**3GPP TSG-CT WG3 Meeting #116e C3-213310**

**E-Meeting, 19th – 28th May 2021 (Revision of C3-213213)**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **29.561** | **CR** | **0107** | **rev** | **2** | **Current version:** | **17.1.0** |  |
|  |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* |
|  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME |  | Radio Access Network |  | Core Network | **X** |

|  |
| --- |
|  |
| ***Title:***  | Updates to support L2TP for CUPS |
|  |  |
| ***Source to WG:*** | Ericsson |
| ***Source to TSG:*** | CT3 |
|  |  |
| ***Work item code:*** | BEPoP |  | ***Date:*** | 2021-05-06 |
|  |  |  |  |  |
| ***Category:*** | **B** |  | ***Release:*** |  Rel-17 |
|  | *Use one of the following categories:****F*** *(correction)****A*** *(mirror corresponding to a change in an earlier release)****B*** *(addition of feature),* ***C*** *(functional modification of feature)****D*** *(editorial modification)*Detailed explanations of the above categories canbe found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | *Use one of the following releases:Rel-8 (Release 8)Rel-9 (Release 9)Rel-10 (Release 10)Rel-11 (Release 11)…Rel-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** | CT4 has studied and agreed L2TP supporting for CUPS in WI BEPoP,TR 29.820 has also concluded to support L2TP tunneling over N6/SGi for 5GC/EPS is to be standardized based on the solution#8 as described in 6.8 in Rel-17, and CT3 scope has been added in WI BEPoP.Meanwhile, SA2 LS Reply on the support of L2TP with CUPS in rel-17 to support L2TP tunnelling over N6/SGi for 5GS and EPS, with TS 23.501 CR 2691 and TS 23.502 CR 2602 approved.So before preparing the detail attributes/AVPs for RADIUS/Diameter messages, the general support L2TP tunneling for CUPS across N6 interface is prepared in this CR. |
|  |  |
| ***Summary of change:*** | Adding L2TP RFC 2661 and general description and procedures supporting L2TP for CUPS across N6 interface. |
|  |  |
| ***Consequences if not approved:*** | Missing the general description and procedures on L2TP support for CUPS across N6 interface, cannot further implement the RADIU/Diameter message supporting L2TP in this specification. |
|  |  |
| ***Clauses affected:*** | 2, 3.2, X(new) |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** | **X** |  |  Other core specifications  | TS 23.501 CR 2691TS 23.502 CR 2602 |
| ***affected:*** |  | **X** |  Test specifications |  |
| ***(show related CRs)*** |  | **X** |  O&M Specifications |  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** |  |

**Additional discussion(if needed):**

**Proposed changes:**

\*\*\* 1st Change \*\*\*

# 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] 3GPP TS 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".

[54] BBF TR-456: "AGF Functional Requirements".

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

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

[x] IETF RFC 2661: " Layer Two Tunneling Protocol "L2TP".

[y] 3GPP TS 29.244: "Interface between the Control Plane and the User Plane of EPC Nodes; Stage 3".

\*\*\* 2nd Change \*\*\*

## 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

AMF Access and Mobility Management Function

BBF Broadband Forum

CHAP Challenge Handshake Authentication Protocol

CHF Charging Function

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

FQDN Fully Qualified Domain Name

GCI Global Cable Identifier

GLI Global Line Identifier

GPSI Generic Public Subscription Identifier

HFC Hybrid Fiber Coax

I-SMF Intermediate SMF

L2TP Layer Two Tunneling Protocol

LAC L2TP Access Concentrator

LNS L2TP Network Server

N3IWF Non-3GPP InterWorking Function

NGAP NG Application Protocol

NSS Network Slice Specific

NSSAAF Network Slice-Specific Authentication and Authorization Function

PAP Password Authentication Protocol

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

V-SMF Visited SMF

WAN Wide Area Network

\*\*\* 3rd Change \*\*\*

# X(new) Interworking with DN (L2TP tunnel)

## X.1(new) Support L2TP for CUPS across N6

L2TP (described in RFC 2661 [x]) is a standard method for tunneling encapsulated Point-to-Point Protocol (PPP) frames over an IP network. L2TP operates between two L2TP endpoints (LAC and LNS), and tunnels PPP-encapsulated IP traffic between these endpoints. L2TP runs over UDP/IP and was originally defined for systems where PPP is used by an end-device to connect to a network (e.g. via DSL connections, or 2G/3G PPP PDP context). In these cases, a LAC could be deployed in the network (e.g. in a BNG or GGSN/PGW) to tunnel the PPP traffic to a server (LNS) over an IP network.

For 5GC with the UE using IP PDU Session, the PPP functionality that is required to use L2TP is instead supported by the UPF or UPF+PGW-U, as illustrated in below figure. Upon receiving a PDU Session/PDN Connection establishment request from the UE via AMF or MME, SMF or SMF+PGW-C may depend on local L2TP configuration per DNN or the received L2TP information from a DN AAA server in Access-Accept message, request the UPF or UPF+PGW-U to setup L2TP tunnel towards an L2TP network server (LNS) in the external DN and tunnel the PDU Session user plane traffic in this L2TP tunnel. In this case the UPF or UPF+PGW-U acts as a L2TP access concentrator (LAC).

To enable this, the SMF or SMF+PGW-C may provide L2TP information to the UPF or UPF+PGW-U as LAC, such as LNS IP address or FQDN, as described in 3GPP TS 29.244 [y]. This L2TP information may be configured on the SMF or SMF+PGW-C as part of the DNN configuration or received from the DN-AAA server. Alternatively, the L2TP tunnel parameters may be configured in the UPF or UPF+PGW-U. The L2TP tunnel parameters include necessary parameters for setting up L2TP tunnel towards the LNS (e.g. LNS address, tunnel password).

In addition, the SMF or SMF+PGW-C may provide PAP/CHAP authentication information to the UPF or UPF+PGW-U, for use in L2TP session establishment, in case it was received from the UE in the ePCO IE of the PDU Session Establishment Request.

When L2TP is to be used for a PDU Session, the SMF or SMF+PGW-C may select a UPF or UPF+PGW-U and requests the UE IP address to be allocated by LNS according to 3GPP TS 29.244 [y], the UPF (LAC) may retrieve this IP address from the LNS.



Figure X.1-1: L2TP Tunnel between 5GC and external DN

Below figure describes the L2TP connection procedures between 5GC and external DN, upon the UE is accessed in 5GC and the SMF or SMF+PGW-C and UPF or UPF+PGW-U has been negotiated supporting L2TP feature.



Figure X.1-2: L2TP connection procedures between 5GC and external DN

0. The SMF or SMF+PGW-C and the UPF or UPF+PGW-U negotiated supporting L2TP feature as specified in 3GPP TS 29.244 [114].

1. The SMF or SMF+PGW-C receives a PDU Session or PDN Connection establishment request from the UE via AMF or MME and SGW.

 The UE may include the authentication information for PAP and/or CHAP in ePCO IE. The SMF or SMF+PGW-C may locally configure the UE authentication information for a given DNN.

 The SMF or SMF+PGW-C may determine that an L2TP session is required for the PDU Session based on local configured L2TP parameters per DNN.

2. The SMF or SMF+PGW-C may receive the L2TP Tunnel parameters (e.g. LNS IP address or FQDN, tunnel password) from the DN-AAA server in Access-Accept message or Diameter EAP Answer (DEA) message, or local configured.

3. If L2TP protocol is determined to support the PDU Session, the SMF or SMF+PGW-C selects a UPF or UPF+PGW-U supporting L2TP and be configured with the LAC name/addresses and then requests the UPF or UPF+PGW-U to setup an L2TP tunnel if needed and/or L2TP session towards the L2TP network server (LNS). For a given DNN requiring L2TP function, multiple LACs may be configured to be connected with multiple LNSs in the Data Network.

 The SMF or SMF+PGW-C sends PFCP Session Establishment Request to the UPF or UPF+PGW-U, which may include L2TP Tunnel Information for setting up a L2TP tunnel and L2TP session information to setup a L2TP session, together with the information for authentication used during L2TP Tunnel setup, as well as for L2TP session.

 The L2TP Tunnel Information includes LNS IPv4 address or IPv6 address of LNS, Tunnel Password.

 The L2TP Session Information includes specific information related to the PDU Session, e.g. a Calling Number which may be set to UE's GPSI, an indication to instruct that the UPF or UPF+PGW-U shall request the LNS to allocate an IP address for the PDU Session, indications to instruct that the UPF or UPF+PGW-U shall request the LNS to provide DNS server addresses or NBNS server addresses etc. as specified in 3GPP TS 29.244 [114].

4. The UPF or UPF+PGW-U checks if any existing L2TP tunnel can be used to serve the PDU Session according to the information provided in the L2TP Tunnel Information.

If the UPF or UPF+PGW-U decides to setup a new L2TP tunnel, it initiates L2TP Tunnel establishment by sending an SCCRQ (Start-Control-Connection-Request) message towards the LNS, the UPF or UPF+PGW-U will allocate a Tunnel ID, and it may include a CHAP Challenge to authenticate the LNS. The Challenge and Challenge Response (to be included in SCCCN) is produced by the UPF or UPF+PGW-U using the Tunnel Password received from the SMF or SMF+PGW-C.

 The LNS responds with an SCCRP (Start-Control-Connection-Reply) message, containing its allocated Tunnel ID and a CHAP Challenge Response to the Challenge in SCCRQ.

 The UPF or UPF+PGW-U then responds with a Challenge response for tunnel authentication in the SCCCN (Start-Control-Connection-Connected) message. An L2TP tunnel is established after the tunnel authentication is successful, with the reception of the SCCCN message sent by the LAC to the LNS.

 If the UPF or UPF+PGW-U decides to use an already existing L2TP tunnel for the requested PDU Session from the UPF or UPF+PGW-C, it proceeds with step 5 below directly without current step.

5. Once the L2TP Tunnel is established (or already present) between the LAC and the LNS for the PDU Session/PDN Connection requested by the UE, the UPF or UPF+PGW-U proceeds with L2TP session setup towards the LNS.

 The UPF or UPF+PGW-U sends an ICRQ (Incoming-Call-Request) message towards the LNS, which contains the Tunnel ID assigned by the LNS, its assigned Session ID, and optionally, the Calling Number and Called Number. The LNS responds with an ICRP (Incoming-Call-Reply) message and provides the Session ID assigned by it to the LAC.

 The LAC then sends an ICCN (Incoming-Call-Connected) message. The UPF or UPF+PGW-U includes the UE authentication information from the SMF or SMF+PGW-C received via ePCO IE in step 1. In addition, the UPF or UPF+PGW-U (LAC) will act as a PPP endpoint to use LCP to communicate some link control parameters, e.g. MRU; to use PAP/CHAP to perform an authentication procedure; to use IPCP to request PDU Session IP Address, DNS server address and/or NBNS server address(es).

 Otherwise, after the reception of the ICCN message, the LNS responds with a ZLB Ack message. After the reception of ZLB Ack message, the LAC and LNS will use PPP LCP to communicate link specific control parameter, and indicate authentication type, then either PPP PAP/CHAP takes place. The PPP IPCP transactions takes places to retrieve UE IP Address, DNS server address and/or NBNS server address.

6. The status of the L2TP session setup is sent by the SMF or SMF+PGW-C to the UPF or UPF+PGW-U in a PFCP Session Establishment Response.

7. The SMF or SMF+PGW-C sends a PDU Session Establishment Response to the UE and the user data session is initiated, which may contain the DNS and NBNS Server information.

\*\*\* End of Changes \*\*\*