ETSI TS 124 526 V15.2.0 (2019-04)

5G;
User Equipment (UE) policies for 5G System (5GS);
Stage 3
(3GPP TS 24.526 version 15.2.0 Release 15)

Reference
RTS/TSGC-0124526vf20

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 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is 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 IPR Policy, no investigation, 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.

Foreword

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, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under http://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 document defines UE policies for 5G System (5GS) as specified in 3GPP TS 23.503 [2] including:

- UE route selection policy; and
- Access network discovery and selection policy.

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 23.503: " Policy and Charging Control Framework for the 5G System; Stage 2".

[3] 3GPP TS 24.502: "Access to the 3GPP 5G Core Network (5GCN) via Non-3GPP Access Networks (N3AN); Stage 3".

[4] 3GPP TS 23.003: "Numbering, addressing and identification".

[5] 3GPP TS 25.331: "Radio Resource Control (RRC); Protocol Specification".

[6] 3GPP TS 36.331: "Evolved Universal Terrestrial Radio Access (E-UTRA) Radio Resource Control (RRC); Protocol specification".

[7] 3GPP TS 23.032: "Universal Geographical Area Description (GAD)".

[8] IEEE Std 802.11™-2012: "Information Technology- Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications".

[9] Wi-Fi Alliance: "Hotspot 2.0 (Release 2) Technical Specification, version 1.0.0", 2014-08-08.

[10] ITU-T Recommendation E.212: "The international identification plan for public networks and subscriptions", 2016-09-23.

[11] 3GPP TS 24.501: "Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3".

[12] IETF RFC 1035: "Domain names - implementation and specification".

[13] ISO 8601:2004: "Data elements and interchange formats -- Information interchange -- Representation of dates and times".

[14] 3GPP TS 38.413: "NG-RAN; NG Application Protocol (NGAP)".

[15] 3GPP TS 23.501: "System Architecture for the 5G System; Stage 2".

[16] IETF RFC 4122: "A Universally Unique IDentifier (UUID) URN Namespace".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [1]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].

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.501 [15] apply:

non-seamless non-3GPP offload

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.503 [2] apply:

UE local configuration

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].

5GCN	5G Core Network
5GS	5G System
ANDSP	Access Network Discovery and Selection Policy
DNN	Data Network Name
ePDG	evolved Packet Data Gateway
FQDN	Fully Qualified Domain Name
H-PCF	A PCF in the HPLMN
IMS	IP Multimedia Subsystem
LADN	Local Area Data Network
MCC	Mobile Country Code
ME	Mobile Equipment
MMS	Multimedia Messaging Service
MNC	Mobile Network Code
N3AN	Non-3GPP Access Network
N3IWF	Non-3GPP InterWorking Function
OS	Operating System
PCF	Policy Control Function
S-NSSAI	Single Network Slice Selection Assistance Information
SSC	Session and Service Continuity
SUPI	Subscriber Permanent Identifier
SUPL	Secure User Plane Location
URSP	UE Route Selection Policy
USIM	User Services Identity Module
V-PCF	A PCF in the VPLMN
WLANSP	WLAN Selection Policy

4 Descriptions of UE policies for 5GS

4.1 Overview

The UE policies for 5GS include:

- UE route selection policy(URSP)(see subclause 4.2); and
- Access network discovery and selection policy(ANDSP)(see subclause 4.3).

The UE policies can be delivered from the PCF to the UE. The UE policy delivery procedure is specified in 3GPP TS 24.501 [11].

The UE policies can also be pre-configured in the UE. The pre-configured policy shall be applied by the UE only when the UE has not received the same type of policy from the PCF. The implementation of pre-configured UE policies is out of scope of this specification.

4.2 UE route selection policy (URSP)

4.2.1 General

The URSP is defined in 3GPP TS 23.503 [2] and is a set of one or more URSP rules, where a URSP rule is composed of:

a) a precedence value of the URSP rule identifying the precedence of the URSP rule among all the existing URSP rules;

b) a traffic descriptor, including either:

   1) match-all traffic descriptor; or

   2) at least one of the following components:

      A) one or more application identifiers;

      B) one or more IP 3 tuples as defined in 3GPP TS 23.503 [2] i.e. the destination IP address, the destination port number, and the protocol in use above the IP;

      C) one or more non-IP descriptors, i.e. destination information of non-IP traffic;

      D) one or more DNNs;

      E) one or more connection capabilities; and

      F) one or more domain descriptors, i.e. destination FQDN(s); and

c) one or more route selection descriptors each consisting of a precedence value of the route selection descriptor and either

   1) at least one of the followings:

      A) SSC mode;

      B) one or more S-NSSAIs;

      C) one or more DNNs;

      D) PDU session type; and

      E) preferred access type; or

   2) non-seamless non-3GPP offload indication.

Only one URSP rule in the URSP can be a default URSP rule and the default URSP rule shall contain a match all traffic descriptor. If a default URSP rule and one or more non-default URSP rules are included in the URSP, any non-default URSP rule shall have lower precedence value than (i.e. shall be prioritised over) the default URSP rule.

If a traffic descriptor lists one or more application identifiers together with one or more connection capabilities, the UE shall consider that the application identifiers identify the applications requesting access to the connection capabilities.

NOTE 1: The connection capabilities requested by the applications are OS dependent. The connection capability identifiers defined in table 5.2.1 are OS independent. It is based on the UE implementation how the UE matches the connection capabilities requested by the applications to the connection capability identifiers in table 5.2.1.

NOTE 2: If the UE has multiple concurrently active OS, the traffic descriptor can list as many multiple OS Ids.

If one or more DNNs are included in the traffic descriptor of a URSP rule, the route selection descriptor of the URSP rule shall not include any DNN.

NOTE 3: It is recommended to avoid the combination of more than two components in the traffic descriptor.

4.2.2 Association between an application and either a PDU session or non-seamless non-3GPP offload

When the upper layers request information of the PDU session via which to send a PDU of an application, information on the non-3GPP access outside of a PDU session shall be provided to the upper layers, without evaluating the URSP rules, if due to UE local configuration non-seamless non-3GPP offload is requested. Otherwise, the UE shall proceed in the following order:

a) the UE shall evaluate the URSP rules, except the default URSP rule, with a traffic descriptor matching the application information in increasing order of their precedence values, if any. If the traffic descriptor contains more than one component, all of them shall be matched.

   If the UE finds the traffic descriptor in a non-default URSP rule matching the application information, and:

   I) if there is one or more PDU sessions matching at least one of the route selection descriptors of the URSP rule, the UE shall provide information on the PDU session that matches the route selection descriptor of the lowest precedence value to the upper layers;

NOTE 1: It is up to the UE implementation which PDU session to select if there exist multiple PDU sessions matching the same route selection descriptor of the lowest precedence value.

   II) otherwise:

      1) the UE shall select a route selection descriptor with the next smallest precedence value which has not yet been evaluated;

      2) if:

         i) the selected route selection descriptor contains a non-seamless non-3GPP offload indication:

            A) if the information on the non-3GPP access outside of a PDU session is available, it shall be provided to the upper layers and the UE shall stop selecting a route selection descriptor matching the application information.

            B) if the information about the non-3GPP access outside of a PDU session is not available, or non-3GPP access is not available the UE shall proceed to step 3); or

         ii) the selected route selection descriptor does not contain a non-seamless non-3GPP offload indication, the URSP handling layer requests the UE NAS layer to establish a PDU session providing at least one of the following PDU session attributes:

            A) SSC mode if there is a SSC mode in the route selection descriptor;

NOTE 2: The SSC mode 3 is only used when the PDU session type is IPv4, IPv6 or IPv4v6.

            B) one S-NSSAI if the S-NSSAI is in the route selection descriptor; and the S-NSSAI is in the allowed NSSAI

               Otherwise, the S-NSSAI shall not be used as a PDU session attribute for establishing a PDU session;

NOTE 3: If there are multiple S-NSSAIs in the route selection descriptor, an S-NSSAI is chosen among the S-NSSAIs based on UE implementation.

            C) one DNN, if the DNN in the route selection descriptor; and if the DNN is an LADN DNN and the UE is in the service area of that LADN;

NOTE 4: If one or more DNNs are included in the traffic descriptor of a URSP rule, the existing DNNs in the route selection descriptor for the application are ignored.

NOTE 5: If there is no DNN in the traffic descriptor and there are multiple DNNs in the route selection descriptor, a DNN is chosen based on UE implementation.

            D) PDU session type if the PDU session type is in the route selection descriptor; and

E) preferred access type if the preferred access type is in the route selection descriptor.

The UE NAS layer indicates the result of the PDU session establishment. Upon successful completion of the PDU session establishment, the UE NAS layer shall additionally indicate the attributes of the established PDU session (e.g. PDU session identity, SSC mode, S-NSSAI, DNN, PDU session type, access type, PDU address) to the URSP handling layer, and shall provide information (e.g. PDU address) of the successfully established PDU session to the upper layers. The UE shall stop selecting a route selection descriptor matching the application information. If the PDU session establishment is unsuccessful, the UE shall proceed to step 3); and

3) if there is any route selection descriptor which has not yet been evaluated, the UE shall proceed to step 1). If all route selection descriptors for the matching non-default URSP rule have been evaluated and there is one or more non-default matching URSP rule which has not yet been evaluated, the UE shall proceed to step a). If all non-default matching URSP rules have been evaluated, the UE shall inform the upper layers of the failure.

b) if no non-default matching URSP rule can be found and if UE local configuration for the application is available, the UE shall perform the association of the application to a PDU session accordingly. If no matching PDU session exists, the UE NAS layer shall attempt to establish a PDU session using UE local configuration.

NOTE 6: Any missing information in the UE local configuration needed to build the PDU session establishment request can be the appropriate corresponding component from the default URSP rule with the "match-all" traffic descriptor.

If the PDU session establishment is successful, the UE NAS layer shall provide information (e.g. PDU address) of the successfully established PDU session to the upper layers. Otherwise, the UE shall go to step c);

c) if no non-default matching URSP rule can be found and if either UE local configuration for the application is not available or the PDU session establishment based on UE local configuration for the application was unsuccessful, the UE shall perform the association of the application to a PDU session or to non-seamless non-3GPP offload according to the default URSP rule with the "match-all" traffic descriptor, if any. If the association is unsuccessful, the UE shall inform the upper layers of the failure.

The HPLMN may pre-configure the UE with URSP or may provide URSP to the UE by signallingas described in annex D of 3GPP TS 24.501 [11]. The pre-configured URSP and the signalled URSP shall be stored in a non-volatile memory in the ME together with the SUPI from the USIM. If the UE has both pre-configured URSP and signalled URSP, the UE shall only use the signalled URSP. The pre-configured URSP shall be stored until a new URSP is configured by HPLMN or the USIM is removed. The signalled URSP may be modified by the procedures defined in annex D of 3GPP TS 24.501 [11] and shall be stored until USIM is removed. The URSP can only be used if the SUPI from the USIM matches the SUPI stored in the non-volatile memory of the ME. If the SUPI from the USIM does not match the SUPI stored in the non-volatile memory of the ME, the UE shall delete the URSP.

The UE may re-evaluate the URSP rules and change the association of an application to a PDU session when:

NOTE 7: The time when the UE performs the re-evaluation is up to UE implementation. It is recommended that the UE performs the re-evaluation in a timely manner.

a) the UE performs periodic URSP rules re-evaluation based on UE implementation;

b) the UE NAS layer indicates that an existing PDU session used for routing traffic of an application based on a URSP rule is released;

c) the URSP is updated by the PCF;

d) the UE NAS layer indicates that the UE performs inter-system change from S1 mode to N1 mode;

e) the UE NAS layer indicates that the UE is successfully registered in N1 mode over 3GPP access or non-3GPP access;

f) the UE establishes or releases a connection to a WLAN access and transmission of a PDU of the application via non-3GPP access outside of a PDU session becomes available/unavailable;

g) the allowed NSSAI is changed; or

h) the LADN information is changed.

The URSP handling layer may request the UE NAS layer to release an existing PDU session after the re-evaluation.

4.2.3 Unknown or unexpected URSP rules

If the network provides URSP rules including any new component in the traffic descriptor or in the route selection descriptor which is not recognized by the UE, such URSP rules are unknown or unexpected to the UE. In this case, the UE shall ignore the unknown or unexpected URSP rules when evaluating the URSP rules to associate an application either with a PDU session or with non-seamless non-3GPP offload.

4.3 Access network discovery and selection policy (ANDSP)

4.3.1 Overview

The ANDSP is used to control UE behaviour related to access network discovery and selection over non-3GPP access network.

ANDSP consists of:

- WLAN Selection Policy (WLANSP) which is described in subclause 4.3.2.; and
- non-3GPP access network (N3AN) node configuration information which is described in subclause 4.3.3.

4.3.2 WLAN selection policy (WLANSP)

4.3.2.1 General

The WLANSP is used to control UE behaviour related to selection and reselection of a WLAN.

The WLANSP consists of zero or more WLANSP rules.

Each WLANSP rule consists of:

- rule identifier;
- one or more groups of WLAN selection criteria;
- validity area;
- zero or more time of day;
- rule priority;
- roaming.

Each group of WLAN selection criteria contains:

- criteria priority;
- home network indication;
- preferred roaming partner list;
- min backhaul threshold;
- maximum BSS load value;
- required proto port tuple;
- SP exclusion list; and
- preferred SSID list.

The priority of a selection criteria is encoded in the criteria priority field. The WLAN priority defined in the preferred SSID list (see figure 5.3.2.4c) represents the priority of the WLAN matching the selection criteria.

The validity of the WLANSP rule can be restricted by validity conditions. The validity of the WLANSP rule takes into account validity area, roaming, and time of day where each condition shall match in order to make the WLANSP rule valid.

Each validity area consists of:

- 3GPP location;
- WLAN location; and
- Geo location.

Each time of day consists of:

- time start;
- time stop;
- date start;
- date stop; and
- day of week.

The WLANSP rule is considered valid if none of the validity conditions exist or all validity conditions match.

There can be multiple valid WLANSP rules at the same time. In addition to validity conditions and selection criteria, there is a rule priority that shall be set for each WLANSP rule. The rule priority is encoded in the rule priority field, and it enables the UE to determine which WLANSP rule, out of potentially several valid WLANSP rules, it should consider as active. A WLANSP rule is active if it is valid and has highest rule priority out of the valid WLANSP rules. At any point in time, there shall be at most one active WLANSP rule. A WLAN that matches a selection criteria of the active WLANSP rule is considered as matching the selection criteria.

If the UE is roaming and WLANSP rules from both HPLMN and VPLMN are available, visited WLANSP rules shall take precedence.

4.3.2.2 WLAN access selection

The procedure of UE selecting WLAN access network based on WLAN selection policy is specified in 3GPP TS 24.502 [3].

4.3.3 N3AN node configuration information

4.3.3.1 General

Non-3GPP access network (N3AN) node configuration information is used to control UE behaviour related to selection of either N3IWF or ePDG for accessing 5GCN via non-3GPP access.

The non-3GPP access network (N3AN) node configuration information consists of:

- Non-3GPP access network (N3AN) node selection information;
- optionally, home ePDG identifier configuration; and
- optionally, home N3IWF identifier configuration.

4.3.3.2 N3AN node selection

The procedure of UE selecting an N3AN node based on N3AN node configuration information is specified in 3GPP TS 24.502 [3].

4.4 Interworking with EPC

If the UE supports both S1 mode and N1 mode:

- the UE shall always use the ANDSP information and applicable user preferences, if available at the UE, for non-3GPP access node selection;

NOTE: This includes the case when the UE is registered to the 5GCN via 3GPP access, the case when the UE is registered to the EPC via 3GPP access, and the case when the UE is not registered to any CN via 3GPP access.

- if the UE is:

  a) registered to the 5GCN via 3GPP access and not registered to any CN via non-3GPP access; or

  b) registered to the 5GCN via 3GPP access and registered to the 5GCN via non-3GPP access,

  the UE shall apply URSP rules and applicable user preferences, if available at the UE, to all uplink user data;

- if the UE is registered to the 5GCN via 3GPP access and registered to the EPC via non-3GPP access, the UE shall:

  a) use the ANDSF rules and RAN rules, if available at the UE, for uplink user data sent via the ePDG; and

  b) apply URSP rules and applicable user preferences, if available at the UE, to all other uplink user data;

- if the UE is:

  a) registered to the EPC via 3GPP access and not registered to any CN via non-3GPP access; or

  b) registered to the EPC via 3GPP access and registered to the EPC via non-3GPP access,

  the UE shall use the ANDSF rules and RAN rules, if available at the UE, for all uplink user data, except for the rules and parameters related to non-3GPP access node selection; and

- if the UE is registered to the EPC via 3GPP access and registered to the 5GCN via non-3GPP access, the UE shall:

  a) apply URSP rules and applicable user preferences, if available at the UE, to uplink user data sent via the N3IWF; and

  b) use the ANDSF rules and RAN rules, if available at the UE, for all other uplink user data, except for the rules and parameters related to non-3GPP access node selection.

5 Encoding of UE policies

5.1 Overview

The content of UE policies is included in the UE policy part contents defined in annex D.6.2 of 3GPP TS 24.501 [11].

The UE policy part contents include URSP or ANDSP.

For URSP definition, the encoding is defined in subclause 5.2.

For ANDSP definition, it includes encoding of WLANSP and encoding of N3AN node configuration information. The encoding of WLANSP is defined in subclause 5.3.2. The encoding of N3AN node configuration information is defined in subclause 5.3.3.

5.2 Encoding of UE policy part type URSP

The UE policy part type URSP contains one or more URSP rules which may be included in the UE policy part contents as defined in annex D.6.2 of 3GPP TS 24.501 [11].

If the UE policy part contents includes one or more URSP rules (i.e. the UE policy part type field is set to "URSP"), the UE policy part contents including URSP rules is encoded as shown in figures 5.2.1 to 5.2.4 and table 5.2.1.

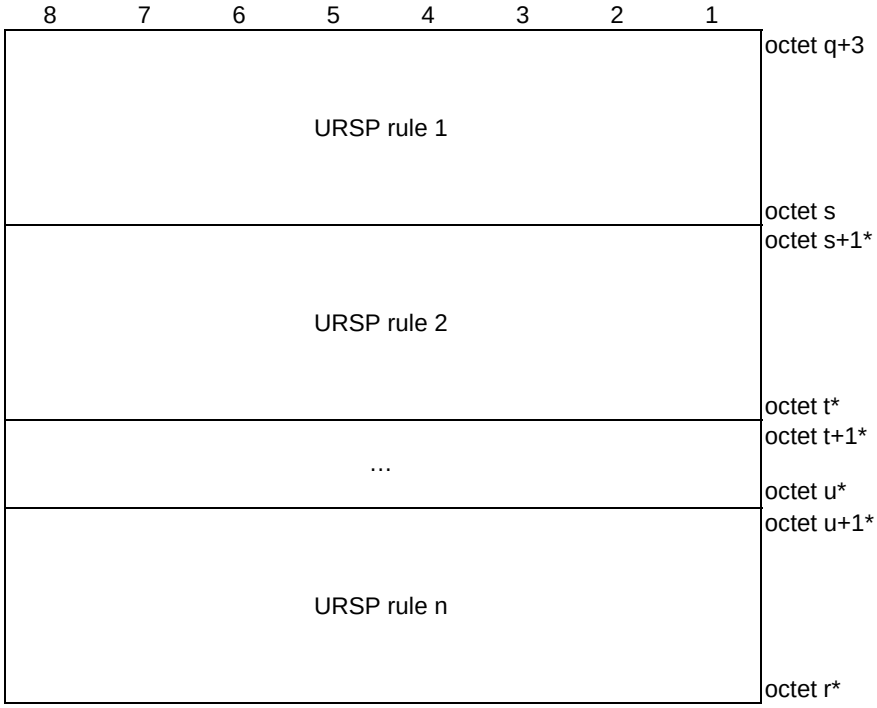

Figure 5.2.1: UE policy part contents including one or more URSP rules

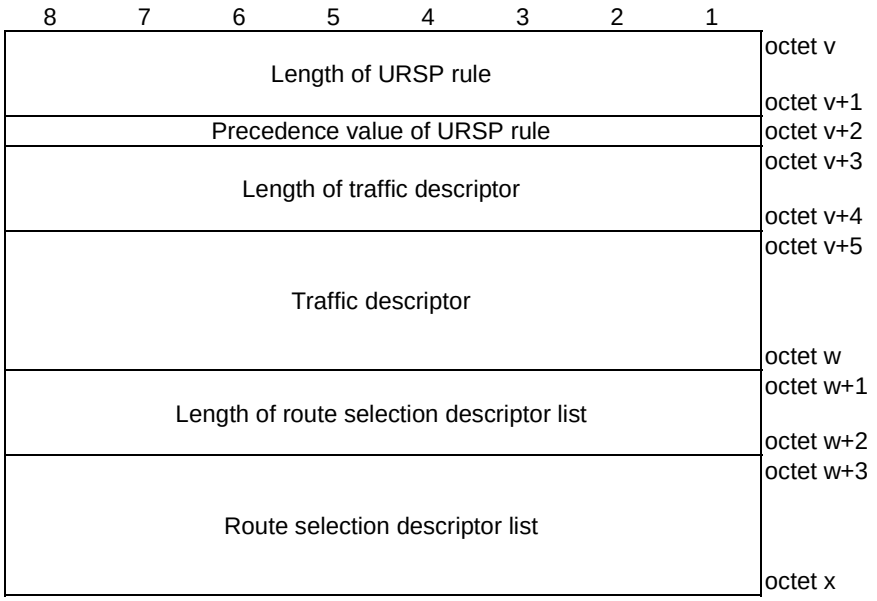

Figure 5.2.2: URSP rule

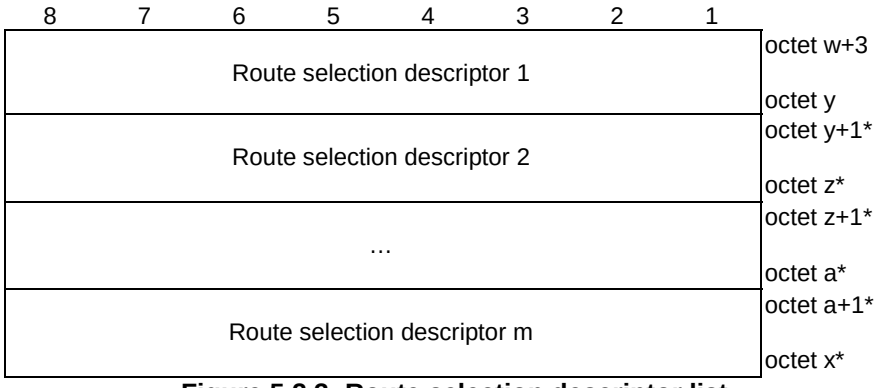

Figure 5.2.3: Route selection descriptor list

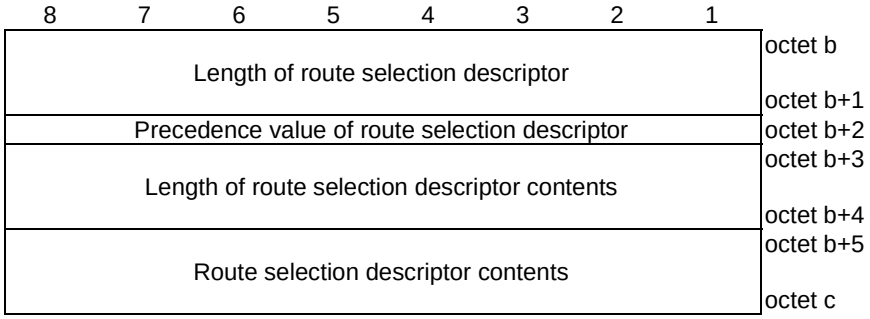

Figure 5.2.4: Route selection descriptor

Table 5.2.1: UE policy part contents including a URSP rule

Precedence value of URSP rule (octet v+2)
The precedence value of URSP rule field is used to specify the precedence of the URSP rule among all URSP rules in the URSP. This field includes the binary encoded value of the precedence value in the range from 0 to 255 (decimal). The higher the value of the precedence value field, the lower the precedence of the URP rule is. Multiple URSP rules in the URSP shall not have the same precedence value.

Traffic descriptor (octets v+5 to w)
The traffic descriptor field is of variable size and contains a variable number (at least one) of traffic descriptor components. Each traffic descriptor component shall be encoded as a sequence of one octet traffic descriptor component type identifier and a traffic descriptor component value field. The traffic descriptor component type identifier shall be transmitted first.

Traffic descriptor component type identifier
Bits
8 7 6 5 4 3 2 1
0 0 0 0 0 0 0 1 Match-all type
0 0 0 0 1 0 0 0 OS Id + OS App Id type (NOTE)
0 0 0 1 0 0 0 0 IPv4 remote address type
0 0 1 0 0 0 0 1 IPv6 remote address/prefix length type
0 0 1 1 0 0 0 0 Protocol identifier/next header type
0 1 0 1 0 0 0 0 Single remote port type
0 1 0 1 0 0 0 1 Remote port range type
0 1 1 0 0 0 0 0 Security parameter index type
0 1 1 1 0 0 0 0 Type of service/traffic class type
1 0 0 0 0 0 0 0 Flow label type
1 0 0 0 0 0 0 1 Destination MAC address type
1 0 0 0 0 0 1 1 802.1Q C-TAG VID type
1 0 0 0 0 1 0 0 802.1Q S-TAG VID type
1 0 0 0 0 1 0 1 802.1Q C-TAG PCP/DEI type
1 0 0 0 0 1 1 0 802.1Q S-TAG PCP/DEI type
1 0 0 0 0 1 1 1 Ethertype type
1 0 0 0 1 0 0 0 DNN type
1 0 0 1 0 0 0 0 Connection capabilities type
1 0 0 1 0 0 0 1 Destination FQDN
1 0 1 0 0 0 0 0 OS App Id type
All other values are spare.

For "match-all type", the traffic descriptor component shall not include the traffic descriptor component value field. The "match-all type" traffic descriptor component shall not appear more than once among all traffic descriptors of the whole URSP rules in the URSP. If the "match-all type" traffic descriptor component is included in a traffic descriptor, there shall be no traffic descriptor component with a type other than "match-all type" in the traffic descriptor.

For "OS Id + OS App Id type", the traffic descriptor component value field shall be encoded as a sequence of a sixteen octet OS Id field, a one octet OS App Id length field, and an OS App Id field. The OS Id field shall be transmitted first. The OS Id field contains a Universally Unique IDentifier (UUID) as specified in IETF RFC 4122 [16].

For "IPv4 remote address type", the traffic descriptor component value field shall be encoded as a sequence of a four octet IPv4 address field and a four octet IPv4 address mask field. The IPv4 address field shall be transmitted first.

For "IPv6 remote address/prefix length type", the traffic descriptor component value field shall be encoded as a sequence of a sixteen octet IPv6 address field and one octet prefix length field. The IPv6 address field shall be transmitted first.

For "protocol identifier/next header type", the traffic descriptor component value field shall be encoded as one octet which specifies the IPv4 protocol identifier or Ipv6 next header.

For "single remote port type", the traffic descriptor component value field shall be encoded as two octets which specify a port number.

For "remote port range type", the traffic descriptor component value field shall be encoded as a sequence of a two octet port range low limit field and a two octet port range high limit field. The port range low limit field shall be transmitted first.

For "security parameter index type", the traffic descriptor component value field shall be encoded as four octets which specify the IPSec security parameter index.

For "type of service/traffic class type", the traffic descriptor component value field shall be encoded as a sequence of a one octet type-of-service/traffic class field and a one octet type-of-service/traffic class mask field. The type-of-service/traffic class field shall be transmitted first.

For "flow label type", the traffic descriptor component value field shall be encoded as three octets which specify the IPv6 flow label. The bits 8 through 5 of the first octet shall be spare whereas the remaining 20 bits shall contain the IPv6 flow label.

For "destination MAC address type", the traffic descriptor component value field shall be encoded as 6 octets which specify a MAC address.

For "802.1Q C-TAG VID type", the traffic descriptor component value field shall be encoded as two octets which specify the VID of the customer-VLAN tag (C-TAG). The bits 8 through 5 of the first octet shall be spare whereas the remaining 12 bits shall contain the VID.

For "802.1Q S-TAG VID type", the traffic descriptor component value field shall be encoded as two octets which specify the VID of the service-VLAN tag (S-TAG). The bits 8 through 5 of the first octet shall be spare whereas the remaining 12 bits shall contain the VID.

For "802.1Q C-TAG PCP/DEI type", the traffic descriptor component value field shall be encoded as one octet which specifies the 802.1Q C-TAG PCP and DEI. The bits 8 through 5 of the octet shall be spare, and the bits 4 through 2 contain the PCP and bit 1 contains the DEI.

For "802.1Q S-TAG PCP/DEI type", the traffic descriptor component value field shall be encoded as one octet which specifies the 802.1Q S-TAG PCP. The bits 8 through 5 of the octet shall be spare, and the bits 4 through 2 contain the PCP and bit 1 contains the DEI.

For "ethertype type", the traffic descriptor component value field shall be encoded as two octets which specify an ethertype.

For "DNN type", the traffic descriptor component value field shall be encoded as a sequence of a one octet DNN length field and a DNN value field of a variable size. The DNN value contains an APN as defined in 3GPP TS 23.003 [4].

For "connection capabilities" type, the traffic descriptor component value field shall be encoded as a sequence of one octet for number of network capabilities followed by one or more octets, each containing a connection capability identifier encoded as follows:

Bits
8 7 6 5 4 3 2 1
0 0 0 0 0 0 0 1 IMS
0 0 0 0 0 0 1 0 MMS
0 0 0 0 0 1 0 0 SUPL
0 0 0 0 1 0 0 0 Internet
All other values are spare.

For "destination FQDN" type, the traffic descriptor component value field shall be encoded as a sequence of one octet destination FQDN length field and a destination FQDN value of variable size. The destination FQDN value field shall be encoded as defined in IETF RFC 1035 [12].

For "OS App Id type", the traffic descriptor component value field shall be encoded as a one octet OS App Id length field and an OS App Id field.

Precedence value of route selection descriptor (octet b+2)
The precedence value of route selection descriptor field is used to specify the precedence of the route selection descriptor among all route selection descriptors in the URSP rule. This field includes the binary encoded value of the precedence value in the range from 0 to 255 (decimal). The higher the value of the precedence value field, the lower the precedence of the route selection descriptor is.

Route selection descriptor contents (octets b+5 to c)
The route selection descriptor contents field is of variable size and contains a variable number (at least one) of route selection descriptor components. Each route selection descriptor component shall be encoded as a sequence of a one octet route selection descriptor component type identifier and a route selection descriptor component value field. The route selection descriptor component type identifier shall be transmitted first.

Route selection descriptor component type identifier
Bits
8 7 6 5 4 3 2 1
0 0 0 0 0 0 0 1 SSC mode type
0 0 0 0 0 0 1 0 S-NSSAI type
0 0 0 0 0 1 0 0 DNN type
0 0 0 0 1 0 0 0 PDU session type type
0 0 0 1 0 0 0 0 Preferred access type type
0 0 1 0 0 0 0 0 Non-seamless non-3GPP offload indication type
All other values are spare.

For "SSC mode type", the route selection descriptor component value field shall be encoded as a one octet SSC mode field. The bits 8 through 4 of the octet shall be spare, and the bits 3 through 1 shall be encoded as the value part of the SSC mode information element defined in subclause 9.11.4.16 of 3GPP TS 24.501 [11]. The "SSC mode type" route selection descriptor component shall not appear more than once in the route selection descriptor.

For "S-NSSAI type", the route selection descriptor component value field shall be encoded as a sequence of a one octet S-NSSAI length field and an S-NSSAI value field of a variable size. The S-NSSAI value shall be encoded as the value part of NSSAI information element defined in subclause 9.11.3.37 of 3GPP TS 24.501 [11].

For "DNN type", the route selection descriptor component value field shall be encoded as a sequence of a one octet DNN length field and a DNN value field of a variable size. The DNN value contains an APN as defined in 3GPP TS 23.003 [4].

For "PDU session type", the route selection descriptor component value field shall be encoded as a one octet PDU session type field. The bits 8 through 4 of the octet shall be spare, and the bits 3 through 1 shall be encoded as the value part of the PDU session type information element defined in subclause 9.11.4.11 of 3GPP TS 24.501 [11]. The "PDU session type" route selection descriptor component shall not appear more than once in the route selection descriptor.

For "preferred access type", the route selection descriptor component value field shall be encoded as a one octet preferred access type field. The bits 8 through 3 shall be spare, and the bits 2 and 1 shall be encoded as the value part of the access type information element defined in subclause 9.11.3.11 of 3GPP TS 24.501 [11]. The "preferred access type" route selection descriptor component shall not appear more than once in the route selection descriptor.

For "non-seamless non-3GPP offload indication type", the route selection descriptor component shall not include the route selection descriptor component value field. The "non-seamless non-3GPP offload indication type" route selection descriptor component shall not appear more than once in the route selection descriptor. If the "non-seamless non-3GPP offload indication type" route selection descriptor component is included in a route selection descriptor, there shall be no route selection descriptor component with a type other than "non-seamless non-3GPP offload indication type" in the route selection descriptor.

NOTE: For "OS Id + OS App Id type", the traffic descriptor component value field does not specify the OS version number or the version number of the application.

5.3 Encoding of UE policy part type ANDSP

5.3.1 General

The purpose of the ANDSP is to indicate the WLAN Selection Policy (WLANSP) and non-3GPP access network (N3AN) node configuration information related to access network discovery and selection and N3AN node selection for non-3GPP access network.

The ANDSP is encoded as shown in figures 5.3.1.1 to 5.3.1.3 and table 5.3.1.1 according to UE policy part top level format (see Annex D of 3GPP TS 24.501 [11]).

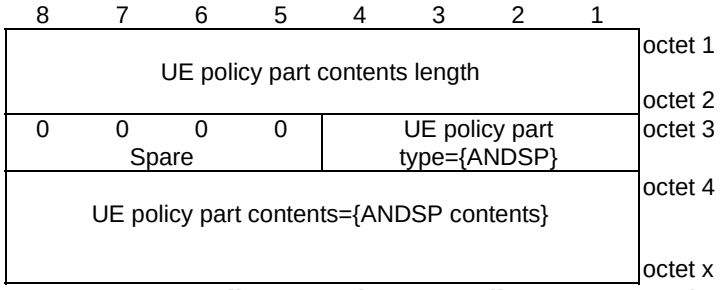

Figure 5.3.1.1: UE policy part when UE policy part type = {ANDSP}

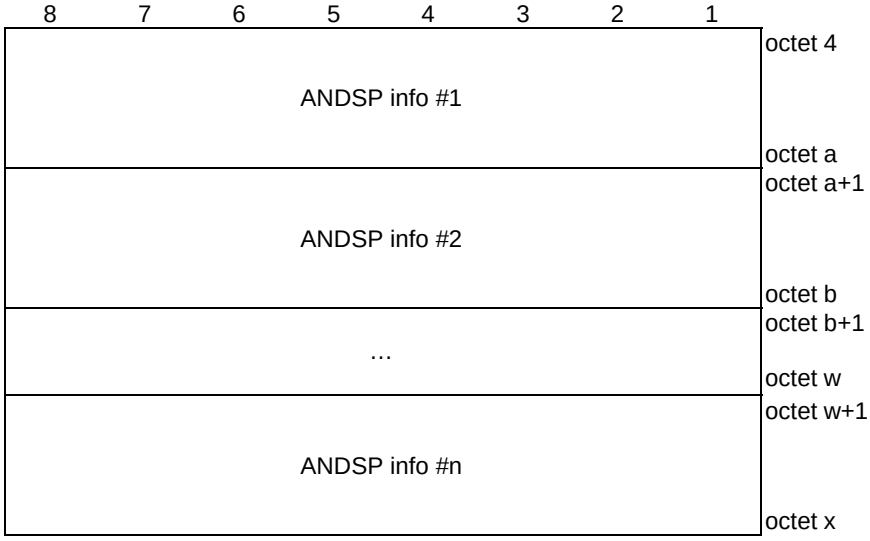

Figure 5.3.1.2: ANDSP contents

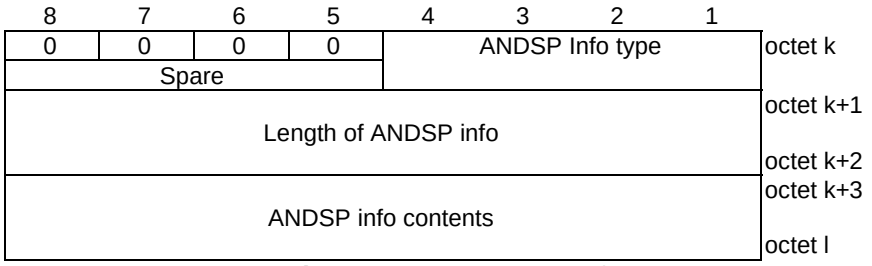

Figure 5.3.1.3: ANDSP Info

Table 5.3.1.1: ANDSP information format

UE policy type field is set to '00000010' (=ANDSP) as specified in 3GPP TS 24.501 [4] Annex D. UE policy part contents length field indicate the length of the ANDSP contents in octets. ANDSP contents (octets 4 to x) ANDSP contents consist of 1 or more ANDSP info (see figure 5.3.1.2). ANDSP Info type (bit 1 to 4 of octet k) shall be set according to the following: Bits **4 3 2 1** 0 0 0 0 Reserved 0 0 0 1 WLANSP 0 0 1 0 N3AN node configuration information All other values are reserved. Bits 8 to 5 of octet k are spare and shall be encoded as zero. Length of ANDSP info (octets k+1 to k+2) ANDSP info contents (octets k+3 to l) can be WLANSP (see subclause 5.3.2) or N3AN node configuration information (see subclause 5.3.3).

5.3.2 Encoding of WLANSP

The purpose of the WLANSP field is to indicate the rules related to selection and reselection of a WLAN.

The WLANSP field is encoded as shown in figures 5.3.2.1 to 5.3.2.20 and table 5.3.2.1.

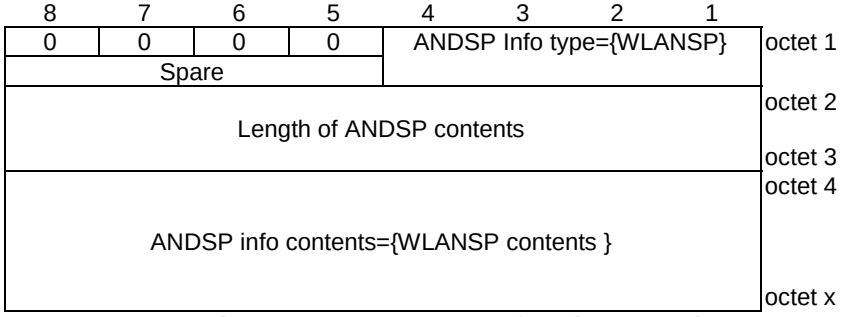

Figure 5.3.2.1: ANDSP Info = {WLANSP}

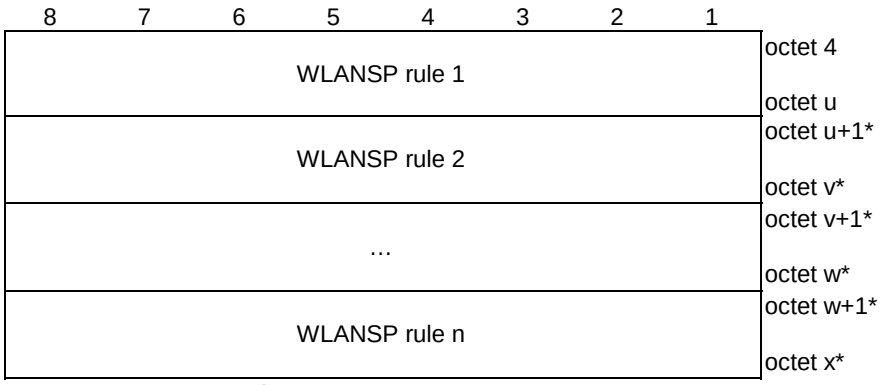

Figure 5.3.2.2: WLANSP contents

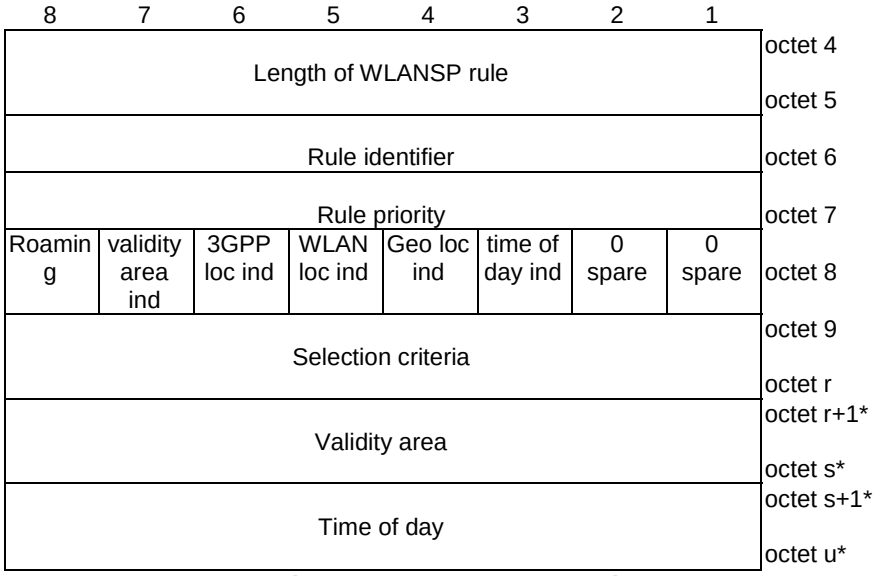

Figure 5.3.2.3: WLANSP rule

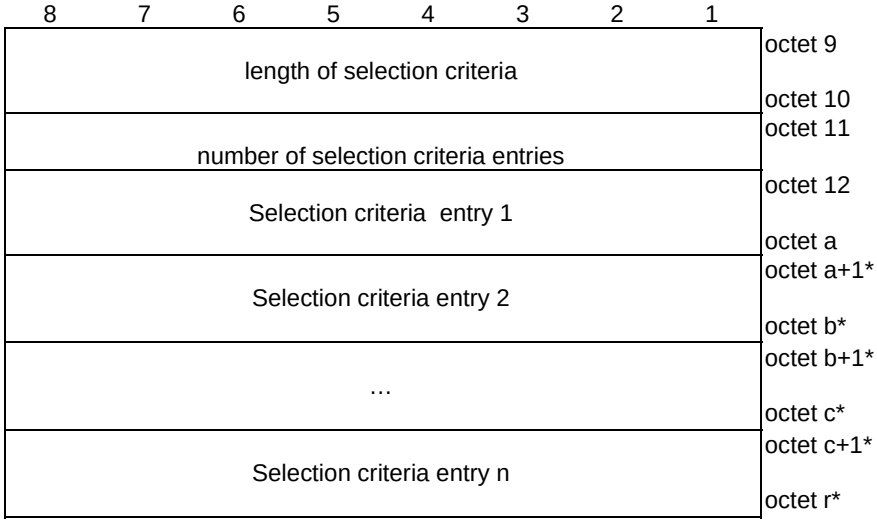

Figure 5.3.2.4: Selection criteria

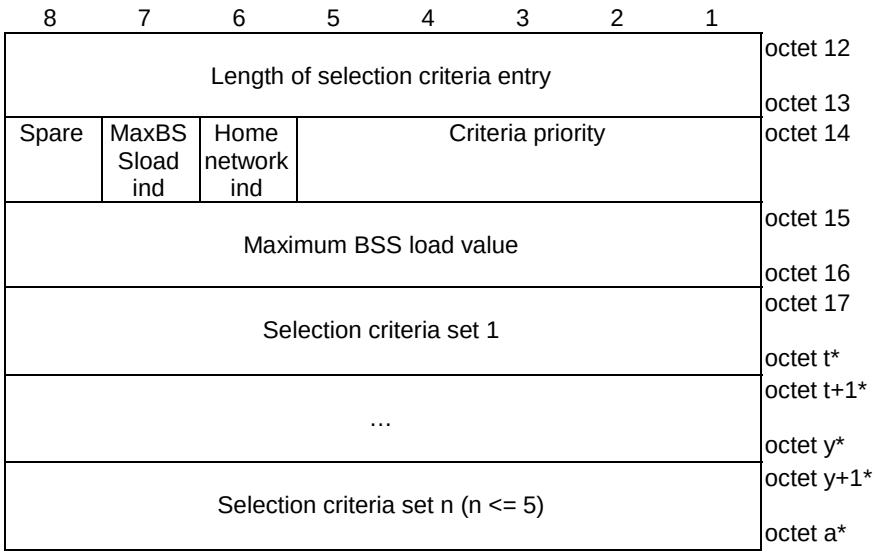

Figure 5.3.2.4a: Selection criteria entry

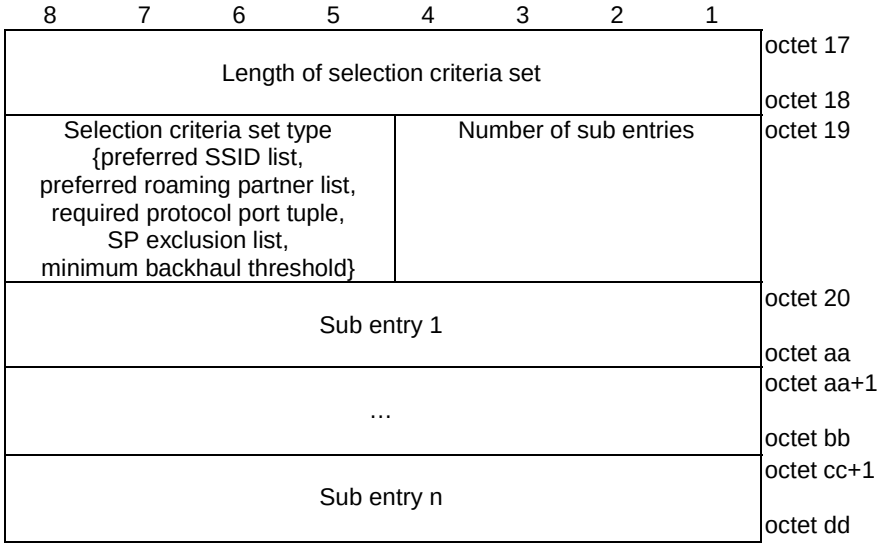

Figure 5.3.2.4b: Selection criteria set

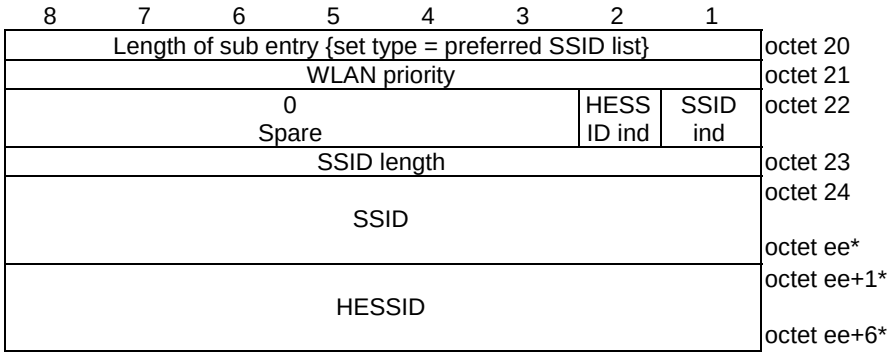

Figure 5.3.2.4c: Selection criteria sub entry {selection criteria set type = preferred SSID list}

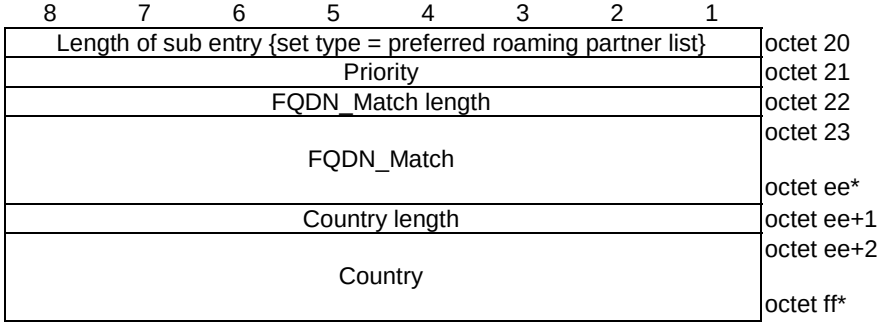

Figure 5.3.2.4d: Selection criteria sub entry {selection criteria set type = preferred roaming partner list}

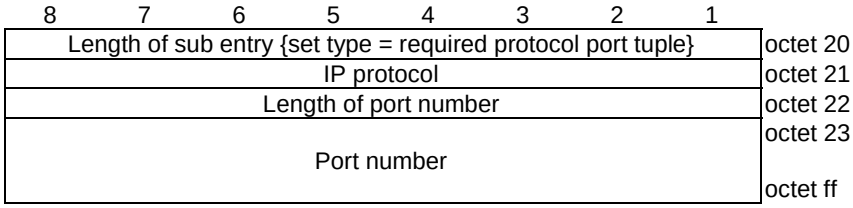

Figure 5.3.2.4e: Selection criteria sub entry {selection criteria set type = required protocol port tuple}

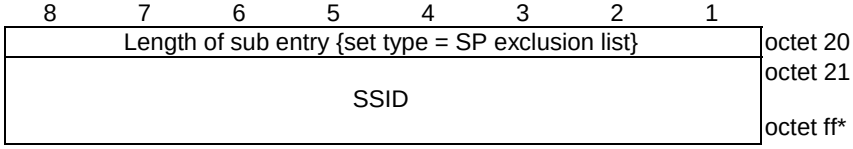

Figure 5.3.2.4f: Selection criteria sub entry {selection criteria set type = SP exclusion list}

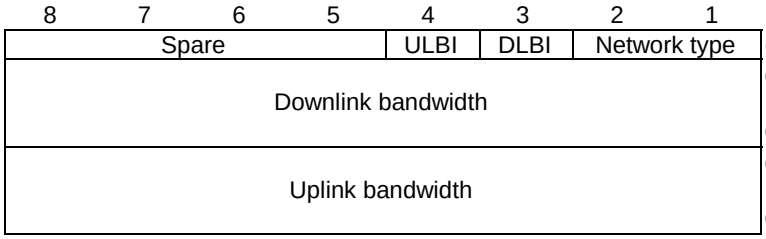

Figure 5.3.2.4g: Selection criteria sub entry {selection criteria set type = minimum backhaul threshold}

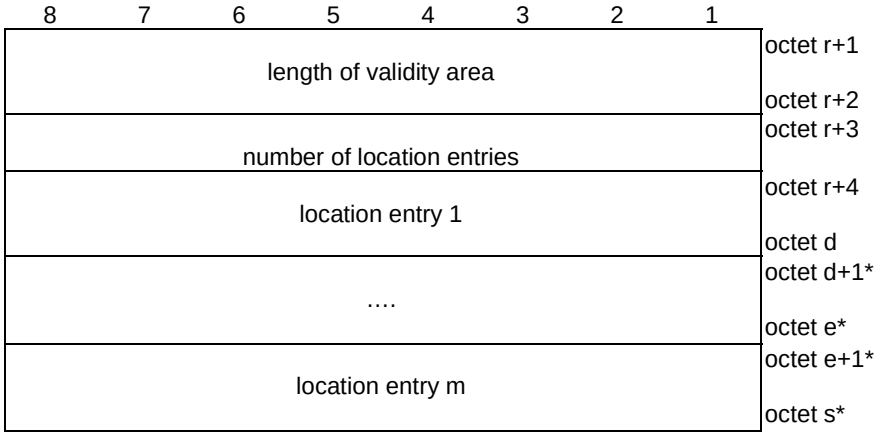

Figure 5.3.2.5: Validity area

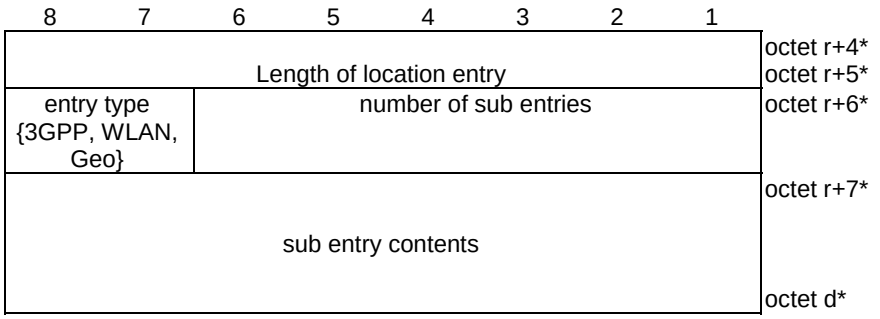

Figure 5.3.2.6: Location entry

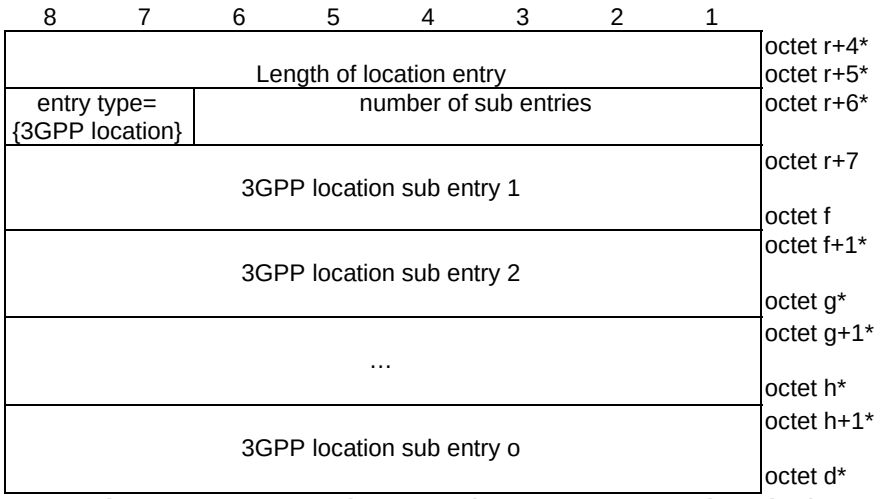

Figure 5.3.2.7: Location entry {entry type =3GPP location}

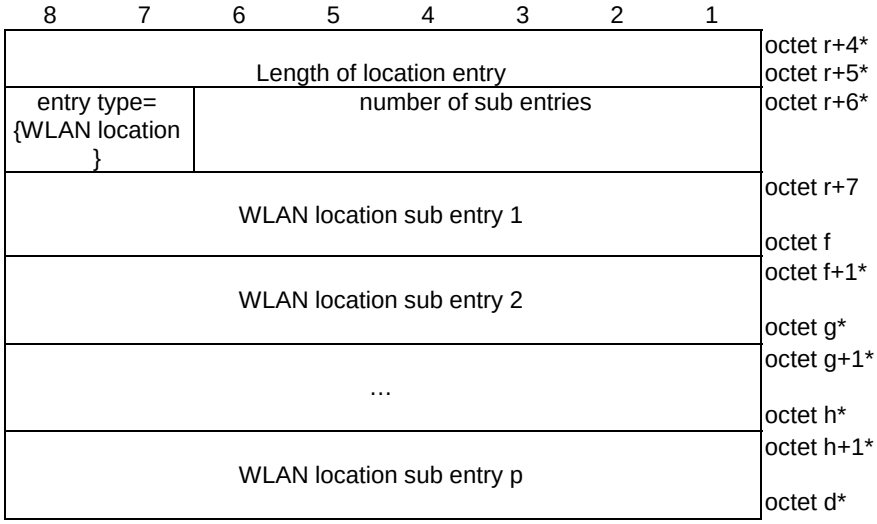

Figure 5.3.2.8: Location entry {entry type =WLAN location}

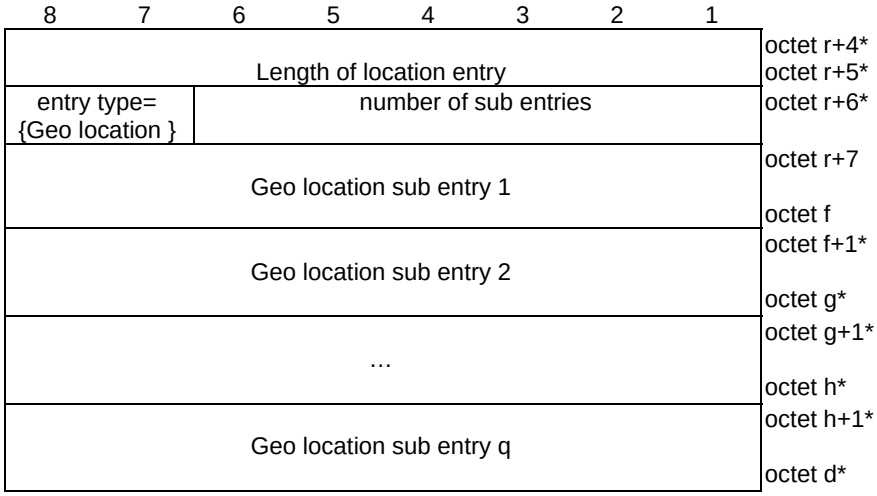

Figure 5.3.2.9: Location entry {entry type =Geo location}

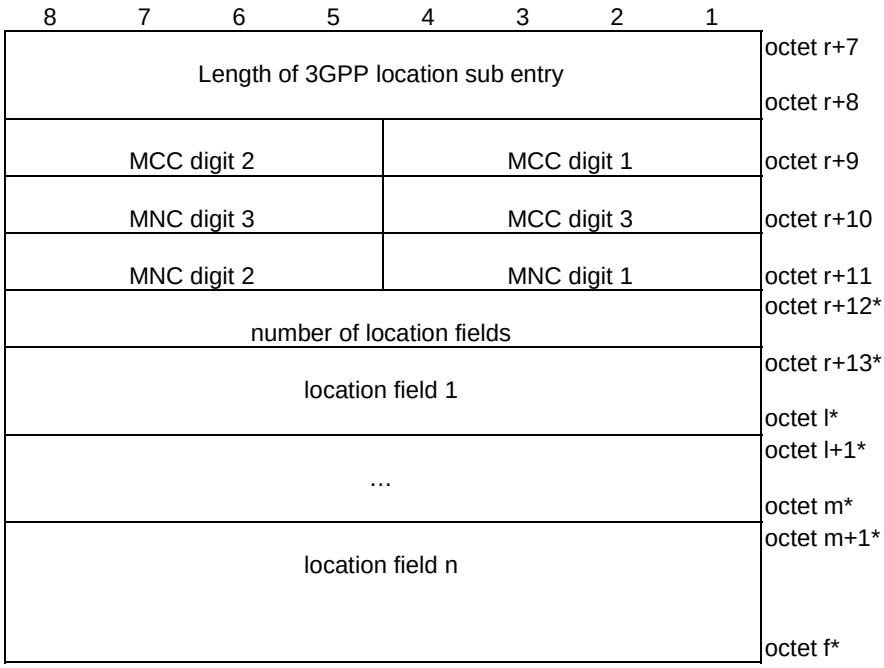

Figure 5.3.2.10: Location sub entry {entry type= 3GPP location}

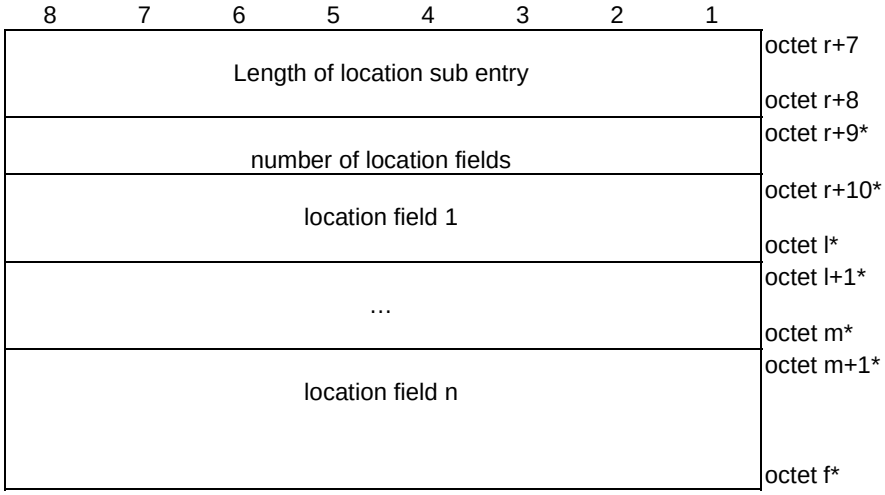

Figure 5.3.2.10a: Location sub entry {entry type= WLAN location or Geo location}

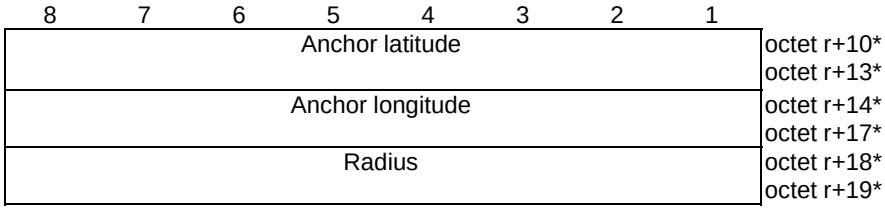

Figure 5.3.2.11a: Location field {entry type= Geo location}

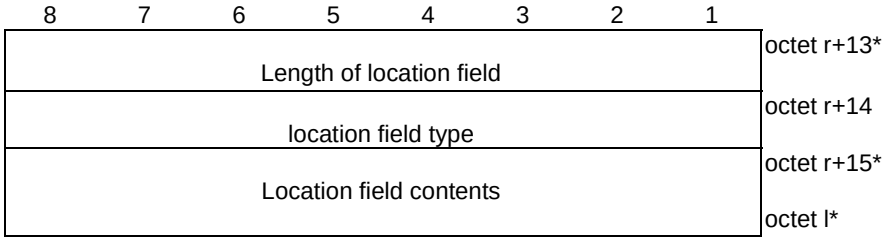

Figure 5.3.2.11b: Location field {entry type= 3GPP location}

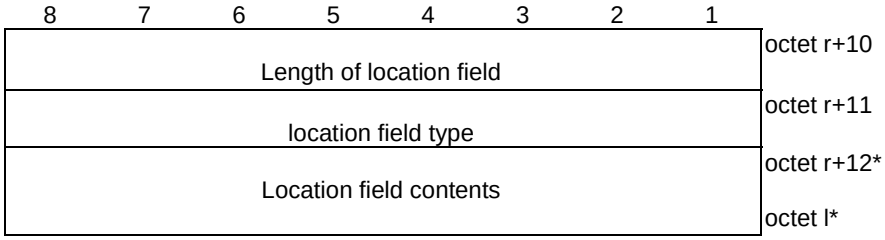

Figure 5.3.2.11c: Location field {entry type= WLAN location}

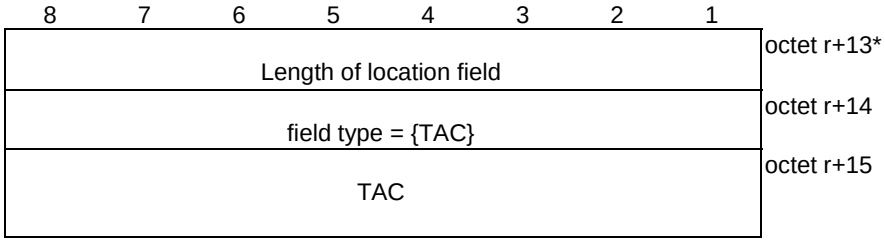

Figure 5.3.2.12: Location field {field type = TAC}

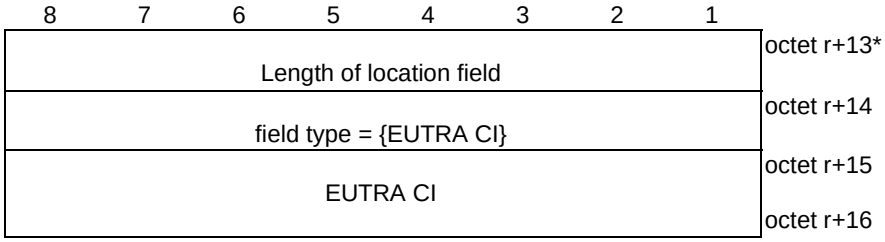

Figure 5.3.2.13: Location field {field type = EUTRA CI}

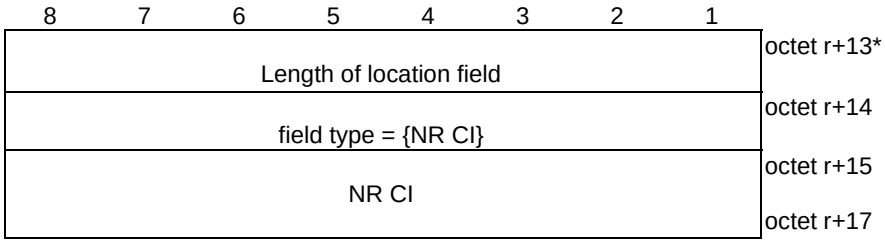

Figure 5.3.2.14: Location field {field type = NR CI}

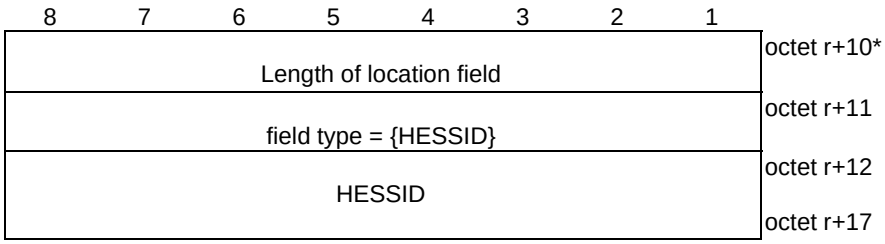

Figure 5.3.2.14a: Location field {field type = HESSID}

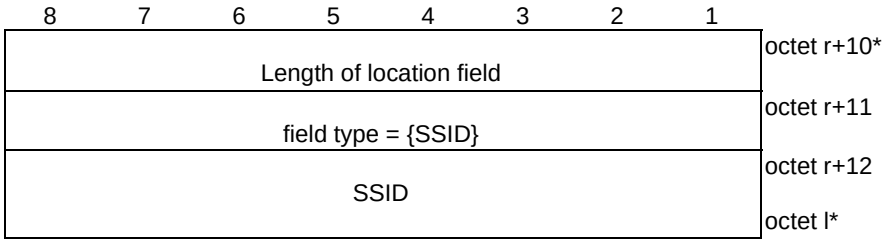

Figure 5.3.2.14b: Location field {field type = SSID}

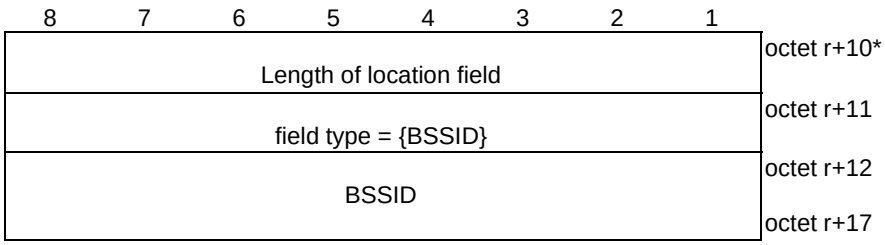

Figure 5.3.2.14c: Location field {field type = BSSID}

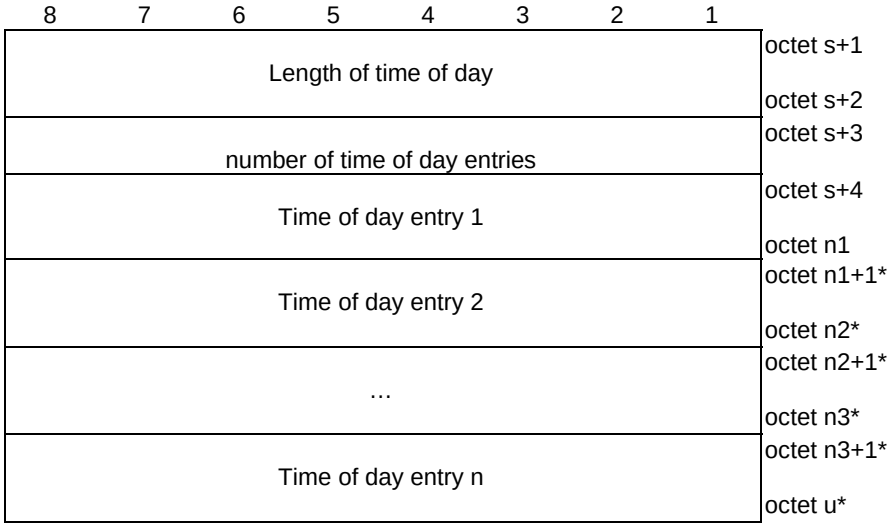

Figure 5.3.2.15: Time of day

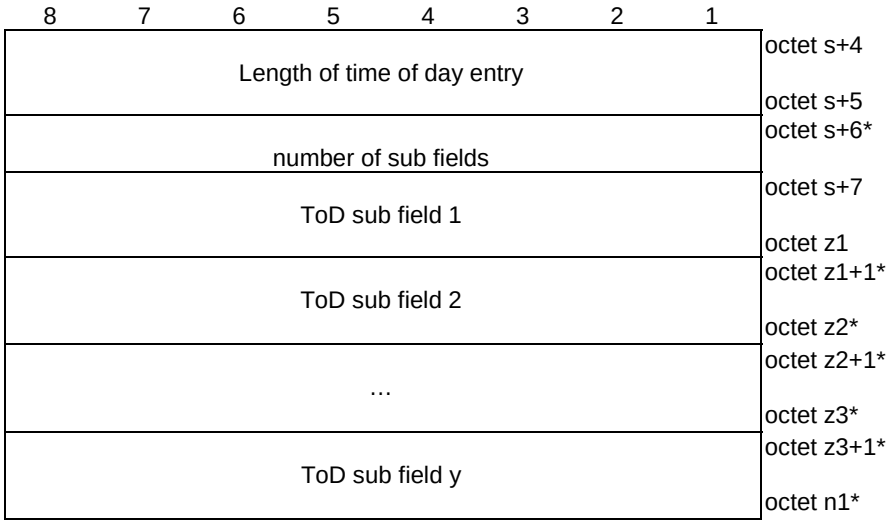

Figure 5.3.2.16: Time of day sub field

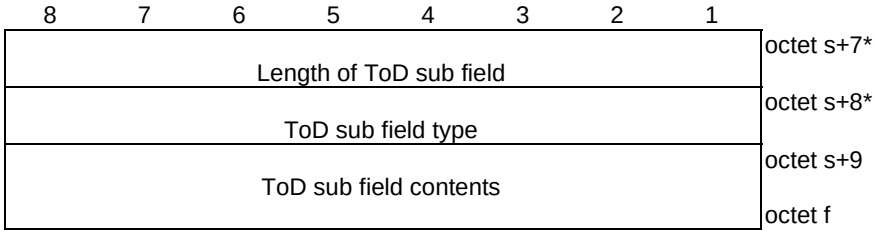

Figure 5.3.2.17: ToD sub field

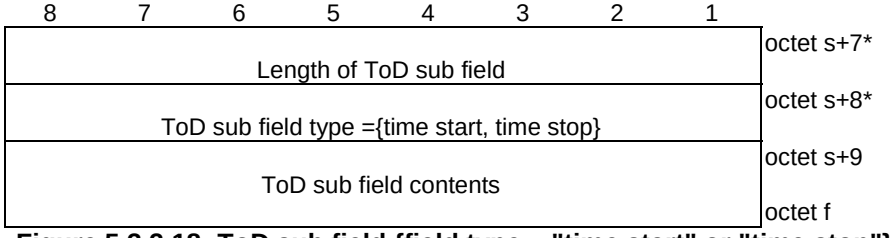

Figure 5.3.2.18: ToD sub field {field type = "time start" or "time stop"}

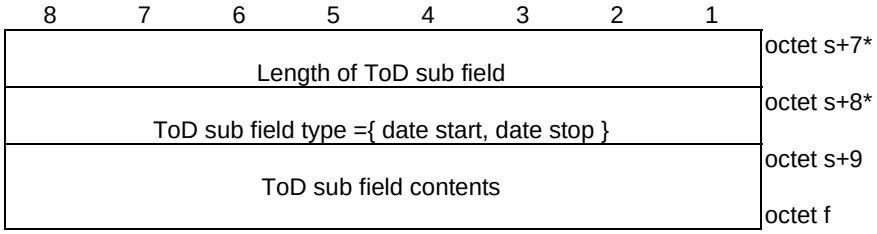

Figure 5.3.2.19: ToD sub field {field type = "date start" or "date stop"}

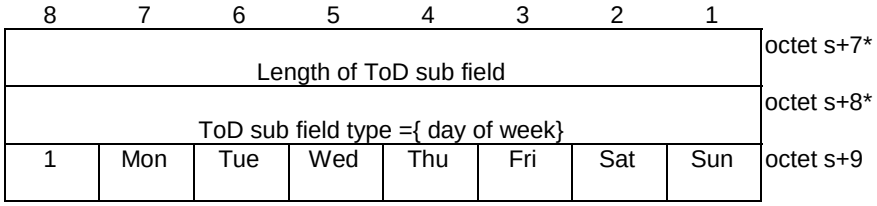

Figure 5.3.2.20: ToD sub field {field type = "day of the week"}

Table 5.3.2.1: WLANSP information element

Value part of the WLANSP information element (octets 4 to x)

ANDSP Info type (bit 1 to 4 of octet 1) shall be set to "0001" (WLANSP)

Bits 8 to 5 of octet 1 are spare and shall be encoded as zero.

Length of WLANSP contents (octets 2 to 3)

Length of WLANSP rule (octets 4 to 5)

Rule Identifier (octet 6)

This field contains the binary encoding of the WLANSP rule identifier

Rule priority (octet 7)

This field contains the binary encoding of the WLANSP rule priority

Spare bits and shall be encoded as zero (bits 1 to 2 of octet 8)

Time of day index (bit 3 of octet 8)

Bit **3**	
0	WLANSP rule does not include time of day information
1	WLANSP rule includes time of day information

Geo location index (bit 4 of octet 8)

Bit **4**	
0	WLANSP rule does not include Geo location information
1	WLANSP rule includes Geo location information

WLAN location index (bit 5 of octet 8)

Bit **5**	
0	WLANSP rule is not for WLAN location
1	WLANSP rule is for WLAN location

3GPP location index (bit 6 of octet 8)

Bit **6**	
0	WLANSP rule is not for 3GPP location
1	WLANSP rule is for 3GPP location

Validity area index (bit 7 of octet 8)

Bit **7**	
0	WLANSP rule is not for validity area
1	WLANSP rule is for validity area

Roaming (bit 8 of octet 8) (NOTE 1)

Bit **8**	
0	WLANSP rule is only valid when the UE is not roaming
1	WLANSP rule is only valid when the UE is roaming

Selection criteria (octets 9 to r)

This field contains the binary encoding of the selection criteria for a particular WLANSP rule.

Selection criteria entry (octets 12 to z) (NOTE 2)
Length of selection criteria entry (octets 12 to 13) indicates length of subsequent fields in the selection criteria entry.

Criteria priority (bits 1-5 of octet 14): the lower value indiates the selection criteria having the higher priority among the selection criteria in the WLANSP rule.

Home network ind (bit 6 of octet 14): (NOTE 3)
Bit
6
0 all WLANs could match this selection criteria entry.
1 only the WLANs that are operated by the home operator could match this selection criteria entry.

MaxBSSload ind (bit 7 of octet 14):
Bit
7
0 maximum BSS load value (octets 15 to 16) not present
1 maximum BSS load value (octets 15 to 16) present

Maximum BSS load value (octets 15 to 16) is as the node PerProviderSubscription/<X+>/Policy/MaximumBSSLoadValue defined in Hotspot 2.0 (Release 2) Technical Specification [9].

Selection criteria set (octets 17 to dd) contains the contents of a specific criteria set. In this release of specification there can be 5 types of criteria sets.

Selection criteria set type (bits 5-8 of octet 19) is coded as follows.
Bits
8 7 6 5
0 0 0 1 preferred SSID list (NOTE 4)
0 0 1 0 preferred roaming partner list (NOTE 5)
0 0 1 1 required protocol port tuple
0 1 0 0 SP exclusion list
0 1 0 1 minmum backhaul threshold
All other values are reserved.

Selection criteria sub entry (octets 20 to ff) when set type is "*preferred SSID list*" is coded as follows.
Length of sub entry (octet 20) indicates length of subsequent fields in the selection criteria sub entry.

WLAN priority (octet 21): the lower WLAN priority value indicates the WLAN having the higher priority among the WLANs in the preferred SSID list.

SSID ind (bit 1 of octet 22):
Bit
5
0 SSID field (octets 22 to ee) is not present.
1 SSID field (octets 22 to ee) is present.

HESSID ind (bit 2 of octet 22):
Bit
6
0 HESSID field (octets ee+1 to ff) is not present.
1 HESSID field (octet ee+1 to ff) is present.

SSID length (octet 23) indicates the length of the SSID field.
SSID field (octets 24 to ee) is an Octet String which shall have a maximum length of 32 octets (see IEEE Std 802.11-2012 [8]).

HESSID field (octets ee+1 to ee+6) is a 6 octet MAC address that identifies the homogeneous ESS (see IEEE Std 802.11-2012 [8]).

Selection criteria sub entry (octets 20 to ff) when set type is "*preferred roaming partner list*" is coded as follows.
Length of sub entry (octet 20) indicates length of subsequent fields in the selection criteria sub entry.

Priority (octet 21): the lower priority value indicates the higher priority in the preferred roaming partner list.

FQDN_Match length (octet 22) indicates the length of the FQDN_Match field.
FQDN_Match field (octets 23 to ee) is as the node PerProviderSubscription/<X+>/Policy/PreferredRoamingPartnerList/<X+>/FQDN_Matc h defined in Hotspot 2.0 (Release 2) Technical Specification [9].

Country length (octet ee+1) indicates the length of the country field.
Country field (octets ee+2 to ff) is as the node PerProviderSubscription/<X+>/Policy/PreferredRoamingPartnerList/<X+>/Country defined in Hotspot 2.0 (Release 2) Technical Specification [9].

Selection criteria sub entry (octets 20 to ff) when set type is "*required protocol port tuple*" is coded as follows.
Length of sub entry (octet 20) indicates length of subsequent fields in the selection criteria sub entry.

IP protocol field (octet 21) shall be present in the sub entry and refers to IP protocol field in IPv4 packets or the next header field in IPv6 packets. It is required by operator-supported application(s) on UE as specified in Hotspot 2.0 (Release 2) Technical Specification [9].

Length of port number (octet 22) indicates the length of port number field.
Port number field (octets 23 to ff) is as the node PerProviderSubscription/<X+>/Policy/RequiredProtoPortTuple/<X+>/PortNumber defined in Hotspot 2.0 (Release 2) Technical Specification [9].

Selection criteria sub entry (octets 20 to ff) when set type is "*SP exclusion list*" is coded as follows.
Length of sub entry (octet 20) indicates length of subsequent fields in the selection criteria sub entry, i.e. the length of SSID field.

SSID field (octets 21 to ff) is as the node PerProviderSubscription/<X+>/Policy/SPExclusionList/<X+>SSID defined in Hotspot 2.0 (Release 2) Technical Specification [9].

Selection criteria sub entry (octets 20 to 28) when set type is "*minmum backhaul threshold*" is coded as follows.

Network type (bit 1-2 of octet 20) is coded as follows according to the definition of the node PerProviderSubscription/<X+>/Policy/MinBackhaulThreshold/<X+>/NetworkType in Hotspot 2.0 (Release 2) Technical Specification [9].
Bits
2 1
0 0 home
0 1 roaming
All other values are reserved.

DLBI (bit 3 of octet 20):
Bit
3
0 Downlink bandwidth field (octets 21 to 24) is not present.
1 Downlink bandwidth field (octets 21 to 24) is present.

ULBI (bit 7 of octet 14):
Bit
7
0 Uplink bandwidth field (octets 25 to 28) is not present.
1 Uplink bandwidth field (octets 25 to 28) is present.

Downlink bandwidth field (octets 21 to 24) is as the node PerProviderSubscription/<X+>/Policy/MinBackhaulThreshold/<X+>/DLBandwidth defined in Hotspot 2.0 (Release 2) Technical Specification [9].

Uplink bandwidth field (octets 25 to 28) is as the node PerProviderSubscription/<X+>/Policy/MinBackhaulThreshold/<X+>/ULBandwidth defined in Hotspot 2.0 (Release 2) Technical Specification [9].

Validity area (octets r+1 to s)

This field contains the binary encoding of the validity area for a particular WLANSP rule.

Time of day (octets s+1 to u)

This field contains the binary encoding of the time of day condition for a particular WLANSP rule.

Length of 3GPP location sub entry (octets r+7 to r+8)

This field contains the length of the location entry when the WLANSP rule is for validity area of a 3GPP location.

MCC, Mobile country code (octet r+9, and bits 4 to 1 of octet r+10)

The MCC field is coded as in ITU-T Recommendation E.212 [10], annex A.

MNC, Mobile network code (bits 8 to 5 of octet r+10, and octet r+11)

The encoding of this field is the responsibility of each administration but BCD encoding shall be used. The MNC shall consist of 2 or 3 digits. If a network operator may decide to use only two digits in the MNC over the radio interface, MNC digit 3 shall be encoded as "1111".

When the location entry type is "geo location", the location field in this entry has fixed length as shown in figure 5.3.2.11a.
Anchor latitude (octets r+10 to r+13) is defined in subclause 6.1 of 3GPP TS 23.032 [7].
Anchor longitude (octets r+14 to r+17) is defined in subclause 6.1 of 3GPP TS 23.032 [7].
Radius (octets r+18 to r+19) is given in meters and is defined in subclause 6.6 of 3GPP TS 23.032 [7].

Location field type (octet r+14) when entry type is 3GPP location, or
Location field type (octet r+11) when entry type is WLAN location.
This field indicates the type of location field.

Bits
8 7 6 5 4 3 2 1
0 0 0 0 0 0 0 1 TAC
0 0 0 0 0 0 1 0 EUTRA CI
0 0 0 0 0 1 0 0 NR CI
1 0 0 0 0 0 0 1 HESSID
1 0 0 0 0 0 1 0 SSID
1 0 0 0 0 1 0 0 BSSID
All other values are reserved.

When location field type is set to "TAC", the TAC field is as defined in 3GPP TS 23.003 [4].

When location field type is set to "EUTRA CI", the EUTRA CI field is set to the cell identity part of the Evolved Cell Global Identifier, as described in 3GPP TS 36.331 [6].

When location field type is set to "NR CI", the NR CI field is set to the NR cell identity part of the NR Cell Global Identifier as defined in 3GPP TS 38.413 [14].

When location field type is set to "HESSID", the HESSID field is set to a 6 octet MAC address that identifies the homogeneous ESS (see IEEE Std 802.11-2012 [8]).

When location field type is set to "SSID", the SSID field is set to an Octet String which shall have a maximum length of 32 octets (see IEEE Std 802.11-2012 [8]).

When location field type is set to "BSSID", the BSSID field is set to an Octet String which shall be 6 octets long (see IEEE Std 802.11-2012 [8]).

ToD sub field type ={time start, time stop, date start, date stop, day of week} (octet s+8)

Bits
8 7 6 5 4 3 2 1
0 0 0 0 0 0 0 1 time start
0 0 0 0 0 0 1 0 time stop
0 0 0 0 0 1 0 0 date start
0 0 0 0 1 0 0 0 date stop
0 0 0 1 0 0 0 0 day of the week
All other values are reserved.

when field type is set to "time start" or "time stop", the value of this ToD sub field contents is time of the day represented in string format, as defined in ISO 8601:2004 [13]

When field type is set to "date start" or "date stop", the value of this ToD sub field contents is a date represented in string format, as defined in ISO 8601:2004 [13].

When field type is set to "day of the week", the value of this ToD sub field contents is an 8-bit integer formated as a bitmap representing days of the week. The most significant bit is set to one. The remaining bits represent days of the week.

NOTE 1: The value of roaming is valid only if the WLANSP rule is provided by the H-PCF.
NOTE 2: The group of selection criteria as described in subclause 4.3.2.1 is encoded as selection criteria entry.
NOTE 3: The home network indication shall not be set by V-PCF.
NOTE 4: If the home network indication bit is set to "1", the preferred SSID list shall not be present.
NOTE 5: If the home network indication bit is set to "1", the preferred roaming partner list shall not be present. The preferred roaming partner list is provided by H-PCF only.

5.3.3 Encoding of N3AN node configuration information

5.3.3.1 General

The purpose of the N3AN node configuration information is to indicate the non-3GPP access network (N3AN) node configuration information to the UE for selection of either N3IWF or ePDG for accessing 5GCN via non-3GPP access.

The N3AN node configuration information is encoded as shown in figure 5.3.3.1.1, table 5.3.3.1.1, figure 5.3.3.1.2, table 5.3.3.1.2.

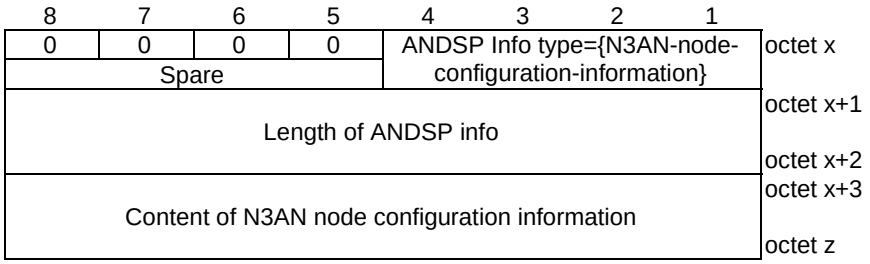

Figure 5.3.3.1.1: ANDSP info containing N3AN node configuration information, where x=k

Table 5.3.3.1.1: N3AN node configuration information

ANDSP Info type (bit 1 to 4 of octet x) shall be set to "0010" (N3AN node configuration information)
Bits 8 to 5 of octet 1 are spare and shall be encoded as zero.
Length of ANDSP info (octets x+1 to x+2)

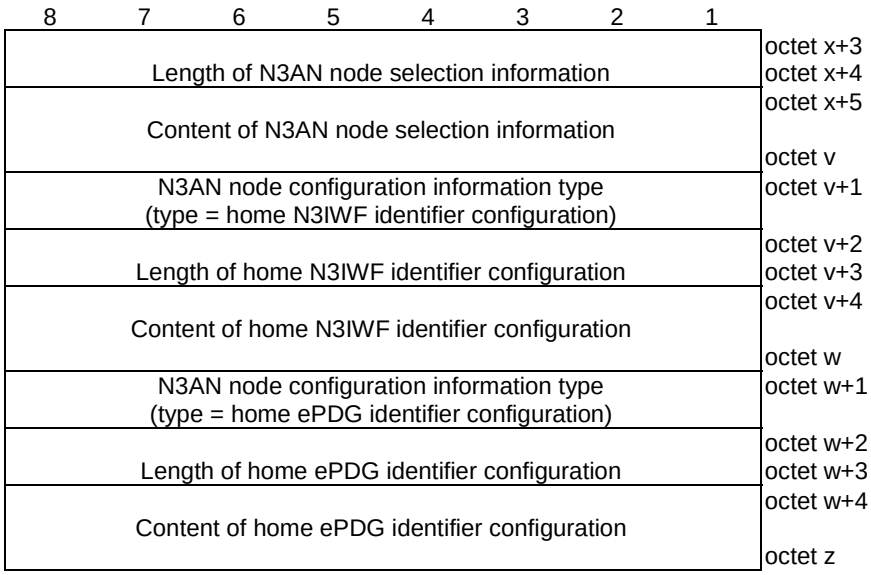

Figure 5.3.3.1.2: Content of N3AN node configuration information

Table 5.3.3.1.2: Content of N3AN node configuration information

N3AN node configuration information type is coded as follows.

8	7	6	5	4	3	2	1	
0	0	0	0	0	0	0	1	Home N3IWF identifier configuration
0	0	0	0	0	0	1	0	Home ePDG identifier configuration

All other values are reserved.

N3AN node selection information field (octet x+5 to v) shall be present and the content is as encoded in subclause 5.3.3.2.

Home N3IWF identifier configuration field (octet v+1 to w) may be present and the content is as encoded in subclause 5.3.3.3.

Home ePDG identifier configuration field (octet w+1 to z) may be present and the content is is as encoded in subclause 5.3.3.4.

5.3.3.2 N3AN node selection information

The content of N3AN node selection information contains a sequence of the N3AN node selection information entries. Each N3AN node selection information entry contains a PLMN ID and information for the PLMN ID. The content of N3AN node selection information contain at least an N3AN node selection information entry with information for the HPLMN and an N3AN node selection information entry for any PLMN.

The content is encoded according to figure 5.3.3.2.1, figure 5.3.3.2.2 and table 5.3.3.2.1.

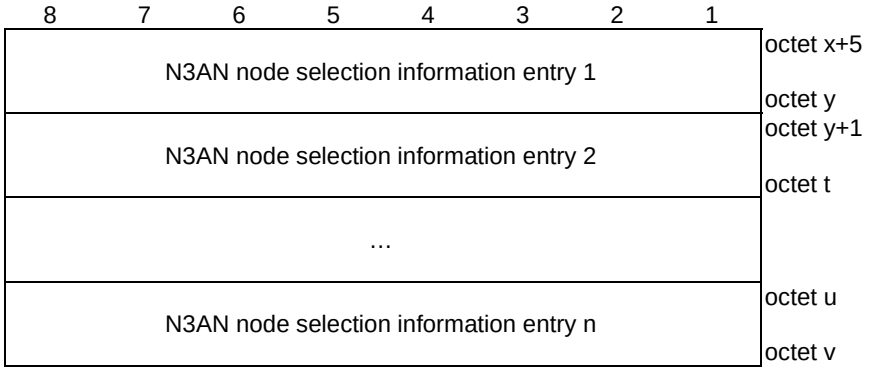

Figure 5.3.3.2.1: Content of N3AN node selection information

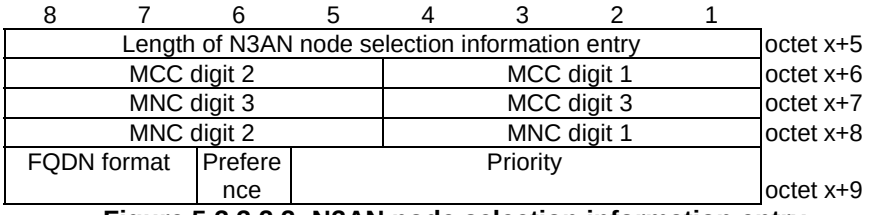

Figure 5.3.3.2.2: N3AN node selection information entry

Table 5.3.3.2.1: N3AN node selection information

Length of N3AN node selection information entry (octet x+5) contains length of subsequent fields in the N3AN node selection information entry.

PLMN ID (octet x+6 to x+7) field shall be set to zero if it indicates "any PLMN". Otherwise,

MCC, Mobile country code (octet x+6, and bits 5 to 1 of octet x+7)

The MCC field is encoded as in ITU-T Recommendation E.212 [10], annex A.

MNC, Mobile network code (bits 8 to 5 of octet x+7, and octet x+8)
The encoding of this field is the responsibility of each administration but BCD coding shall be used. The MNC shall consist of 2 or 3 digits. If a network operator decides to use only two digits in the MNC, MNC digit 3 shall be encoded as "1111".

Priority (bits 5 to 1 of octet x+9) indicates the preference order given to N3AN nodes of a PLMN. The lower value indicates higher priority. If the PLMN is the UE's HPLMN or the PLMN ID indicates "any PLMN", this priority filed shall be ignored.

Preference (bit 6 of octet x+9) indicates which N3AN node type is preferred in this PLMN and is encoded as follows.

6	
0	N3IWF is preferred
1	ePDG is preferred

FQDN format (bits 8 to 7 of octet x+9) indicates format to be used when the FQDN is constructed by the UE. This field is encoded as follows.

8	**7**	
0	0	Operator identifier based ePDG FQDN format or operator identifier based N3IWF FQDN.
0	1	Tracking/location area identity based ePDG FQDN format or tracking area identity based N3IWF FQDN format.

All other values are reserved.

5.3.3.3 Home N3IWF identifier configuration

The content of home N3IWF identifier configuration contains a list of home N3IWF identifier entries.

The content of home N3IWF identifier configuration is encoded according to figure 5.3.3.3.1.

The content of each home N3IWF identifier entry is coded according to figure 5.3.3.3.2, table 5.3.3.3.1, figure 5.3.3.3.3 and table 5.3.3.3.2.

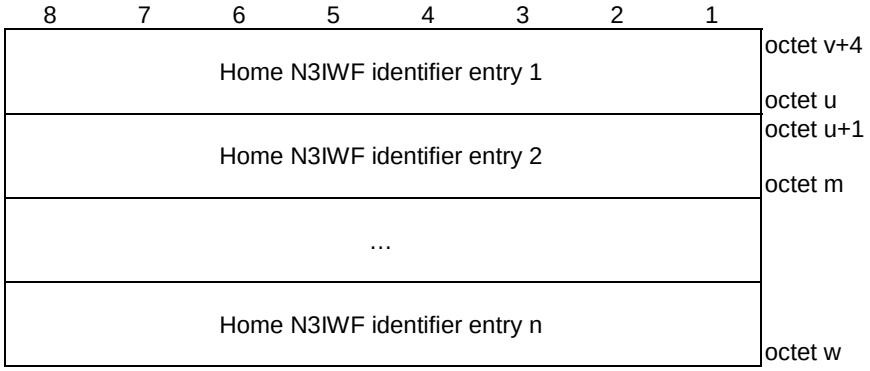

Figure 5.3.3.3.1: Content of home N3IWF identifier configuration

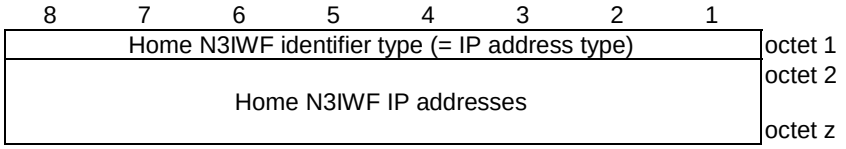

Figure 5.3.3.3.2: Home N3IWF identifier entry (type = IP address type)

Table 5.3.3.3.1: Home N3IWF identifier entry (type = IP address type)

Home N3IWF identifier type (octet 1) is set as follows when the type is IP address.

8	**7**	**6**	**5**	**4**	**3**	**2**	**1**	
0	0	0	0	0	0	0	1	IPv4
0	0	0	0	0	0	1	0	IPv6
0	0	0	0	0	0	1	1	IPv4IPv6

If the home N3IWF identifier type indicates IPv4, then the home N3IWF IP addresses field contains an IPv4 address in octet 2 to octet 5.

If the home N3IWF identifier type indicates IPv6, then the home N3IWF IP addresses field contains an IPv6 address in octet 2 to octet 17.

If the home N3IWF identifier type indicates IPv4IPv6, then the home N3IWF IP addresses field contains two IP addresses. The first IP address is an IPv4 address in octet 2 to octet 5. The second IP address is an IPv6 address in octet 6 to octet 21.

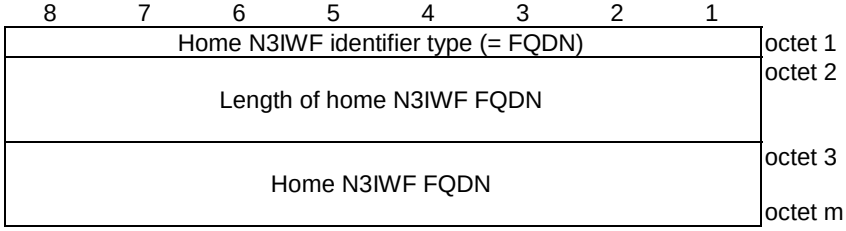

Figure 5.3.3.3.3: Home N3IWF identifier entry (type = FQDN)

Table 5.3.3.3.2: Home N3IWF identifier entry (type = FQDN)

Home N3IWF identifier type (octet 1) is set as follows when the type is FQDN.

8	**7**	**6**	**5**	**4**	**3**	**2**	**1**	
0	0	0	0	0	1	0	0	FQDN

Length of home N3IWF FQDN field (octet 2) indicates the length of home N3IWF FQDN.

Home N3IWF FQDN field (octet 3 to octet m) is encoded as defined in IETF RFC 1035 [12].

5.3.3.4 Home ePDG identifier configuration

The content of home ePDG identifier configuration contains a list of home ePDG identifier entries.

The content of home ePDG identifier configuration is encoded according to figure 5.3.3.4.1.

The content of each home ePDG identifier entry is encoded according to figure 5.3.3.4.2, table 5.3.3.4.1, figure 5.3.3.4.3 and table 5.3.3.4.2.

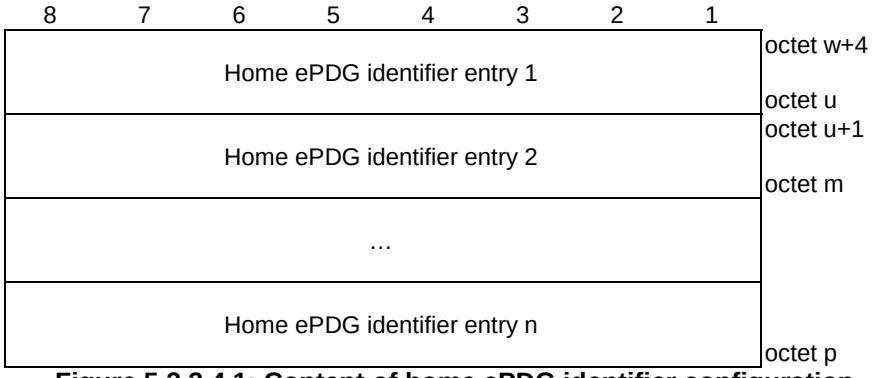

Figure 5.3.3.4.1: Content of home ePDG identifier configuration

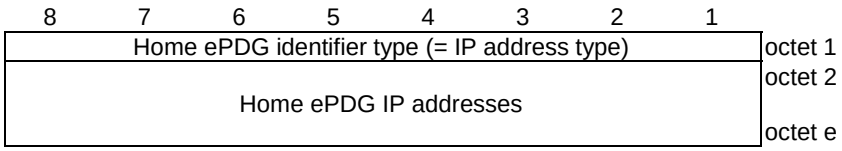

Figure 5.3.3.4.2: Home ePDG identifier entry (type = IP address type)

Table 5.3.3.4.1: Home ePDG identifier entry (type = IP address type)

Home ePDG identifier type (octet 1) is set as follows when the type is IP address.

8	**7**	**6**	**5**	**4**	**3**	**2**	**1**	
0	0	0	0	0	0	0	1	IPv4
0	0	0	0	0	0	1	0	IPv6
0	0	0	0	0	0	1	1	IPv4IPv6

If the home ePDG identifier type indicates IPv4, then the home ePDG IP addresses field contains an IPv4 address in octet 2 to octet 5.

If the home ePDG identifier type indicates IPv6, then the home ePDG IP addresses field contains an IPv6 address in octet 2 to octet 17.

If the home ePDG identifier type indicates IPv4IPv6, then the home ePDG IP addresses field contains two IP addresses. The first IP address is an IPv4 address in octet 2 to octet 5. The second IP address is an IPv6 address in octet 6 to octet 21.

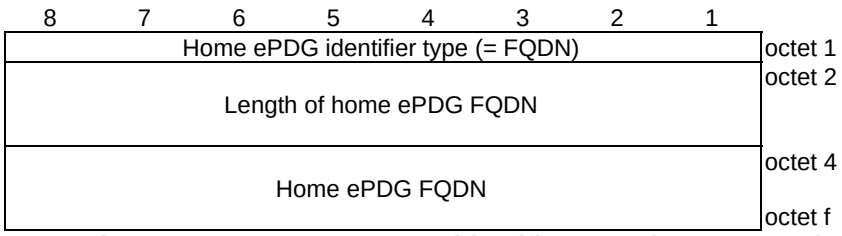

Figure 5.3.3.4.3: Home ePDG identifier entry (type = FQDN)

Table 5.3.3.4.2: Home ePDG identifier entry (type = FQDN)

Home ePDG identifier type (octet 1) is set as follows when the type is FQDN. **8 7 6 5 4 3 2 1** 0 0 0 0 0 1 0 0 FQDN Length of home ePDG FQDN field (octet 2) indicates the length of home ePDG FQDN. Home ePDG FQDN field (octet 3 to octet f) is encoded as defined in IETF RFC 1035 [12].

Annex A (informative): Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2018-04	CT1#110					TS skeleton is provided by C1-182823. C1-182793, C1-182795, C1-182798, C1-182821, C1-182822 are implemented as Annex A.	0.0.0
2018-05	CT1#111					Includes the following contributions agreed by CT1 at CT#111: C1-183550, C1-183551, C1-183552, C1-183553, C1-183555, C1-183556, C1-183862, C1-183863.	0.1.0
2018-06	CT-80					version 1.0.0 created for presentation for information	1.0.0
2018-07	CT1#111 bis					Includes the following contributions agreed by CT1 at CT#111bis: C1-184345, C1-184627, C1-184691, C1-184859, C1-184927, C1-184945, C1-184948.	1.1.0
2018-08	CT1#112					Includes the following contributions agreed by CT1 at CT#112: C1-185149, C1-185630, C1-185636, C1-185641, C1-185679.	1.2.0
2018-09	CT-81	CP-182112				version 2.0.0 created for presentation for approval	2.0.0
2018-09	CT-81					version 15.0.0 created after approval	15.0.0
2018-12	CT-82	CP-183043	0001	2	F	Modifications to ANDSP	15.1.0
2018-12	CT-82	CP-183043	0002	2	F	Aligning the subclauses and correcting the reference and requirements	15.1.0
2018-12	CT-82	CP-183043	0003	2	B	Adding connection capabilities in URSP rules	15.1.0
2018-12	CT-82	CP-183043	0004	2	F	Editorial and other changes	15.1.0
2018-12	CT-82	CP-183043	0005	1	B	Coding of WLAN selection criteria entry	15.1.0
2018-12	CT-82	CP-183043	0006	2	B	Complete location entry definition	15.1.0
2018-12	CT-82	CP-183043	0011	2	F	Clarification on PDU session selection	15.1.0
2018-12	CT-82	CP-183043	0013	2	F	Clarification on URSP traffic descriptor and SSC mode	15.1.0
2018-12	CT-82	CP-183043	0015	2	F	OS App Id with a variable length	15.1.0
2019-03	CT-83	CP-190090	0012	7	F	Clarification on UE local configuration and URSP preference	15.2.0
2019-03	CT-83	CP-190210	0016	6	F	PCF does not send OS Id to UE	15.2.0
2019-03	CT-83	CP-190090	0017	1	F	The formats of OS Id	15.2.0
2019-03	CT-83	CP-190090	0018	2	F	Add destination FQDN as additional traffic descriptor	15.2.0
2019-03	CT-83	CP-190090	0019	1	D	Update abbreviations	15.2.0
2019-03	CT-83	CP-190090	0020	3	F	Correcting the name of ITU-T Recommendation E.212	15.2.0
2019-03	CT-83	CP-190090	0021	2	F	Correction on WLANSP rules description	15.2.0
2019-03	CT-83	CP-190090	0022	2	F	Correction to Length of URSP rule and Length of route selection descriptor	15.2.0
2019-03	CT-83	CP-190090	0024	1	F	Clarification on OS Id + OS App Id field of URSP	15.2.0
2019-03	CT-83	CP-190211	0026	2	F	UE with multiple OS Ids	15.2.0
2019-03	CT-83	CP-190090	0027	1	F	Correction to length of location sub entry in WLANSP rule	15.2.0
2019-03	CT-83	CP-190090	0028	2	F	Unknown or unexpected URSP rules	15.2.0

History

Document history		
V15.0.0	September 2018	Publication
V15.1.0	April 2019	Publication
V15.2.0	April 2019	Publication