ETSI TS 129 561 V16.9.0 (2024-07)

5G;
5G System;
Interworking between 5G Network and external Data Networks;
Stage 3
(3GPP TS 29.561 version 16.9.0 Release 16)

Reference
RTS/TSGC-0329561vg90

Keywords
5G

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Legal Notice

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found under https://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Foreword

This Technical Specification 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

The present specification defines the stage 3 interworking procedures for 5G Network interworking between PLMN and external DN or Network Slice Specific AAA.

The stage 2 requirements and procedures are contained in 3GPP TS 23.501 [2] and 3GPP TS 23.502 [3].

For interworking between 5G PLMN and external DNs, the present document is valid for both 3GPP accesses and non-3GPP accesses.

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 23.501: "System Architecture for the 5G System; Stage 2".

[3] 3GPP TS 23.502: "Procedures for the 5G System; Stage 2".

[4] 3GPP TS 29.281: "General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U)".

[5] 3GPP TS 29.061: "Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN)".

[6] IETF RFC 3748: "Extensible Authentication Protocol (EAP)".

[7] IETF RFC 3579: "RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)".

[8] IETF RFC 2865: "Remote Authentication Dial In User Service (RADIUS)".

[9] IETF RFC 3162: "RADIUS and IPv6".

[10] IETF RFC 4818: "RADIUS Delegated-IPv6-Prefix Attribute".

[11] IETF RFC 5216: "The EAP-TLS Authentication Protocol".

[12] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

[13] 3GPP TS 24.229: "IP Multimedia Call Control Protocol based on SIP and SDP; Stage 3".

[14] IETF RFC 2132: "DHCP Options and BOOTP Vendor Extensions".

[15] IETF RFC 3361: "Dynamic Host Configuration Protocol (DHCP-for-IPv4) Option for Session Initiation Protocol (SIP) Servers".

[16] IETF RFC 3646: "DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)".

[17] IETF RFC 3319: "Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers".

[18] IETF RFC 2131: "Dynamic Host Configuration Protocol".

[19] IETF RFC 1542: "Clarification and Extensions for the Bootstrap Protocol".

[20] IETF RFC 4039: "Rapid Commit Option for the Dynamic Host Configuration Protocol version 4 (DHCPv4)".

[21] IETF RFC 3315: "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)".

[22] IETF RFC 3736: "Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6".

[23] IETF RFC 7155: "Diameter Network Access Server Application".

[24] IETF RFC 6733: "Diameter Base Protocol".

[25] IETF RFC 4072: "Diameter Extensible Authentication Protocol (EAP) Application".

[26] IETF RFC 2866: "RADIUS Accounting".

[27] IETF RFC 5176: "Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)".

[28] 3GPP TS 23.003: "Numbering, addressing and identification".

[29] IETF RFC 1825: "Security Architecture for the Internet Protocol".

[30] IETF RFC 1826: "IP Authentication Header".

[31] IETF RFC 1827: "IP Encapsulating Security Payload (ESP)".

[32] IETF RFC 4291: "IP Version 6 Addressing Architecture".

[33] IETF RFC 4861: "Neighbor Discovery for IP Version 6 (IPv6)".

[34] IETF RFC 4862: "IPv6 Stateless Address Autoconfiguration".

[35] IETF RFC 1027: "Using ARP to Implement Transparent Subnet Gateways".

[36] 802.3-2015 - IEEE Standard for Ethernet.

[37] IETF RFC 5281: "Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0)".

[38] 3GPP TS 23.380: "IMS Restoration Procedures".

[39] 3GPP TS 29.571: "5G System; Common Data Types for Service Based Interfaces; Stage 3".

[40] 3GPP TS 29.502: "5G System; Session Management Services; Stage 3".

[41] 3GPP TS 29.229: "Cx and Dx interfaces based on Diameter protocol; Protocol details".

[42] 3GPP TS 24.501: "Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3".

[43] 3GPP TS 23.316: "Wireless and wireline convergence access support for the 5G System (5GS)".

[44] IETF RFC 7761: "Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)".

[45] IETF RFC 3973: "Protocol Independent Multicast - Dense Mode (PIM-DM): Protocol Specification (Revised)".

[46] 3GPP TS 29.571: "5G System; Common Data Types for Service Based Interfaces Stage 3".

[47] IETF RFC 2132: "DHCP Options and BOOTP Vendor Extensions".

[48] IETF RFC 3925: "Vendor-Identifying Vendor Options for Dynamic Host Configuration Protocol version 4 (DHCPv4)".

[49] IETF RFC 8415: "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)".

[50] 3GPP TS 29.274: "3GPP Evolved Packet System. Evolved GPRS Tunnelling Protocol for EPS (GTPv2)".

[51] CableLabs WR-TR-5WWC-ARCH: "5G Wireless Wireline Converged Core Architecture".

[52] BBF WT-470: "5G FMC Architecture".

[53] CableLabs DOCSIS MULPI: "Data-Over-Cable Service Interface Specifications DOCSIS 3.1, MAC and Upper Layer Protocols Interface Specification".

[54] IETF RFC 7542: "The Network Access Identifier".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

5G-BRG	5G Broadband Residential Gateway
5G-CRG	5G Cable Residential Gateway
BBF	Broadband Forum
CSMA/CD	Carrier Sense Multiple Access/Collision Detection
DHCPv4	Dynamic Host Configuration Protocol version 4
DHCPv6	Dynamic Host Configuration Protocol version 6
DN	Data Network
DR	Designated Router
DSL	Digital Subscriber Line
FN-BRG	Fixed Network Broadband RG
FN-CRG	Fixed Network Cable RG
GPSI	Generic Public Subscription Identifier
GCI	Global Cable Identifier
GLI	Global Line Identifier
HFC	Hybrid Fiber Coax
N3IWF	Non-3GPP InterWorking Function
NGAP	NG Application Protocol
NSS	Network Slice Specific
NSSAAF	Network Slice-Specific Authentication and Authorization Function
PIM	Protocol-Independent Multicast
PIM-DM	Protocol-Independent Multicast- Dense Mode
PIM-SM	Protocol-Independent Multicast- Sparse Mode
PON	Passive Optical Network
PtP	Point-to-Point
RG	Residential Gateway
RP	Rendezvous Point
SD	Slice Differentiator
SFD	Start Frame Delimiter
SMF	Session Management Function
S-NSSAI	Single Network Slice Selection Assistance Information
SNPN	Stand-alone Non-Public Network

SSC	Session and Service Continuity
SST	Slice/Service Type
TNAP	Trusted Non-3GPP Access Point
TWAP	Trusted WLAN Access Point
UPF	User Plane Function
WAN	Wide Area Network

4 Network Characteristics

4.1 Key characteristics of PLMN

The PLMN is fully defined in the 3GPP technical specifications. The 5G Network related key characteristics are defined in 3GPP TS 23.501 [2].

4.2 Key characteristics of IP Networks

The Internet is a conglomeration of networks utilising a common set of protocols. IP protocols are defined in the relevant IETF RFCs. The networks topologies may be based on LANs (e.g. Ethernet), Point to Point leased lines, PSTN, ISDN, X.25 or WANs using switched technology (e.g. SMDS, ATM).

4.3 Key characteristics of Ethernet

The Ethernet is a family of computer networking technologies commonly used in LAN and is often used to refer to all Carrier Sense Multiple Access/Collision Detection (CSMA/CD) LANs that generally conform to Ethernet Specifications, including IEEE 802.3 [36]. The key characteristics for Ethernet are defined in IEEE 802.3 [36].

5 Interworking Classifications

5.1 Service Interworking

Service interworking is required when the Teleservice at the calling and called terminals are different. No service interworking is specified in this specification.

5.2 Network Interworking

Network interworking is required whenever a PLMN is involved in communications with another network to provide end-to-end communications. The PLMN shall interconnect in a manner consistent with that of a normal Data Network (type defined by the requirements e.g. IP). Interworking appears exactly like that of Data Networks.

6 Reference Architecture

Figure 6-1 shows the access interfaces for the 5G Network. The 5G Network includes both the 3GPP access and the non-3GPP access.

The NSS-AAA may belong to the H-PLMN in the 5G Network (without AAA-P interworking) or a 3rd party (with AAA-P interworking).

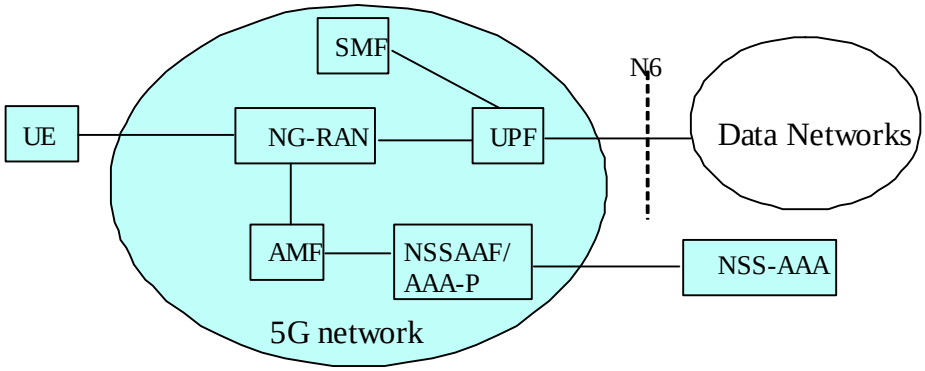

Figure 6-1: Reference Architecture for 5G Network Interworking

NOTE: The SMF represents the H-SMF in the home routed scenario.

7 Interface to 5G Network services (User Plane)

The user plane for 5G Network services is defined in subclause 8.3 of 3GPP TS 23.501 [2] and 3GPP TS 29.281 [4].

8 Interworking with DN (IP)

8.1 General

5GS shall support interworking with DNs based on the Internet Protocol (IP). These interworked networks may be either intranets or the Internet.

8.2 DN Interworking Model

8.2.1 General

When interworking with the IP networks, the 5GS can operate IPv4 and/or IPv6. The interworking point is shown in clause 6.

The UPF for interworking with the IP network is the 5GS access point (see figure 8.2.1-1).

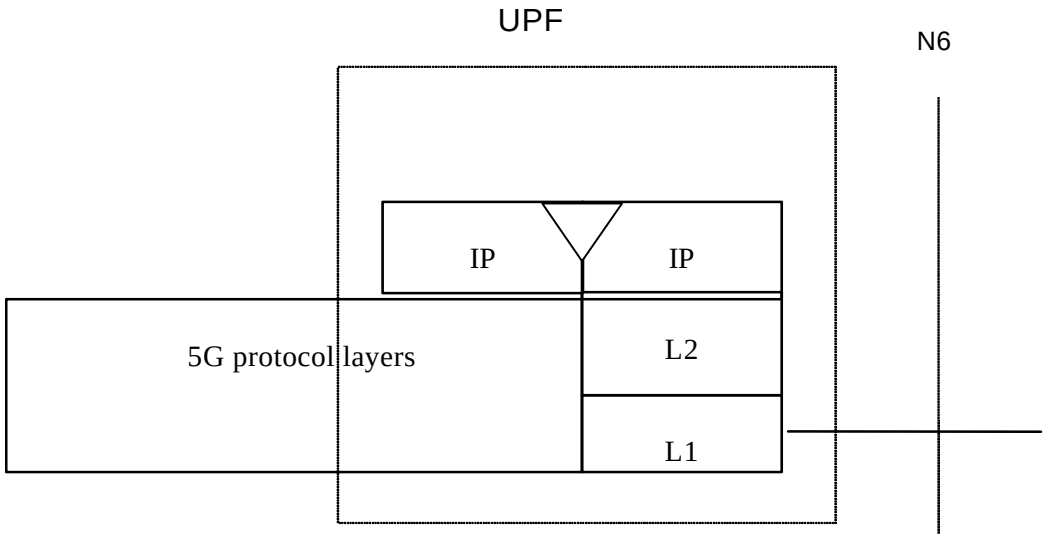

Figure 8.2.1-1: The protocol stacks of UPF for the IP network interworking

Typically, in the IP networks, the interworking with subnetworks is done via IP routers. The N6 reference point is between the UPF and the external IP network. From the external IP network's point of view, the UPF is seen as a normal IP router. The L2 and L1 layers are operator specific.

It is out of the scope of the present document to standardise the router functions and the used protocols in the N6 reference point.

Interworking with user defined ISPs and private/public IP networks is subject to interconnect agreements between the network operators.

8.2.2 Access to DN through 5G Network

8.2.2.1 Transparent access to DN

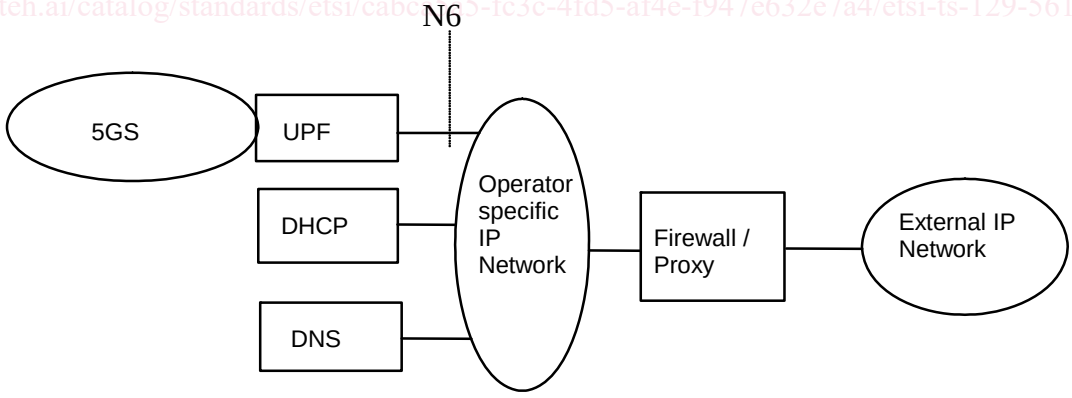

Figure 8.2.2.1-1: Example of the DN Interworking Model, transparent case

In figure 8.2.2.1-1, an example DN interworking model for transparent access to the Internet is provided for an UPF in the 5GS and its N6 reference point.

In transparent access to the Internet case:

- the UE is given an IPv4 address and/or an IPv6 prefix belonging to the operator addressing space. The IPv4 address and/or IPv6 prefix is assigned either at subscription in which case it is a static address or at PDU session establishment in which case it is a dynamic address. This IPv4 address and/or IPv6 prefix if applicable is used for packet forwarding between the Internet and the UPF and within the 5GS. With IPv6, Stateless Address Autoconfiguration shall be used to assign an IPv6 address to the UE. These procedures are as described in the IPv6 non-transparent access case except that the addresses belong to the operator addressing space.

- the UE need not send any authentication request at PDU session establishment procedure and the SMF/UPF need not take any part in the user authentication/authorization process.

The transparent case provides at least a basic ISP service. As a consequence of this it may therefore provide a QoS flow service for a tunnel to a private Intranet. The user level configuration may be carried out between the UE and the intranet, the 5GS is transparent to this procedure. The used protocol stack is depicted in figure 8.2.2.1-2.

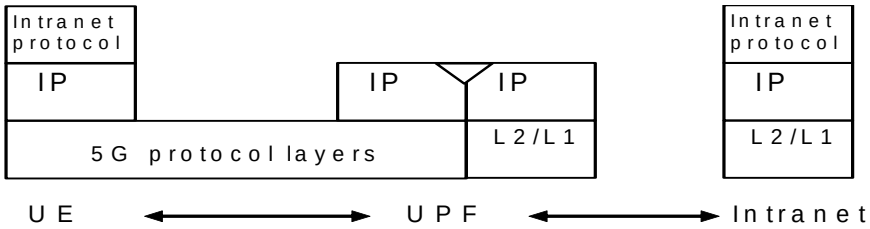

Figure 8.2.2.1-2: Transparent access to an Intranet

The communication between the PLMN and the Intranet may be performed over any network, even an insecure network e.g. the Internet. There is no specific security protocol between the UPF and the Intranet because security is ensured on an end to end basis between the UE and the intranet by the "Intranet Protocol".

User authentication and encryption of user data are done within the "Intranet Protocol" if either of them is needed. This "Intranet Protocol" may also carry private (IP) addresses belonging to the address space of the Intranet.

An example of an "Intranet Protocol" is IPsec (see IETF RFC 1825 [29]). If IPsec is used for this purpose, then IPsec authentication header or security header may be used for user (data) authentication and for the confidentiality of user data (see IETF RFC 1826 [30] and IETF RFC 1827 [31]). In this case private IP tunnelling within public IP takes place.

8.2.2.2 IPv4 Non-transparent access to DN

In this case:

- a static or a dynamic IPv4 address belonging to the Intranet/ISP addressing space is allocated to a UE at PDU session establishment. The methods of allocating IP address to the UE are specified in 3GPP TS 23.501 [2]. The allocated IPv4 address is used for packet forwarding within the UPF and for packet forwarding on the Intranet/ISP;

- as a part of the PDU session establishment, the SMF may request user authentication from an external DN-AAA server (i.e. RADIUS, Diameter) belonging to the Intranet/ISP;

- the IPv4 address allocation to the UE may be performed based on the subscription or a local address pool, which belongs to the Intranet/ISP addressing space, provisioned in the SMF; or via the address allocation servers (i.e. DHCPv4, RADIUS DN-AAA, Diameter DN-AAA) belonging to the Intranet/ISP;

- if requested by the UE at PDU session establishment, the SMF may retrieve the Protocol Configuration Options or IPv4 configuration parameters from a locally provisioned database in SMF and/or from some external server (i.e. DHCPv4, RADIUS DN-AAA, Diameter DN-AAA) belonging to the Intranet/ISP;

- the communication between the 5GS and the Intranet/ISP may be performed over any network, even an insecure network, e.g. the Internet. In case of an insecure connection between the UPF and the Intranet/ISP, there may be a specific security protocol in between. This security protocol is defined by mutual agreement between PLMN operator and Intranet/ISP administrator.

Table 8.2.2.2-1 summarizes the IPv4 address allocation and parameter configuration use cases between the UE and the SMF that may lead the SMF to interwork with the external DHCPv4, DN-AAA servers. For detailed description of the signalling flows between the UE and the SMF, see the references in the table.