International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2041

(03/2017)

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

Next Generation Networks – Frameworks and functional architecture models

Policy control mechanism in multi-connection

Recommendation ITU-T Y.2041

International Telecommunication Union

ITU-T Y-SERIES RECOMMENDATIONS

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

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	**Y.2000–Y.2099**
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Enhancements to NGN	Y.2300–Y.2399
Network management	Y.2400–Y.2499
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
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	
General	Y.4000–Y.4049
Definitions and terminologies	Y.4050–Y.4099
Requirements and use cases	Y.4100–Y.4249
Infrastructure, connectivity and networks	Y.4250–Y.4399
Frameworks, architectures and protocols	Y.4400–Y.4549
Services, applications, computation and data processing	Y.4550–Y.4699
Management, control and performance	Y.4700–Y.4799
Identification and security	Y.4800–Y.4899
Evaluation and assessment	Y.4900–Y.4999

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

Recommendation ITU-T Y.2041

Policy control mechanism in multi-connection

Summary

Recommendation ITU-T Y.2041 describes a policy control mechanism in multi-connection. Recommendation ITU-T Y.2041 also covers scenarios, requirements, solutions and information flows.

Multi-connection architecture is designed for heterogeneous networks, has the ability to provide multi-connection user equipment (MUE) and networks the functionality to maintain more than one access network connection simultaneously. It controls policies, flows, quality of service (QoS), etc.

Policy control is useful or even necessary for multi-connection. Policy control determines how to use multiple access network connections. There can be several policies in multi-connection, such as those for QoS and service transfer. Recommendation ITU-T Y. 2041 provides a coordination mechanism to ensure that all policies work together in a coherent manner for multi-connection.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.2041	2017-03-29	13	11.1002/1000/13248

Keywords

Multi-connection, policy control

* 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.2041

Policy control mechanism in multi-connection

1 Scope

This Recommendation describes scenarios, requirements, solutions and information flows for policy control in multi-connection.

NOTE – Security and charging requirements for policy control in multi-connection are addressed in [b-ITU-T Y.2251].

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 connection [b-ITU-T X.200]: 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.

3.1.2 multi-connection [b-ITU-T Y-Sup.9]: Multi-connection is the collection of several simultaneous connections between two or more peer-(N)-entities. At least one of the connections is required to be associated with a physical layer connection different from the rest of the connections. All connections are dynamically coordinated with each other by the subscriber or the network to provide service to higher layer entities.

3.1.3 IP-CAN session [b-3GPP TS 23.203]: The association between a UE and an IP network. The association is identified by one IPv4 and/or an IPv6 prefix together with UE identity information, if available, and a PDN represented by a PDN ID (e.g., an APN). An IP-CAN session incorporates one or more IP-CAN bearers. Support for multiple IP-CAN bearers per IP-CAN session is IP-CAN specific. An IP-CAN session exists as long as UE IP addresses/prefix are established and announced to the IP network.

3.1.4 policy control [b-3GPP TS 23.203]: The process whereby the PCRF indicates to the PCEF how to control the IP-CAN session. Policy control includes QoS control and/or gating control.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 enhanced policy and charging enforcement function (ePCEF): A function that addresses the enhanced requirements of the policy and charging enforcement function (PCEF) to support multi-connection related policy control enforcement function. The PCEF is a logical entity that enforces policy decisions. The PCEF is responsible for traffic policy enforcement of unicast traffic. Policy enforcement may be applied at an Internet protocol (IP) session, IP flow and aggregate level.

3.2.2 enhanced policy and charging rule function (ePCRF): A function that addresses the enhanced requirements of the policy and charging rule function (PCRF) to support multi-connection related policy and charging rule function. The PCRF is a functional entity making policy decisions for network control, gating, quality of service (QoS) and charging. Such policy decisions are based

on subscriber preferences and are applied on an Internet protocol (IP) session, IP flows or aggregate flows basis.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

2G second Generation
3G third Generation
APN Access Point Name
ePCEF enhanced Policy and Charging Enforcement Function
ePCRF enhanced Policy and Charging Rule Function
FSC Flow-based Service Continuity
ID Identification
IP Internet Protocol
IP-CAN IP Connectivity Access Network
IPv4 Internet Protocol version 4
IPv6 Internet Protocol version 6
LTE Long-Term Evolution
MC-FE Multi-connection Coordination Functional Entity
MMF Multi-connection Media Function
MPC-FE Multi-connection Policy Control Functional Entity
MUE Multi-connection User Equipment
MUP-FE Multi-connection User Profile Functional Entity
OTT Over the Top
PCEF Policy and Charging Enforcement Function
PCRF Policy and Charging Rule Function
PDN Packet Data Network
QoS Quality of Service
RAT Radio Access Technology
SCF Service Control Function
TV Television
UE User Equipment
WLAN Wireless Local Area Network

5 Conventions

In this Recommendation:

The keywords "is required to" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

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

The keywords "is recommended" indicate a requirement which is recommended but which is not absolutely required. Thus this requirement need not be present to claim conformance.

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

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

6 Requirements

6.1 Overview

Policy control is useful or even necessary for multi-connection. Policy control determines how to use multiple access network connections, there can be several policies in multi-connection, such as those for QoS and service transfer. It is necessary to have a coordination mechanism to ensure that all policies work together in a coherent manner for multi-connection. For example, QoS policies match the service to the access network to ensure proper QoS for application and services while service transfer policies control multi-connection network flow transfer during access to a different network. Generally, the multiple policy control mechanism requires combination in a multi-connection service action, such as multi-connection service transfer.

In terms of related scenarios, consider that, in a video conference or over the top (OTT) video TV at home, the user equipment (UE) accesses heterogeneous access networks, the audio is transmitted by 2G, 3G or long-term evolution (LTE) to assure real time service and the video is transmitted by a wireless local area network (WLAN). After a while, we leave home with the service active, but we lose the WLAN connection, we need to transfer the video flow to a 3G or LTE connection, in this process, consider the multiple policy control combination and coordination to serve the application.

In this scenario, the application contains policies relating to access selection, service transfer, QoS and others. So, a coordination mechanism is required to ensure that all policies work together in a coherent manner.

6.2 Requirements

6.2.1 General requirements

The following elements describe the general requirement.

- The ePCRF should be able to send policies to the ePCEF.
- The ePCRF should be able to provision policy rules at ePCEF based on a request from the ePCEF (PULL mode), or based on a request from the service control function (SCF), a timer expiration or a subscription profile modification (PUSH mode).
- The ePCEF should be able to initiate, modify and terminate the IP-CAN session.
- The ePCEF should be able to request policies from the ePCRF.
- The PCEF should be able to receive policies from the ePCRF.
- The ePCEF should be able to apply policies to subscriber IP-CAN sessions.
- The ePCEF should be able to enforce policy for multi-connection traffic.

- The ePCEF should support policy enforcement for both downstream and upstream traffic.
- The ePCEF should acknowledge the reception of policies from the ePCRF.
- The ePCEF should be able to activate or deactivate pre-provisioned policies per list received from the ePCRF.
- The ePCEF should be able to give precedence to the policies provided by the ePCRF over the others.
- If the ePCRF is not available at the time of subscriber or host instantiation, the ePCEF should be able to provide the subscriber or host with default policies.

6.2.2 Requirements for quality of service control

If the QoS information contained in a policy rule is applicable to the multi-connection scenario, the ePCRF should be able to override the default QoS when it is received from the ePCEF at device attachment or log-in.

6.2.3 Requirements for usage monitoring

In order to support multi-connection dynamic policy management based on network usage, usage monitoring defines the ability to enforce dynamic policy decisions based on the total network usage in real-time. Usage monitoring can be done at different levels, at those of: IP session, IP flow or group of IP flow(s).

Using this functionality, the ePCRF shall set and send volume and time thresholds to the ePCEF. Those thresholds shall be valid for an individual IP session, IP flow or a group of IP flow(s) that are parts of the subscriber IP session.

6.2.4 Requirements for charging control

The ePCEF is required to support charging based on configuration.

The ePCEF is required to count separately the data volumes on both the uplink and downlink direction of the subscriber IP session on multi-connections.

The ePCEF is required to identify data volumes, elapsed time and credit reauthorization triggers for individual flows that are parts of the subscriber IP session.

6.2.5 Requirements for event triggers and credit reauthorization triggers

The ePCRF is required to indicate to the ePCEF the events it wants notification of. Such events are called event triggers. The ePCEF must support the event triggers. When an event matches an event trigger, the ePCEF must report it to the ePCRF. Event triggers are defined as follows:

- QoS change;
- out of credit;
- usage report;
- IP session start or /stop.

The OCS is required to indicate to the ePCEF the events it wants notification of. Such events are called credit reauthorization triggers. The ePCEF must support the credit reauthorization triggers. When an event matches a given credit reauthorization trigger, the ePCEF must report it to OCS. Credit reauthorization triggers are defined as follows:

- credit authorization lifetime expiry;
- idle timeout;
- QoS change.

6.2.6 Requirements for IP flow transfer routing

In the multi-connection environment, in the case of network congestion or loss of radio signal in the access network connections, the network is required to dynamically control the user access and resource allocation to obtain the optimal distribution of applications or IP flows. This is achieved according to multi-connection policies generated by both the user and network.

7 Policy control mechanism

7.1 Functionality entities of multi-connection policy control

This clause describes the functionality of each network entity that comprises the multi-connection policy management architecture. See Figure 7-1.

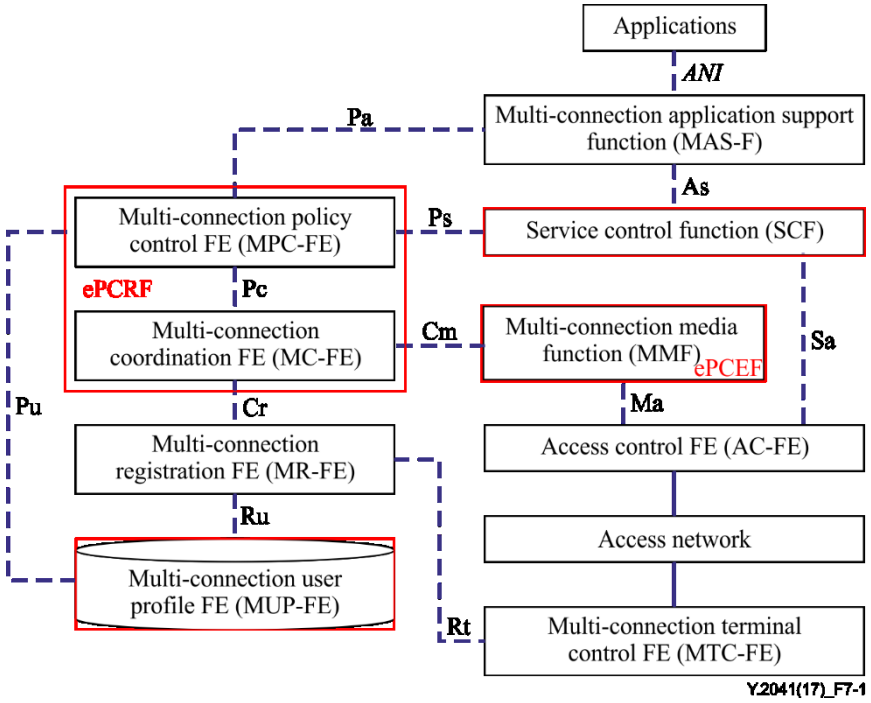

Figure 7-1 – Multi-connection policy control related functional entities

7.1.1 Enhance policy and charging control (ePCRF)

The ePCRF is composed of a multi-connection policy control functional entity (MPC-FE) and multi-connection coordination functional entity (MC-FE), it is a functional entity making policy decisions for multi-connection network control, gating, QoS and charging. Such policy decisions are based on subscriber preferences and are applied on an IP session, IP flow or aggregate flows basis.

The policy and charging rule function (PCRF) functionality is defined in 3GPP TS 23.203, the ePCRF addresses the requirements to support multi-connection policy control.

7.1.2 Enhance policy and charging enforcement function (ePCEF)

The ePCEF is a logical entity that enforces multi-connection policy decisions. The ePCEF is responsible for traffic policy enforcement of multi-connection traffic.

Policy enforcement may be applied at an IP session, IP flow and aggregate level.

The PCEF is specified in 3GPP TS 23.203, the ePCEF addresses the requirements to support multi-connection policy control enforcement, which is located at the broadband network gateway, gateway general packet radio service support node, and packet data network gateway etc.

7.1.3 Service control function

The SCF is a logical entity offering applications that require dynamic policy and charging control. It requires a certain minimum bandwidth for the service to be delivered with an acceptable end-user experience. The SCF interacts with the ePCRF communicating the required service information, and receives and authorizes QoS resource requests from the ePCRF.

The service information from the SCF to the ePCRF includes, but it is not limited to:

- IP filter information to identify the flow for policy control or differentiated charging;
- media or application bandwidth requirements for QoS control and media priority relative to other media in a multi-media session;
- a service identifier;
- priority of the connection that reflects the user's priority;
- an emergency service indication.

7.1.4 Multi-connection user profile functional entity

The multi-connection user profile functional entity (MUP-FE) provides information for the ePCRF to make policy decisions and responds to queries for user profiles that can be stored in one database or separated into several databases.

7.2 Description of the mechanism

7.2.1 IP-CAN session establishment

During IP-CAN session establishment, the ePCEF informs the ePCRF about the multi-connection user equipment (MUE) and network support for multi-connection, supported polices, the IP-CAN type and the radio access technology (RAT) type. The ePCRF takes decisions on whether policies may apply to the IP-CAN session and informs the ePCEF about its decisions.

7.2.2 Addition of an access

When the ePCEF receives both a handover request and a flow-based service continuity (FSC) indication from the MUE, the ePCEF initiates an IP-CAN modification procedure. The ePCRF takes policy decisions and communicates them to the ePCEF; the ePCRF may reject the addition of the access, indicates and provides the default access to the ePCEF, verifies the default access provided by the MUE complies with the subscription and rejects routing rules received from the MUE due to subscription limitations. Otherwise, the ePCRF determines the impacted policy rules and provides or modifies these policy rules.

7.2.3 Removal of an access

When the ePCEF is informed of the removal of an access of a multi-connection IP-CAN session, the ePCEF initiates an IP-CAN modification procedure to notify the ePCRF about the removal of the access together with the IP-CAN type and the RAT type of this access. The ePCEF notifies the ePCRF of the policy rules that are removed.

7.2.4 Network-initiated flow-based service continuity

In network-initiated FSC mode, the ePCRF may at any time determine that flows should be moved from a source access to a target access. In that case, the ePCRF provides updated policy rules with information on the new allowed access type using an IP-CAN session modification procedure.

The ePCRF request sending routing rules to the MUE may be rejected by the MUE due to local radio conditions. In that case, the ePCRF gets notified that PCC rules cannot be created or modified; this notification from the ePCEF contains an indication of the cause of the rejection received from the MUE.

7.2.5 User equipment-initiated flow-based service continuity

When the ePCEF has received a decision from the MUE to create, modify or delete FSC routing rules, the ePCEF initiates an IP-CAN modification procedure and provides the FSC routing rules received from the MUE to the ePCRF. The ePCRF may reject FSC routing rules received from the MUE due to subscription limitations. Otherwise, the ePCRF determines the impacted policy rules and provides updated policy rules with information on the new allowed access type to the ePCEF.

7.2.6 An access becomes not usable or usable again or (radio access network rule-related) indication

The ePCEF initiates an IP-CAN modification procedure to notify the ePCRF about the change of availability of an access to the ePCRF. The ePCRF may update the policy rules, e.g., by changing the allowed access and providing the updated policy rules to the ePCEF.

7.2.7 Reporting access network information to the service control function

The ePCRF reports to the SCF when different media of the application session are carried by different accesses.

If the ePCRF has received a request for access network information from the SCF, the ePCRF selects one policy rule to be associated with access network information reported by the ePCEF.

7.2.8 Usage monitoring control specific information

The usage monitoring control information comprises the information that is required to enable user plane monitoring of resources for individual or groups of applications or services for an IP-CAN session.

Usage monitoring on an IP-CAN session or monitoring key level is active in the ePCEF, provided that certain conditions are met. The conditions for continued monitoring on session level are:

– For IP-CAN session level monitoring at the ePCEF, an IP-CAN session is active and a volume or time threshold value for the IP-CAN session has been provided.

For usage monitoring on monitoring key level at the ePCEF the following conditions are applicable:

– A volume or time threshold has been provided for a monitoring key to the ePCEF and there is at least one PCC rule activated for the IP-CAN session that is associated with that monitoring key.

7.2.9 Quality of service control rule

The quality of service (QoS) control rule comprises the information that is required to enable the user plane detection and QoS control for service data flow. The packets detected are designated to a service data flow by applying the service data flow template of a QoS rule.

QoS control rule operations consist of activation, modification and de-activation of QoS rules.

An active QoS rule means that:

– the service data flow template shall be used for service data flow detection;

– the service data flow template shall be used for mapping of downlink packets to the IP-CAN bearer determined by the bearer binding;

– the service data flow template shall be used for service data flow detection of uplink packets on the IP-CAN bearer determined by the bearer binding;

– QoS procedures associated with the QoS rule, if any, shall be invoked.

The ePCRF may modify an active QoS rule at any time.

The ePCRF may deactivate an active QoS rule at any time.

7.2.10 IP flow mobility routing rule

The routing rule comprises the information that is required for the ePCRF to install the QoS rules for a service data flow in flow mobility scenarios. The ePCRF relies on the IP flow mobility routing information contained in the IP flow mobility routing rule. The IP flow mobility rules are provided by the ePCEF to the ePCRF during session establishment or modification.

IP flow transfer routing rule operations consist of installation, modification and removal of routing rules. The ePCRF uses all installed routing rules related to an IP session to select an ePCEF for any service data flow related to that session.

The ePCEF may modify or remove an installed routing rule based on updated flow binding information received from the MUE at any time.

7.3 Procedures

7.3.1 Procedures for quality of service control

See Figure 7-2.

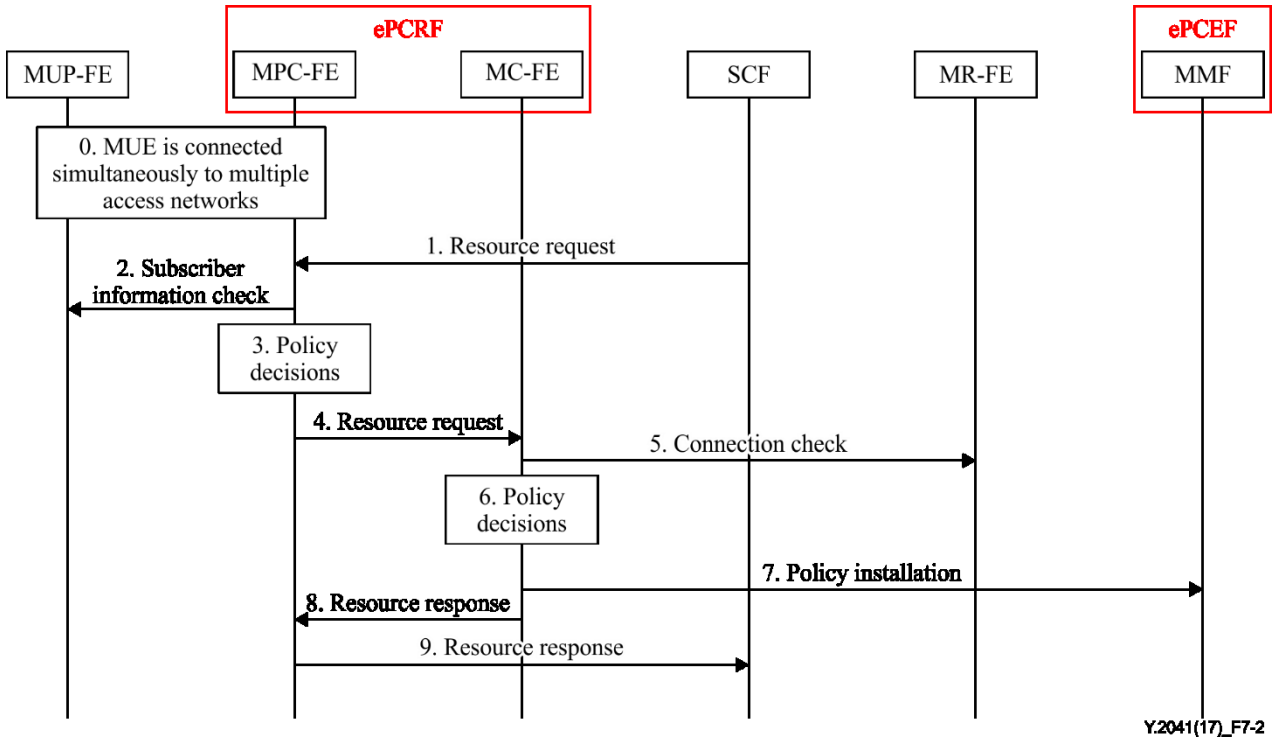

Figure 7-2 – Procedures for quality of service control

0) The MUE is connected to multiple access networks simultaneously and uses multiple connections to send and receive IP flows.

1) The SCF extracts or derives the resource requirements for the requested service, and sends a resource request to the MPC-FE in the ePCRF for resource authorization and reservation.

2) The MPC-FE sends a subscriber information check to the MUP-FE to verify subscription-related information of the MUE, subscription-related information containing the information about the user information, allowed services, allowed QoS, such as bandwidth and priority.

3) The MPC-FE makes policy decisions based on the information in 0)–2).

4) The MPC-FE sends a resource request to the MC-FE to support the traffic over multiple accesses.

5) The MC-FE sends a connection check to the MR-FE to check the currently available connections of the MUE.

6) The MC-FE makes policy decisions based on the information in 4)–5).

7) The MC-EF updates and assigns related rules for each access network and assigns them to the multi-connection media function (MMF), the MMF installs the rules.

8) The MC-FE sends a resource response to the MPC-FE.

9) The MPC-FE sends a resource response to the SCF.

7.3.2 Procedures for usage monitoring control

See Figure 7-3.

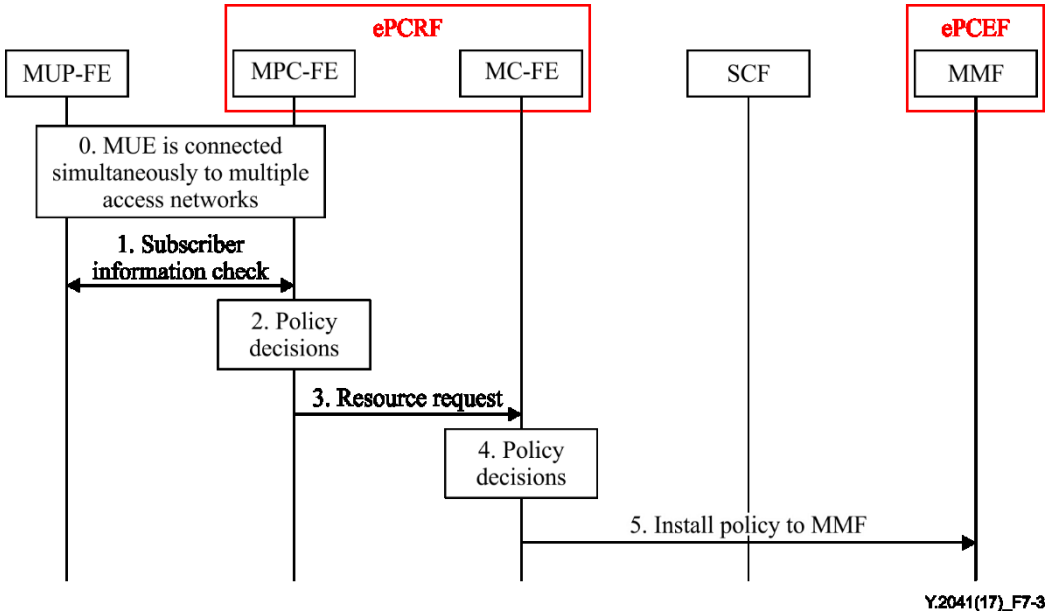

Figure 7-3 – Procedures for usage monitoring control

0) The MUE is connected to multiple access networks simultaneously and uses multiple connections to send and receive IP flows.

1) The MPC-FE sends a subscriber information check to the MUP-FE to check the subscription-related information of the MUE.

2) The MPC-FE makes policy decisions based on the information in 0)–1).

3) The MPC-FE sends a resource request to the MC-FE to support the traffic over multiple accesses.

4) The MC-FE makes policy decisions based on the information in 3).

5) The MC-FE sends the policies to the MMF for installation.

7.3.3 Procedures for IP flow

See Figure 7-4.

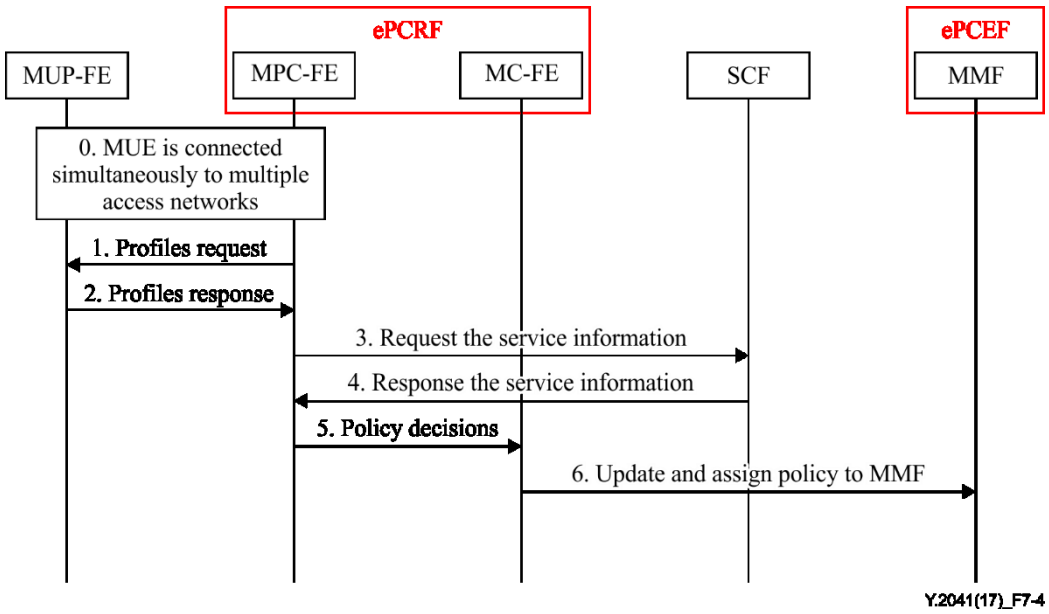

Figure 7-4 – Procedures for IP flow

0) The MUE is connected to multiple access networks simultaneously and uses multiple connections to send and receive IP flows.

1) If the ePCRF does not have the subscriber's subscription-related information, the function entity MPC-FE in the ePCRF sends a request to the MUP-FE in order to receive the information related to the IP session. The MPC-FE may request notifications from the MUP-FE on changes in the subscription information.

2) The ePCRF stores subscription-related information about the user, allowed services, allowed QoS, etc.

3) The MPC-FE then sends the request for the service information message to the SCF to require supply of the service information and policy control rules information of the subscriber (such as the priority of the connection, QoS resource and service identifier).

4) After receiving the request message, the SCF responds with the IP filter information to identify the flow for policy control, application bandwidth requirements for QoS control, etc. to the MPC-FE.

5) The MPU-FE selects new QoS policy rules for the connection based on the operator policy and the updated connection information. The MPC-FE also makes a decomposed service transmission adjustment and service separation decision, as well as providing the decisions to the MC-FE.

6) The MC-EF updates relevant rules for each access network and assigns them to the MMF, which then installs the rules.

Bibliography

[b-ITU-T X.200] Recommendation ITU-T X.200 (1994), *Information technology – Open Systems Interconnection – Basic Reference Model: The basic model*.

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

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

[b-3GPP TS 23.203] 3rd Generation Partnership Project Technical Specification 23.203 V14.3.0 (2017), *Technical Specification Group Services and System Aspects; Policy and charging control architecture (Release 14)*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2017