the media content request to the final media server.

9.1.3 Request scheduling for MEC-CDN

Clause 7.3 describes the way of applying an enhanced DNS solution for the MEC-CDN. But the different implementation of LDNS, GSLB and network routing policy may cause the differentiated scheduling policies and solutions. Therefore, clauses 9.1.3.1 to 9.1.3.3 present the possible scheduling methods that can be used in the MEC-CDN case.

Typically, if MEC traffic steering is enabled, the application data traffic can be offloaded locally onto a MEC node when it passe through the data plane device closest to the end-user. For example, a MEC node combined or connected with a 5G UPF is able to configure the traffic steering policy on the data plane device. However, as a virtualized application, MEC-CDN may not be run on the same MEC node. Therefore, CRRS is strongly recommended to apply the different scheduling methods for selecting the most appropriate MEC-CDN node.

9.1.3.1 EDNS-based request scheduling

MEC-CDN node can be treated as a light-weight legacy CDN node and its scheduling policy can be compliant with the common DNS-based scheduling specified in clause 9.1.1. When a user moves into a MEC-CDN service area, an accurate MEC-CDN node selection will be executed by CRRS (may involve MEC-CRRS function) if the user location information is recognized from a DNS query.

The user location information contained in the traditional DNS query can be represented as user's device IP or client subnet IP. But if an end-user is in a MEC service area, the location of MEC node can alternatively be used to represent the user location. Therefore, it is possible for the MEC node to create a new EDNS query by adding its identification information into the received DNS query. This procedure is shown in Figure 9-3.

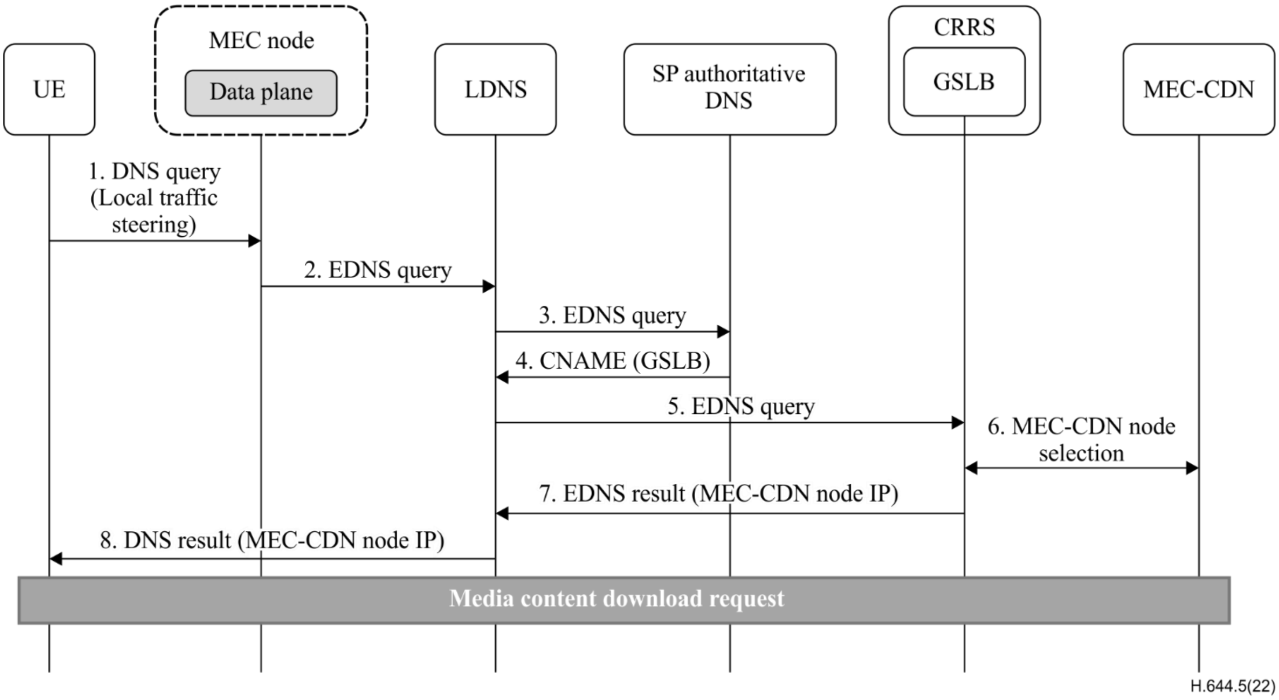

MEC node
Data plane
UE
LDNS
SP authoritative DNS
CRRS
GSLB
MEC-CDN
1. DNS query (Local traffic steering)
2. EDNS query
3. EDNS query
4. CNAME (GSLB)
5. EDNS query
6. MEC-CDN node selection
7. EDNS result (MEC-CDN node IP)
8. DNS result (MEC-CDN node IP)
Media content download request
H.644.5(22)

Figure 9-3 – EDNS query flows with local traffic steering case

The steps of the procedure are:

1) An end-user (DNS client) sends a DNS query to the local DNS.

2) The DNS query is offloaded to the MEC node. If the EDNS function is enabled on the MEC node, a new EDNS query is created by adding the MEC ID into the original DNS query.

NOTE – MEC ID is one of the identifications. MEC IP or NAT IP can be used as well.

3) The new EDNS query is forwarded to the LDNS. If LDNS supports EDNS, this EDNS query will be forwarded again to the SP authoritative DNS server. Otherwise, the the EDNS query could be dropped/returned or forwarded as a normal DNS query without additional resource record.

4) The SP authoritative DNS server returns a DNS record containing a CNAME of GLSB (CRRS). In addition, if SP authoritative DNS server supports EDNS and a special MEC-CRRS is applied, the EDNS record containing a CNAME of GLSB (MEC-CRRS) will be returned.

5) Local DNS forwards the EDNS query to the GSLB.

6) GSLB selects a MEC-CDN server node by checking the scheduling policy, together with the additional information contained in EDNS query.

7) A MEC-CDN node IP address is returned to LDNS.

8) LDNS will return the MEC-CDN node IP address to the end-user. Note that the MEC node may need to restore the EDNS result to the normal DNS result before the final result is sent back to the end-user.

9.1.3.2 NAT+HTTP request redirection-based scheduling

In the other case, if EDNS query is not supported, CRRS is recommended to apply the application-layer based request scheduling method. In this clause, NAT+HTTP request redirection are illustrated as the alternative solution for scheduling.

Simliar to the previous DNS-based case, this method intends to replace the IP of HTTP requestor with the MEC node IP by NAT, while the HTTP request is offloaded on the MEC node. This procedure can be showed in the following Figure 9-4:

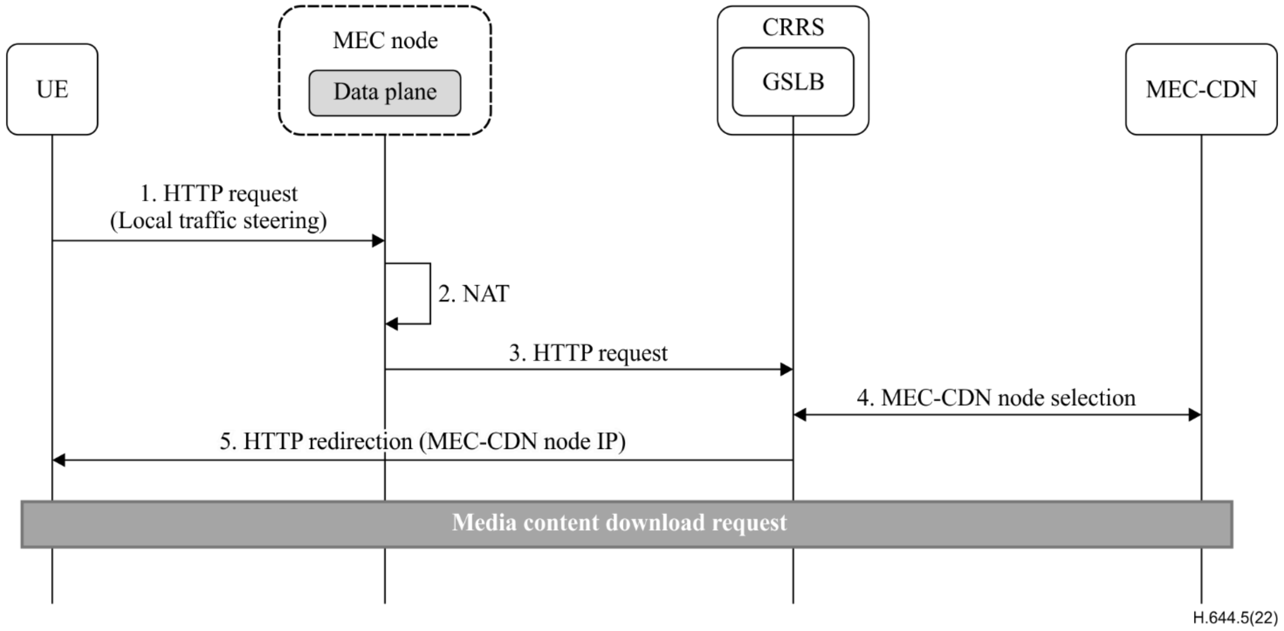


Figure 9-4 – HTTP request redirection with local traffic steering case

NOTE – In this case, CRRS is recommended to be capable of resolving the application layer request.

The steps of the procedure are:

1) An end-user (application client) sends a HTTP request with the content URI.

2) This HTTP request is offloaded onto the MEC node. The MEC node will implement NAT by replacing the original IP of HTTP requestor with the MEC node IP.

3) The HTTP request then is forwarded to GSLB.

4) GSLB selects the most appropriate MEC-CDN node based on the MEC node IP in HTTP request.

5) The MEC-CDN node IP will be returned to the end-user by HTTP redirection message. Note that the NAT may need to be implemented again on the MEC node for restoring the original requestor's IP.

9.1.3.3 Enhanced HTTP header-based scheduling (optional)

This case is similar to the case in clause 9.1.3.2. The only difference is that the HTTP header will be extended for carrying the additional information, such as MEC ID.

This procedure is shown in Figure 9-5.

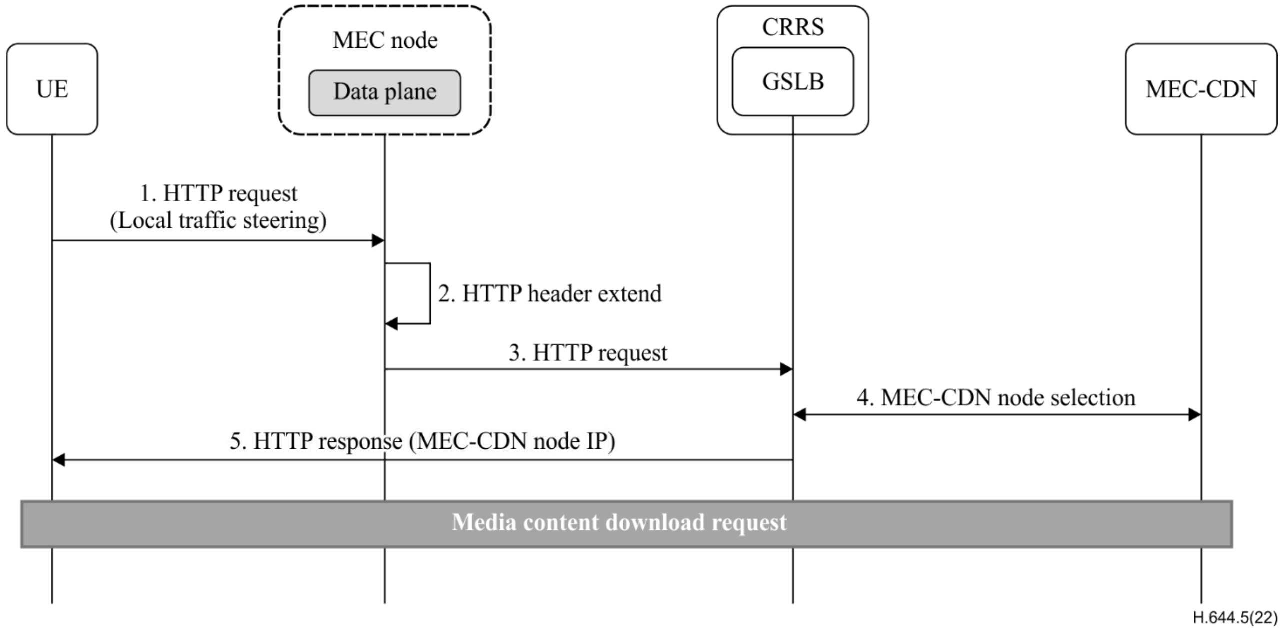


Figure 9-5 – HTTP header extension with local traffic steering case

The steps of the procedure are:

1) An end-user (application client) sends a HTTP request with the content URI.

2) This HTTP request is offloaded onto the MEC node. The MEC node will fill the extension domain in the HTTP header with the MEC node ID.

3) The HTTP request then is forwarded to GSLB.

4) GSLB selects the most appropriate MEC-CDN node based on the MEC ID in HTTP header.

5) The MEC-CDN node IP will be returned to the end-user by HTTP response.

9.2 Mechanism of service load balance

SLB, also called local service load balance, is used to present an entry point for the end-user to obtain the real media stream. Usually, an SLB can work as a transport-layer SLB (L4 SLB), an application-layer SLB (L7 SLB) or a hybrid SLB (L4+L7 SLB).

9.2.1 L4 SLB

An L4 SLB processes the request data at the network layer. It can be configured with a virtual IP address for gating the content request from the end-user. When the content request reaches the L4-SLB, the L4-SLB will select a server from its server list based on the packets' IP+Port) and all the subsequent responses can be processed by that server directly, as shown in Figure 9-6.

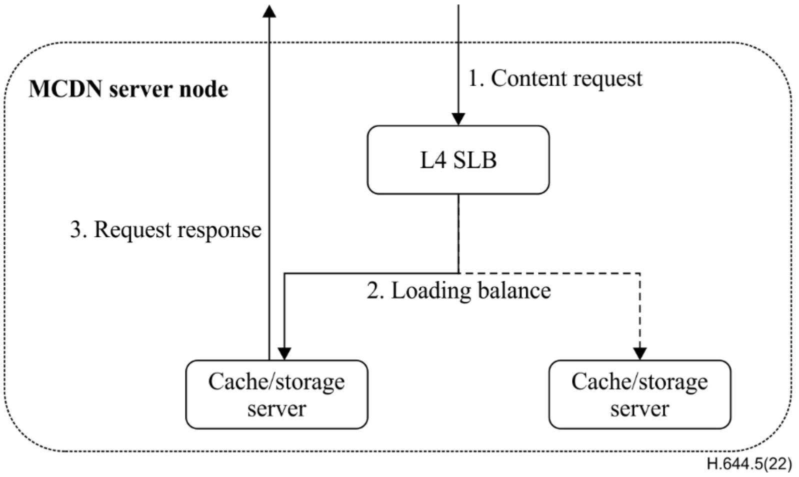


Figure 9-6 – L4 SLB

Once a candidate server is determined, the L4 SLB modifies the original packets' IP by using the destination server IP and then forwards them to that server.

The following methods are recommended for the L4 SLB:

- Round robin: content requests are distributed to servers in the cluster in turn, regardless of the actual number of connections and device loads on the server.
- Weighted round robin: content requests are scheduled in turn, in accordance with different processing capabilities of servers to ensure that servers with high processing capabilities will process more access traffic.
- Least connections: schedules content requests to the server with the least number of established links.
- Minimum RTT: schedules content requests to the server with the minimum response time.

9.2.2 L7 SLB

An L7 SLB processes the request data at the application layer. It can be entitled to a virtual URL or hostname for it to receive the content request. When the content request reaches the L7-SLB, the L7-SLB will select a server from its server list based on the real content identifier contained in the application messages. However, to get and resolve the application message, the SLB should establish a link with the UE first, and then establish another link with the destination server to forward the content request, as a proxy of media content server. Figure 9-7 shows a deployment case of L7 SLB.

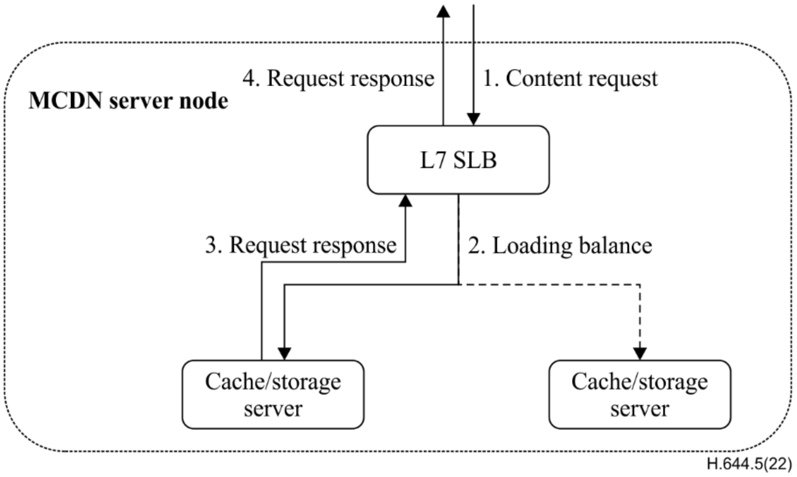


Figure 9-7 – L7 SLB

The L7-SLB is extremely useful for server nodes that may have huge traffic, live session keeping and high concurrency process requirements. The following methods are recommended for the L7 SLB:

- Round robin based on domain/URL/IP: content requests are distributed to servers in the cluster in turn, based on the domain name, URL or IP address.
- Weighted round robin: content requests are scheduled in turn, in accordance with different priorities of domain/URL/IP.
- Hash based on domain/URL/IP: content requests are scheduled according to the hash consistency of the access domain name, URL or IP address.

9.2.3 Hybrid (L4+L7) SLB

A hybrid SLB means the SLB can process the request data both on L4 and L7 modes. L4 SLB can provide coarse-granularity scheduling in the first place. While the detailed resolving is required, L7 SLB can later provide fine-granularity scheduling.

Figure 9-8 shows a deployment case of a hybrid SLB.

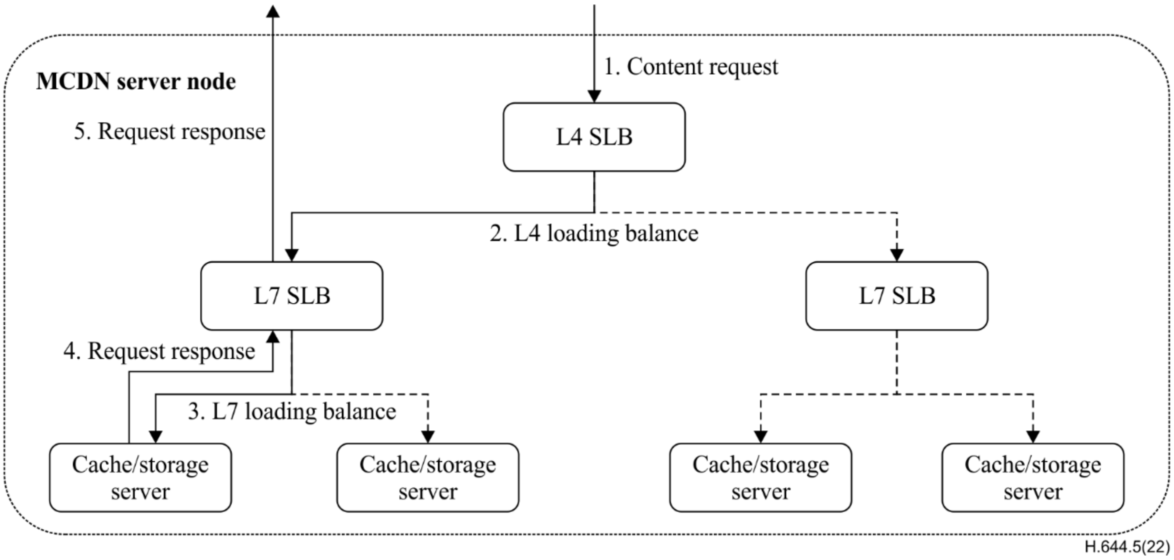


Figure 9-8 – L4+L7 SLB

The methods used in L4 SLB and L7 SLB can also be used for hybrid SLBs, and the following additional requirements should be met:

– L4 SLB is recommended to be deployed in front of L7 SLB.

– L7 SLB is recommended to be a proxy of media content server.

– L7 SLB is recommended to support flexible expansion and reduction.

9.3 Mechanism of content back-to-source

Clause 7.2.2.2 describes four cases of content request routing and redirection. Typically, when the request is a cache miss in the first MCDN edge node, i.e., there is no cache on the edge node, the request should be redirected or forwarded to the content source by following a back-to-source policy. For example, a back-to-source path is defined as an URL pointing to the content source. However, the content source can be the upper layer MCDN node or the real original content source. In fact, multiple paths can be defined, and an optimizing path should be selected for future forwarding.

Figure 9-9 shows the related functional components of the back-to-source procedure.

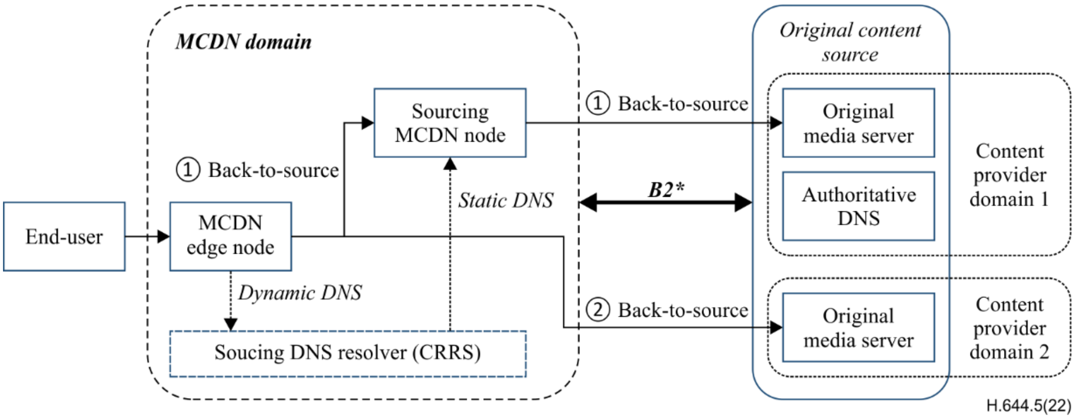


Figure 9-9 – Request routing: back-to-source

NOTE – Reference point **B2** is used for retrieving the real media content from the content source, which has been defined in [ITU-T H.644.3]. It can be used for any MCDN node which is able to download the content from content source.

In general, the media files of a content may be distributed to multiple domains or positions. For an MCDN edge node, the content source to be selected may be determined according to various factors. Clauses 9.3.1 to 9.3.4 define the general requirements and modes of the back-to-source mechanism.

9.3.1 General requirements for back-to-source mechanism

If the back-to-source mechanism is applied, the following requirements need to be complied with:

– It is recommended to use different sourcing MCDN nodes to process the back-to-source request. Moreover, the sourcing MCDN node is recommended to support real-time content distribution while at the same time the content is downloading.

– It is recommended to configure the different sourcing domains for retrieving media content, according to the original content provider domain, e.g., IPTV domain and OTT domain.

– It is recommended to set up the pre-configured sourcing URL replacing rules for transferring the original user request URL to a dedicated sourcing URL.

– It is recommended to support multiple back-to-source modes for the different cases, such as static mode and dynamic mode.

- The back-to-source mechanism can optionally support to use a dedicated sourcing DNS resolver for analysing the final IP address of the original media server.
- The back-to-source mechanism can optionally support to aggregate the sourcing requests if all of them are pointing to the same content source.
- The back-to-source mechanism can optionally support the automatic source switching mechanism while the content source is temporally unavailable.

9.3.2 Sourcing modes

In this Recommendation, two sourcing modes are recommended to be used: static sourcing mode and dynamic sourcing mode These are described in clauses 9.3.2.1 and 9.3.2.2.

9.3.2.1 Static sourcing mode

The static sourcing mode is used when the IP address of the original content source server is fixed. In this mode, the sourcing MCDN node is able to build a back-to-source request with source media server IP address by IP address configuration or domain name resolution.

This mode is usually used for the original content source hosted in the original content provider domain. In addition, the following two methods can be applied:

- IP address-based sourcing: modifying the user request URL into a dedicated sourcing URL, which is pointed to the original content source IP address. Multiple content source IP addresses are recommended to be configured and to be used sequentially by priority.
- Static DNS based sourcing: to set up a static DNS resolver for mapping the user request URL into a fixed original media server IP address without changing the user request itself. The DNS resolver is recommended to be installed in the sourcing MCDN node.

9.3.2.2 Dynamic sourcing mode

The dynamic sourcing mode is used when the original content source server is possibly not fixed. Thus, the original media server IP address for sourcing should be determined each time by DNS scheduling or application layer scheduling.

This mode is usually used for the content source in distributed networking, and the MCDN should select the nearest original media server as the content source. Two following methods can be applied:

- DNS based sourcing: to return the original media server IP address by DNS resolver for the sourcing MCDN node while the user request is received. Multiple IP addresses can be returned in order to improve reliability.
- Application layer-based sourcing: the content access URL that points to the nearest media server can be returned by application layer request redirection. Usually, this method is controlled by the content source scheduling system, such as RR.

9.3.3 Back-to-source service configuration

Each sourcing MCDN node is recommended to enable the back-to-source service by setting up a back-to-source service configuration table. Therefore, MCDN can provide the back-to-source policy for different content providers and to create sourcing URL according to the related back-to-source policy.

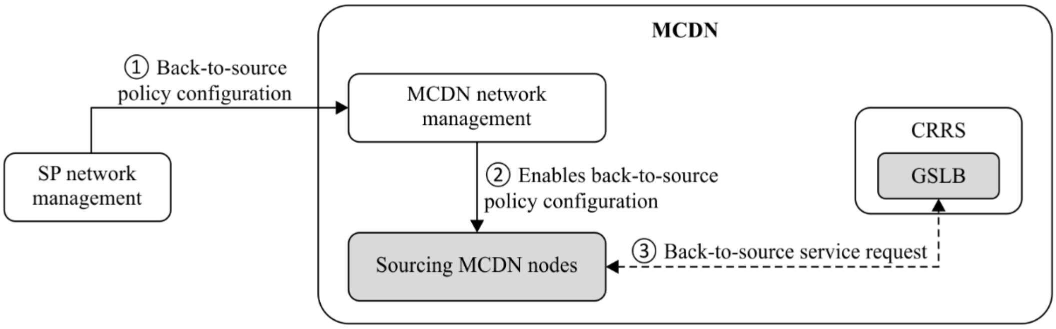

MCDN
① Back-to-source policy configuration
SP network management
MCDN network management
② Enables back-to-source policy configuration
CRRS
GSLB
Sourcing MCDN nodes
③ Back-to-source service request

Figure 9-10 – Back-to-source service configuration example

Usually, the MCDN network management system receives the back-to-source configuration request from the upper layer management system, such as an IPTV service management system. It will complete the back-to-source service configuration by enabling the policy on each sourcing MCDN node.

Table 9-1 provides the basic parameters for the back-to-source service configuration table, which is used to enable the back-to-source policy.

Table 9-1 – Basic parameters for back-to-source service configuration table

Name	Type	Mandatory (M/O)	Notes
Index	Int	M	It is a sequence number used to identify each record.
ProviderID	String	M	The unique identification for a content provider in a certain domain.
OriginURLMode	Int	M	It indicates which sourcing URL mode will be used: 0 – The original user request URL, including all parameters 1 – The dedicated sourcing URL
URLReplaceRule	String	O	It indicates which URL placing rule should be used: If OriginURLMode is "1", a new sourcing URL should be created from the original user request URL. If OriginURLMode is "0", "NULL" is applied.

Table 9-2 provides an example of protocols and messages exchanged between an SP network management system and an MCDN network management system.

Table 9-2 – Parameters for back-to-source service configuration table

Adding back-to-source service configuration
Protocol: SOAP
From: SP network management To: MCDN network management
Request Message: AddContentOriginConfRsp addContentOriginConf(AddContentOriginConfReq addContentOriginConfReq)

Table 9-2 – Parameters for back-to-source service configuration table

Adding back-to-source service configuration

Request example:

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
<SOAP-ENV:Header/>
<SOAP-ENV:Body>
<oxy:addContentAccessConf xmlns:oxy=http://glsb.sg16.com/
SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
<addContentAccessConfReq>
<Index>1</Index>
<ProviderID>1</ProviderID>
<ProviderType>0</ProviderType>
</addContentAccessConfReq>
</oxy:addContentAccessConf>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Response example:

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
<SOAP-ENV:Header/>
<SOAP-ENV:Body>
<oxy:addContentAccessConf xmlns:oxy="http://glsb.sg16.com/"
SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"/>
<addContentAccessConfReturn>
<resultCode>0</resultCode>
<resultMsg>Operation Succeed.</resultMsg>
</addContentAccessConfReturn>
</oxy: addContentAccessConf >
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

9.3.4 Back-to-source service procedure flows

9.3.4.1 IP address-based sourcing

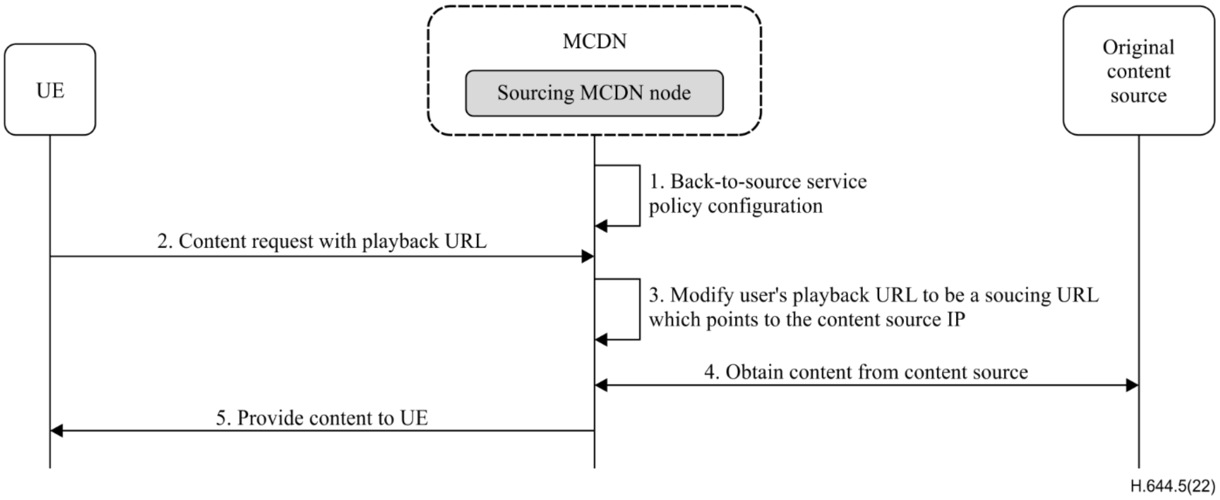

UE
MCDN
Sourcing MCDN node
Original content source
1. Back-to-source service policy configuration
2. Content request with playback URL
3. Modify user's playback URL to be a soucing URL which points to the content source IP
4. Obtain content from content source
5. Provide content to UE
H.644.5(22)

Figure 9-11 – IP address-based sourcing procedure flows

Figure 9-11 describes the procedure flows for the IP address-based sourcing method defined in clause 9.3.2.1. The main steps include:

1) The MCDN management system enables the back-to-source service policy on sourcing MCDN nodes. The policy may include the setting of content request routing table, back-to-source service configuration, content service table, etc.

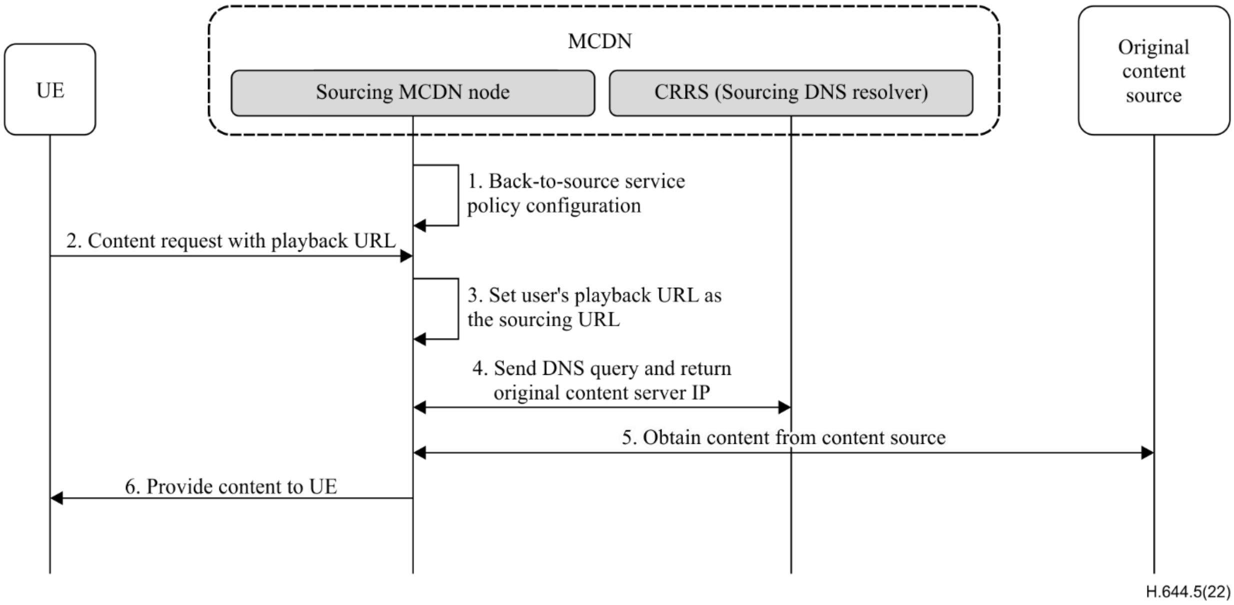
2) The UE sends a content request to the MCDN with the content URL obtained previously.

3) If there is no content in the MCDN node, the sourcing MCDN node will modify the user's content playback URL by changing it into a sourcing URL that points to the original content source IP.
For example, the user's playback URL could be "*http://glsb.sg16.com/q13/OTT00001/index.m3u8?param1*". According to the back-to-source policy, the sourcing node can change the above URL into *http://202.185.163.24/OTTvideo/00001/index.m3u8?param1, where 202.185.163.24 is the original content source IP address.*

4) The MCDN therefore obtains the content from the original content source.

5) The MCDN sourcing node can provide the content dispatching service while the content is downloading. Then the MCDN edges node can provide content delivery service to the end-user.

9.3.4.2 Domain name-based sourcing



MCDN
UE
Sourcing MCDN node
CRRS (Sourcing DNS resolver)
Original content source
1. Back-to-source service policy configuration
2. Content request with playback URL
3. Set user's playback URL as the sourcing URL
4. Send DNS query and return original content server IP
5. Obtain content from content source
6. Provide content to UE
H.644.5(22)

Figure 9-12 – Domain name-based sourcing procedure flows

Figure 9-12 describes the procedure flows for the domain-name based sourcing method defined in clause 9.3.2.1. The main steps include:

1) The MCDN management system enables the back-to-source service policy to sourcing MCDN nodes. The policy may include the setting of content request routing table, back-to-source service configuration, content service table, etc.

2) The UE sends a content request to the MCDN with the content URL obtained previously.

3) If there is no content in the MCDN node, the sourcing MCDN node will set the user's content playback URL as the sourcing URL.

4) The sourcing MCDN node sends the DNS query to CRRS/Sourcing DNS resolver. CRRS returns the response with the original content source server IP. The DNS resolve result can be cached in the sourcing MCDN node.

5) The MCDN therefore obtains content from the original content source.

6) The MCDN sourcing node can provide the content dispatching service while the content is downloading. Then MCDN edges node can provide content delivery service to the end-user.

9.3.4.3 DNS scheduling-based sourcing

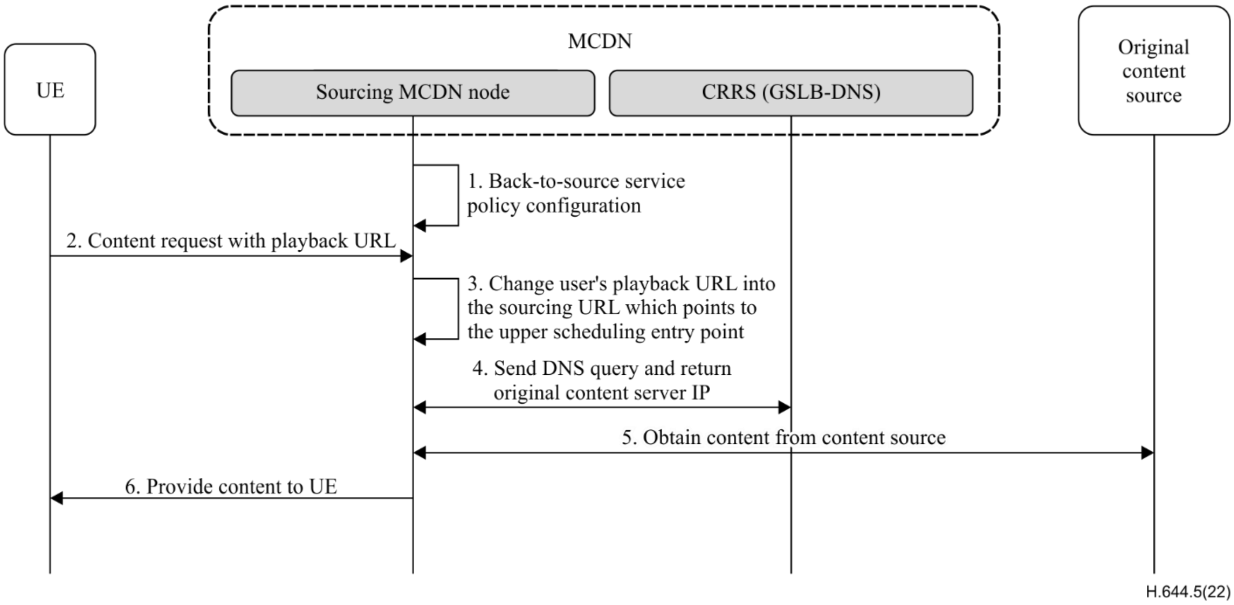

MCDN
UE
Sourcing MCDN node
CRRS (GSLB-DNS)
Original content source
1. Back-to-source service policy configuration
2. Content request with playback URL
3. Change user's playback URL into the sourcing URL which points to the upper scheduling entry point
4. Send DNS query and return original content server IP
5. Obtain content from content source
6. Provide content to UE
H.644.5(22)

Figure 9-13 – DNS based sourcing procedure flows

Figure 9-13 describes the procedure flows for DNS scheduling-based on the sourcing method defined in clause 9.3.2.2. The main steps include:

1) The MCDN management system enables the back-to-source service policy to sourcing MCDN nodes. The policy may include the setting of content request routing table, back-to-source service configuration, content service table, etc.

2) The UE sends a content request to the MCDN with the content URL obtained before.

3) If there is no content in the MCDN node, the sourcing MCDN node will modify the user's content playback URL as the sourcing URL which points to the upper scheduling entry point, i.e., CRRS/DNS.

4) The sourcing MCDN node sends the DNS query to CRRS. CRRS returns the response with the original content source server IP. The DNS resolve result can be cached in the sourcing MCDN node.

5) The MCDN therefore obtains content from the original content source.

6) The MCDN sourcing node can provide the content dispatching service while the content is downloading. Then MCDN edges node can provide content delivery service to the end-user.

9.3.4.4 Application-layer scheduling-based sourcing

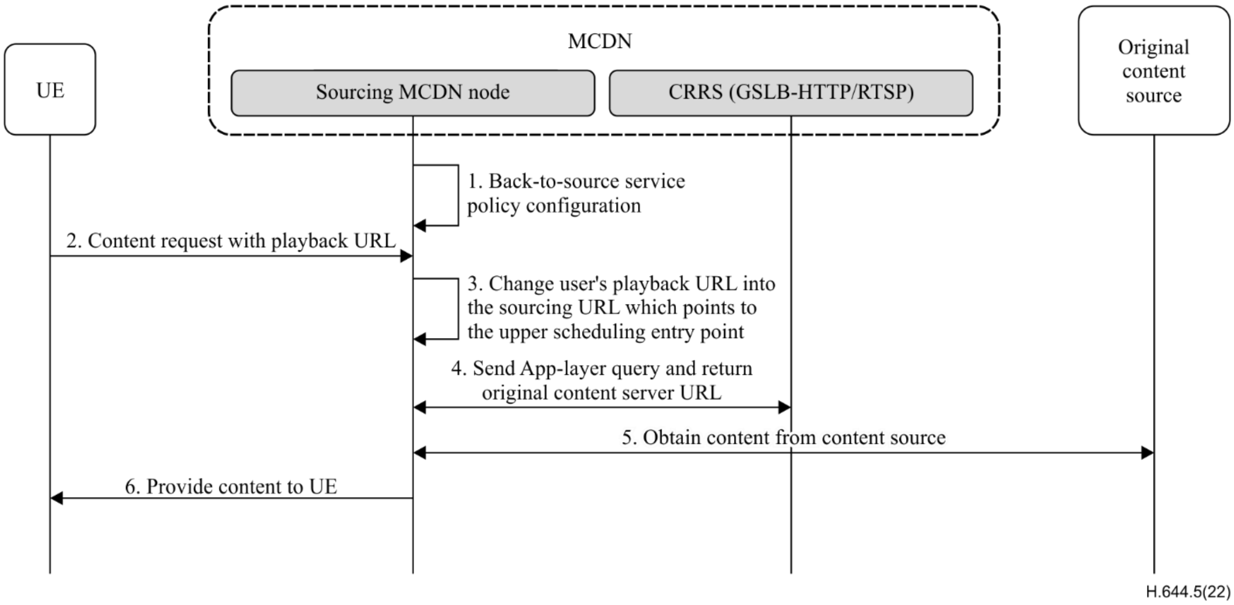

MCDN
UE
Sourcing MCDN node
CRRS (GSLB-HTTP/RTSP)
Original content source
1. Back-to-source service policy configuration
2. Content request with playback URL
3. Change user's playback URL into the sourcing URL which points to the upper scheduling entry point
4. Send App-layer query and return original content server URL
5. Obtain content from content source
6. Provide content to UE
H.644.5(22)

Figure 9-14 – Application-layer based sourcing procedure flows

Figure 9-14 describes the procedure flows for the application-layer based sourcing method defined in clause 9.3.2.2. The main steps include:

1) The MCDN management system enables the back-to-source service policy to MCDN nodes. The policy may include the setting of content request routing table, back-to-source service configuration, content service table, etc.

2) The UE sends a content request to the MCDN with the content URL obtained previously.

3) If there is no content in the MCDN node, the sourcing MCDN node will modify the user's content playback URL as the sourcing URL which points to the upper scheduling entry point, i.e., GSLB-HTTP/RTSP.

4) The sourcing MCDN node sends the application-layer request to CRRS. CRRS returns the response with the original content source server URL.

5) The MCDN therefore obtains content from the original content source.

6) The MCDN sourcing node can provide the content dispatching service while the content is downloading. Then MCDN edge node can provide content delivery service to the end-user.

Appendix I

Use cases of content request routing procedures over multiple network environments

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

The following diagram shows the general user request processing principle. In the conventional IPTV or OTT user scenarios, the CRRS helps the end-user to attach to the nearest media service node by using DNS redirection based on the user's IP or using application-level redirection based on the content URI. In the traditional fixed-line or mobile network, the IP address for the CDN server in the public Internet or in an operator's dedicated network is permanent in most cases. However, in the current market, by taking advantage of virtualization technology, the media server or the CDN node can be virtualized and be deployed in an edge network deeper than before. Moreover, many media streaming services can be consumed by a mobile device while the device holder is moving. All those scenarios may cause the unpredictability regarding the real user or server location if only an IP address is used.

Therefore, the CRRS should upgrade its user request routing mechanism by detecting the real user location. The location information may be retrieved from many places such as the mobile core network, pre-configuration in CDN manager, etc. The routing mechanism may be adopted according to the different network environments.

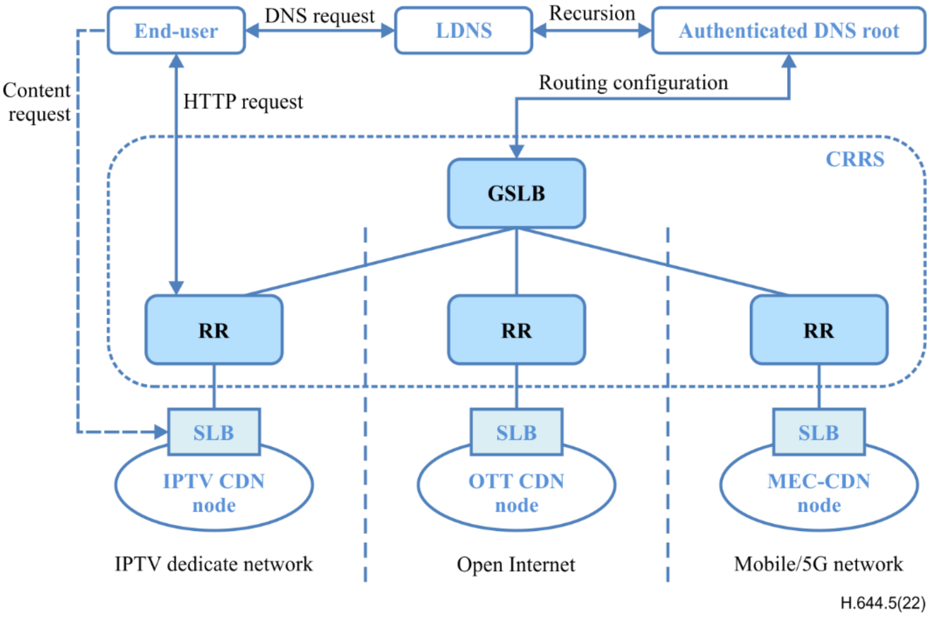


Figure I.1 – Use case of CRRS in different network environments

Bibliography

[b-ITU-T F.743.10] Recommendation ITU-T F.743.10 (2019), *Requirements for mobile edge computing-enabled content delivery networks*.

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

[b-ITU-T Y.1901] Recommendation ITU-T Y.1901 (2009), *Requirements for the support of IPTV services*.

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

[b-DNSCurve] DNSCurve: Usable security for DNS. https://dnscurve.org (viewed 2023-03-24).

[b-IETF-RFC 4033] IETF RFC 4033 (2005), *DNS Security Introduction and Requirements*.

[b-IETF RFC 7871] Informational RFC 7871 (2016), *Client Subnet in DNS Queries*.

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

Published in Switzerland
Geneva, 2023