3GPP TR 23.855 V11.0.0 (2011-12)

Technical Report

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
Data Identification in Access Network Discovery and Selection Function (ANDSF) (DIDA)
(Release 11)

Keywords

3GPP, Architecture, EPS, WLAN, ANDSF

3GPP

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet

http://www.3gpp.org

Copyright Notification

Contents

Foreword 4
1 Scope 5
2 References 5
3 Definitions and abbreviations 5
3.1 Definitions 5
3.2 Abbreviations 5
4 Justification, Scenarios and Architectural Requirements 5
4.1 Justification 5
4.2 Architectural requirements 6
4.3 Scenarios 6
4.3.1 Identification of traffic based on throughput 6
4.3.2 Identification of traffic based on application 6
4.3.3 Identification of traffic based on content type 7
4.3.4 Identification of traffic based on destination domain 7
4.3.5 Identification of traffic based on content size 7
5 Solutions 7
5.1 Alternative 1: Extensions to ISRPs for DIDA 7
5.1.1 General 7
5.1.2 ISRPs based on destination domain 8
5.1.3 ISRPs based on application 8
5.1.4 ISRPs based on content type 8
5.1.5 ISRP based on content size 8
6 Conclusions 9
6.1 Analysis of Scenarios 9
6.2 Recommendations 10
Annex A: Change history 11

Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

This Technical Report describes proposed extensions to ANDSF Inter-System Routing Policies (ISRP) to provide to operators a better control of the network resources used for each application or IP flow. Specifically the Technical Report focuses on additional mechanism to identify classes of traffic an ISRP applies to.

Any extension to the ANDSF framework which is not related to identification of traffic is outside the scope of this Technical Report.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 23.402: "Architecture enhancements for non-3GPP accesses".

[3] 3GPP TS 23.261: "IP flow mobility and seamless WLAN offload".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [1] apply.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1] apply.

4 Justification, Scenarios and Architectural Requirements

4.1 Justification

Editor's note: This clause describes the shortcomings of current ISRP design and the justifications of DIDA work.

In Release 10 simultaneous network connections to multiple radio access technologies have been enabled by MAPCON, IFOM and non seamless WLAN offload. To take this into account, the ANDSF framework has been enhanced with the introduction of Inter System Routing Policies (ISRP), allowing the operator to provide policies based on the traffic exchanged by the UE.

Based on the current Release 10 specification the operator can indicate different preferred or forbidden radio access technologies as a function of the type of traffic the UE sends. As an example an ISRP can be based on:

- the APN the UE uses for a given connection;
- the destination IP address the UE sends traffic to;
- the destination port number the UE connects to;
- a combination of the three elements above.

The current specification has limitations on how the traffic is identified in the UE, e.g. due to the growing aggregation of Internet traffic onto few transport port numbers. This trend negatively impacts the ability of an ANDSF policy to specify how traffic should be routed by the UE. For example the operator with the current framework is not able to provide policies to the UE that allow to discriminate between video streaming (e.g. www.videostreaming.example.com) and web browsing (e.g. www.news.example.com) based on the port number because both are carried over HTTP.

4.2 Architectural requirements

The following architectural requirements apply for the DIDA solution(s):

- Support for DIDA should enable IP flows to be identified in the UE even though encryption is enabled e.g. using SSL/TLS.

4.3 Scenarios

Editor's note: This clause describes the scenarios to be taken into account for the definition of solutions.

Editor's note: Combinations of the following scenarios will also be analyzed.

4.3.1 Identification of traffic based on throughput

The operator may be interested in providing policies in order to influence the radio technology used by the UE for high-throughput traffic. As an example, the operator may indicate via ANDSF policies that IP flows which require a data rate above a certain threshold are to be sent over a given access.

Editor's note: More detailed scenarios need to be provided.

Editor's note: It is desirable to avoid the UE measuring the data rate of all IP flows to enable this scenario.

Criteria of the identification: IP flows are identified based on the required data rate

4.3.2 Identification of traffic based on application

The operator may want to set the preferred or restricted access technology for specific applications (e.g., a specific video streaming application). For example this would be useful in the following scenarios:

- The operator may want some applications to use non-seamless WLAN (NS-WLAN) offload, and other applications to be routed through the 3GPP core network. Given the high number of IP addresses used by some application servers, it is difficult to support this scenario using Rel-10 policies.
- Some applications will not work with NS-WLAN offload because service requests (i.e. control traffic) need to go through the 3GPP core network, although media traffic may be performed with NS-WLAN offload. As an example, an RTSP session may need to go through the 3GPP core (e.g. to identify and bill the subscriber) but RTP/RTCP traffic may be routed over NS-WLAN and offload the 3GPP system. To accommodate such scenarios, it is required to support ISRP policies for NS-WLAN offload of the form: "Traffic of application X and of protocol Y shall be restricted on the WLAN radio access".

Editor's note: FFS how separation of RTP and RTSP would work with NAT, Firewalls and security.

- Some applications will work with NS-WLAN offload but should preferably be routed over 3GPP access for example to enjoy improved performance from guaranteed QoS. Traffic from such applications should be identified in the UE and routed to the 3GPP radio access. For this purpose, it is required to support ISRP policies for NS-WLAN offload of the form: "Traffic of application X shall be restricted on the WLAN radio access".

This is a way for the operator to provide control over the usage of resources even for different applications which use the same port number and for services which are hosted in the same servers.

Criteria of the identification: IP flows are identified based on an application identifier or the name of the application which generated them.

4.3.3 Identification of traffic based on content type

The operator may want to set the preferred or restricted access technology for IP flows which carry a specific content type (e.g. all IP flows associated with a given MIME media type such as video, image, text). This may be needed for those applications which cannot be easily identified. This would be useful in the following scenarios:

- The operator prefers that all IP flows associated with video streaming content are routed through WLAN when available. In this case the group of applications is all applications which provide a video streaming service.

Criteria of the identification: IP flows are identified based on the content type.

4.3.4 Identification of traffic based on destination domain

With the advent of virtual hosts and Content Delivery Networks, a single IP address can actually host different services. Moreover the same service can be provided via different IP addresses depending on the location of the UE. This implies that the destination IP address and destination port that currently can be used in ISRP policies are not enough to describe a specific IP flow. To overcome this limitation, the FQDN of the application peer could be used instead. This would be useful in the following scenarios:

- The operator prefers that all traffic destined to www.example.com is routed through WLAN when available.

Criteria of the identification: IP flows are identified based on the application peer's FQDN.

4.3.5 Identification of traffic based on content size

The operator may need to restrict large content from being transferred over 3GPP access in order to protect users with limited data plans and/or to offload the 3GPP network from excess data traffic. To fulfil this need, it would be beneficial to extend data identification in the ANDSF in order to support policies, as an example, of the form:

- "Content larger than X bytes should not use 3GPP access between 10am and 5pm".

Editor's Note: It is FFS how to ensure a consistent user experience with such an operator policy.

It is expected that the content size determination will be carried out in the UE with implementation specific means. The ANDSF policies that identify traffic based on content size should be considered as operator preferences applied by the UE only when the UE can determine the size of the content.

5 Solutions

5.1 Alternative 1: Extensions to ISRPs for DIDA

5.1.1 General

Enhancements to current ISRPs can be defined to accommodate the scenarios described in section 4. The overall format of an ISRP is not expected to be affected.

The ANDSF can provide a list of ISRP to the UE based on Release 10 procedures described in TS 23.402 [2]. In order to enable enhanced IP flow identification based on the scenarios in section 4, the ISRP provided to the UE will include the following information:

- Validity conditions as per current 23.402 (Release 10).
- For IFOM: one or more Filter Rules, each one identifying a prioritised list of access technologies / access networks which should be used by the UE when available to route traffic that matches specific IP filters on a specific APN or on any APN. This is the same as in Release 10 procedure.
- For non-seamless WLAN offload: one or more Filter Rules, each one identifying which flows corresponding to specific IP filters shall or shall not be non-seamlessly offloaded to a WLAN when available. This is the same as in Release 10 procedure.
- The Filter Rules can include:
    - Previous Release 10 parameters (protocol type, source IP address, destination IP address, source port number, destination port number, address type, DSCP value);
    - Additional information as listed in the following subsections.

5.1.2 ISRPs based on destination domain

To enable ANDSF policies based on destination domain, the Filter Rules include:

- Fully Qualified Domain Name (e.g. www.example.com) that was resolved into the destination IP address.

For example, when the UE receives an ISRP with www.example.com in IP filter and WLAN as preferred access technology, it should route all traffic with destination IP addresses resolved from www.example.com through WLAN.

A combination of different IP filters parameters is possible. For example, the operator can indicate that all traffic with destination IP addresses resolved from www.example.com and with a specific destination port number should be routed through a preferred access.

5.1.3 ISRPs based on application

To enable ANDSF policies based on application, the Filter Rules include:

- A globally unique identifier of the application.

NOTE 1: Detailed definition of these IDs and respective namespace is left to stage 3.

NOTE 2: This solution assumes that the UE can bind the connection request with the application which generated that request.

For example, when the UE receives an ISRP with an application identifier in the filter and WLAN as preferred access technology, it should route all traffic generated by that application(s) through WLAN.

5.1.4 ISRPs based on content type

To enable ANDSF policies based on content type, the Filter Rules include:

- Content Type (e.g. video, image, text).

For example, when the UE receives an ISRP with content type in the filter and WLAN as preferred access technology, it should route all traffic carrying contents of which type is matched with the received content type through WLAN. The content type may be one of Internet media types included in the MIME Content-Type header.

5.1.5 ISRP based on content size

To enable ANDSF policies based on content size, the Filter Rules include:

- Range of content size.

For example, when the UE receives an ISRP with a range of content size in the filter and WLAN as preferred access technology, it should route all traffic of which size is within the received range through the WLAN. The range of content size in ISRP can be a pair of minimum and maximum of content size in bytes and the UE applies this rule if it can determine content size.

Editor's note: It is FFS how the UE determines its content size before retrieving a content.

Editor's note: Evaluation for the feasibility of this solution is also FFS.

6 Conclusions

6.1 Analysis of Scenarios

This clause provides some analysis and concluding remarks for the scenarios documented in clause 4.3.

NOTE: All references to UE refer to a UE that is capable of routing IP traffic simultaneously over multiple radio access interfaces, e.g. an IFOM capable UE or a UE capable of non-seamless WLAN offload.

Identification of traffic based on throughput

- This scenario requires the UE to identify IP flows with specific throughput requirements and route these flows based on the provisioned ANDSF policies. It is assumed that the throughput requirement of a specific IP flow is explicitly provided by the application that generates this IP flow or it is derived by the UE's operating system by other means, e.g. by pre-configuring the throughput requirements of specific IP flows. This assumption makes it unnecessary for the UE to measure the traffic rate of all IP flows in real-time and can thus avoid excessive complexity and power consumption in the UE.

- It is envisioned that in several situations the UE may not be able to determine the required throughput of an IP flow. For example, a streaming application may request a video content but does not know if the content will be provided by the server in high-definition format or not, so it cannot pre-determine how much throughput will be required to support the streaming session. In another case, the application may be able to pre-determine the required throughput of an IP flow but there is no API to provide this information to the operating system (most mobile operating systems today do not support such API). Even when the operating system is upgraded to support a new API that will enable applications to provide the required throughput of an IP flow, there is no guarantee that application developers will make use of this API.

- Based on the above considerations, it is concluded that the UE will not be able to identify the throughput requirements of IP flows in many cases. Therefore the ANDSF policies that rely on traffic identification based on throughput can only be applied on a "best-effort basis", meaning that the UE will not be able to guarantee the enforcement of these policies and the behaviour will vary a lot based on UE implementations.

Identification of traffic based on destination domain

- This scenario requires the UE to identify IP flows based on the destination FQDN, i.e. identify all flows to www.example.com.

- The UE could easily identify traffic based on the destination FQDN. For example, the UE could store all IP addresses associated with a specific FQDN (these addresses are discovered with DNS queries) and then detect which IP flows have a destination address that matches one of these IP addresses.

- It is expected that the UE could support ANDSF policies that identify traffic based on the destination FQDN and would be able to contact specific domain names over the desired radio access.

Identification of traffic based on application

- This scenario requires the UE to identify IP flows based on the application that generated them. It means to provide operators with a tool for steering the traffic of some applications to a specific radio access, for example, "traffic of application X should use 3GPP access".

- In practice, it is expected that operators will require the UE to identify the traffic of a limited number of applications; notably, of applications that the operator prefers not to use 3GPP access in the presence of a more preferred access or that are preferred to use exclusively 3GPP access. Therefore, it is not expected that operators will need to determine the identities of hundreds of applications and it is not expected that the UE will need to be provisioned with hundreds of policies for traffic identification based on application ids.

- The traffic identification in the UE based on the application identity does not intent to address all possible scenarios. For example, it may not be possible to identify malicious applications that change their identities or applications downloaded in the UE from various application repositories.

- There is no need to create a 3GPP-specific "application registry" which assigns unique identities to all possible mobile applications. Each application contains its own identity which is known to the UE and can be included in the applicable routing policies.

- Current major mobile platforms today provide some means for assigning application identities or names that are unique in the default application repository. For example, Java applications use identities/names of the form com.organization.app-name. Unique application identifiers are also used in platforms with non-Java applications. In addition, current major mobile platforms provide means to identify the traffic created by specific applications. Thus, traffic identification based on application id is expected to be feasible for UEs based on such platforms.

- Based on the above considerations, it is concluded that (*i*) it is possible to identify an application in most mobile platforms today (*ii*) the ANDSF has the means to know the UE's platform so it can provide platform specific policies to UE and (iii) traffic identification based on application id is expected to be feasible for the UE.

NOTE: Whether platform-specific ANDSF policies are distributed to the UE is left for stage 3 to decide.

Identification of traffic based on content type

- This scenario requires the UE to identify IP flows which are used to retrieve content of a specific type (e.g. audio, video, text, etc). An example use case is when the operator wants to restrict video retrieval over a specific radio access only.

- When the content is retrieved with the HTTP protocol, the UE can determine the content type before retrieving the content, e.g. by using the HEAD method. Similarly, when RTSP is used, the UE can determine the content type before retrieving the content, e.g. by sending a DESCRIBE request.

- However, to enforce IP flow routing based on content type, it is expected that the mobile platform should be capable to intercept content requests from applications and determine the content type before retrieving the requested content on the desired radio access. The use of HTTPS may also impose additional restrictions.

Identification of traffic based on content size

- This scenario requires the UE to identify IP flows which are used to retrieve content with specific size attributes. A typical example is when the operator wants to restrict very large content (e.g. more than 10Mbytes) from being transferred over 3GPP access.

- Most content retrieval on mobile devices is based on the HTTP, FTP and RTSP protocols. All of these protocols provide means for determining the content size before retrieving the content. For example, with the FTP protocol the SIZE command could be used, with the HTTP protocol the HEAD method could be used and with the RTSP protocol the DESCRIBE command could be used.

- However, to enforce IP flow routing based on the content size, it is expected that the mobile platform should be capable to intercept content requests from applications and determine the content size before retrieving the requested content on the desired radio access. The use of HTTPS may also impose additional restrictions.

6.2 Recommendations

This Technical Report has proposed and analyzed several scenarios that extend the data identification capabilities of ANDSF policies. As a result of the analysis, the following scenarios are recommended for normative specification:

- Identification of traffic based on domain name.

- Identification of traffic based on application ID.

Editor's note: Is it FFS whether other scenarios should be recommended for normative specification.

In addition, a solution based on the extension of ISRPs as the one documented in clause 5.1 is recommended for inclusion in the normative specifications.

Annex A:
Change history

Date	TSG #	TSG Doc.	CR	Rev	Cat	Subject/Comment	Old	New
2011-12	SP-54	SP-110757	-	-	-	MCC Update to version 1.0.0 for presentation to TSG SA for information and approval	0.4.0	1.0.0
2011-12	SP-54	-	-	-	-	MCC Update to version 11.0.0 after TSG SA approval	1.0.0	11.0.0