ETSI TS 129 585 V18.0.0 (2024-05)

5G;
5G System (5GS);
Session Management Function (SMF) /
Centralized User Configuration (CUC) to
Access Network Talker Listener (AN-TL) and
Core Network Talker Listener (CN-TL)
protocol aspects;
Stage 3
(3GPP TS 29.585 version 18.0.0 Release 18)

Reference
DTS/TSGC-0429585vi00

Keywords
5G

ETSI

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

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

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

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

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

Legal Notice

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

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

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

Modal verbs terminology

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

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

Contents

Foreword

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

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

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

In the present document, modal verbs have the following meanings:

shall indicates a mandatory requirement to do something

shall not indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

should indicates a recommendation to do something

should not indicates a recommendation not to do something

may indicates permission to do something

need not indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

can indicates that something is possible

cannot indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

will indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

will not indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

might indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

might not indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

is (or any other verb in the indicative mood) indicates a statement of fact

is not (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

1 Scope

The present document specifies the protocol of communication in the 5G System between:

- the SMF/CUC and the (R)AN/AN-TL, and
- the SMF/CUC and the UPF/CN-TL,

when the (R)AN and the UPF support the Talker and Listener functionality, for the support of Time Sensitive Networking (TSN) enabled Transport Network (TN) as specified in clauses 4.4.8, 5.28a and Annex M of 3GPP TS 23.501 [2] and Annex F of 3GPP TS 23.502 [3].

2 References

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

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

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

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

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

[4] IEEE Std 802.1Q-2022: "IEEE Standard for Local and Metropolitan Area Networks-Bridges and Bridged Networks".

[5] 3GPP TS 38.413: "NG-RAN; NG Application Protocol (NGAP)".

[6] 3GPP TS 29.244: "Interface between the Control Plane and the User Plane nodes".

[7] IEEE Std 802.1CBdb-2021: "IEEE Standard for Local and metropolitan area networks-Frame Replication and Elimination for Reliability".

[8] IETF RFC 2474: "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers".

[9] IEEE P802.1Qdj-d1.3: "IEEE Draft Standard for Local and metropolitan area networks - Bridges and Bridged Networks - Amendment XX: Configuration Enhancements for Time-Sensitive Networking".

3 Definitions of terms, symbols and abbreviations

3.1 Terms

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

Stream: A unidirectional flow of time-sensitive data from one source to one or more destinations, and at the highest level, one Talker end system to one or more Listener end systems.

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.501 [2] apply:

5G System

3.2 Symbols

No symbol is defined in this release of the specification.

3.3 Abbreviations

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

5GS	5G System
AN-TL	Access Network Talker Listener function
CN-TL	Core Network Talker Listener function
CNC	Centralized Network Configuration
CUC	Centralized User Configuration
ES	End Station
(R)AN	(Radio) Access Network
SMF	Session Management Function
TL	Talker Listener
TN	Transport Network
TSN	Time-Sensitive Networking
UPF	User Plane Function

4 General

4.1 Introduction

The 5GS supports interworking with IEEE 802.1 TSN deployed in the transport network. The interworking is applicable when the transport network deploys the fully centralized configuration model as defined in IEEE Std 802.1Q [4]. In this scenario, a TSN TN is deployed to realize the N3 interface between the (R)AN and the UPF. From the perspective of the TSN enabled TN, the (R)AN and the UPF act as End Stations (ES) of the TSN TN.

Figure 4.1-1 depicts the reference model for 5GS interworking with TSN enabled TN, with focus on the interfaces between the SMF/CUC and the (R)AN/AN-TL and between the SMF/CUC and the UPF/CN-TL which are in scope of this specification.

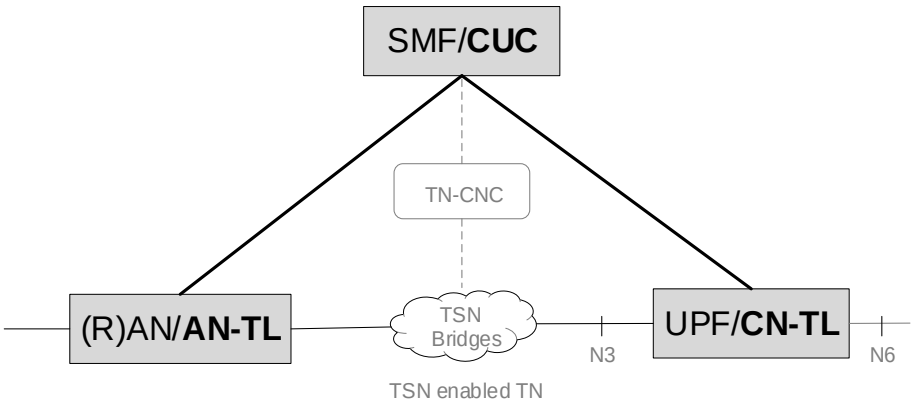

Figure 4.1-1: Reference Model – 5GS interworking with TSN enabled TN

If the (R)AN and the UPF support the TSN Talker and Listener (TL) functionality (i.e. they implement the AN-TL and CN-TL, respectively), the SMF/CUC can communicate with the AN-TL and CN-TL to:

- retrieve the ES capabilities (list of interfaces and interface capabilities) of the AN-TL and CN-TL; and
- configure TSN features in the ES (e.g. for stream identification, stream association with TSN resources, stream transformation, hold and buffer functionality, as described in IEEE Std 802.1Q [4]) of the AN-TL and CN-TL.

The messages defined in this specification are exchanged between the SMF/CUC and the (R)AN/AN-TL and UPF/CN-TL via TL-Containers sent within NGAP Session Management signaling as specified in 3GPP TS 38.413 [5] and PFCP Session related signaling as specified in 3GPP TS 29.244 [6]. The related stage 2 call flows are specified in 3GPP TS 23.502 [3].

5 Elementary procedures between SMF/CUC and AN-TL and CN-TL

5.1 General

5.2 Procedures

5.2.1 SMF/CUC-initiated Get procedure

5.2.1.1 General

The SMF/CUC may retrieve the following ES information of the AN-TL and CN-TL (see Table M.2-1 of 3GPP TS 23.501 [2]) during the establishment of a PDU session:

1) ES interfaces, consisting of a list of one or more Interface IDs, where each Interface ID identifies a physical interface (distinct point of attachment) in the ES acting as Talker/Listener (see clause 46.2.3.3 of IEEE Std 802.1Q [4]); and/or
2) Interface capabilities, describing the network capabilities of all the ES interfaces. The following capabilities may be signaled in this release of the specification:
   - Vlan Tag capability, indicating whether the ES interfaces support the ability to tag/untag frames using a Customer VLAN Tag (C-TAG) provided by the network (see clause 46.2.3.7.1 of of IEEE Std 802.1Q [4]);

- Buffering capability, indicating the maximum possible buffer duration for a packet of a stream with the maximum size of an Ethernet packet (1522 Bytes) that is supported by the AN-TL/CN-TL when acting as a Talker (see Table M.2-1 of 3GPP TS 23.501 [2]).

NOTE: Interface Capabilities are identical for all Interfaces/Ports of the ES.

5.2.1.2 SMF/CUC-initiated Get procedure initiation

In order to retrieve the ES parameters of the AN-TL or CN-TL, the SMF/CUC shall:

a) encode the information about the requested ES parameters (Interface IDs and/or Interface capabilities) in the Requested ES Parameters IE in a Get Request message;

b) send the Get Request message to the AN-TL or CN-TL as specified in 3GPP TS 23.502 [3]; and

c) start the timer Tget.

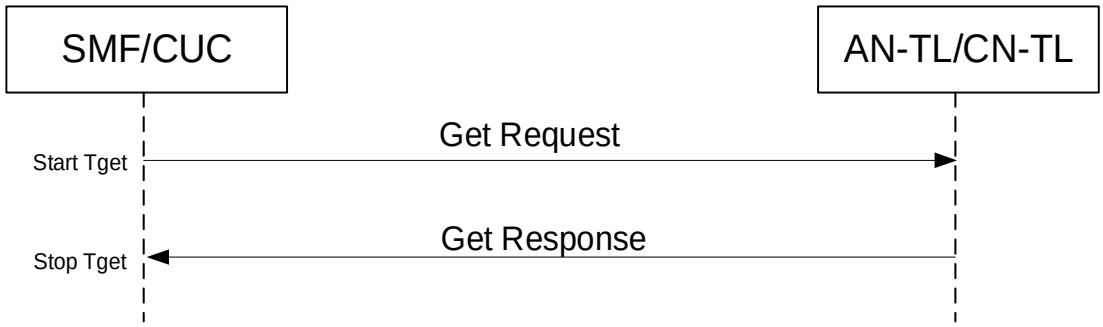

Figure 5.2.1.2-1: SMF/CUC-initiated Get procedure

5.2.1.3 SMF/CUC-initiated Get procedure completion

Upon receipt of the Get Request message, the AN-TL/CN-TL shall:

- report the list of its interfaces in Interface ID IE(s) of the Get Response message, if the ITF ID bit was set to 1 in the Requested ES Parameters IE in the Get Request message;

- report the network capabilities of its interfaces in the Interface Capabilities IE, if the ITF CAP bit was set to 1 in the Requested ES Parameters IE in the Get Request message; and

- send the Get Response message to the SMF/CUC as specified in 3GPP TS 23.502 [3].

5.2.1.4 Abnormal cases in the SMF/CUC

The following abnormal cases can be identified:

a) SMF/CUC receives a PFCP Session Establishment Response or a NGAP PDU Session Resource Setup Response message not including a Get Response.

This case may occur e.g. if the SMF/CUC assumes that the NG-RAN or UPF supports the AN/CN-TL functionality when they actually don't, due to some misconfiguration.

The SMF/CUC implementation shall abort the procedure, should consider that the NG-RAN/UPF does not support the AN/CN-TL functionality, and should log information about the misconfiguration.

b) SMF/CUC does not receive any PFCP Session Establishment Response or NGAP PDU Session Resource Setup Response message.

The Get Request within the PFCP Session Establishment Request or NGAP PDU Session Resource Setup Request message is retransmitted using procedures for reliable delivery of PFCP or NGAP messages towards the UPF/NG-RAN, e.g. retransmitting the requests (or responses) relying on the Reliable Delivery of PFCP messages procedure defined in clause 6.4 of TS 29.244 or relying on TCP (HTTP/HTTPS) or SCTP (NGAP) retransmissions.

On the expiry of the Tget timer, the SMF/CUC shall abort the procedure and should log error information.

5.2.1.5 Abnormal cases in the AN-TL/CN-TL

The following abnormal cases can be identified:

a) Transmission failure of the Get Response message indication (e.g. transient communication failure over N4).

The AN-TL/CN-TL shall not diagnose an error and consider the SMF/CUC-initiated Get procedure complete.

5.2.2 SMF/CUC-initiated Set procedure

5.2.2.1 General

The SMF/CUC may initiate the Set procedure towards the AN-TL and CN-TL (at the Talker and Listener), per TN stream of a PDU session, during the PDU session modification procedure to:

- configure a new TN stream at the AN-TL/CN-TL. If the SMF/CUC received a TimeAwareOffset from the CNC for the new TN stream, the configuration shall contain additionally the TimeAwareOffset and the other parameters to calculate the gate control information shall be added to the gate control input information of the addressed interface/port of the End Station (ES);

- delete the configuration of an existing TN stream at the AN-TL/CN-TL (e.g. when a QoS flow is terminated). This may also include to delete the TimeAwareOffset together with the other parameters to calculate the gate control information from the gate control input information of the addressed interface/port of the End Station (ES); and

- modify an existing TN stream configuration by deleting the existing TN stream configuration and configuring a new TN stream.

NOTE 1: When gate control input information at an interface/port changes, the AN-TL and CN-TL recalculates the Gate Control Information with respect to the changed information.

The SMF/CUC shall initiate the Set procedure towards the AN-TL and CN-TL, per TN stream of a PDU session, during the PDU session release procedure to:

- delete the configuration of the existing TN stream of the PDU session at the AN-TL and CN-TL; and

- update for the scheduled TN streams the gate control input information to enable the AN-TL and CN-TL to calculate for the addressed interface/port Gate Control Information for the remaining TN streams of the other PDU sessions.

NOTE 2: PDU sessions are established as Always-on PDU sessions for time-sensitive communication, time synchronization and deterministic network, as specified in clause 5.27.0 of 3GPP TS 23.501 [2]. Therefore, the Set procedure is not invoked during a Service Request procedure.

During the above procedures, the SMF/CUC shall configure the following IEEE 802.1 End Station (ES) information at the AN-TL and CN-TL (see Table M.2-1 of 3GPP TS 23.501 [2]):

1) when configuring a new stream:

   a) TN streamID uniquely identifying the TN stream configuration at the ES.

   b) TN stream identification information, identifying the packets belonging to the new stream being configured. It shall either comprise:

      - a mask-and-match information, containing the destination GTP-U F-TEID of the GTP-U tunnel of the PDU session and with the QFI assigned to the TN stream; or

- a Data Frame Specification, with the IPv4-tuple or IPv6-type set with the destination GTP-U IP address of the GTP-U tunnel of the TN stream of the PDU session.

NOTE 3: The Data Frame Specification can be used to identify the packets of the TN stream if a separate GTP-U tunnel, with a distinct IP address (of the GTP-U F-TEID) is established for the TN stream.

c) Interface ID of the AN-TL and CN-TL for the new TN stream, indicating the ES interface/port which transfers the new TN stream.

d) Interface configuration part, indicating the Source MAC address, Destination MAC address, Priority Code Point and/or VLAN ID (if the ES interface is VLAN capable) to be used for the new TN stream before it is transmitted via the interface/port of the ES, if stream transformation is required to be performed at the AN-TL/CN-TL.

e) Interface configuration part and other parameters to enable the Talker to calculate for the interface/port of the ES Gate Control Information, comprising the Time Aware Offset, Interval, and MaxFrameSize parameters of the TN stream, if the SMF/CUC received a TimeAwareOffset from the CNC for the new TN stream.

2) when deleting the configuration of an existing stream:

a) TN stream ID uniquely identifying the stream's configuration at the ES.

NOTE 4: Multiple SMF/CUCs can operate in parallel in the same configuration domain and serve PDU sessions established at the same AN-TL/CN-TL, i.e. an ES (i.e. AN-TL/CN-TL) need not be dedicated to a single SMF/CUC. See IEEE Std P802.1Qdj [9].

NOTE 5: The SMF/CUC can send multiple concurrent Set Requests towards the AN-TL/CN-TL, for the same or different PDU sessions, to establish or terminate TN streams.

5.2.2.2 SMF/CUC-initiated Set procedure initiation

In order to configure the TN stream information in the AN-TL and CN-TL, the SMF/CUC shall:

a) encode the information about the requested configuration in a Set Request message with an Add TN Stream Configuration IE or a Delete TN Stream Configuration IE, if it is requested to configure a new stream or delete the configuration of an existing TN stream, respectively, with the information described in clause 5.2.2.1.

The Set Request message may contain a Delete TN Stream Configuration IE followed by an Add TN Stream Configuration IE to modify an existing stream configuration by deleting it and configuring the new TN stream.

b) send the Set Request message to the AN-TL or CN-TL as specified in 3GPP TS 23.502 [3]; and

c) start the timer Tset.

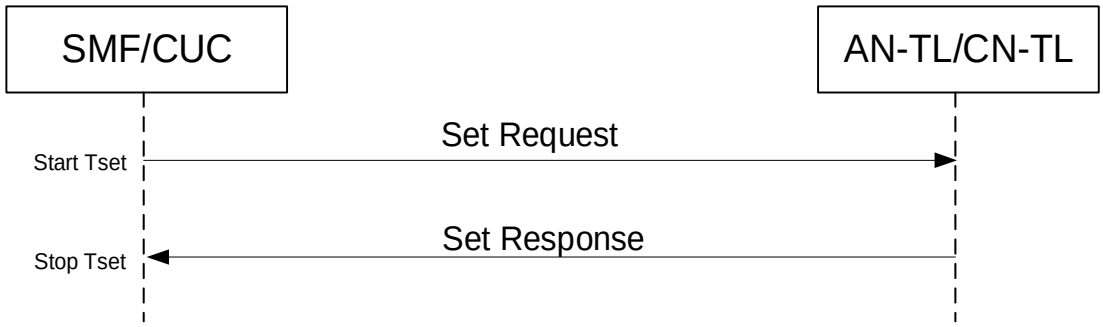

Figure 5.2.2.2-1: SMF/CUC-initiated Set procedure

5.2.2.3 SMF/CUC-initiated Set procedure completion

Upon receipt of the Set Request message, the AN-TL/CN-TL shall:

- store and attempt to apply the new TN stream configuration, for the TN stream configuration requested to be added;
- delete the TN stream configuration, for the TN stream configuration requested to be deleted;
- recalculate the Gate Control Information for the TN streams associated with the ES interface/port which transfers the new TN stream or which was transferring the deleted TN stream, if gate control input information was provided during the configuration of the new or deleted TN stream; and
- send the Set Response message to the SMF/CUC as specified in 3GPP TS 23.502 [3].

5.2.2.4 Abnormal cases in the SMF/CUC

The following abnormal cases can be identified:

a) SMF/CUC receives a PFCP Session Modification/Deletion Response or a NGAP PDU Session Resource Modify/Release Response message not including a Set Response.

The SMF/CUC implementation shall abort the procedure and should log the error information.

b) SMF/CUC does not receive any PFCP Session Modification/Deletion Response or NGAP PDU Session Resource Modify/Release Response message.

The Set Request within the PFCP Session Modification/Deletion Request or NGAP PDU Session Resource Release Command/Modify Request message is retransmitted using procedures for reliable delivery of PFCP or NGAP messages towards the UPF/NG-RAN, e.g. retransmitting the requests (or responses) relying on the Reliable Delivery of PFCP messages procedure defined in clause 6.4 of TS 29.244 or relying on TCP (HTTP/HTTPS) or SCTP (NGAP) retransmissions.

On the expiry of the Tset timer, the SMF/CUC shall abort the procedure and should log error information.

5.2.2.5 Abnormal cases in the AN-TL/CN-TL

The following abnormal cases can be identified:

a) Transmission failure of the Set Response message indication (e.g. transient communication failure over N4).

The AN-TL/CN-TL shall not diagnose an error and consider the SMF/CUC-initiated Set procedure complete.

NOTE 1: Considering the SMF/CUC-initiated Set procedure complete as a result of this abnormal case does not cause the AN-TL/CN-TL to revert the execution of the operations included in the SET Request message.

b) Mismatch between the Data Frame Specification and the GTP-U information received outside of the TL-Container

The (R)AN/AN-TL and UPF/CN-TL shall return a Failure Code if it detects a mismatch between the Data Frame Specification and the GTP-U information received outside of the TL-Container, as specified in NOTE 13 of Table M.2-1 of 3GPP TS 23.501 [2].

NOTE 2: This assumes that the AN-TL/CN-TL receives the GTP-U information of the PDU session from the (R)AN/UPF, respectively, by implementation specific means.

6 Handling of unknown, unforeseen, and erroneous data

6.1 General

Clause 6 specifies procedures for the handling of unknown, unforeseen, and erroneous data by the receiving entity. These procedures are called error handling procedures.

A protocol error is defined as a message or an Information Element received from a peer entity with an unknown type, or if it is unexpected, or if it has an erroneous content.

The term silently discarded is used in the following clauses to mean that the receiving entity's implementation shall discard such a message without further processing or that the receiving entity discards such an IE and continues processing the message. The conditions for the receiving entity to silently discard an IE are specified in the subsequent clauses.

The handling of unknown, unexpected or erroneous messages and IEs shall provide support for forward compatibility with future extensions of the protocol. Therefore, the sending entity shall be able to safely include in a message a new conditional-optional or an optional IE. Such an IE may also have a new type value. Any legacy receiving entity shall, however, silently discard such an IE and continue processing the message.

If a protocol error is detected by the receiving entity, it should log the event including the erroneous message and may include the error in a statistical counter.

For Response messages containing a rejection Cause value, see clause 7.1.3.2.

The receiving entity shall apply the error handling specified in the subsequent clauses.

If the received erroneous message is a reply to an outstanding request, the entity receiving the reply shall stop retransmissions of the related request.

6.2 Message of Invalid Length

If an entity receives a message that is too short to contain the message header, that message shall be silently discarded.

6.3 Unknown Message

If an entity receives a message with an unknown Message Type value, it shall silently discard the message.

6.4 Unexpected Message

If an entity receives an unexpected request message, for example a message for which the message is defined, but the direction is incorrect, then the entity shall silently discard the message and shall log an error.

If an entity receives an unexpected response message, for example a message for which there is no corresponding outstanding request, it shall discard the message and may log an error.

6.5 Missing Information Elements

An entity shall check if all mandatory IEs are present in the received Request message. If one or more mandatory information elements are missing in the received Request message, the entity should log the error and shall send a Response message with the Cause IE value set to "Mandatory IE missing" with the type of the missing mandatory IE.

An entity shall check if all mandatory IEs are present in the received Response message without a rejection Cause value. If one or more mandatory information elements are missing, the entity shall stop retransmissions of the corresponding request message and should log the error.

An entity shall check if conditional information elements are present in the received Request message, if possible (i.e. if the receiving entity has sufficient information available to check if the respective conditions were met). If one or more conditional information elements are missing, an entity should log the error and shall send a Response message with the Cause IE value set to "Conditional IE missing" together with the type of the missing conditional IE.

An entity shall check if conditional information elements are present in the received Response message without a rejection Cause value, if possible (i.e. if the receiving entity has sufficient information available to check if the respective conditions were met). If one or more conditional information elements are missing, the entity shall stop retransmissions of the corresponding Request message and should log the error.

The absence of an optional information element shall not trigger any error handling.

6.6 Semantically incorrect Information Element

The receiver of a Request message including a mandatory or a verifiable conditional information element with a semantically invalid value shall discard the request, should log the error, and shall send a response with the Cause IE value set to "Mandatory IE incorrect" together with a type and instance of the offending IE.

The receiver of a Response message including a mandatory or a verifiable conditional information element with a semantically invalid value shall stop retransmissions of the corresponding request message and should log the error.

If an entity receives an information element with a value which is shown as reserved, it shall treat that information element as invalid and should log the error. If the invalid IE is received in a Request, and it is a mandatory IE or a verifiable conditional IE, the entity shall send a response with Cause set to "Mandatory IE incorrect" together with a type and instance of the offending IE.

The use of reserved values invokes error handling; the use of spare values can be silently discarded and for IEs with spare values used, processing shall be continued ignoring the spare values.

The receiver of a signalling message including an optional information element with a value that is not in the range defined for this information element value shall discard this IE, but shall treat the rest of the message as if this IE was absent and continue processing. The receiver shall not check the content of an information element field that is defined as "spare".

All semantically incorrect optional information elements in a signalling message shall be treated as not present in the message.

6.7 Unknown or unexpected Information Element

The receiver of a message including an unexpected information element with a known Type value that is not defined for this message shall discard the IE and log an error. The receiver shall process the message.

NOTE: An Information Element in an encoded message or grouped IE is identified by the IE Type.

6.8 Repeated Information Elements

An Information Element is repeated if there is more than one IE with the same IE Type in the scope of the message (or in the scope of the grouped IE). Such an IE is a member in a list.

If an information element is repeated in a signalling message in which repetition of the information element is not specified, only the contents of the information element appearing first shall be handled and all subsequent repetitions of the information element shall be ignored. When the number of repetitions of information elements is specified, only the contents of specified repeated information elements shall be handled and all subsequent repetitions of the information element shall be ignored.

6.9 Information Element of Invalid Length

An information element has an invalid length when the actual length of the IE is different from the value of the Length field in the IE header. Here, the actual length of the IE means the length of the content field of the received IE.

If a message contains more than one information elements and one or more of them have invalid length, the receiving entity may detect which of the IEs have invalid length only in the following cases:

- If the Length value in the IE header is greater than the overall length of the message; and
- If the invalid length IE is the last one in the message.

If a receiving entity detects information element with invalid length in a Request message, it shall send an appropriate error response with the Cause IE value set to "Invalid length" together with the type of the offending IE.

7 Messages and Message Format

7.1 Message format and encoding

7.1.1 Transmission Order and Bit Definitions

Messages shall be transmitted in network octet order starting with octet 1 with the most significant bit sent first.

The most significant bit of an octet in a message is bit 8. If a field in a message spans over several octets, the most significant bit is bit 8 of the octet with the lowest number, unless specified otherwise.

7.1.2 Message Format

7.1.2.1 General

The format of a message is depicted in Figure 7.1.2.1-1.

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to m	Message header							
m+1 to n	Zero or more Information Element(s)							

Figure 7.1.2.1-1: Message Format

A message shall contain the message header and may contain subsequent information element(s) dependent on the type of message.

The encoding of the Information elements is specified in clause 8.1.

7.1.2.2 Message Header

Messages use a fixed length header of 4 octets. Figure 7.1.2.2-1 illustrates the format of the Header.

	Bits							
Octets	8	7	6	5	4	3	2	1
1	Version			Spare				
2	Message Type							
3	Sequence Number (1st Octet)							
4	Sequence Number (2nd Octet)							
5	Sequence Number (3rd Octet)							
6-8	Spare							

Figure 7.1.2.2-1: Message Header

The first octet of the header shall be used as follows:

- Bit 1-5 are spare bits. The sending entity shall set it to "0" and the receiving entity shall ignore it.
- Bits 6 to 8 represent the version of the protocol which shall be set to decimal value 1 ("001").

The usage of the fields in octets 2 - 4 of the header shall be as specified below.

- Octet 2 represents the Message type field, which shall be set to the unique value for each type of message. Message type values are specified in Table 7.3-1 "Message types".
- Octets 3 to 5 represent the Sequence Number field which enables to correlate a response with a request.

- Octets 6 to 8 are spare. The sender shall set these octets to all zeros and the receiver shall ignore them.

NOTE: The SMF/CUC can send multiple Set Request messages to the AN-TL/CN-TL for the same PDU session or different PDU sessions in parallel. The response message contains the same sequence number as the corresponding request message.

7.1.3 Information Elements

7.1.3.1 General

The format of Information Elements are defined in clauses 8.1 and 8.2.

7.1.3.2 Presence Requirements of Information Elements

IEs within messages shall be specified with one of the following presence requirements:

- Mandatory: this means that:
  - the IE shall be included by the sending entity;
  - the receiver diagnoses a "Mandatory IE missing" error when detecting that the IE is not present. If a mandatory IE is missing, then the receiver shall abort the procedure. A response including a "Mandatory IE missing" cause shall include the type of the missing IE.
- Conditional: this means that:
  - the IE shall be included by sending entity if the conditions specified are met;
  - the receiver shall check the conditions as specified in the corresponding message type description, based on the parameter combination in the message and/or on the state of the receiving node, to infer if a conditional IE shall be expected. Only if a receiver has sufficient information, if a conditional IE, which is necessary for the receiving entity to complete the procedure, is missing, then the receiver shall abort the procedure. A response including a "Conditional IE missing" cause shall include the type of the missing IE.
- Optional: this means that:
  - the IE shall be included as a service option. Therefore, the IE may be included or not in a message. The handling of an absent optional IE, or an erroneous optional IE is specified in clause 7.4.

For conditional IEs, the clause describing the message explicitly defines the conditions under which the inclusion of each IE becomes mandatory or optional for that particular message. These conditions shall be defined so that the presence of a conditional IE only becomes mandatory if it is critical for the receiving entity.

For grouped IEs, the presence requirement of the embedded IE shall follow the rules:

- If the grouped IE is Mandatory within a given message: the presence requirements of individual embedded IEs are as stated within the Mandatory grouped IE for the given message;
- if the grouped IE is Conditional within a given message: if the embedded IE in the grouped IE is Mandatory or Conditional, this embedded IE is viewed as Conditional IE by the receiver. If the embedded IE in the grouped IE is Conditional-Optional, this embedded IE is viewed as Optional IE by the receiver. If the embedded IE in the grouped IE is Optional, this embedded IE is viewed as Optional IE by the receiver;
- if the grouped IE is Conditional-Optional within a given message: if the embedded IE in the grouped IE is Mandatory or Conditional, this embedded IE is viewed as Conditional-Optional IE by the receiver. If the embedded IE in the grouped IE is Conditional-Optional, this embedded IE is viewed as Optional IE by the receiver. If the embedded IE in the grouped IE is Optional, this embedded IE is viewed as Optional IE by the receiver;
- if the grouped IE is Optional within a given message: all embedded IEs in the grouped IE are viewed as Optional IEs by the receiver.

In all of the above cases, appropriate error handling as described in clause 7.4 shall be applied for protocol errors of the embedded IEs.

Only the Cause IE at message level shall be included in the response if the Cause contains a value that indicates that the request is not accepted, regardless of whether there are other mandatory or conditional IEs defined for a given response message.

7.1.3.3 Grouped Information Elements

A Grouped IE is an IE which may contain other IEs.

Grouped IEs have a length value in the TLV encoding, which includes the added length of all the embedded IEs. Overall coding of a grouped IE with 4 octets long IE header is defined in clause 8.2. Each IE within a grouped IE also shall also contain 4 octets long IE header.

Grouped IEs are not marked by any flag or limited to a specific range of IE type values. The clause describing an IE in this specification shall explicitly state if it is a Grouped IE.

NOTE: Each entry into each Grouped IE creates a new scope level. Exit from the grouped IE closes the scope level. The message level is the top most scope.

If more than one grouped IEs of the same type, but for a different purpose are sent within the same message level, these IEs shall have different IE types.

If more than one grouped IEs of the same type and for the same purpose are sent within the same message level, these IEs shall have exactly the same IE type to represent a list.

Assigning the same IE type to grouped IEs which don't have the same content is not recommended, even if these grouped IEs are in different message levels.

7.1.3.4 Information Element Type

An IE in a message or Grouped IE is identified by its IE Type and described by a specific row in the corresponding tables in clause 7.

If several IEs with the same Type are included in a message or Grouped IE, they represent a list for the corresponding IE name.

An IE Type value uniquely identifies a specific IE.

One IE type value is specified for Vendor Specific IEs.

7.2 Message Types

The message types are defined in Table 7.2-1.

Table 7.2-1: Message Types

Message Type value (Decimal)	Message
0	Reserved
1	Get Request
2	Get Response
3	Set Request
4	Set Response
5 to 255	For future use

7.3 Messages

7.3.1 Get Request

7.3.1.1 Message definition

The Get Request message is sent by the SMF/CUC to the AN-TL or CN-TL to retrieve ES parameters of the AN-TL or CN-TL, see Table 7.3.1.1-1.

Message type: Get Request

Direction: SMF/CUC to AN-TL, SMF/CUC to CN-TL

Table 7.3.1.1-1: Information Elements in Get Request

Information elements	P	Condition / Comment	IE Type
Requested ES Parameters	M	This IE shall indicate the ES parameters requested to be retrieved from the AN-TL/CN-TL.	Requested ES Parameters

7.3.2 Get Response

7.3.2.1 Message definition

The Get Response message is sent by the AN-TL or CN-TL to the SMF/CUC to report the requested ES parameters of the AN-TL or CN-TL, see Table 7.3.2.1-1.

Message type: Get Response

Direction: AN-TL to SMF/CUC, CN-TL to SMF/CUC

Table 7.3.2.1-1: Information Elements in Get Response

Information elements	P	Condition / Comment	IE Type
Cause	M	Indicates success or failure of the request, and in the latter case, the reason for the failure.	Cause
Interface ID	C	This IE shall be included if the SMF/CUC has set the ITF ID bit to 1 in the Requested ES Parameters IE in the Get Request message. Several IEs with the same IE type may be present to report multiple Interface IDs.	Interface ID
Interface Capabilities	C	This IE shall be included if the SMF/CUC has set the ITF CAP bit to 1 in the Requested ES Parameters IE in the Get Request message.	Interface Capabilities

7.3.3 Set Request

7.3.3.1 Message definition

The Set Request message is sent by the SMF/CUC to the AN-TL or CN-TL to configure ES parameters of the AN-TL or CN-TL, see Table 7.3.3.1-1.

Message type: Set Request

Direction: SMF/CUC to AN-TL, SMF/CUC to CN-TL

Table 7.3.3.1-1: Information Elements in Set Request

Information elements	P	Condition / Comment	IE Type
Add TN Stream Configuration	C	This IE shall be present if it is requested to configure a new TN stream. See Table 7.3.3.1-2.	Add TN Stream Configuration
Delete TN Stream Configuration	C	This IE shall be present if it is requested to delete the configuration of an existing TN stream. See Table 7.3.3.1-3.	Delete TN Stream Configuration

Table 7.3.3.1-2: Add TN Stream Configuration

Octet 1 and 2		Add TN Stream Configuration IE Type = 5 (decimal)	
Octets 3 and 4		Length = n	
Information elements	**P**	**Condition / Comment**	**IE Type**
TN Stream ID	M	This IE shall contain a TN stream ID uniquely identifying the stream's configuration at the ES.	TN Stream ID
TN Stream Identification with mask-and-match	C	This IE shall be present if packets belonging to the TN stream are identified using mask-and-match information. (NOTE)	Mask-and-match information
TN Stream Identification with Data Frame Specification	C	This IE shall be present if packets belonging to the TN stream are identified using a Data Frame Specification. See Table 7.3.3.1-4. (NOTE)	Data Frame Specification
Interface ID	M	This IE shall indicate the interface/port of the ES which transfers the new TN stream.	Interface ID
Interface configuration	C	This IE shall be present if: - stream transformation is required to be performed at the AN-TL/CN-TL; and/or - the SMF/CUC received a TimeAwareOffset from the CNC for the new TN stream. See Table 7.3.3.1-5.	Interface configuration
Other Parameters for Gate Control Information Calculation	C	This IE shall be sent to an AN-TL and CN-TL acting as Talker, if the TimeAwareOffset is received from the CNC. When present, it shall contain other parameters for the new TN stream that enable the AN-TL/CN-TL to calculate gate control information for the Interface/Port of the ES which transfers the TN stream being added.	Other Parameters for Gate Control Information Calculation
NOTE: Either the TN Stream Identification with mask-and-match IE or the TN Stream Identification with Data Frame Specification shall be present.			

Table 7.3.3.1-3: Delete TN Stream Configuration

Octet 1 and 2		Delete TN Stream Configuration IE Type = 7 (decimal)	
Octets 3 and 4		Length = n	
Information elements	**P**	**Condition / Comment**	**IE Type**
TN Stream ID	M	This IE shall contain the TN stream ID of the stream's configuration to be deleted.	TN Stream ID

Table 7.3.3.1-4: Data Frame Specification

Octet 1 and 2		Data Frame Specification IE Type = 8 (decimal)	
Octets 3 and 4		Length = n	
Information elements	**P**	**Condition / Comment**	**IE Type**
Destination MAC Address	C	Destination MAC address. If absent, the destination MAC address shall be ignored for the purpose of Stream identification.	Destination MAC address
Source MAC Address	C	Source MAC address. If absent, the source MAC address shall be ignored for the purpose of Stream identification.	Source MAC address
VLAN Tag Info	C	Priority Code Point and/or VLAN ID used for stream identification	Vlan Tag Info
IPv4 tuple	C	IPv4 tuple for stream identification.	IPv4 tuple
IPv6 tuple	C	IPv6 tuple for stream identification.	IPv6 tuple
NOTE: At least one IE shall be present.			

Table 7.3.3.1-5: Interface Configuration

Octet 1 and 2		Interface Configuration IE Type = 17 (decimal)	
Octets 3 and 4		Length = n	
Information elements	**P**	**Condition / Comment**	**IE Type**
Source MAC Address	O	Source MAC address to be used for the stream	Source MAC Address
Destination MAC Address	O	Destination MAC address used for stream transformation	Destination MAC Address
VLAN Tag Info	O	Priority Code Point and/or VLAN ID used for stream transformation	VLAN Tag Info
IPv4 tuple	O	IPv4 tuple used for stream transformation	IPv4 tuple
IPv6 tuple	O	IPv6 tuple used for stream transformation	IPv6 tuple
Time Aware Offset	C	This IE shall be present and contain the Time Aware Offset, if the SMF/CUC received a TimeAwareOffset from the CNC for the new TN stream.	Time Aware Offset
NOTE: See Annex M.1 and Table M.2-1 of 3GPP TS 23.501 [2] for the description and use of the parameters of the Interface Configuration.			

7.3.4 Set Response

7.3.4.1 Message definition

The Set Response message is sent by the AN-TL or CN-TL to the SMF/CUC to report the outcomes of the ES parameters configuration request, see Table 7.3.4.1-1.

Message type: Set Response

Direction: AN-TL to SMF/CUC, CN-TL to SMF/CUC

Table 7.3.4.1-1: Information Elements in Set Response

Information elements	P	Condition / Comment	IE Type
Cause	M	This IE shall indicate success or failure of the request, and in the latter case, the reason for the failure.	Cause

8 Information elements coding

8.1 Information Elements Format

Figure 8.1-1 depicts the format of an Information Element.

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = xxx (decimal)							
3 to 4	Length = n							
p to (p+1)	Enterprise ID							
k to (n+4)	IE specific data or content of a grouped IE							

Figure 8.1-1: Information Element Format

NOTE 1: If the Bit 8 of Octet 1 is not set, this indicates that the IE is defined by 3GPP and the Enterprise ID is absent. If Bit 8 of Octet 1 is set, this indicates that the IE is defined by a vendor and the Enterprise ID is present identified by the Enterprise ID.

An IE has the following mandatory fields:

- Type: this field indicates the type of the Information Element. IE type values within the range of 0 to 32767 are reserved for IE defined by 3GPP and are listed in clause 8.2.1 IE type values within the range of 32768 to 65535 are used for vendor-specific IE and the value allocation is controlled by the vendor.

- Length: this field contains the length of the IE excluding the first four octets, which are common for all IEs (Type and Length) and is denoted "n" in Figure 8.1-1 and in Figure 8.1-2. Bit 8 of the lowest numbered octet is the most significant bit and bit 1 of the highest numbered octet is the least significant bit.

An IE has the following optional fields:

- Enterprise ID: if the IE type value is within the range of 32768 to 65535, this field shall contain the IANA-assigned "SMI Network Management Private Enterprise Codes" value of the vendor defining the IE. The Enterprise ID set to "10415" (IANA-assigned "SMI Network Management Private Enterprise Codes") shall not be used for the vendor specific IEs.

For illustration, Figure 8.1-2 depicts the format of an Information Element (IE) defined by 3GPP and is specified in this specification. For IE's defined by 3GPP, the IE type shall be within the range of 0 to 32767.

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = xxx (decimal)							
3 to 4	Length = n							
5 to (n+4)	IE specific data or content of a grouped IE							

Figure 8.1-2: 3GPP defined Information Element Format

NOTE 2: Bit 8 of Octet 1 is not set. This indicates that the Information Element type value has been allocated by 3GPP.

For illustration, Figure 8.1-3 depicts the format of a vendor-specific Information Element, which content is not specified and the IE type value shall be within the range of 32768 to 65535.

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = xxx (decimal)							
3 to 4	Length = n							
5 to 6	Enterprise ID							
7 to (n+4)	IE specific data or content of a grouped IE							

Figure 8.1-3: Vendor-Specific Information Element Format

NOTE 3: Bit 8 of Octet 1 is set. This indicates that the IE type value has been allocated by the vendor identified by the Enterprise ID. The content of this IE is vendor specific and therefore out of scope of this specification.

8.2 Information Element Types

8.2.1 General

A message may contain several IEs. In order to have forward compatible type definitions for the Ies, all of them shall be TLV (Type, Length, Value) coded. IE type values are specified in the Table 8.2.1-1.

The 3rd column of this table specifies if the IE is either Extendable or has a variable length or a fixed length and a reference to the clause where the IE is specified:

- Fixed Length: the IE has a fixed set of fields, and a fixed number of octets;

- Variable Length: the IE has a fixed set of fields, and has a variable number of octets.
  For example, the last octets may be numbered similar to "5 to (n+4)". In this example, if the value of the length field, n, is 0, then the last field is not present;

- Extendable: the IE has a variable number of fields, and has a variable number of octets.
  The last fields are typically specified with the statement: "These octet(s) is/are present only if explicitly specified". The legacy receiving entity shall ignore the unknown octets.

In order to improve the efficiency of troubleshooting, it is recommended that the IEs should be arranged in the signalling messages as well as in the grouped IEs, according to the order the IEs are listed in the message definition table or grouped IE definition table in clause 7. However the receiving entity shall be prepared to handle the messages with IEs in any order.

Within IEs, certain fields may be described as spare. These bits shall be transmitted with the value set to "0". To allow for future features, the receiver shall not evaluate these bits.

Table 8.2.1-1: Information Element Types

IE Type value (Decimal)	Information elements	Comment / Reference
0	Reserved	
1	Cause	Fixed Length / 8.2.2
2	Requested ES Parameters	Extendable / 8.2.3
3	Interface ID	Extendable / 8.2.4
4	Interface Capabilities	Extendable / 8.2.5
5	Add TN Stream Configuration	Extendable / Table 7.3.3.1-2
6	Other Parameters for Gate Control Information Calculation	Extendable / 8.2.15
7	Delete TN Stream Configuration	Extendable / Table 7.3.3.1-3
8	Data Frame Specification	Extendable / Table 7.3.3.1-4
9	Time Aware Offset	Fixed Length / 8.2.13
10	TN Stream ID	Fixed Length / 8.2.6
11	Mask-and-match information	Extendable / 8.2.7
12	Destination MAC address	Fixed Length / 8.2.8
13	Source MAC address	Fixed Length / 8.2.9
14	Vlan Tag Info	Fixed Length / 8.2.10
15	IPv4 tuple	Extendable / 8.2.11
16	IPv6 tuple	Extendable / 8.2.12
17	Interface Configuration	Extendable / Table 7.3.3.1-5
18	Interface Name	Variable length / 8.2.14
19 to 32767	Spare. For future use.	
32768 to 65535	Reserved for vendor specific IEs	

8.2.2 Cause

Cause IE is coded as depicted in Figure 8.2.2-1.

.	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 1 (decimal)							
3 to 4	Length = 1							
5	Cause value							

Figure 8.2.2-1: Cause

The Cause value shall be included in a response message. In a response message, the Cause value indicates the acceptance or the rejection of the corresponding request message. The Cause value indicates the explicit reason for the rejection.

Table 8.2.2-1: Cause values

Message Type	Cause value (decimal)	Meaning	Description
	0	Reserved.	Shall not be sent and if received the Cause shall be treated as an invalid IE
Acceptance in a response	1	Request accepted (success)	"Request accepted (success)" is returned when the request was accepted.
	2-63	Spare	This value range shall be used by Cause values in an acceptance response message. See NOTE 1.
Rejection in a response	64	Request rejected (reason not specified)	This cause shall be returned to report an unspecified rejection cause
	65	Mandatory IE missing	This cause shall be returned when the receiver detects that a mandatory IE is missing in a request message
	66	Conditional IE missing	This cause shall be returned when the receiver detects that a Conditional IE is missing in a request message.
	67	Invalid length	This cause shall be returned when the receiver detects that an IE with an invalid length in a request message
	68	Mandatory IE incorrect	This cause shall be returned when the receiver detects that a Mandatory IE is incorrect in a request message, e.g. the Mandatory IE is malformed or it carries an invalid or unexpected value.
	69	No resources available	This cause shall be returned to indicate a temporary unavailability of resources to process the received request. This cause may be used e.g. if the AN-TL/CN-TL is congested.
	70	Insufficient Resources for scheduled TN streams	This cause shall be returned to indicate that a new scheduled TN stream could not be configured, or that an existing scheduled TN stream could not be modified, due to insufficient resources at the AN-TL/CN-TL for scheduled TN streams for the ES interface/port requested to transfer the new or modified TN stream.
	71	Temporary Rejection due to on-going calculation of gate control information	This cause shall be returned to indicate that a new scheduled TN stream could not be configured, or that an existing scheduled TN stream could not be modified, due to the AN-TL/CN-TL re-calculating gate control information for the ES interface/port requested to transfer the new or modified TN stream, due to previous requests, and the AN-TL/CN-TL being not able to provide a timely response to the new request.
	72	Unavailable Interface ID	This cause shall be used to indicate that an Interface ID received in a Set Request to configure a new TN stream is not available at the AN-TL/CN-TL.
	73 to 255	Spare for future use in a response message. See NOTE 2.	This value range shall be used by Cause values in a rejection response message. See NOTE 2.

NOTE 1: This value is or may be used in future version of the specification. If the receiver cannot comprehend the value, it shall be interpreted as an unspecified acceptance cause. Unspecified/unrecognized acceptance cause shall be treated in the same ways as the cause value 1 " Request accepted (success)".

NOTE 2: This value is or may be used in a future version of the specification. If the receiver cannot comprehend the value, it shall be interpreted as an unspecified rejection cause. Unspecified/unrecognized rejection cause shall be treated in the same ways as the cause value 64 "Request rejected (reason not specified)".

8.2.3 Requested ES Parameters

The Requested ES Parameters IE type shall be encoded as shown in Figure 8.2.3-1. It indicates the ES parameters that are requested to be retrieved from the AN-TL or CN-TL.

Octets	Bits 8	7	6	5	4	3	2	1
1 to 2	Type = 2 (decimal)							
3 to 4	Length = n							
5	Spare	Spare	Spare	Spare	Spare	Spare	ITF CAP	ITF ID
6 to (n+4)	These octet(s) is/are present only if explicitly specified							

Figure 8.2.3-1: Requested ES Parameters

Octet 5 shall be encoded as follows:

- Bit 1 –ITF ID (Interface ID): when set to "1", this indicates a request to retrieve the End Station Interface IDs.
- Bit 2 – ITF CAP (Interface capabilities): when set to "1", this indicates a a request to retrieve the Interface capabilities.
- Bit 3 to 8 Spare, for future use and set to 0.

8.2.4 Interface ID

The Interface ID IE type shall be encoded as shown in Figure 8.2.4-1. It conveys the description of one Interface ID.

Octets	Bits 8	7	6	5	4	3	2	1
1 to 2	Type = 3 (decimal)							
3 to 4	Length = n							
5 to 10	MAC address value							
11	Length of Interface Name							
m to o	Interface Name value							
p to (n+4)	These octet(s) is/are present only if explicitly specified							

Figure 8.2.4-1: Interface ID

Octets 5 to 10 shall contain the value of the MAC address of the ES interface as specified in IEEE Std 802.1Q [4] Table 46-3.

Octet 11 shall contain the length of the Interface Name value field in octets. It shall be set to zero if no Interface Name value field is provided.

Octets m to o shall contain the value of the Interface Name of the ES interface as specified in IEEE Std 802.1Q [4] Table 46-3.

8.2.5 Interface Capabilities

The Interface Capabilities IE type shall be encoded as shown in Figure 8.2.5-1. It indicates the ES interface capabilities of the AN-TL or CN-TL to the SMF/CUC as defined in 3GPP TS 23.501 [2] table M.2-1.

Octets	Bits 8	7	6	5	4	3	2	1
1 to 2	Type = 4 (decimal)							
3 to 4	Length = n							
5	Spare	Spare	Spare	Spare	Spare	Spare	BUF CAP	VLAN TAG
m to (m+1)	Buffer Capability value							
o to (n+4)	These octet(s) is/are present only if explicitly specified							

Figure 8.2.5-1: Interface Capabilities

Octet 5 shall be encoded as follows:

- Bit 1 – VLAN TAG (VLAN Tag Capability): when set to "1", this indicates that the interface supports VLAN Tag capability as defined in IEEE Std 802.1Q [4] clause 46.2.3.7.1.
- Bit 2 – BUF CAP (Buffer capabilities): when set to "1", this indicates that the Buffer Capability value field is provided.
- Bit 3 to 8 Spare, for future use and set to 0.

Octet m to (m+1) shall be present if the BUF CAP flag in octet 5 is set to "1". When present, they encode, for a Talker, the maximum possible buffer duration in ms for a packet with the maximum size of an Ethernet packet (1522 Bytes).

8.2.6 TN Stream ID

The TN Stream ID IE type shall be encoded as shown in Figure 8.2.6-1.

Octets	Bits 8	7	6	5	4	3	2	1
1 to 2	Type = 10 (decimal)							
3 to 4	Length = 8							
5 to 10	MAC address							
11 to 12	Unique ID							

Figure 8.2.6-1: TN Stream ID

The MAC address shall be encoded as defined in clause 46.2.3.1.1 of IEEE Std 802.1Q [4].

The Unique ID shall be encoded as defined in clause 46.2.3.1.2 of IEEE Std 802.1Q [4].

8.2.7 Mask-and-match information

The Mask-and-match information IE type shall be encoded as shown in Figure 8.2.7-1.

Octets	Bits 8	7	6	5	4	3	2	1
1 to 2	Type = 11 (decimal)							
3 to 4	Length = n							
5 to 6	tsnCpeMmIdMsduMaskLength							
7 to m	tsnCpeMmIdMsduMask							
(m+1) to p	tsnCpeMmIdMsduMatch							
p+1 to (n+4)	These octet(s) is/are present only if explicitly specified							

Figure 8.2.7-1: Mask-and-match-information

Octets 5 to 6 shall encode the tsnCpeMmIdMsduMaskLength, i.e. the length, in octets, of tsnCpeMmIdMsduMask and and tsnCpeMmIdMsduMatch,as defined in clause 9.1.6.5 of IEEE Std 802.1CBdb [7].

Octets 7 to m shall encode the tsnCpeMmIdMsduMask, i.e. a mask of tsnCpeMmIdMsduMaskLength octets, as defined in clause 9.1.6.6 of IEEE Std 802.1CBdb [7].

Octets (m+1) to p shall encode the tsnCpeMmIdMsduMatch, i.e. the value of the mask to be matched for the stream identification, of tsnCpeMmIdMsduMaskLength octets, as defined in clause 9.1.6.7 of IEEE Std 802.1CBdb [7].

8.2.8 Destination MAC address

The Destination MAC address IE type shall be encoded as shown in Figure 8.2.8-1.

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 12 (decimal)							
3 to 4	Length = 6							
5 to 10	MAC address value							

Figure 8.2.8-1: Destination MAC address

8.2.9 Source MAC address

The Source MAC address IE type shall be encoded as shown in Figure 8.2.9-1.

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 13 (decimal)							
3 to 4	Length = 6							
5 to 10	MAC address value							

Figure 8.2.9-1: Source MAC address

8.2.10 VLAN Tag Info

The VLAN Tag Info IE type shall be encoded as shown in Figure 8.2.10-1.

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 14 (decimal)							
3 to 4	Length = 2							
5	PCP value			DEI Flag	VLAN ID value			
6	VLAN ID value							

Figure 8.2.10-1: VLAN Tag Info

The PCP value in octet 5 shall encode the Priority Code Point value (value range is 0 to 7 inclusive) as defined in clause 46.2.3.4.2 of IEEE Std 802.1Q [4].

The DEI (Drop Eligible Indicator) flag in octet 5 is not relevant from the perspective of a TSN Talker/Listener. It shall be ignored by the receiver.

The VLAN ID value field in octets 5 to 6 shall contain the VlanId value (value range is 0 to 4095 inclusive) as defined in clause 46.2.3.4.2 of IEEE Std 802.1Q [4]. Octet 5 / Bit 4 shall be the most significant bit of the VLAN ID value and Octet 6 / Bit 1 shall be the least significant bit.

8.2.11 IPv4 tuple

The IPv4 tuple IE type shall be encoded as shown in Figure 8.2.11-1. It encodes an IPv4 tuple as defined in clause 46.2.3.4.3 of IEEE Std 802.1Q [4].

Octets	Bits 8	7	6	5	4	3	2	1
1 to 2	Type = 15 (decimal)							
3 to 4	Length = n							
5	Spare	Spare	DPN	SPN	Protoc	DSCP	DIPA	SIPA
m to (m+3)	Source IPv4 address							
o to (o+3)	Destination IPv4 address							
p	Spare		DSCP value					
q to (q+1)	Protocol value							
r to (r+1)	Source Port Number							
s to (s+1)	Destination Port Number							
t to (n+4)	These octet(s) is/are present only if explicitly specified							

Figure 8.2.11-1: IPv4 tuple

Octet 5 shall be encoded as follows:

- Bit 1 – SIPA (Source IP Address): when set to "1", this indicates that the Source IPv4 address field is present.
- Bit 2 – DIPA (Destination IP Address): when set to "1", this indicates that the Destination IPv4 address field is present.
- Bit 3 – DSCP: when set to "1", this indicates that the DSCP value field is present.
- Bit 4 – Protoc (Protocol): when set to "1", this indicates that the Protocol value field is present.
- Bit 5 – SPN (Source Port Number): when set to "1", this indicates that the Source Port Number field is present.
- Bit 6 – DPN (Destination Port Number): when set to "1", this indicates that the Destination Port Number field is present.
- Bit 7 to 8 Spare, for future use and set to 0.

When present, source IPv4 address, destination IPv4 address, Protocol, Source Port Number and Destination Port Number shall be encoded as defined in clause 46.2.3.4.3 of IEEE Std 802.1Q [4].

The DSCP value shall be encoded as the DSCP in TOS (IPv4) or TC (IPv6) information (see IETF RFC 2474 [8]).

8.2.12 IPv6 tuple

The IPv6 tuple IE type shall be encoded as shown in Figure 8.2.12-1. It encodes an IPv6 tuple as defined in clause 46.2.3.4.4 of IEEE Std 802.1Q [4].

Octets	Bits 8	7	6	5	4	3	2	1
1 to 2	Type = 16 (decimal)							
3 to 4	Length = n							
5	Spare	Spare	DPN	SPN	Protoc	DSCP	DIPA	SIPA
m to (m+15)	Source IPv6 address							
o to (o+15)	Destination IPv6 address							
p	Spare		DSCP value					
q to (q+1)	Protocol value							
r to (r+1)	Source Port Number							
s to (s+1)	Destination Port Number							
t to (n+4)	These octet(s) is/are present only if explicitly specified							

Figure 8.2.12-1: IPv6 tuple

Octet 5 shall be encoded as follows:

- Bit 1 – SIPA (Source IP Address): when set to "1", this indicates that the Source IPv6 address field is present.

- Bit 2 – DIPA (Destination IP Address): when set to "1", this indicates that the Destination IPv6 address field is present.
- Bit 3 – DSCP: when set to "1", this indicates that the DSCP value field is present.
- Bit 4 – Protoc (Protocol): when set to "1", this indicates that the Protocol value field is present.
- Bit 5 – SPN (Source Port Number): when set to "1", this indicates that the Source Port Number field is present.
- Bit 6 – DPN (Destination Port Number): when set to "1", this indicates that the Destination Port Number field is present.
- Bit 7 to 8 Spare, for future use and set to 0.

When present, source IPv6 address, destination IPv6 address, Protocol, Source Port Number and Destination Port Number shall be encoded as defined in clause 46.2.3.4.4 of IEEE Std 802.1Q [4].

The DSCP value shall be encoded as the DSCP in TOS (IPv4) or TC (IPv6) information (see IETF RFC 2474 [8]).

8.2.13 Time Aware Offset

The Time Aware Offset IE type shall be encoded as shown in Figure 8.2.13-1.

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 9 (decimal)							
3 to 4	Length = n							
5 to 8	Time Aware Offset							
9 to (n+4)	These octet(s) is/are present only if explicitly specified							

Figure 8.2.13-1: Time Aware Offset

The Time Aware Offset field shall contain the TimeAwareOffset as defined in clause 46.2.5.3.5 of IEEE Std 802.1Q [4].

8.2.14 Interface Name

The Interface Name IE type shall be encoded as shown in Figure 8.2.14-1.

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 18 (decimal)							
3 to 4	Length = n							
5 to n	Interface Name value							

Figure 8.2.14-1: Interface Name

The Interface Name value shall contain the value of the Interface Name of the ES interface as specified in IEEE Std 802.1Q [4] Table 46-3.

8.2.15 Other Parameters for Gate Control Information Calculation

The Other Parameters for Gate Control Information Calculation IE type shall be encoded as shown in Figure 8.2.15-1.

Octets	Bits 8	7	6	5	4	3	2	1
1 to 2	Type = 6 (decimal)							
3 to 4	Length = n							
5	Spare						MFS	INT
m to (m+3)	Interval numerator							
o to (o+3)	Interval denominator							
p to (p+1)	Max Frame Size							
q to (n+4)	These octet(s) is/are present only if explicitly specified							

Figure 8.2.15-1: Other Parameters for Gate Control Information Calculation

Octet 5 shall be encoded as follows:

- Bit 1 – INT (Interval): when set to "1", this indicates that the Interval numerator and Interval denominator fields are present.
- Bit 2 – MFS (Max Frame Size): when set to "1", this indicates that the Max Frame Size field is present.
- Bit 3 to 8 Spare, for future use and set to 0.

When present, the Interval numerator and Interval denominator fields shall contain the interval numerator and denominator as defined in Table 46-8 of IEEE Std 802.1Q [4].

When present, the Max Frame Size field shall contain the MaxFrameSize as defined in Table 46-8 of IEEE Std 802.1Q [4].

9 Timers

Timers supported by the protocol between the SMF/CUC and AN-TL/CN-TL are shown in table 9.1.

Table 9-1: Timers – SMF/CUC side

TIMER	TIMER VALUE	CAUSE OF START	NORMAL STOP	ON THE EXPIRY (NOTE 2)
Tget	NOTE 1	Transmission of Get Request message	Get Response message received	Abort the procedure
Tset	NOTE 1	Transmission of Set Request message	Set Response message received	Abort the procedure
NOTE 1: The value of this timer is network dependent. NOTE 2: Get Request and Set Request are retransmitted using procedures for reliable delivery of PFCP or NGAP messages towards the UPF/NG-RAN (see clauses 5.2.1.4 and 5.2.2.4). The procedure is aborted if no response is received.				

Annex A (informative): Change history

Change history							
Date	Meeting	TDoc	CR	Rev	Cat	Subject/Comment	New version
2023-06	CT4#116	C4-232444				Initial draft	0.1.0
2023-09	CT4#117	C4-233809				Implementation of agreed pCRs: C4-233162, C4-233163, C4-233164, C4-233165, C4-233166, C4-233167, C4-233168, C4-233169	0.2.0
2023-09	CT#101	CP-232022				TS presented for information	1.0.0
2023-10	CT4#118	C4-234586				Implementation of agreed pCRs: C4-234111, C4-234112	1.1.0
2023-11	CT4#119	C4-235659				Implementation of agreed pCRs: C4-235099, C4-235100, C4-235101, C4-235102, C4-235103, C4-235104, C4-235105, C4-235106, C4-235526	1.2.0
2024-03	CT4#121	C4-240851				Implementation of agreed pCRs: C4-240164, C4-240165, C4-240166, C4-240167, C4-240168, C4-240169, C4-240170.	1.3.0
2024-03	CT#103	CP-240024				Presented for approval	2.0.0
2024-03	CT#103					Approved in TSG CT#103	18.0.0

History

Document history		
V18.0.0	May 2024	Publication