International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2253

(01/2014)

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

Next Generation Networks – Service aspects: Interoperability of services and networks in NGN

Capabilities of multi-connection to support streaming services

Recommendation ITU-T Y.2253

ITU-T Y-SERIES RECOMMENDATIONS

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

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

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

Recommendation ITU-T Y.2253

Capabilities of multi-connection to support streaming services

Summary

The objective of this Recommendation is to describe the requirements for the network transport capabilities and the service layer to support streaming services over multi-connection. It also defines the characteristics of the streaming service over multi-connection.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.2253	2014-01-13	13	11.1002/1000/12073-en

Keywords

Multi-connection architecture, NGN, streaming service.

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

FOREWORD

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

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

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

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

NOTE

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

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

INTELLECTUAL PROPERTY RIGHTS

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

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

Table of Contents

Recommendation ITU-T Y.2253

Capabilities of multi-connection to support streaming services

1 Scope

This Recommendation describes the requirements, architecture, information flows and other aspects such as security and charging for streaming services over multi-connection.

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 G.722] Recommendation ITU-T G.722 (2012), *7 kHz audio-coding within 64 kbit/s*.

[ITU-T H.264] Recommendation ITU-T H.264 (2014), *Advanced video coding for generic audiovisual services*.

[ITU-T X.200] Recommendation ITU-T X.200 (1994) | ISO/IEC 7498-1:1994, *Information technology – Open Systems Interconnection – Basic Reference Model: The basic model*.

[ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open System Interconnection for CCITT applications*.

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

[ITU-T Y.2233] Recommendation ITU-T Y.2233 (2010), *Requirements and framework allowing accounting and charging capabilities in NGN*.

[ITU-T Y.2251] Recommendation ITU-T Y.2251 (2011), *Multi-connection requirements*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 access control [ITU-T X.800]: The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.

3.1.2 authorization [ITU-T X.800]: The grant of rights, which includes the granting of access based on access rights.

3.1.3 availability [ITU-T X.800]: The property of being accessible and useable upon demand by an authorized entity.

3.1.4 confidentiality [ITU-T X.800]: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

3.1.5 connection [ITU-T X.200], clause 5.3.3.2.1: A connection is an association established for the transfer of data between two or more peer-(N)-entities. This association binds the peer-(N)-entities together with the (N-1)-entities in the next lower layer.

3.1.6 content protection [ITU-T Y.1901]: Ensuring that an end-user can only use the content they have already acquired in accordance with the rights that they have been granted by the rights holder.

3.1.7 data integrity [ITU-T X.800]: The property that data has not been altered or destroyed in an unauthorized manner.

3.1.8 data origin authentication [ITU-T X.800]: The corroboration that the source of data received is as claimed.

3.1.9 denial of service [ITU-T X.800]: The prevention of authorized access to resources or the delaying of time-critical operations.

3.1.10 Internet Protocol Television (IPTV) [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.

3.1.11 mobility [b-ITU-T Q.1706]: The ability for the user or other mobile entities to communicate and access services irrespective of changes of the location or technical environment.

3.1.12 multi-connection [ITU-T Y.2251]: The functionality which provides capability to the user equipment (UE) and network to maintain more than one access network connection simultaneously.

NOTE 1 – All connections are coordinated to provide service to higher layer entities.

NOTE 2 – In a multi-connection communications at least one UE is required to be a multi-connection UE.

3.1.13 next generation network (NGN) [b-ITU-T Y.2001]: A packet-based network able to provide telecommunication services and able to make use of multiple broadband, QoS-enabled transport technologies and in which service-related functions are independent from underlying transport related technologies. It enables unfettered access for users to networks and to competing service providers and/or services of their choice. It supports generalized mobility which will allow consistent and ubiquitous provision of services to users.

3.1.14 offline charging [ITU-T Y.2233]: Charging mechanism where charging information does not affect, in real-time, the service rendered.

3.1.15 online charging [ITU-T Y.2233]: Charging mechanism where charging information can affect, in real-time, the service rendered and therefore a direct interaction of the charging mechanism with resource/session/service control is required.

3.1.16 service protection [ITU-T Y.1901]: Ensuring that an end-user can only acquire a service, and, by extension, the content contained therein, that he or she is entitled to receive.

3.1.17 terminal device [ITU-T Y.1901]: An end-user device which typically presents and/or processes the content, such as a personal computer, a computer peripheral, a mobile device, a TV set, a monitor, a VoIP terminal or an audiovisual media player.

3.1.18 terminal device protection [ITU-T Y.1901]: Ensuring that a terminal device employed by an end-user in the reception of a service can reliably and securely use content while enforcing the rights of use granted for that content, and while physically and electronically protecting the integrity of the terminal device, and the confidentiality of the content and critical security parameters not otherwise protected by encryption or watermarking.

3.1.19 threat [ITU-T X.800]: A potential violation of security.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 MC-Streaming (streaming service over multi-connection): Streaming service over multi-connection provides multimedia features such as video/audio/text/graphics/data in real time supported by the required level of QoS/QoE, security, interactivity and reliability.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AC-FE Application Control Functional Entity
ACK Acknowledgement
AN Access Network
ANI Application Network Interface
AP Access Point
BS Base Station
CDN Content Delivery Network
CDR Charging Data Record
CS Circuit Switched
DDoS Distributed Denial Of Service
DES Data Encryption Standard
DNS Domain Name System
DoS Denial of Service
DRM Digital Rights Management
IDS Intrusion Detection System
IP Internet Protocol
IPSec Internet Protocol Security
IPTV Internet Protocol Television
MAS-F Multi-connection Application Support Function
MC-FE Multi-connection Coordination Functional Entity
MMF Multi-connection Media Function
MPC-FE Multi-connection Policy Control Functional Entity
MR-FE Multi-connection Registration Functional Entity
MSAC-FE MC-Streaming Application Control Functional Entity
MSCC-FE MC-Streaming Content Control Functional Entity
MSCD-FE MC-Streaming Content Delivery Functional Entity
MSUP-FE MC-Streaming Application-User Profile Functional Entity
MUE Multi-connection User Equipment
MUP-FE Multi-connection User Profile Functional Entity
NGN Next Generation Network

OAM&P	Operations, Administration, Maintenance and Provisioning
OCS	Online Charging System
P2P	Peer-to-Peer
PDA	Personal Digital Assistant
PIN	Personal Identification Number
PS	Packet Switched
QoE	Quality of Experience
QoS	Quality of Service
RSA	RSA algorithm by Ron Rivest, Adi Shamir and Leonard Adleman
SCF	Service Control Function
SIP	Session Initiation Protocol
SSL	Security Socket Layer
SSO	Single Sign On
TV	Television
UE	User Equipment
VoD	Video on Demand
WLAN	Wireless LAN

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 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 specification can still be claimed even if this requirement is presented.

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.

6 Service definition and general requirements

6.1 Service definition

MC-Streaming (streaming service over multi-connection) is a streaming service which is supported by the multi-connection architecture to provide multimedia service features such as video/audio/text/graphics/data in real time and provides the required level of QoS/QoE, security, interactivity and reliability to its users.

The terms MUE and UE are used in this Recommendation to distinguish full support of MC-Streaming by the multi-connection architecture and the MC-Streaming functional elements, or only required support of MC-Streaming by any UE accessing the multi-connection network streaming services.

Different from traditional streaming services over single connection environments, MC-Streaming provides more features and better experience in a multi-connection environment, e.g., smoother stream playback with broader bandwidth, stream composition from different sources, stream decomposition to multiple devices, service continuity by transferring data flows among multiple network accesses, etc.

6.2 General requirements

The general requirements of MC-Streaming can be classified into four categories: multimedia content, interaction, QoS/QoE and utilization of MC-Streaming.

6.2.1 Multimedia content requirement

1) MC-Streaming has all the features of current streaming services. Various kinds of multimedia content (i.e., video/audio/text/graphics/data) can be rendered at the same time and in real time.
2) MC-Streaming is recommended to support different media types (e.g., audio and video) as well as formats (e.g., [ITU-T G.722]) to be delivered from a single source to one or multiple destinations/UE.
3) MC-Streaming is recommended to support the delivery of multimedia content throughout different connections simultaneously, especially when multi-connection capability is supported by underlying network elements and accesses.
4) MC-Streaming can optionally support multiple kinds of coding resolutions and aspects ratios (e.g., ITU-T H.264 video compression).
5) MC-Streaming can optionally support live and/or video on-demand (VoD) content offering.
6) MC-Streaming can optionally support content or programme selection.
7) MC-Streaming can optionally support integration with other telecommunication services (e.g., instant message, presence, telephony, etc.).
8) Multimedia content can optionally be transmitted to a single destination (e.g., VoD), or to multiple destinations simultaneously (e.g., broadcasting service).

6.2.2 Interaction requirement

1) User interaction is recommended to be supported. Service provider and subscriber of MC-Streaming can share interesting information within or between them, including programme information, image, data, text, audio, etc.
2) MC-Streaming can optionally support interactive capabilities such as educational applications, entertainment applications (e.g., games), communication services (e.g., mail, chat and messaging), and information services (e.g., stock and weather services).

3) MC-Streaming can optionally support user generated content to be uploaded and shared to other subscribers.

4) MC-Streaming can optionally support download of user generated content.

5) MC-Streaming can optionally support mechanisms for users to send user preferences to the server during a streaming session, so that the service providers may offer personalized content markers to the users.

6) MC-Streaming can optionally enable a subscriber to share content marker(s) with other subscribers in accordance to legal aspects and operator policies.

7) MC-Streaming can optionally support content pushing by the service provider to the UE, which can be requested or not requested by subscriber.

8) MC-Streaming can optionally support content filtering mechanisms so that a subscriber can filter unwanted content.

6.3 QoS/QoE requirements

The requirements of quality of service (QoS) and quality of experience (QoE) are listed below:

1) MC-Streaming is recommended to support a subscriber's required level of QoS/QoE, security and reliability.

2) MC-Streaming is recommended to support service continuity (i.e., seamless connection handover).

3) MC-Streaming is recommended to support service control to provide a quality at least as good as the quality of any individual access technology under its control.

4) MC-Streaming is recommended to allow the delivery of MC-Streaming services with a subscriber's defined quality of experience (QoE).

5) MC-Streaming can optionally support mechanisms to monitor audio and video quality.

6) MC-Streaming can optionally support consistent QoS.

7) MC-Streaming can optionally support mechanisms for QoE/QoS parameters adjustment due to the changes of content characteristics in a connection.

6.4 Use case of MC-Streaming

MC-Streaming can be utilized in scenarios, such as:

1) Traditional Internet protocol television (IPTV). Subscribers can receive multimedia information using different kinds of connections. This scenario includes linear TV, on demand services (i.e., video on demand and content on demand). Subscribers can playback the content after its initial transmission. Subscribers can also pause, rewind or forward stored content.

2) Pushing interaction information. MC-Streaming providers can push some content towards the subscribers (e.g., most popular programme guides, advertisements, subscribers' on-demand programmes, etc.). Subscribers can also share information of interest, e.g., programme, image, data and audio.

7 Network and MUE requirements

7.1 Network transport capability requirements

1) MC-Streaming is recommended to support and use connection related information (e.g., bandwidth, subscriber's preferences, QoS, etc.) to select one or more appropriate connections to deliver multimedia content.

2) MC-Streaming can optionally support maintaining simultaneous CS and PS applications over different access technologies.

7.1.1 Admission control

1) MC-Streaming is required to support authentication and authorization of subscribers to the utilized access network(s).

2) MC-Streaming can optionally support access network selection, e.g., according to QoS requirements, network status, UE status, subscriber's preferences or operator's policies. In this latter case, the selection mechanism is recommended to provide consistent QoS for subscribers' experience.

7.1.2 Transport control

1) MC-Streaming is recommended to support delivery of multimedia content over different access networks simultaneously, e.g., 2G/3G/WLAN, especially when multi-connection capability is supported by underlying network elements.

2) MC-Streaming is recommended to provide efficient usage of multiple access networks.

3) MC-Streaming is recommended to coordinate the transmission of multimedia content over multiple networks.

7.1.3 Mobility support

1) MC-Streaming can optionally support service continuity in case multiple access networks are connected to the UE.

2) MC-Streaming can optionally provide the same service experience when the subscriber roams into another operator's network.

3) MC-Streaming can optionally support switching from one subscriber's UE to another.

7.1.4 Security support

1) MC-Streaming is required to support authentication and authorization of the subscriber and her/his UE.

2) MC-Streaming is required to prevent unauthorized usage.

3) MC-Streaming is required to deliver content only to appropriate subscribers.

4) MC-Streaming can optionally identify and block illegal or unwanted traffic by itself, or rely on other network elements' support.

5) MC-Streaming can optionally prevent unauthorized network topology discovery by itself, or rely on other network elements' support.

7.2 MUE requirements

The MC-Streaming MUE:

1) Is required to support multiple network connections simultaneously, and it is recommended to support more than one kind of access network.

2) Is recommended to support more than one kind of video and audio formats.

3) Is required to support subscriber authentication and identification management.

4) Is recommended to support synchronization and composition of media flows received from different network connections.

5) Can optionally support user interaction, including programme selection, play, pause, fast forward, rewind, recording, replay, etc.

6) Can optionally support user generated content to be uploaded and shared to other subscribers.

7) Can optionally support acquiring and collecting equipment capability by the network to provide better service provisioning.

8) MC-Streaming is recommended to support various types of user equipment, e.g., mobile phone, PDA, personal computer, pad, etc.

8 Architecture

8.1 General architecture

The architecture of MC-Streaming impacts all layers of the multi-connection architecture. Some new functional entities are introduced into the application layer. Figure 8-1 provides an overview of the MC-Streaming functional architecture.

The general architecture of MC-Streaming provides the following major functionality, it:

a) Receives MC-Streaming related requests from the MUE and provides user interaction capabilities.

b) Provides authentication and authorization for MC-Streaming.

c) Obtains original content from the content provider.

d) Pre-processes original content to make it appropriate to be transferred over access networks.

e) Delivers content to the MUE using network resources from multiple networks.

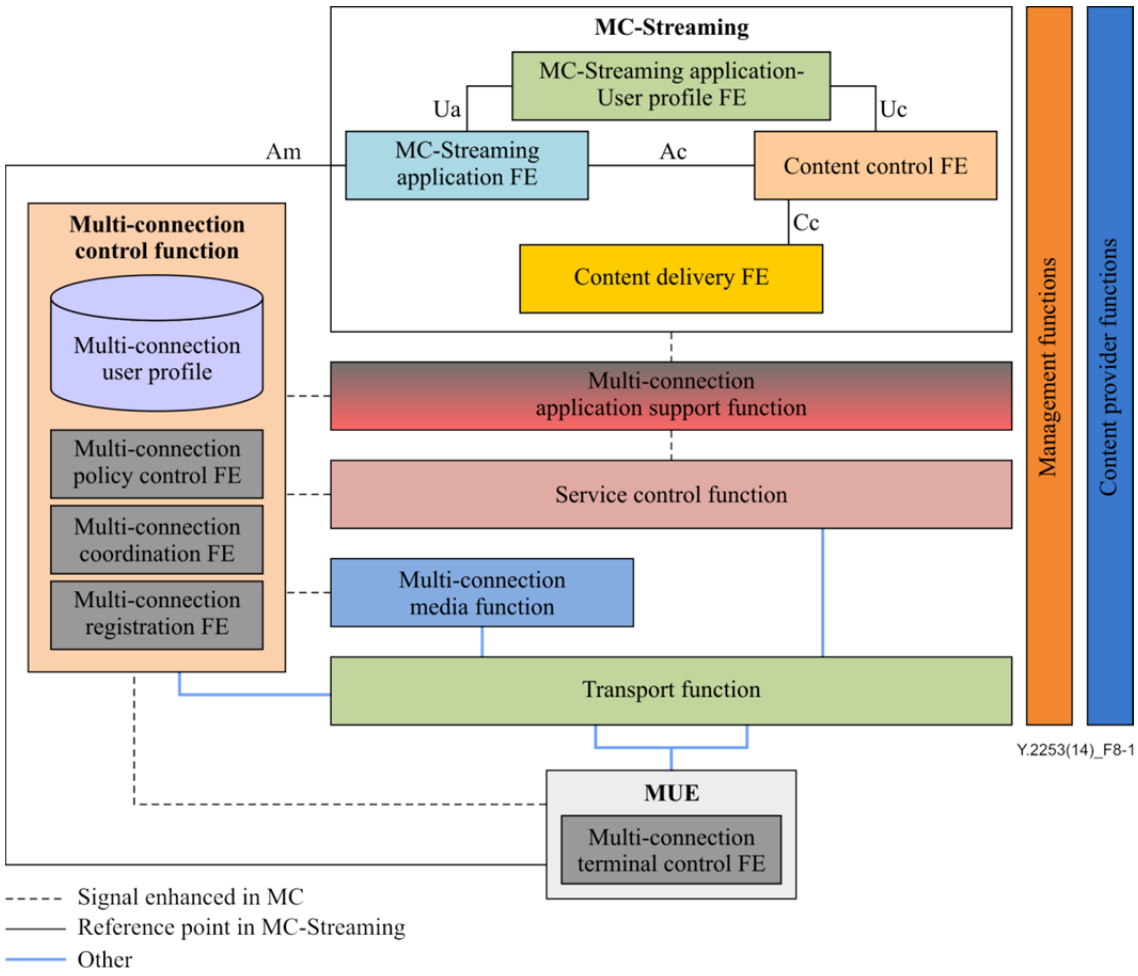

Figure 8-1 – MC-Streaming architecture

8.2 High level description of functions

8.2.1 Management functions

The management functions are a set of functions providing operation, administration, maintenance, and provisioning (OAM&P) for the MC-Streaming service. Network operators can deploy this set of functions in a centralized or in a distributed environment. The detailed discussion is outside the scope of this Recommendation, and is not discussed herein.

8.2.2 Content provider functions

This set of functions is offered by authorized entities owning content copyright. Content provider functions provide the content and associated metadata (e.g., content-protection-rights sources, content sources, and metadata sources for the streaming service) for content control. Since this part is offered by third parties, it is also outside the scope of this Recommendation.

8.3 Functional entities

Functional entities in MC-Streaming impact all the functional entities in the multi-connection architecture. But, additionally, four new entities are introduced in the application layer:

1. MSAC-FE
2. MSUP-FE
3. MSCC-FE
4. MSCD-FE

Figure 8-2 shows the functional entities in the MC-Streaming architecture.

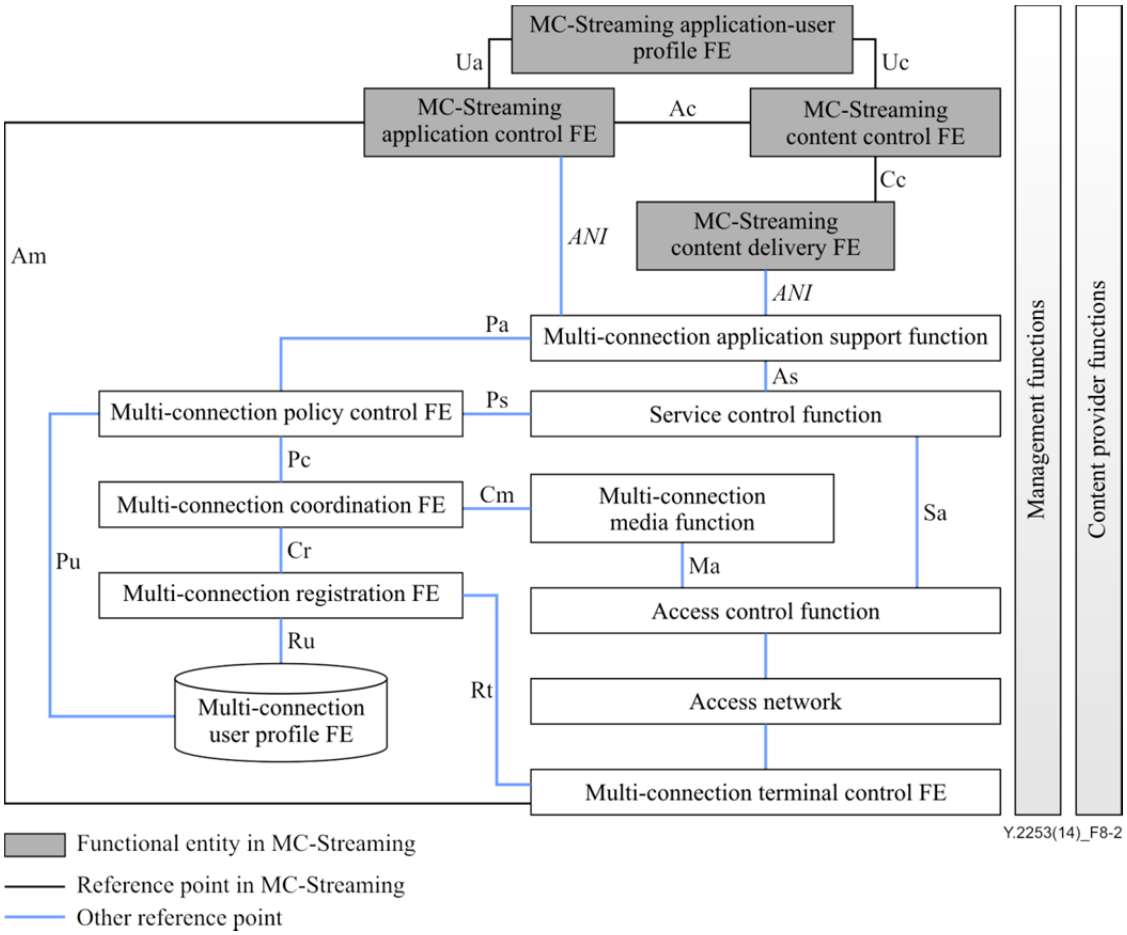

Figure 8-2 – Functional entities in MC-Streaming architecture

8.3.1 MC-Streaming application control functional entity (MSAC-FE)

MSAC-FE allows multi-connection devices, i.e., the MUE, to choose and/or purchase content on demand. When it receives a request from a MC-Streaming device, MSAC-FE fulfils authentication and authorization by interacting with MSUP-FE, or with related information obtained from MSUP-FE. MSAC-FE provides application control logic based on the application-user profile, content metadata and other relevant information. MSAC-FE is also responsible for interaction control, such as programme selection, and forwarding and rewinding. Interaction between users (i.e., "users share programmes among friends") is one of the MSAC-FE's responsibilities.

If needed, MSAC-FE can optionally request or inspect the content preparation procedure, which is fulfilled by MSCC-FE, since MSAC-FE is able to interact with the MUE and can obtain some MUE or user related information.

8.3.2 MC-Streaming application-user profile functional entity (MSUP-FE)

MSUP-FE stores relevant information about streaming application and service subscribers. Information in MSUP-FE can optionally include:

a) Global settings (e.g., language preference).

b) Capabilities of MC-Streaming terminal devices.

c) Authentication and authorization information of MC-Streaming terminal devices and subscribers.

d) MC-Streaming service settings, e.g., linear TV settings, on demand service settings, etc.

e) User preferences and subscription information, such as user specific settings, programmes being ordered, etc.

f) Security and privacy settings, e.g., required security level of a subscriber, parent control information, etc.

8.3.3 MC-Streaming content control functional entity (MSCC-FE)

MSCC-FE provides content management and control functions. It is responsible for content preparation and content protection. MSCC-FE can optionally provide content distribution functions.

a) Content preparation

MSCC-FE is responsible for preparing and aggregating the contents as received from the content provider functions. MSCC-FE may edit the content or insert some watermark for content tracing before dispatching it to other functional entities.

b) Content protection

MSCC-FE is responsible for protecting the service and contents from illegal access. This is performed by verifying the subscriber's or service authorization, according to the subscriber's profile, subscription information and authorization token. Encryption methods and access control mechanisms (e.g., role based access control) can be employed to fulfil this functionality.

c) Content distribution

MSCC-FE can optionally provide content distribution function in some cases, especially if the multi-connection architecture is not supported by the underlying network. Content delivery mechanisms and technologies (e.g., CDN, multicasting, broadcasting, and P2P overlay network) can be employed; this is decided according to the existing underlying network, operation requirements, etc.

8.3.4 MC-Streaming content delivery functional entity (MSCD-FE)

MSCD-FE is responsible for delivering streaming content from MSCC-FE to the subscriber. In this Recommendation, the multi-connection architecture is the preferred model to provide content delivery. However if the multi-connection architecture is not supported, existing distribution mechanisms such as multicast, P2P and CDN can also be employed.

In other words, the content is recommended to be delivered through different connections simultaneously. Based on the underlying distribution mechanisms, MSCD-FE may cooperate with related entities to fulfil content delivery. For example, MSCD-FE may cooperate with MAS-F in the multi-connection environment. In addition, MSCD-FE is recommended to coordinate the transmission of content over different connections, according to connection related information, e.g., bandwidth, QoS, user preferences, etc. When the multi-connection architecture is not supported, MSCD-FE may cooperate with the underlying P2P network to distribute content from/to multiple peer nodes.

MSCD-FE is responsible to cache and store content and associated information.

MSCD-FE is recommended to interact with MAS-F to deliver content in coordination with the multi-connection architecture. Thus, emphasizing, the multi-connection architecture is the preferred technology to support MC-Streaming.

MSCD-FE can optionally support insertion, watermarking, transcoding and encryption pertaining to the content.

Finally, MSCD-FE can optionally generate charging information.

8.4 Reference points

8.4.1 Reference point Ua

The Ua reference point exists between the MC-Streaming application control FE (MSAC-FE) and the MC-Streaming application-user profile functional entity (MSUP-FE).

Through this reference point, MC-Streaming application control FE (MSAC-FE) retrieves application and user profiles. These profiles include authorization information (e.g., whether the subscriber is permitted to view the specific programme), service settings, user preferences, etc.

8.4.2 Reference point Uc

The Uc reference point exists between the MC-Streaming application-user profile functional entity (MSUP-FE) and MC-Streaming content control functional entity (MSCC-FE).

Through this reference point, MC-Streaming content control functional entity (MSCC-FE) obtains security-related information and content authorization information from the MC-Streaming application-user profile functional entity (MSUP-FE) such as the subscriber's right to access a specific content. Uc is designed for content authorization control (i.e., content security control).

8.4.3 Reference point Ac

The Ac reference point exists between the MC-Streaming application control functional entity (MSAC-FE) and MC-Streaming content control functional entity (MSCC-FE).

Through this reference point, the MC-Streaming application control functional entity (MSAC-FE) can optionally obtain service metadata and content protection information stored in MC-Streaming content control functional entity (MSCC-FE).

The MC-Streaming application control functional entity (MSAC-FE) is recommended to use this reference point to send service control and user interaction information to MC-Streaming content control functional entity (MSCC-FE), such as play, fast forwarding, rewinding, pause, stop, etc. If needed, the MSAC-FE can optionally send content control related requests to the MSCC-FE through this reference point, e.g., transcode or edit a piece of media content.

8.4.4 Reference point Am

The Am reference point exists between the MUE and MC-Streaming application control functional entity (MSAC-FE).

Through this reference point, the MUE sends the MC-Streaming related control request and subscriber's interaction requests to the MC-Streaming application control functional entity (MSAC-FE), such as a request for a specific programme.

8.4.5 Reference point Cc

The Cc reference point exists between the MC-Streaming content control functional entity (MSCC-FE) and MC-Streaming content delivery functional entity (MSCD-FE).

This reference point is used to send content from the MC-Streaming content control functional entity (MSCC-FE) to the MC-Streaming content delivery functional entity (MSCD-FE), such as specific programme content which can be delivered utilizing the underlying network.

Through this reference point, the MC-Streaming content control functional entity (MSCC-FE) also sends the MC-Streaming content delivery functional entity (MSCD-FE) the delivery control requests, e.g., starting or stopping the delivery procedure as per a subscriber's request.

9 Information flows

9.1 Authorization and streaming establishment

Before accessing a streaming service, a MUE must be verified as having permission to access the service and relevant resources, according to the subscriber's application profile. Afterwards, the streaming connections can be established. This information flow generally occurs when a user accesses the service. It is shown as Figure 9-1.

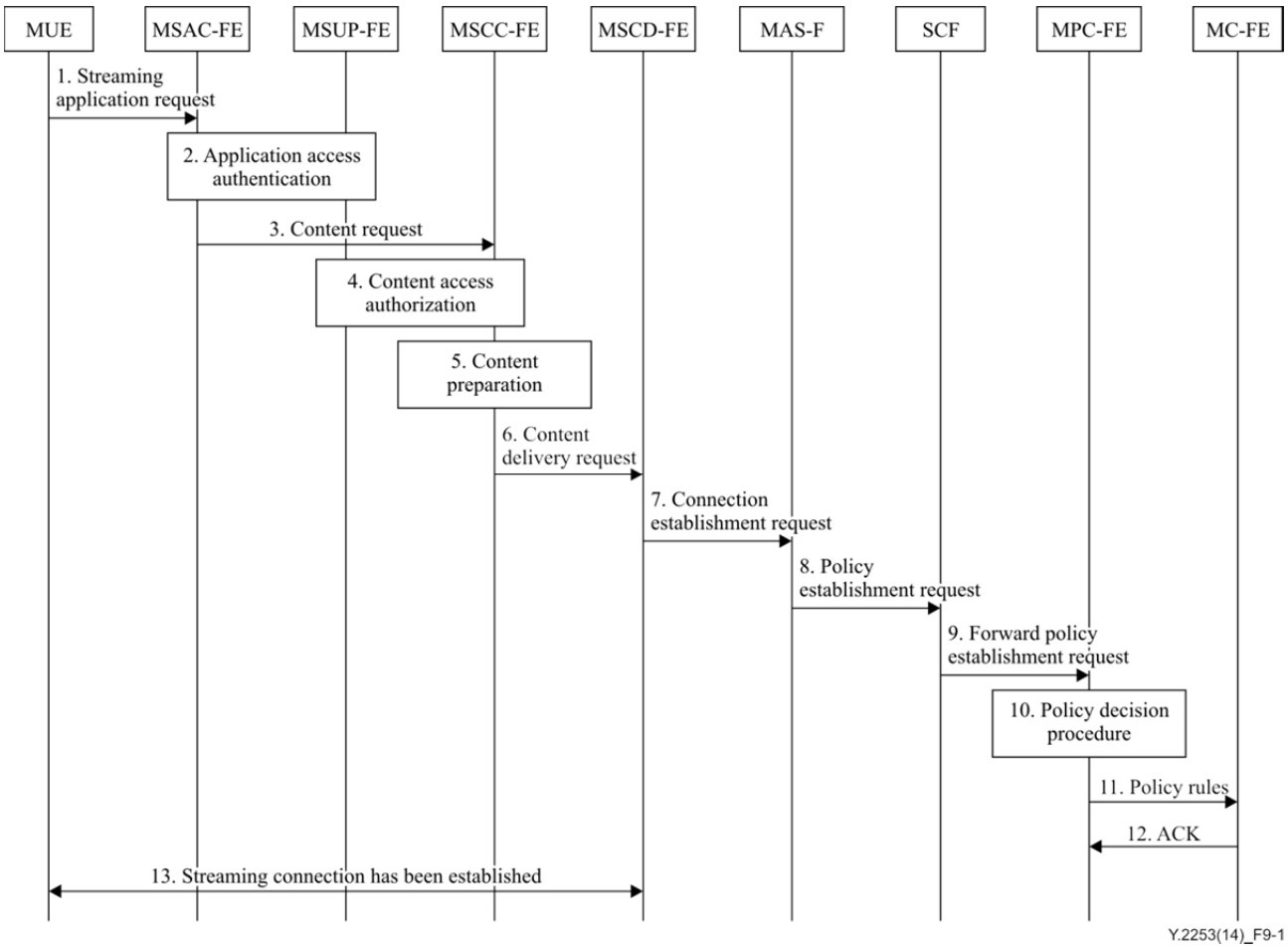

Figure 9-1 – Authorization and streaming establishment

1) MUE sends a streaming access request message to MSAC-FE, to require a specific streaming content.

2) MSAC-FE obtains streaming application and MUE information from MSUP-FE, to verify whether the MUE has the permission to access this service.

3) If the MUE has the permission, MSAC-FE sends a content request message to MSCC-FE to obtain related content.

4) MSCC-FE obtains streaming application and MUE related information from MSUP-FE, to verify whether the MUE has the permission to access the content. If it has, the MUE is authorized to access the content.

5) MSCC-FE prepares requested streaming content. The content may be previously obtained from content providers, or be transmitted in real time, e.g., in a monitoring scenario.

6) MSCC-FE sends a content delivery request message to MSCD-FE to indicate that streaming content is available for delivery.

7) MSCD-FE sends a connection establishment request to MAS-F, to request to establish connections to transport streaming content to MUE.

8) MAS-F sends policy establishment request messages to an underlying SCF, even to multiple SCFs, to request to establish a transmission policy.

9) SCF forwards this policy establishment request message to MPC-FE.

10) MPC-FE selects a set of QoS rules for a new connection based on the operator policy and the information of the new connection.

11) MPC-FE makes policy rules for the streaming based on the policies, and sends policy rules to MC-FE.

12) MC-FE sends an ACK message to MPC-FE after receiving the policy rules. Hence, the connection between the MUE and MSCD-FE is established.

13) The streaming connection(s) has been established between the MUE and MSCD-FE, and then the streaming can be transported from MSCD-FE to MUE.

9.2 Streaming decomposition

This flow shows streaming decomposition after streaming connections have been established, according to the subscriber's request, service requirements, network status, etc. The purpose of streaming decomposition is to transfer streaming flows with multiple connections to achieve the best service quality, e.g., smooth replay and no interruption. The information flow is shown in Figure 9-2.

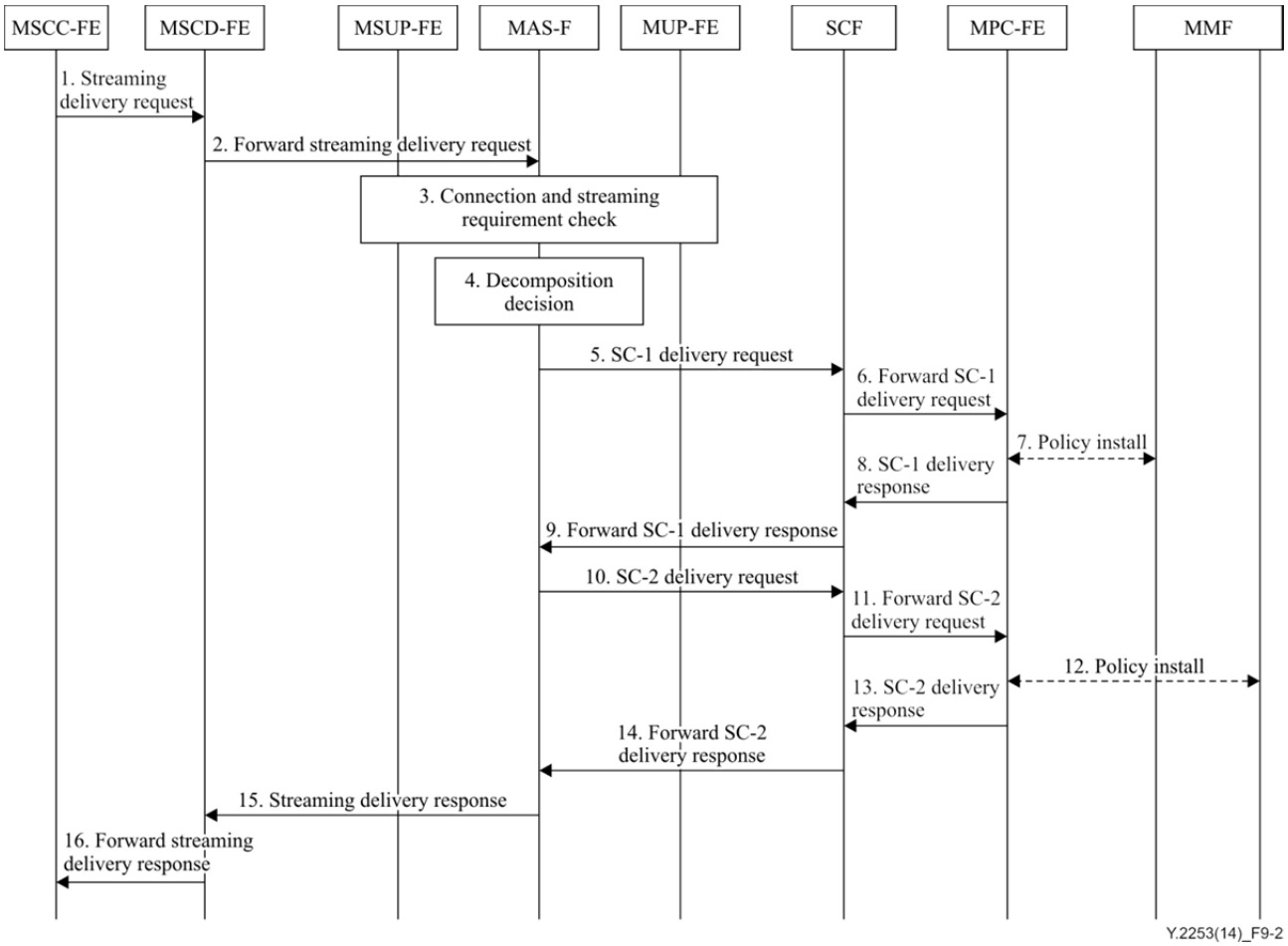

Figure 9-2 – Streaming decomposition

1) MSCC-FE sends a streaming delivery request message to MSCD-FE, to request to transfer the prepared streaming content.

2) MSCD-FE forwards this streaming delivery request message to MAS-F.

3) MAS-F obtains related information (such as available connections of the MUE, the requirements of the streaming transmission or the user's requirements, etc.) from MUP-FE and MSUP-FE to decide which one or several connections can be used to deliver the decomposed streaming flows.

4) MAS-F makes a decomposition decision according to the information already obtained.

5) After the streaming flow is split into two components, i.e., streaming component 1 (SC-1) and streaming component 2 (SC-2), MAS-F sends a delivery request message with streaming requirements to initiate a connection for SC-1.

6) SCF forwards the request message to MPC-FE, to request to establish a related transmission policy for SC-1.

7) MPC-FE makes policy rules based on QoS requirements, then sends a request to MMF to install the QoS rules for SC-1.

8) MPC-FE returns a delivery response message to SCF after the rules have been installed.

9) SCF forwards the delivery response message to MAS-F.

10) MAS-F sends a delivery request message to SCF with streaming requirements to initiate a connection for SC-2.

11) SCF forwards the request message to MPC-FE, to request to establish a related transmission policy for SC-2.

12) MPC-FE makes policy rules based on QoS requirements, then sends a request to MMF to install the rules for SC-2.

13) MPC-FE returns a delivery response message to SCF after the rules have been installed.

14) SCF forwards the delivery response message to MAS-F.

15) MAS-F returns a streaming delivery response message to MSCD-FE after the streaming components are established.

16) MSCD-FE forwards the streaming delivery response message to MSCC-FE.

9.3 Streaming composition

When multiple UE create several streaming components through multiple network interfaces, the streaming components can be composed into one to serve the application and the remote MUE. For example, multiple streaming flows from different cameras can be composed into one, which is then transferred to the end MUE in a monitoring service. The information flow is shown in Figure 9-3. This procedure happens during streaming flow establishment.

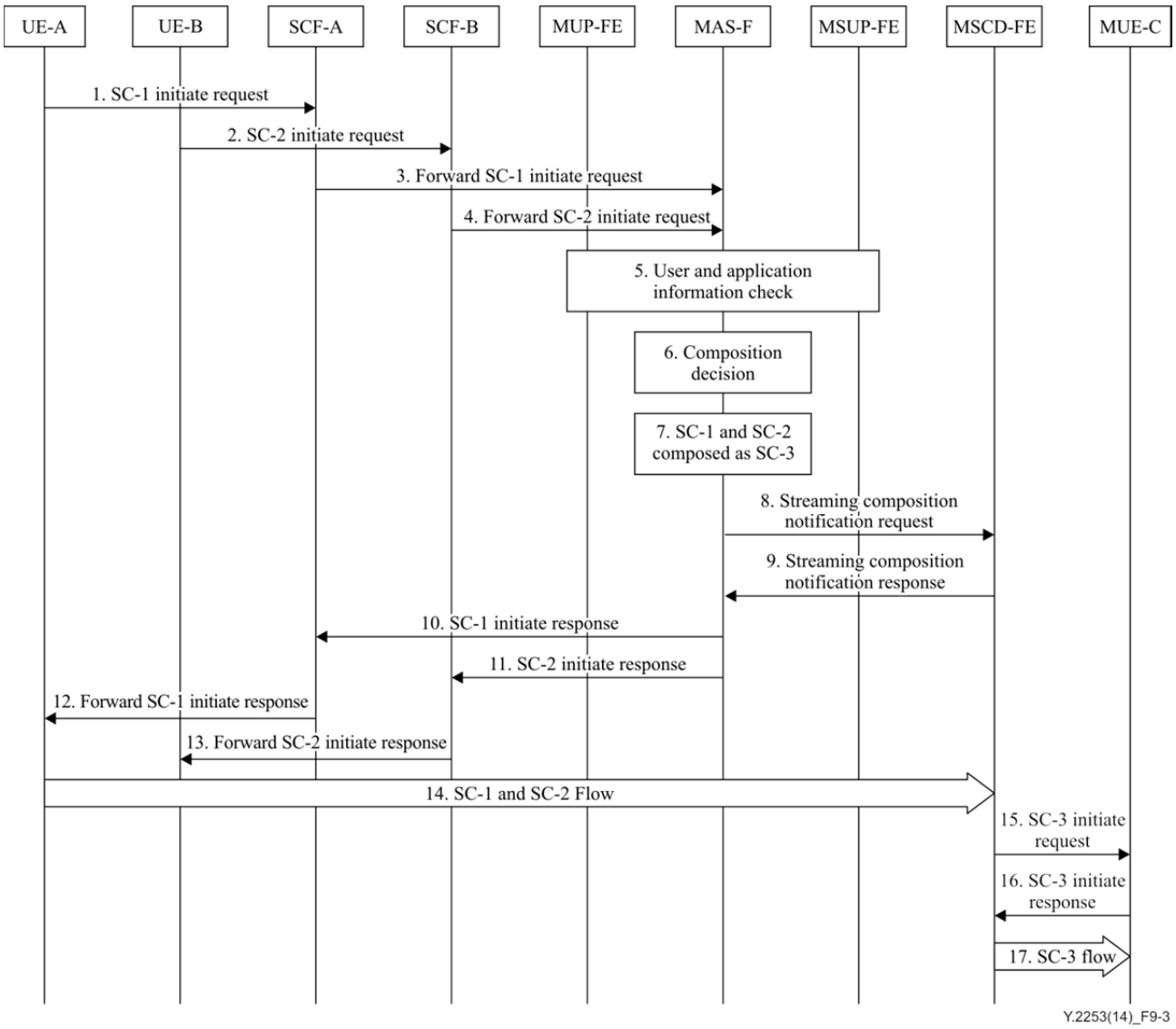

Figure 9-3 – Streaming composition

1) UE-A sends an initiation request message to SCF-A to create a streaming component (SC-1).
2) UE-B sends an initiation request message to SCF-B to create another streaming component (SC-2).
3) SCF-A forwards the initiation request message of SC-1 to MAS-F.
4) SCF-B forwards the initiation request message of SC-2 to MAS-F.
5) MAS-F obtains related information (such as the UE that the messages come from, the applications that the messages belong to, etc.) from MUP-FE and MSUP-FE, to decide whether the streaming components (SC-1 and SC-2) can be composed together.
6) MAS-F makes the composition decision according to the information already obtained.
7) MAS-F composes SC-1 and SC-2 as SC-3.
8) MAS-F sends a streaming composition notification request message to MSCD-FE, to request to compose the streaming components (i.e., SC-1 and SC-2).
9) MSCD-FE returns a streaming composition notification response message to MAS-F.
10) MAS-F returns an initiation response message for SC-1 to SCF-A.
11) MAS-F returns an initiation response message for SC-2 to SCF-B.

12) SCF-A forwards the initiation response message of SC-1 to UE-A.

13) SCF-B forwards the initiation response message of SC-2 to UE-B.

14) The streaming components (SC-1 and SC-2) are transported from UE-A and UE-B respectively, to MSCD-FE through different networks.

15) MSCD-FE sends an initiation request message for SC-3 to MUE-C.

16) MUE-C returns an initiation response message for SC-3 to MSCD-FE.

17) The streaming component of SC-3 is delivered from MSCD-FE to MUE-C through multiple networks.

9.4 Streaming transfer

After establishment, a streaming flow can be transferred from one connection to another among multiple connections, according to the subscriber's demand or network status, while the streaming service itself is not affected.

9.4.1 MUE initiated streaming transfer

After simultaneously connecting to multiple access networks, according to a subscriber's demand (for example, if the bit rate of the connection for the streaming transmission is too slow), a MUE can request the transfer of one or more streaming flows from one access network to another. In this case, the MUE is able to request a modification of the existing connection parameters. The information flow of a MUE initiated transfer is shown in Figure 9-4.

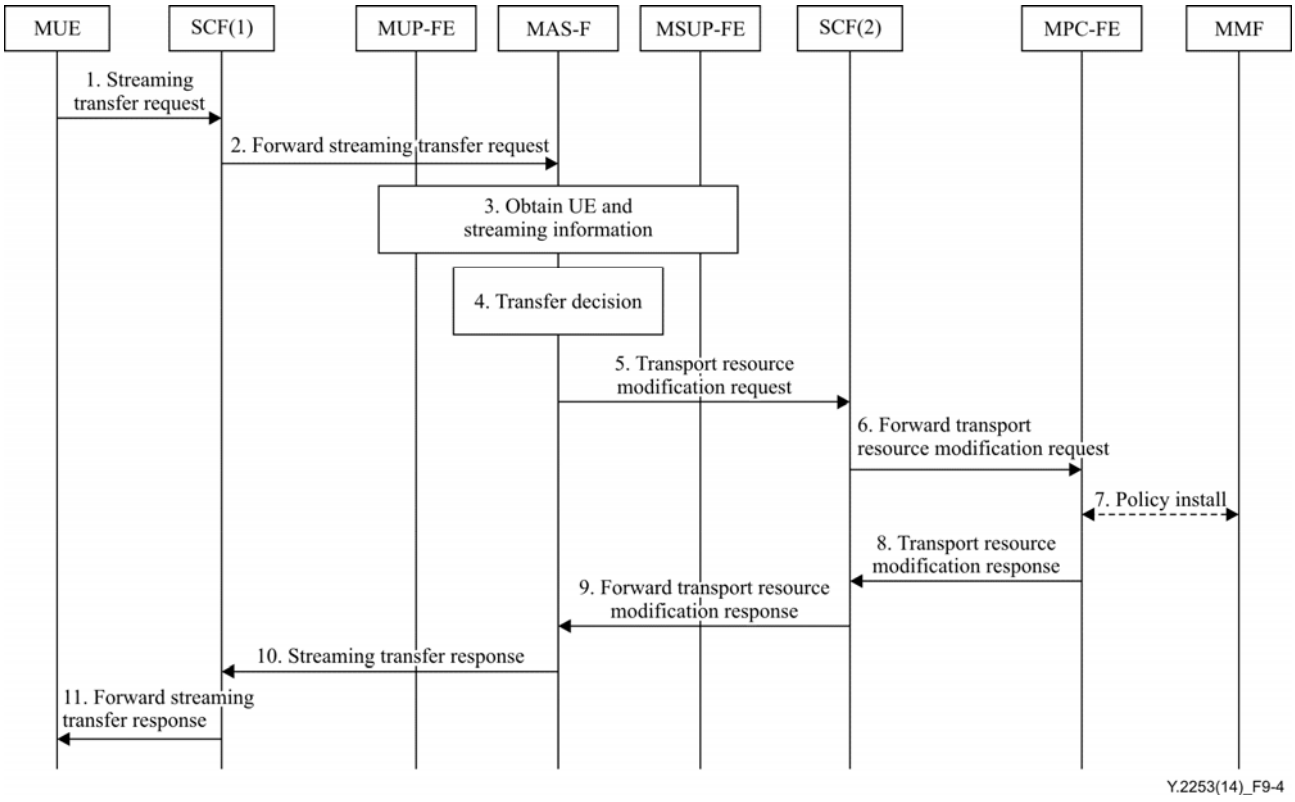

Figure 9-4 – MUE initiated streaming transfer

1) MUE sends a streaming transfer request message to the originating SCF, i.e., SCF(1), to request to transfer a streaming flow from one access network to another.

2) SCF(1) forwards this request message to MAS-F.

3) MAS-F obtains MUE and streaming flow related information from MUP-FE and MSUP-FE.

4) MAS-F makes the decision which connection can be used to transport the streaming flow to be transferred, according to the information already obtained.

5) MAS-F sends a resource modification request, which contains the updated information of the connection, to the destination SCF, i.e., SCF(2).

6) SCF(2) forwards this request message to MPC-FE.

7) MPC-FE makes policy rules based on QoS requirements, then sends a request to MMF to install the QoS rules.

8) MPC-FE returns a resource modification response message to SCF(2).

9) SCF(2) forwards this response message to MAS-F.

10) MAS-F returns a streaming transfer response message to SCF(1).

11) SCF(1) forwards this streaming transfer response message to MUE. Hence, the streaming flow has been transferred from SCF(1) to SCF(2).

9.4.2 Network initiated streaming transfer

Based on the status of an access network (for example, congestion in the network or connection released), the network is recommended to transfer some streaming flows to another access network. The information flow for network initiated transfer is shown as Figure 9-5.

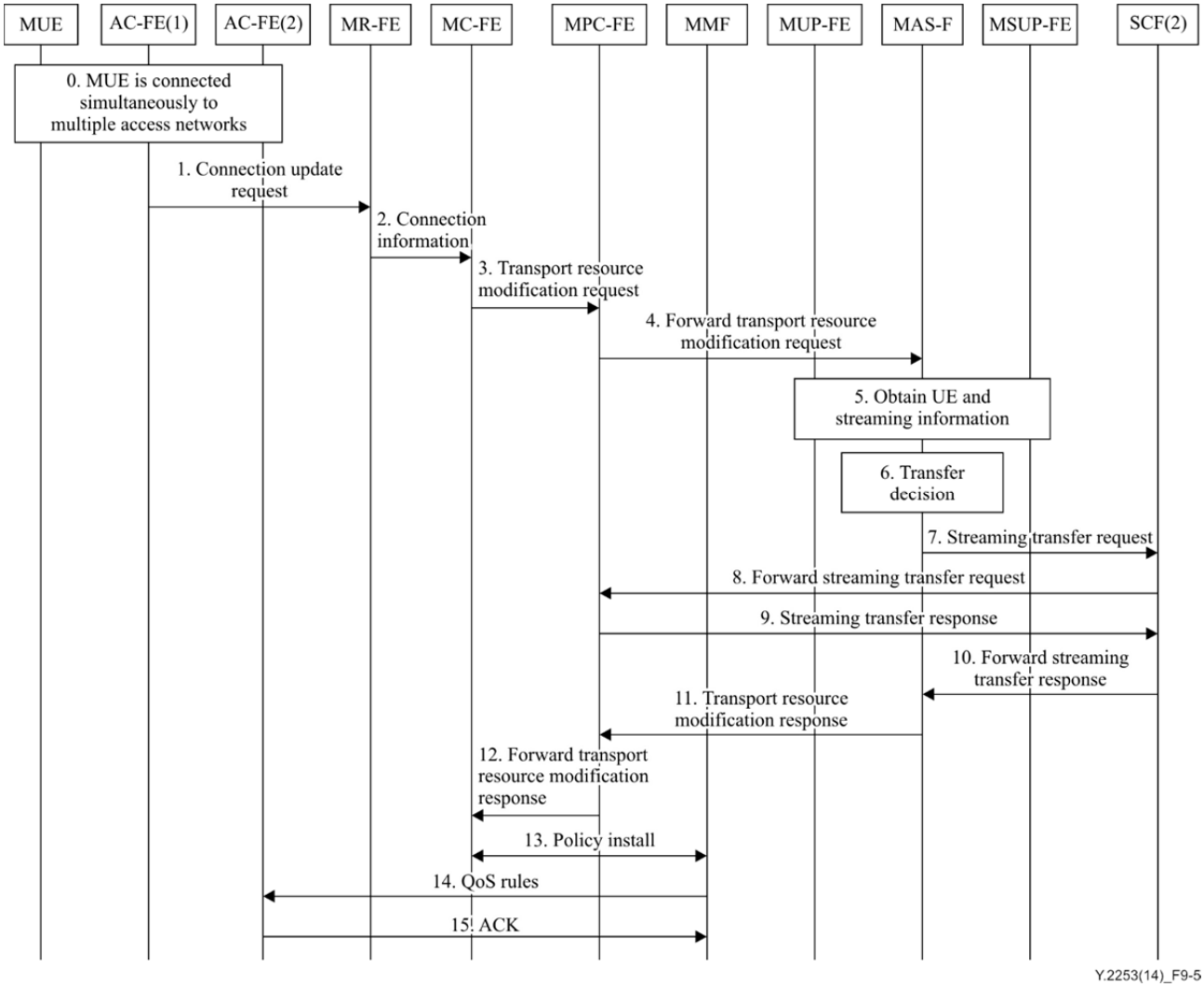

Figure 9-5 – Network initiated streaming transfer

0) An MUE has connected to multiple access networks simultaneously, and establishes several connections to receive streaming.

1) AC-FE(1), which represents the originating access network of this transfer procedure, sends a connection update request message to MR-FE. The message contains the identifier and the information of the connection to be modified.

2) MR-FE updates the information of the connection based on the request message. Then MR-FE sends a connection information message to MC-FE.

3) MC-FE sends a resource modification request message to MPC-FE, to request to revise related transmission policy.

4) MPC-FE forwards this modification request to MAS-F.

5) MAS-F obtains MUE and streaming flow related information from MUP-FE and MSUP-FE.

6) MAS-F makes the decision which connection can be used to transport the streaming flow to be transferred, according to the information already obtained.

7) MAS-F sends a streaming transfer request, which contains the updated information of the connections, to the destination SCF, i.e., SCF(2).

8) SCF(2) forwards this request message to MPC-FE.

9) MPC-FE constructs new QoS rules for the destination connection based on the operator's policies and originating connection information, then returns a streaming transfer response to SCF(2).

10) SCF(2) forwards this response message to MAS-F.

11) MAS-F returns a transport resource modification response message to MPC-FE.

12) MPC-FE forwards this response message to MC-FE.

13) MC-FE makes QoS rules according the response message, and installs the rules on MMF.

14) MMF forwards the QoS rules to AC-FE(2).

15) AC-FE(2) updates the QoS policy rules of the connection. After, it returns an ACK message to MMF. Hence, the streaming flow on AC-FE(1) has been transferred to AC-FE(2).

10 Security considerations

10.1 Subscriber security

Subscriber security of MC-Streaming contains all the relevant problems in a legacy network environment, including privacy protection and access control. In a legacy network environment, a subscriber's privacy mainly deals with a specific service, for example, channel number before and after the channel change, time of change, time of play and so on. For privacy protection, a great effort has been made to prevent subscribers' personal information from being abused.

In the multi-connection environment, in addition to the above information, a subscriber's privacy includes authentication information for multiple access networks, network selection related information and other important privacy information. Once the information is leaked or tampered with, the security risk increases with multiple accesses instantiations.

For MC-Streaming, subscriber security mainly focuses on a subscriber's privacy protection and access control of the service.

10.1.1 Privacy protection

When providing MC-Streaming service, privacy protection is necessary and should seriously be considered, in order to prevent information from being leaked or abused. Subscribers' privacy information includes: service usage, network selection information, authentication information, etc.

For MC-Streaming, subscribers' private information may be leaked out in at least three forms, i.e., from the service provider(s), network operator and terminal device. According to the different disclosure forms, different protection mechanisms should be deployed.

From the service providers' perspective, many sensitive data are stored at their side. Illegal intrusion and unauthorized access may steal the data, bringing threats to the subscribers. Hence, subscribers' personal data is recommended to be classified and managed accordingly. Important data should be controlled securely, e.g., it can be stored after encryption. Access to personal data should also be controlled.

From the network's perspective, personal data can be leaked during transmission. So, encryption algorithms and mechanisms such as DES, RSA, SSL, and others are recommended to be deployed. Communication channels are recommended to be encrypted before data transmission.

From the terminal device's perspective, certain personal data are stored in the terminal device itself, which can be read out if the device is lost. Therefore, it is recommended to deploy a mechanism to completely delete user data on demand by the subscriber himself or the service provider. Sensitive data are required to be encrypted and secured. Hence, a third party cannot easily read out the data even when the device can be accessed. The terminal device should also provide the capability of avoiding malicious software and virus attacks.

10.1.2 Access control

Normal subscribers should be able to set up an access control mechanism (such as using a password) to limit the access to his/her preferred content or services.

For protection of children, some kinds of mechanisms for parent control are recommended to be deployed in order to restrict the streaming contents from being accessed. Specifically, the service provider can set ratings for content to limit access by children, and also can make an authorization in the terminal device for children viewing a particular channel or content, for example, by using a PIN challenge.

10.2 Service security

Service security in MC-Streaming also suffers from all the related problems in legacy networks. For example, authentication, authorization and access control are required to be supported. Before a service is provisioned, terminal device and subscriber are typically required to be authenticated in a secure way. After that, the subscriber is authorized for the access of specific service and content. Service access control also includes encryption mechanisms for service signalling and content flow, to mutually prevent unwanted or unauthorized access for both service provider and subscriber.

Specific to the multi-connection environment some specific security problems are discussed below.

10.2.1 Attacks

The diverse nature of the access networks involved in MC-Streaming requires a number of security procedures to prevent malicious attacks. These attacks may include:

- Denial of service (DoS), in which the attacks consists of flooding with service requests, creating network and server(s) congestion.
- Intrusion, which can destroy the network infrastructure and lead to threats to the MC-Streaming services.

- Trojans, which can steal the subscribers' private information or privacy stored in terminal devices, such as subscriber information, service usage and network related information.

The result of these attacks may violate subscribers' privacy, illegally modify policy information and ultimately cause abnormal behaviour of the MC-Streaming service.

10.2.2 Authentication

Subscribers are commonly required to fulfil authentication and authorization before they are able to access a service. Overpassing these steps lead to malicious threats targeting the service, such as denial of service (DoS), intrusion and malicious programs like Trojans, which can steal the information of subscribers. However, authentication and authorization is somehow complicated in MC-Streaming, since different mechanisms may be deployed in different access networks simultaneously.

From the service's perspective, multiple and repeated authentication procedures for every access network make authentication information potentially prone to be leaked. From the subscribers' perspective, they potentially should login repeatedly when accessing the service through several access networks. This is really inconvenient for subscribers, and may not provide a good user experience. From the perspective of management, large amounts of account information also makes the management complicated.

It is further recommended that authentication and authorization be bound to a verification of the integrity of MC-Streaming ensuring that the service, private subscription information, and policies are not compromised through malicious attacks. See also [ITU-T Y.2251], clause 7.

After the discussion above on various complex issues to be taken care of by the combination of the MC-Streaming service overlying upon the multi-connection architecture, MC-Streaming is recommended to adopt mechanisms to avoid redundant authentication operations.

Single Sign On (SSO), for instance, or a unified registration mechanism can optionally be deployed to simplify the authentication procedure across multiple networks. This authentication results in one access network that can also optionally be utilized to complete the authentication of other access networks.

10.2.3 Digital right management

For MC-Streaming, there also exist security threats such as unauthorized usage, illegal copy and so on.

In the multi-connection environment, the transmission paths of streaming content are more complicated than that of a legacy network environment. Operations such as streaming content distribution, transmission, acquisition, storage and redistribution between content sources, and terminal devices are susceptible to network attacks, causing security threats such as content intercepted, tempered, unauthorized usage, unauthorized copying or unauthorized redistribution.

Unlike the general data service, a streaming flow is composed of media content, such as audio streaming, video streaming, image streaming, etc. In order to prevent unauthorized use and illegal copy, it is recommended that multi-connection streaming supports Digital Right Management (DRM) to protect the copyright of streaming content. Using DRM, only authorized subscribers have permission to access the streaming content. Otherwise, an illegal copy of it cannot be replayed, even when it is been obtained. DRM solutions include digital watermarking, copyright protection, content tracking, digital signature, data encryption and others.

10.3 Network security

Network access authentication is a prerequisite to protect network security. In multi-connection, authentication and authorization are also recommended to be supported to ensure security.

Therefore, the content of MC-Streaming is also recommended to be protected during its transmission throughout the networks, as well as when it is acquired, consumed, stored and retransmitted by end subscribers. The protection mechanisms include encryption, watermarking, tracing, identification and other mechanisms. Otherwise, illegal network monitoring may break data confidentiality.

Detection and prevention mechanisms are recommended to be deployed against network attacks such as denial of service (DoS) and network intrusion, since these threats target specific network elements (e.g., routers and switches) and resources (e.g., bandwidth).

Different access networks may provide different security levels, which may cause vulnerabilities to MC-Streaming. For example, the payment for data when ordering a video is not suitable to be transmitted through WLAN, which is easily monitored and not safe enough. Among the solutions for this case include for instance selecting a network with a higher security level and encrypting data before transmission. In addition, it is also important to provide protection from attacks; e.g., DoS attacks from less secure intruding networks.

10.3.1 Access control

Access control means to protect against unauthorized usage of network resources. It ensures that only authorized personnel or devices are allowed to access network elements, store information, and modify information flows, services and applications.

For MC-Streaming, subscribers are able to access the service through multiple access networks. Different access networks have different security mechanisms and provide different security levels. It is required that MC-Streaming prevents unauthorized users from accessing networks and services through networks with lower security levels. Otherwise, security issues may arise, such as information disclosure and other related security problems to this service and to its underlying networks. Therefore, MC-Streaming is recommended to provide unified access control mechanisms to protect user requests from different access networks.

10.3.2 Authentication

Authentication protects the identities of communicating entities (e.g., person, device, service or application), and provides assurance that an entity is not attempting a masquerade or unauthorized access by replaying a previous legal communication. Unauthorized access to the access networks or to the streaming service breaks the authentication measurements previously taken. For example, unauthorized users may intercept subscribers' registration information from the communication link to then gain access to the access network(s).

In multiple access networks, each of them is required to fulfil the authentication of the terminals and their users. The process is complicated and impacts the user experience, but decreases the risk of disclosure to the subscribers' authentication information. Therefore, SSO or a unified registration mechanism can optionally be introduced to simplify the authentication process, as well as to improve the subscribers' experience and their security.

10.3.3 Non-repudiation

Non-repudiation prevents an individual or an entity from denying that she or he has performed a particular action. For example, subscribers subscribe to a service, but afterwards denied that they subscribed to the service.

In multiple access networks, subscribers' request information can be transmitted through different access networks. Since different reliability exists in different networks, subscribers' request information may be lost during its transmission and/or retransmission. Therefore, it is recommended that MC-Streaming record users' operations and ensure that key requested operations (e.g., service subscription, programmes to purchase, etc.) be neither lost, nor denied by the subscribers themselves.

10.3.4 Data security

Data security includes data confidentiality, data integrity and privacy, etc.

Data confidentiality means to protect data from unauthorized disclosure. It ensures that the data content cannot be understood by unauthorized entities. Unauthorized access to sensitive data will break the confidentiality.

Data integrity ensures the correctness or accuracy of data, and protects against unauthorized modification, deletion, creation and duplication, etc. The unauthorized tampering with sensitive data will break the integrity.

Privacy security provides the protection of information such as a user's geographic location, IP addresses, the contents that a user has visited, and the DNS names of devices in a service provider network.

In multiple access networks, the authentication information from multiple access networks is sensitive and confidential. Once they are stolen and then pretended, some security threats may occur. For example, a subscriber may be charged maliciously. Therefore, MC-Streaming is recommended to employ some kinds of mechanisms to ensure data confidentiality. DES, RSA and other encryption algorithms can optionally be deployed.

In multiple access networks, streaming data transmitted in networks can be classified for signalling data and media content. For media content, it has little effect on user experience even if some parts of the content are lost. But for signalling data, it is necessary to ensure data integrity. Otherwise, the MC-Streaming service cannot work normally. Therefore, it is proposed that the integrity of signalling data be verified. Hashing algorithms such as MD5 and SHA1 are widely used for integrity checks, and are recommended to be employed here.

In MC-Streaming, users' streaming service information includes program registration and login information, program information, program settings and content, etc. Once the information is stolen and then forged or modified, it will result in some security threats such as malicious charging and login. Therefore, MC-Streaming is recommended to protect the privacy of the information. Encryption, watermarking, tracing and marking, and other mechanisms can be deployed here.

10.3.5 Communication security

Communication security ensures that information can only be accessed by authorized end-points, and the information is not diverted or intercepted during transmission between these end-points.

In MC-Streaming, different networks have different security levels. Networks with a lower security level are more vulnerable to attacks, such as DoS attacks and Distributed DoS (DDoS) attacks. Therefore, some types of security systems such as security gateway and firewall are recommended to be deployed to ensure the security boundary of the underlying network. Network scanning can also optionally be used here.

In addition, MC-Streaming needs to ensure availability. Availability means the service is resilient to hardware or software failure, and intrusion attacks. Hence, the service is recommended to be designed and deployed in a distributed architecture. Some kinds of redundant technologies, such as cluster and backup for both hardware and software, are popularly used. An intrusion detection system (IDS) is also an effective technology for protection from network attacks.

10.4 Terminal device security

In multiple access networks, the terminal device security problem becomes more complicated. Attacks may come from different access networks; the attackers may access non-encrypted streaming content by changing terminal devices, or encrypted streaming content by analysing data flows. It may increase the risks of MUE compared with a single network environment. Terminal devices may be infected with virus, Trojan horses, worms and other malicious programs. These harmful programs may cause information disclosure, charging information tampered. They may also make the streaming service work abnormally. In addition, unauthorized subscribers can try to break device security by downloading and running hacker software if they can access the device. These may also make terminal devices unsafe, especially for smartphones.

According to the threats above, some mechanisms are proposed to deal with terminal device protection. For example, pluggable and renewable security processors and components can optionally be deployed to improve the ability of resisting network attacks. Secure and tamper-resistant secret data storage, control signal encryption and decryption are recommended to be used to prevent information disclosure and data tampering, etc. Authorization is recommended to be required to ensure that only legal software can be downloaded, run and stored on terminal devices.

11 Charging

MC-Streaming contains a variety of service types, such as video broadcasting, video on demand, video conference and monitoring, etc. Each different service type has different characteristics, and their charging policies are also different. Charging for MC-Streaming needs to be able to generate usage records, and provide flexible and customized price strategy, so as to fulfil different charging requirements. A charging system is recommended to support a variety of charging resources, including timing, total flow, upstream traffic, downside flow, frequency, etc.

In the multi-connection environment, resources in different networks can be allocated and used by a single user at the same time. Multiple links can also be charged at the same time. Therefore, it is recommended not to charge multiple times for a single usage of the service, even when multiple usage records are generated in different networks.

The charging mechanisms can be divided into different categories. According to the time when to charge, they can be divided into online charging and offline charging. According to the content to be charged, they can be divided into duration charging, content charging, monthly rental charging and combined charging, etc. MC-Streaming is recommended to support more than one charging mechanism to support different service types.

11.1 Charging mechanisms

11.1.1 Online charging

For MC-Streaming, online charging is a charging mechanism where charging is done in real time taking into consideration multiple accesses. Therefore a direct interaction is required between resource/session/service control entities and the charging system. For the MC-Streaming service, several entities can be used to fulfil online charging in different scenarios.

In the architecture of MC-Streaming, MSCC-FE provides a content management and control function, as well as optional content distribution function. It is responsible for content preparation and content protection. All streaming content would pass through it before distributing to subscribers. Therefore, the services to be charged by usage time, e.g., linear TV and video conference can optionally be fulfilled by MSCC-FE.

MSCD-FE is responsible for caching and storing content and associated information, as well as delivering received content from MSCC-FE to subscribers. Therefore, content and streaming related charging can optionally be fulfilled by MSCD-FE.

MSAC-FE is responsible for user interaction control such as programme selection, forwarding and rewinding. It allows multi-connection devices to choose or purchase streaming content on demand. Interaction between users is also a responsibility of MSAC-FE. Therefore, content related charging can optionally be fulfilled by MSAC-FE.

In the multi-connection environment, each network has its own charging strategies and policies. Charging information can be generated by many functional entities. Hence, it is required to avoid redundant charging when accumulating different usage records collected from different networks or from different systems in one network.

11.1.2 Offline charging

Offline charging is a charging mechanism where charging is done periodically (e.g., daily or monthly), instead of in real time. All usage information is provided to a billing system such as a charging data record (CDR), which contains detailed usage information. And charging will be completed by the billing system according to the charging strategy. The billing system does not need to interact with a service directly during the process of the service, which would reduce service performance. For MC-Streaming, offline charging has an intrinsic risk since a subscriber might generate high expenses in short periods of time.

For the MC-Streaming service, charging information can be generated not only by MC-Streaming, but also by the underlying networks. Different functional entities in MC-Streaming can be used to generate charging records, according to a service's charging policy. For example, MSCC-FE or MSCD-FE can be optionally used to charge for flow or transmission related policy, and the service itself can be optionally used to charge for content related policy.

11.2 Charging policies

11.2.1 Duration based charging

In duration charging, a user is to pay for usage duration of a service. The quality of content has little effect on cost. The capacity of the underlying network has a greater influence on the quality of service. This means even if the network is overloaded, users still have the same cost but for a lower service experience. Therefore, it is reasonable to deploy this strategy in the networks which have a stable QoS.

For MC-Streaming, both the service itself and underlying networks can optionally generate charging records. However, it is more reasonable for MC-Streaming to fulfil duration charging, since it has overall information about the service usage. If not, it may be complex and possibly make a mistake when charging across multiple access networks.

11.2.2 Flow based charging

Flow charging is based on the flow of traffic that a user sends or receives, independent of the service being used. Because different links have different rates and may generate different charging records, it is recommended to take the quality of each link into account, such as bandwidth capacity, unit bit cost, bit error rate, etc.

In MC-Streaming, MSCC-FE and MSCD-FE can optionally generate flow charging records, since all streaming content would go through them. Charging information can also be generated by underlying network elements. But some charging conflicts may appear, or some charging information might be omitted, which may lead to a charging error. Hence, it is recommended that the service, instead of the underlying network elements, is responsible for flow charging.

11.2.3 Content based charging

For content charging, it is fulfilled based on streaming content to be accessed. Each piece of content has a price. When ordered, a subscriber will be charged accordingly. This policy is more suitable to VoD (video on demand) related service types, since subscribers focus more on the content itself than on the bandwidth or duration to be used during content transmission. This strategy is simple and easy to be implemented. It can optionally be fulfilled by MC-Streaming itself, more specifically, by the MC-Streaming application control functional entity (MSAC-FE) or MC-Streaming content control functional entity (MSCC-FE).

11.2.4 Monthly rental based charging

Monthly rental charging is a policy wherein a subscriber pays for a certain amount of fees each month for subscribing to the streaming service, no matter how long he or she uses and how much amount of content that he or she accesses. The monthly price is usually a little higher than other charging policies, because of no restriction of service usage. For MC-Streaming, a tremendous amount of network resources may be occupied for content transmission. It is important to design a good policy to balance network costs and operators' benefits, if this kind of charging policy is to be deployed.

11.2.5 Hybrid charging

A single charging policy may not be able to adapt to different deployment of streaming service, since there are different scenarios and application types for the service. Different charging policies can optionally be selected. A variety of policies can optionally be provided to support flexible charging and meet different subscribers' requirements.

Appendix I

Scenarios of streaming services over multi-connection

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

I.1 Video services

Video services mainly include live video and video on-demand (VoD). Live video relies on the Internet and streaming technology. It integrates images, text, voice and other elements. VoD, as the name suggests, is a video on demand service responding to viewers' requests of programmes. This service can transport the video content to users as clicked or selected.

In the environment of multi-connection, the advantages of multi-connection such as increasing service continuity can be used to enhance the video service. For example, benefiting from multi-connection technology, the video service will not be interrupted even if one or more of the connections are lost. Instead, other available connections can be used to maintain the continuity of the service. Figure I.1 is an example for VoD continuity.

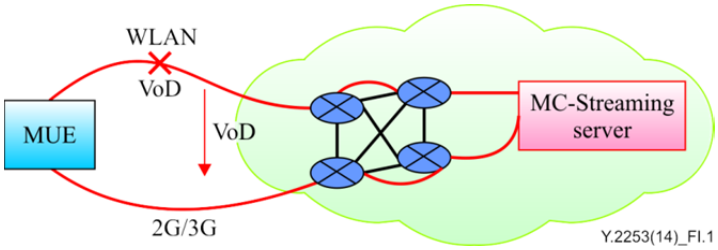

Figure I.1 – VoD service continuity

Alice has both a 3G connection and WLAN connection in her home. She uses a VoD service which establishes two connections through 3G and WLAN simultaneously, since a broad bandwidth is required for video delivering. After a while, she leaves home and moves out of the area of WLAN. WLAN connection is then lost. The service senses the change and automatically starts delivering video streaming over the 3G connection without pausing or stopping the service. Alice is informed of the change by the service or by the network.

I.2 Video conference services

Video conference services mainly include video conference, video chatting, tele-education and so on. Video conference is a kind of communication method. It is held among different users with terminals in different places, by communicating with voice, video and images in real time. The participators can feel the communication just as face-to-face conversation. In fact, it can be used to replace onsite meeting.

In the environment of multi-connection, the advantages of multi-connection, such as multimedia division and load sharing between networks, can be used to enhance this kind of service. For example, benefiting from multi-connection technology, video conference services can be divided into audio flow sand video flows, and then be delivered through different transmission paths in different networks. Figure I.2 is an example of video conference service.

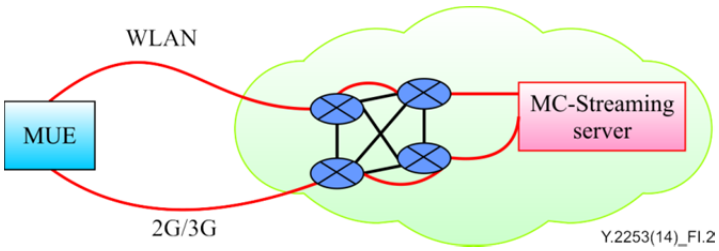

Figure I.2 – Video conference service

Alice has to attend a video conference with business partners via her mobile phone when she is walking to the office. On the way to her office, some WLAN hotspots are available. So Alice decides to initiate the video flow through a WLAN link in order to benefit from higher bandwidth and cheaper cost, whereas she sends and receives the audio flow through the 2G/3G link in order to guarantee the audio flow to be uninterrupted.

I.3 Real-time monitor services

Real-time monitor services mainly include real-time monitor, multi-viewer service and so on. A real-time monitor service collects multimedia streaming from multiple terminals, and distributes to one or more UE after process by the service. Users can view the multimedia information in one screen from different angles or locations.

In the environment of multi-connection, the advantages of multi-connection, such as flexibility in network selection, transparency of multi-connection, service continuity, increased access options, can be used to enhance this kind of service. For example, benefiting from multi-connection technology, multiple terminals are able to send multimedia flows through different connections. After integration by the service, these multimedia flows are distributed to one or more UE. Both transmission efficiency and user experience can be improved in this way. Figure I.3 is an example of real-time monitor service.

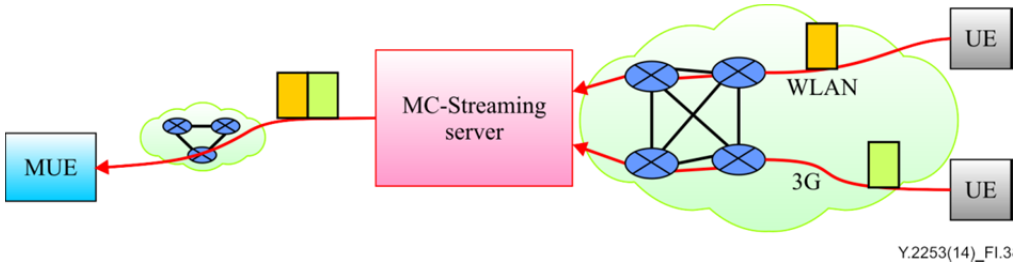

Figure I.3 – Real-time monitor service

Alice is watching a linear broadcast of a baseball game. There are multiple cameras in the stadium, which provide different views of the game. All views are delivered to Alice's terminal through multiple networks. Then Alice is able to choose and watch the preferred view.

With multi-connection technology, multi-view service is able to deliver video streaming from different video sources simultaneously. An end-user can choose the views that he or she would like to watch. It will greatly improve user experience in this way.

Bibliography

[b-ITU-T D.271] Recommendation ITU-T D.271 (2008), *Charging and accounting principles for NGN*.

[b-ITU-T Q.1706] Recommendation ITU-T Q.1706/Y.2801 (2006), *Mobility management requirements for NGN*.

[b-ITU-T X.1191] Recommendation ITU-T X.1191 (2009), *Functional requirements and architecture for IPTV security aspects*.

[b-ITU-T Y.1910] Recommendation ITU-T Y.1910 (2008), *IPTV functional architecture*.

[b-ITU-T Y.2001] Recommendation ITU-T Y.2001 (2004), *General overview of NGN*.

[b-ITU-T Y-Sup.9] ITU-T Recommendation Y-series – Supplement 9 (2010), *ITU-T Y.2000-series – Supplement on multi-connection scenarios*.

SERIES OF ITU-T RECOMMENDATIONS

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

Printed in Switzerland
Geneva, 2014