3GPP TSG CN Plenary Meeting #17 **NP-020408**
4th - 6th September 2002. Biarritz, France.

Source: **TSG CN WG 3**

Title: **CRs to Rel-5 Work Item TEI [GPRS]**

Agenda item: **8.8**

Document for: **APPROVAL**

Introduction:

This document contains **2** CRs on **Rel-5** Work Item **"TEI [GPRS]"**, that have been agreed by **TSG CN WG3**, and are forwarded to TSG CN Plenary meeting #17 for approval.

Doc-2nd-	Spec	CR	Rev	Subject	Cat	Phase	Version-	Workitem
N3-020669	27.060	023	2	Configuration of Domain Name System (DNS) server IPv6 addresses	F	Rel-5	5.1.0	TEI [GPRS]
N3-020688	29.061	061	2	Configuration of Domain Name System (DNS) server IPv6 addresses	F	Rel-5	5.2.0	TEI [GPRS]

3GPP TSG-CN WG3 Meeting #24
Helsinki, Finland, 28th July - 2nd Aug 2002.

Tdoc ⌘N3-020669

CR-Form-v7

CHANGE REQUEST

⌘	**27.060**	**CR**	**023**	⌘ **rev**	**2**	⌘	Current version:	**5.1.0**	⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects:	UICC apps⌘ [ ]	ME [X]	Radio Access Network [ ]	Core Network [ ]	

Title:	⌘	Configuration of Domain Name System (DNS) server IPV6 addresses		
Source:	⌘	TSG_CN WG3		
Work item code:	⌘	TEI [GPRS]	***Date:*** ⌘	22/06/2002
Category:	⌘	F	***Release:*** ⌘	REL-5
		Use one of the following categories: ***F*** *(correction)* ***A*** *(corresponds to a correction in an earlier release)* ***B*** *(addition of feature),* ***C*** *(functional modification of feature)* ***D*** *(editorial modification)* Detailed explanations of the above categories can be found in 3GPP TR 21.900.		*Use one of the following releases:* *2 (GSM Phase 2)* *R96 (Release 1996)* *R97 (Release 1997)* *R98 (Release 1998)* *R99 (Release 1999)* *Rel-4 (Release 4)* *Rel-5 (Release 5)* *Rel-6 (Release 6)*

Reason for change:	⌘	There is currently no support for dynamic configuration of Domain Name System (DNS) server IPV6 addresses in a MS not supporting the DHCPv6 protocol.
Summary of change:	⌘	Introduces the possibility of dynamic configuration of Domain Name System (DNS) server IPV6 addresses via existing Session Management procedures by use of the protocol Configuration Options IE.
Consequences if not approved:	⌘	No support for dynamic configuration of Domain Name System (DNS) server IPV6 addresses in a MS not supporting the optional DHCPv6 protocol.

Clauses affected:	⌘	2, 3.2, 9.1.2				
		Y	**N**			
Other specs affected:	⌘	X		Other core specifications	⌘	24.008, 24.229, 29.061
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

First modified section

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.

[1] Void.

[2] Void.

[3] 3GPP TS 22.060: "General Packet Radio Service (GPRS); Service Description Stage 1".

[4] Void.

[5] Void.

[6] Void.

[7] Void.

[8] Void.

[9] 3GPP TS 23.060: "General Packet Radio Service (GPRS) Service Description Stage 2".

[10] Void.

[11] Void.

[12] Void.

[13] Void.

[14] Void.

[15] Void.

[16] 3GPP TS 27.007: "AT command set for 3GPP User Equipment (UE)".

[17] 3GPP TS 29.061: "Packet Domain; Interworking between the Public Land Mobile Network (PLMN) supporting Packet Based Services and Packet Data Networks (PDN)".

[18] ITU-T Recommendation E.164: "Numbering plan for the ISDN era".

[19] ITU-T Recommendation V.42 bis: "Data communication over the telephone network – Data compression procedures for data circuit-terminating equipment (DCE) using error correction procedures".

[20] Void.

[21] Void.

[22] Void.

[23] Void.

[24] Void.

[25] Void.

[26] IETF RFC 768 (1980): "User Datagram Protocol" (STD 6).

[27] IETF RFC 791 (1981): "Internet Protocol" (STD 5).

[28] IETF RFC 792 (1981): "Internet Control Message Protocol" (STD 5).

[29] IETF RFC 793 (1981): "Transmission Control Protocol" (STD 7).

[30] ITU-T Recommendation V.250 (ex V.25ter): "Serial asynchronous automatic dialling and control".

[31] ITU-T Recommendation V.24: "List of definitions for interchange circuits between data terminal equipment (DTE) and data circuit-terminating equipment (DCE)".

[32] ITU-T Recommendation V.28: "Electrical Chracteristics for unbalanced double-current interchange circuits".

[33] ITU-T Recommendation V.80: "In-band DCE control and synchronous data modes for asynchronous DTE".

[34] IETF RFC 1661 (1994): "The Point-to-Point Protocol (PPP)" (STD 51).

[35] IETF RFC 1662 (1994): "PPP in HDLC-like framing" (STD 51).

[36] IETF RFC 1700 (1994): "Assigned Numbers" (STD 2).

[37] IETF RFC 1570 (1994): "PPP LCP Extensions".

[38] IETF RFC 1989 (1996): "PPP Link Quality Monitoring".

[39] IETF RFC 1332 (1992): "The PPP Internet Protocol Control Protocol (IPCP)".

[40] IETF RFC 1877 (1995): "PPP IPCP Extensions for Name Server Addresses ".

[41] IETF RFC 2153 (1997): "PPP Vendor Extensions".

[42] IETF RFC 1334 (1992): "PPP Authentication Protocols".

[43] IETF RFC 1994 (1996): "PPP Challenge Handshake Authentication Protocol".

[44] IETF RFC 2686 (1999): "The Multi-Class Extension to Multi-Link PPP".

[45] IETF RFC 1990 (1996): "The PPP Multilink Protocol (MP)".

[46] IETF RFC 2472 (1998): "IP Version 6 over PPP".

[47] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[48] 3GPP TS 23.221: "Architectural requirements".

[49] IETF RFC 2373 (1998): "IP version 6 Addressing Architecture".

[50] IETF RFC 1034 (1987): "Domain Names - Concepts and Facilities" (STD 13).

[51] IETF RFC 1035 (1987): "Domain Names - Implementation and Specification" (STD 13).

[52] IETF RFC 1886 (1995): "DNS Extensions to support IP version 6".

Next modified section

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

APN	Access Point Name
DNS	Domain Name System
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
GSN	GPRS Support Node
GTP-U	GPRS Tunnelling Protocol for user plane
HDLC	High Level Data Link Control
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPV6CP	IPv6 Control Protocol
LA	Location Area
LCP	Link Control Protocol
LLC	Logical Link Control
MAC	Medium Access Control
MCML	Multi-Class Multi-Link PPP
ME	Mobile Equipment
MP	Multilink PPP
MS	Mobile Station
MT	Mobile Termination
NCP	Network Control Protocol
PDCP	Packet Data Convergence Protocol
PDN	Packet Data Network
PDP	Packet Data Protocol , e.g., IP or PPP
PDU	Protocol Data Unit
PPP	Point-to-Point Protocol
PS	Packet Switched
PTM	Point To Multipoint
PTP	Point To Point
PVC	Permanent Virtual Circuit
RA	Routing Area
SGSN	Serving GPRS Support Node
SNDCP	SubNetwork Dependent Convergence Protocol
TCP	Transmission Control Protocol
TE	Terminal Equipment
TFT	Traffic Flow Template
UDP	User Datagram Protocol

Next modified section

9.1.2 IPv6 over PPP

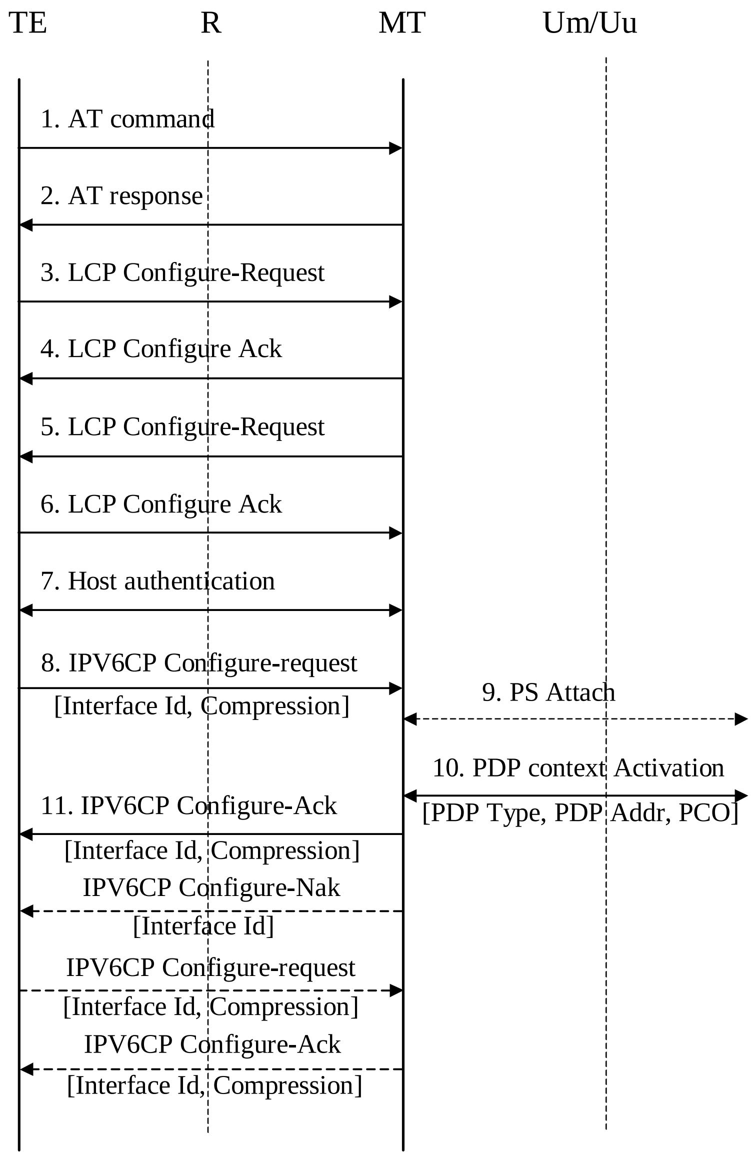


Figure 7b: PDP Context Activation for the IPv6 over PPP based services

1) The TE issues AT commands to set up parameters and enter PPP mode (refer to subclause on- AT commands for further details).

2) The MT sends AT responses to the TE.

3) The PPP protocol in the TE sends a LCP Configure-Request. This command is to establish a PPP link between the TE and the MT.

4) The MT returns LCP Configure-Ack to the TE to confirm that the PPP link has been established. The MT might previously have sent a LCP Configure-Nak in order to reject some options proposed by the TE. This in turn might have triggered a retransmission of the LCP Configure-Request with different options.

5) The PPP protocol in the MT sends a LCP Configure-Request in order to negotiate for the authentication protocol used for authentication of the host TE towards the MT. The MT shall initially negotiate for CHAP, and if this is unsuccessful, for PAP.

6) The TE returns a LCP Configure-Ack to the MT to confirm the use of the specified authentication protocol. The MT might previously have sent a LCP Configure-Nak in order to reject the protocol proposed by the TE. This in turn might have triggered a retransmission of the LCP Configure-Request with different options.

7) If the negotiated authentication protocol is either of CHAP or PAP, the TE authenticates itself towards the MT by means of that protocol. The MT stores the necessary authentication data and sends a locally generated positive acknowledgement of the authentication to the TE. If none of the protocols is supported by the host TE no authentication shall be performed. Refer to 3GPP TS 29.061 for further details on the authentication.

8) The TE requests IPv6 Interface-Identifier negotiation by sending the IPV6CP Configure-Request message to the MT indicating the tentative Interface-Identifier chosen by the TE. The tentative Interface-Identifier has only local significance in the MT and shall not forwarded to the GGSN.

9) If the MS is not yet PS attached, the MT performs the PS Attach procedure as described in 3GPP TS 23.060.

10) The MT sends the Activate PDP context request message to the network, including the PDP Type, PDP Address and Protocol Configuration Options. The Protocol Configuration Options IE may contain negotiated LCP options such as negotiated Authentication Protocol as well as any authentication data previously stored in the MT. It may also contain a request for dynamic configuration of DNS server IPv6 addresses as described in 3GPP TS 29.061 [17]. The MS shall leave PDP Address empty and set PDP Type to 'IPv6'.
Note: The protocol between the TE and MT may not support the same set of information as the interface from the MT to the network (eg. DNS).

    The network responds with an Activate PDP Context Accept or an Activate PDP Context Reject, to the MS. The Protocol Configuration Options IE may contain configuration data such as a list of DNS server IPv6 addresses as described in 3GPP TS 29.061 [17]. In cases where the MS receives more than one server address, the MS shall adhere to the explicit prioritisation order of the list. The PDP Address shall contain an IPv6 address composed of a Prefix and an Interface-Identifier. The size of the Prefix shall be according to the maximum prefix length for a global IPv6 address as specified in the IPv6 Addressing Architecture, see RFC 2373 [49]. The Interface-Identifier shall be used to create a link-local IPv6 address, to be used in continued MS – GGSN user-plane signalling. The Prefix in the PDP Address shall be ignored by the MS.

11) In case a PDP Context Accept was sent to the MS, the MT extracts the Interface-Identifier from the address received in the PDP Address IE and ignores the Prefix part. If this Interface-Identifier is identical to the tentative Interface-Identifier indicated in the IPV6CP Configure-Request message sent from the TE, the MT sends an IPV6CP Configure Ack packet, indicating this Interface-Identifier, to the TE.

    If the Interface-Identifier extracted from the address contained in the PDP Address IE is not identical to the tentative Interface-Identifier indicated in the IPV6CP Configure-Request message sent from the TE, the MT sends an IPV6CP Configure Nak packet, indicating the Interface-Identifier extracted from the address contained in the PDP Address IE, to the TE. The TE then sends a new IPV6CP Configure-Request message to the MT, indicating the same Interface-Identifier as was indicated in the received IPV6CP Configure Nak. Finally the MT responds with an IPV6CP Configure Ack packet. The negotiated Interface-Identifier shall be used in the TE to create a link-local address.

    After finalisation of the IPV6CP negotiations between TE and MT, the user plane link is established. Before the MS can communicate with other hosts on the Intranet/ISP it shall obtain an IPv6 Global or a Site-Local Unicast address. Given that exactly one Prefix is included in the Router Advertisement, depending upon whether the advertised Prefix is globally unique or Site-local unique, the MS can only generate either IPv6 Global address(es) or Site-local address(es) using this Prefix during the lifetime of a particular PDP Context. This is done using either Stateless or Stateful Address Autoconfiguration as described in 3GPP TS 29.061 [17].

    When creating a Global or Site-Local Unicast Address, the MS may use the Interface-Identifier received during the PDP Context Activation phase or it may generate a new Interface-Identifier. There is no restriction on the uniqueness of the Interface-Identifier of the Global or Site-Local Unicast Address, since the Prefix itself is unique. Interface-Identifiers shall in any case be 64-bit long and follow standard interface-identifier guidelines as per IETF RFC 2373 [49] and RFC 2472 [46].

    In case a PDP Context Reject was sent to the MS the MT sends an LCP Terminate-Request to the TE, the TE and MT negotiate for link termination. The MT may then send a final AT-response to inform the TE about the rejected PDP Context activation.

~~Note. When this version of this specification was released, work was still in progress within IETF for how to provide DNS configuration for MS not supporting Stateful Autoconfiguration, i.e. MS not supporting DHCP DNS configuration.~~

End of modified sections

3GPP TSG-CN WG3 Meeting #24
Helsinki, Finland, 28th July - 2nd Aug 2002.

Tdoc ⌘N3-020688

CR-Form-v7

CHANGE REQUEST

⌘	29.061	CR	061	⌘ rev	2	⌘	Current version:	5.2.0	⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ [ ] ME [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Configuration of Domain Name System (DNS) server IPV6 addresses	
Source:	⌘	TSG_CN WG3	
Work item code:	⌘	TEI [GPRS]	***Date:*** ⌘ 22/06/2002
Category:	⌘	**F** *Use one of the following categories:* ***F*** *(correction)* ***A*** *(corresponds to a correction in an earlier release)* ***B*** *(addition of feature),* ***C*** *(functional modification of feature)* ***D*** *(editorial modification)* Detailed explanations of the above categories can be found in 3GPP TR 21.900.	***Release:*** ⌘ REL-5 *Use one of the following releases:* *2 (GSM Phase 2)* *R96 (Release 1996)* *R97 (Release 1997)* *R98 (Release 1998)* *R99 (Release 1999)* *Rel-4 (Release 4)* *Rel-5 (Release 5)* *Rel-6 (Release 6)*

Reason for change:	⌘	There is currently no support for dynamic configuration of Domain Name System (DNS) server IPV6 addresses in a MS not supporting the DHCPv6 protocol.
Summary of change:	⌘	Introduces the possibility of dynamic configuration of Domain Name System (DNS) server IPV6 addresses via existing Session Management procedures by use of the protocol Configuration Options IE.
Consequences if not approved:	⌘	No support for dynamic configuration of Domain Name System (DNS) server IPV6 addresses in a MS not supporting the optional DHCPv6 protocol.

Clauses affected:	⌘	2, 11.2.1.3.1				
		Y	**N**			
Other specs affected:	⌘	X		Other core specifications	⌘	24.008, 24.229, 27.060
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

First modified section

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.

[1] Void.

[2] 3GPP TS 22.060: "General Packet Radio Service (GPRS): Stage 1 Service Description".

[3] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service Description Stage 2".

[4] Void.

[5] Void.

[6] Void.

[7] Void.

[8] Void.

[9] Void.

[10] 3GPP TS 27.060: "Packet Domain; Mobile Station (MS) supporting Packet Switched Services".

[11] ITU-T Recommendation E.164: "Numbering plan for the ISDN era".

[12] <VOID>

[13] <VOID>

[14] <VOID>

[15] IETF RFC 768 (1980): "User Datagram Protocol" (STD 6).

[16] IETF RFC 791 (1981): "Internet Protocol" (STD 5).

[17] IETF RFC 792 (1981): "Internet Control Message Protocol" (STD 5).

[18] IETF RFC 793 (1981): "Transmission Control Protocol" (STD 7).

[19] IETF RFC 1034 (1987): "Domain Names - Concepts and Facilities" (STD 7).

[20] <VOID>

[21] IETF RFC 1661 and 1662 (1994): "The Point-to-Point Protocol (PPP)" (STD 51).

[22] IETF RFC 1700 (1994): "Assigned Numbers" (STD 2).3.

[23] 3GPP TS 44.008: "Mobile radio interface layer 3 specification; Core Network Protocols – Stage 3".

[24] 3GPP TS 29.060: "General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp Interface".

[25] IETF RFC2794 (2000), Pat R. Calhoun and Charles E. Perkins: "Mobile IP Network Address Identifier Extension for IPv4", March 2000.

[26] IETF RFC 2131 (1997): "Dynamic Host Configuration Protocol".

[27] IETF RFC 1542 (1993): "Clarification and Extensions for the Bootstrap Protocol".

[28] IETF RFC2373 (1998): "IP version 6 Addressing Architecture".

[29] IETF RFC 2462 (1998): "IPv6 Stateless Address Autoconfiguration".

[30] IETF RFC 2002 (1996), C. Perkins: "IP Mobility Support".

[31] IETF RFC 2486 (1999), B. Aboba and M. Beadles: "The Network Access Identifier".

[32] IETF RFC1112 (1989), S.E. Deering: "Host extensions for IP multicasting".

[33] IETF RFC2236 (1997), W. Fenner: "Internet Group Management Protocol, Version 2".

[34] IETF RFC2362 (1998), D. Estrin and al: "Protocol Independent Multicast-Sparse Mode (PIM-SM)".

[35] IETF RFC1075 (1988), D. Waitzman and al: "Distance Vector Multicast Routing Protocol".

[36] IETF RFC1585 (1994), J. Moy: "MOSPF"..

[37] IETF RFC2290 (1998), J. Solomon, S. Glass: "Mobile-IPv4 Configuration Option for PPP IPCP "

[38] IETF RFC2865 (2000), C. Rigney, S. Willens, A. Rubens, W. Simpson: "Remote Authentication Dial In User Service (RADIUS)".

[39] IETF RFC2866 (2000), C. Rigney, Livingston: " RADIUS Accounting ".

[40] 3GPP TS 23.003: "3rd Generation Partnership Project; Technical Specification Group Core Network; Numbering, addressing and identification".

[41] IETF RFC2882 (2000), D. Mitton: "Extended RADIUS Practices".

[42] 3GPP TR 21.905: " Vocabulary for 3GPP Specifications".

[43] IETF RFC 2472 (1998), D. Haskins, E. Allen: “IP Version 6 over PPP”

[44] IETF RFC 2461 (1998), T. Narten, E. Nordmark, W. Simpson: “Neighbor Discovery for IP Version 6”

[45] IETF RFC 3118 (2001), R. Droms, W. Arbaugh: “Authentication for DHCP Messages”

[46] IETF Internet-Draft: “Dynamic Host Configuration Protocol for IPv6 (DHCPv6)”, draft-ietf-dhc-dhcpv6-24.txt, work in progress.

[47] 3GPP TS 24.229: “IP Multimedia Call Control Protocol based on SIP and SDP”

[48] IETF RFC 2710 (1999), S. Deering, W. Fenner, B. Haberman: “Multicast Listener Discovery (MLD) for IPv6”

[49] IETF RFC 2460 (1998), S.Deering,, R.Hinden: “Internet Protocol, Version 6 (IPv6) Specification”

[50] IETF RFC 3162 (2001), B. Adoba, G. Zorn, D. Mitton: “RADIUS and IPv6”

[51] IETF RFC 2548 (1999), G.Zorn: “Microsoft Vendor-specific RADIUS Attributes”

[52] IETF RFC 1034 (1987): "Domain Names - Concepts and Facilities" (STD 13).

[53] IETF RFC 1035 (1987): "Domain Names - Implementation and Specification" (STD 13).

[54] IETF RFC 1886 (1995): "DNS Extensions to support IP version 6".

[55] 3GPP TS 24.008: "Mobile radio interface layer 3 specification; Core Network Protocols - Stage 3".

Next modified section

11.2.1.3.1 IPv6 PDP Context Activation

In this case:

- The GGSN provides the MS with an IPv6 Prefix belonging to the Intranet/ISP addressing space. A dynamic IPv6 address shall be given using either stateless or stateful address autoconfiguration. This IPv6 address is used for packet forwarding within the packet domain and for packet forwarding on the Intranet/ISP;
- the MS may send an authentication request at PDP context activation and the GGSN may request user authentication from a server, e.g. AAA, …, belonging to the Intranet/ISP;
- the protocol configuration options are retrieved (if requested by the MS at PDP context activation) from some server, e.g. AAA, …, belonging to the Intranet/ISP;
- in order to avoid any conflict between the link-local address of the MS and that of the GGSN, the Interface-Identifier used by the MS to build its link-local address shall be assigned by the GGSN. The GGSN ensures the uniqueness of this interface-identifier. The MT shall then enforce the use of this Interface-Identifier by the TE. This is valid for both stateless and stateful address autoconfiguration.
- the communication between the Packet Domain and the Intranet/ISP may be performed over any network, even an insecure e.g. the Internet. In case of an insecure connection between the GGSN and the Intranet/ISP there may be a specific security protocol over the insecure connection. This security protocol is defined by mutual agreement between PLMN operator and Intranet/ISP administrator.
- the MS may request for DNS server IPv6 addresses using the PCO IE in e.g. the PDP Context Request message. In that case the GGSN may return the IP address of one or more DNS servers in the PCO in the PDP Context Response message. The DNS address(es) shall be coded in the PCO as specified in 3GPP TS 24.008 [55]. If a list of servers is received, the MS shall adhere to the explicit prioritisation order of the list.

In the following signalling flow example, PPP is used as layer 2 protocol over the R reference point. The MT behaves as a PPP server and translates Protocol Configuration Options into SM message IEs. GTP-C carries this information unchanged to the GGSN which uses the information e.g. for RADIUS authentication. The result of the host authentication is carried via GTP-C back to the SGSN, which then relays the result to the MT. The MT finalises the IPV6CP negotiation by sending an IPV6CP Configure-Ack message to the TE with the appropriate options included, e.g, Interface-Identifier. The Interface-Identifier shall be used in the TE to create a link-local address to be able to perform the IPv6 address autoconfiguration (see subclauses 11.2.1.3.2 and 11.2.1.3.3).

1) The TE sends an AT-command to the MT to set up parameters and enter PPP mode. The MT responds with an AT-response.

2) LCP negotiates Maximum-Receive-Unit and authentication protocol. The negotiated authentication protocol is either CHAP, PAP or 'none'. The MT shall try to negotiate for CHAP as first priority.

3) If the negotiated authentication protocol is either of CHAP or PAP, the TE authenticates itself towards the MT by means of that protocol. The MT stores the necessary authentication data and sends a forced positive acknowledgement of the authentication to the TE.

4) The TE requests IPv6 Interface-Identifier negotiation by sending the IPV6CP Configure-Request message to the MT.

5) The MT sends the Activate PDP Context Request message to the SGSN, including the Protocol Configuration Options. The Protocol Configuration Options IE may contain negotiated LCP options such as negotiated

Authentication Protocol as well as any authentication data previously stored in the MT. It may also contain a request for dynamic configuration of DNS server IPv6 addresses. The MS shall for dynamic address allocation leave PDP Address empty and set PDP Type to IPv6. The SGSN sends the Create PDP context request message to the chosen GGSN including the unmodified Protocol Configuration Options.

6) The GGSN deduces from local configuration data associated with the APN:

- IPv6 address allocation type (stateless or stateful);
- the source of IPv6 Prefixes in the stateless case (GGSN internal prefix pool, or external address allocation server);
- any server(s) to be used for address allocation, authentication and/or protocol configuration options retrieval (e.g. IMS related configuration, see [47]);
- the protocol e.g. RADIUS, to be used with the server(s);
- the communication and security feature needed to communicate with the server(s);

As an example the GGSN may use one of the following options:

- GGSN internal Prefix pool for IPv6 prefix allocation and no authentication;
- GGSN internal Prefix pool for IPv6 prefix allocation and RADIUS for authentication. The AAA server responds with either an Access-Accept or an Access-Reject to the RADIUS client in the GGSN;
- RADIUS for authentication and IPv6 prefix allocation. The AAA server responds with either an Access-Accept or an Access-Reject to the RADIUS client in the GGSN;

NOTE: DHCPv6 may be used for IPv6 prefix allocation when an appropriate RFC becomes available.

IPv6 Prefixes in a GGSN internal Prefix pool shall be configurable and structured per APN.

The GGSN shall in the PDP Address IE in the Create PDP Context Response return an IPv6 address composed of a Prefix and an Interface-Identifier. The Interface-Identifier may have any value and it does not need to be unique within or across APNs. It shall however not conflict with the Interface-Identifier the GGSN has selected for its own side of the MS-GGSN link. The Prefix assigned by the GGSN or the external AAA server shall be globally or site-local unique, if stateless address autoconfiguration is configured on this APN. If, on the other hand, stateful address autoconfiguration is configured on the APN, the Prefix part of the IPv6 address returned in the PDP Address IE shall be set to the link-local prefix (FE80::/64).

The GGSN shall analyse the requested values of all the protocol options contained in the received Protocol Configurations Options IE. The contents of the Protocol Configurations Options IE sent in the GGSN response shall be in accordance with the relevant standards e.g. the PPP ~~or IPCPv6~~ standard~~s~~ [21] ~~and [43]~~.

7) The GGSN sends back to the SGSN a Create PDP Context Response message, containing the PDP Address IE and the Protocol Configuration Options IE. The Protocol Configuration Options IE may contain configuration data such as a list of DNS server IPv6 addresses. The cause value shall be set according to the outcome of the host authentication and configuration.

8) Depending on the cause value received in the Create PDP Context Response, the SGSN either stores the PDP Address and sends an Activate PDP Context Accept to the MS or, sends an Activate PDP Context Reject, to the MS.

   If Protocol Configuration Options are received from the GGSN, the SGSN shall relay those to the MS.

9) The MT extracts the Interface-Identifier from the address received in the PDP Address IE and ignores the Prefix part. If this Interface-Identifier is identical to the tentative Interface-Identifier indicated in the IPV6CP Configure-Request message sent from the TE~~-~~, the MT sends an IPV6CP Configure Ack packet, indicating this Interface-Identifier, to the TE.

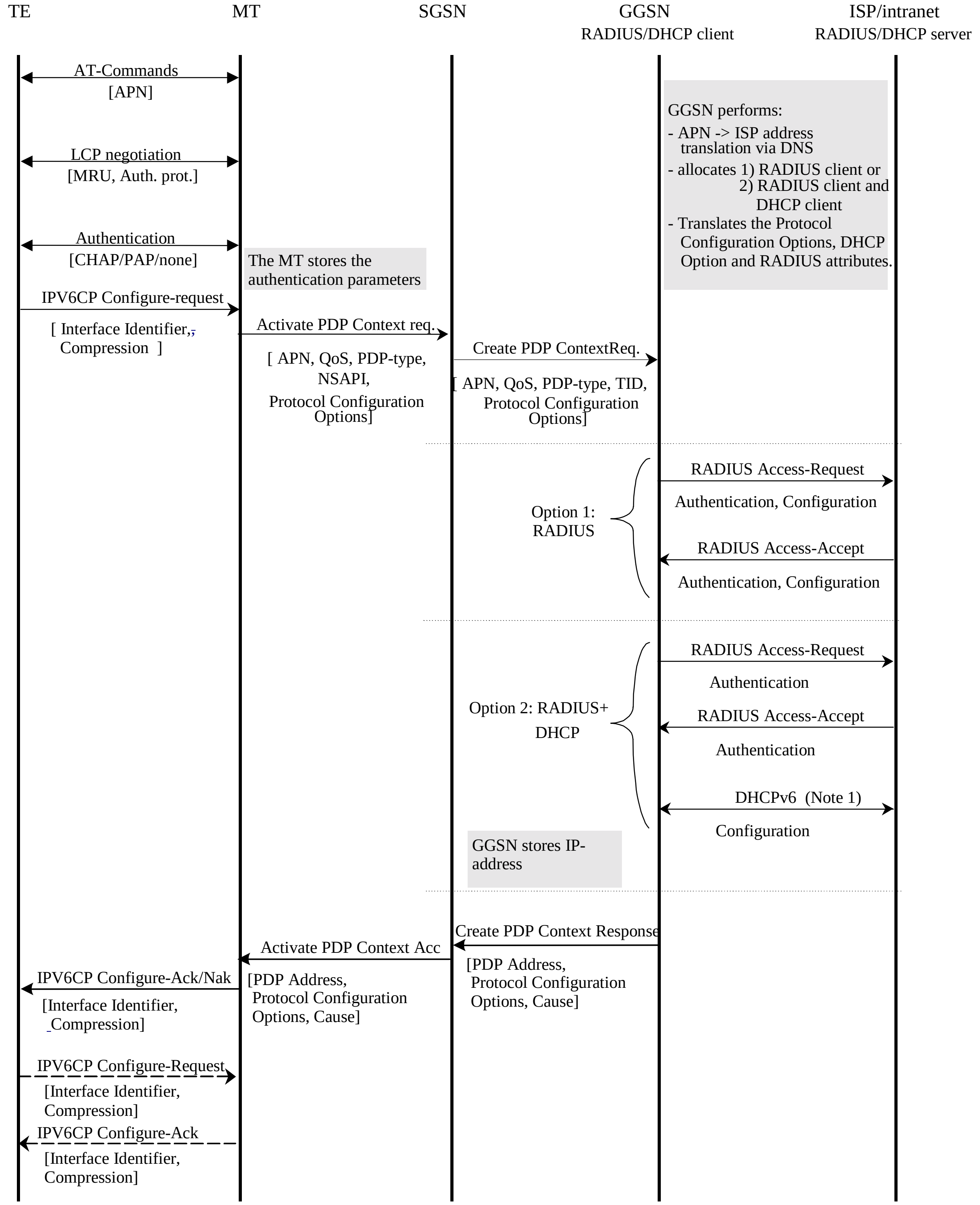
   If the Interface-Identifier extracted from the address contained in the PDP Address IE is not identical to the tentative Interface-Identifier indicated in the IPV6CP Configure-Request message sent from the TE, the MT sends an IPV6CP Configure-Nak packet, indicating the Interface-Identifier extracted from the address contained in the PDP Address IE, to the TE. The TE then sends a new IPV6CP Configure-Request message to the MT, indicating the same Interface-Identifier as was indicated in the received IPV6CP Configure Nak (as indicated by the dotted IPV6CP Configure-Request and Configure-Ack in the figure below). Finally the MT responds with a IPV6CP Configure Ack packet.

In case a PDP Context Reject was sent to the MS the MT sends an LCP Terminate-Request to the TE.

10) When the TE has accepted the Interface-Identifier given by the MT, the user plane link from the TE to the GGSN and the external ISP/Intranet is established and the IPv6 address autoconfiguration may proceed.

In case a link terminate request packet was sent to the TE, the TE and MT negotiates for link termination. The MT may then send a final AT-response to inform the TE about the rejected PDP Context activation.

An LCP Terminate-request causes a PDP context deactivation.



Note 1: DHCPv6 may be used for IPv6 prefix allocation when an appropriate RFC becomes available.

Figure 11ba: PDP Context Activation for the IPv6 Non-transparent case

Figure 11ba above is valid for both Stateless and Stateful Address Autoconfiguration case. In the Stateful case though, option 2 does not apply and option 1 may only be used for authentication. The use of DHCPv6 above is different and used in a different context than when used for Stateful Address Autoconfiguration as in subclause 11.2.1.3.3.