**SA WG2 Meeting #S2-143E S2-21xxxxx**

**24 February - 9 March September, 2021, Electronic (revision of S2-21xxxxx)**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **23.501** | **CR** |  | **rev** | **-** | **Current version:** | **17.0.0** |  |
|  | | | | | | | | |
| *For* ***HE******LP*** *on using this form: comprehensive instructions can be found at  http://www.3gpp.org/Change-Requests.* | | | | | | | | |
|  | | | | | | | | |

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

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | KI#2-1: Capturing the FS\_IIoT conclusions on static filtering entries | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Ericsson | | | | | | | | | |
| ***Source to TSG:*** | SA2 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | FS\_IIoT | | | | |  | ***Date:*** | | | 2021-01-18 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **B** |  | | | | | ***Release:*** | | | Rel-17 |
|  | *Use one of the following categories:* ***F*** *(correction)* ***A*** *(mirror corresponding to a change in an earlier release)* ***B*** *(addition of feature),* ***C*** *(functional modification of feature)* ***D*** *(editorial modification)*  Detailed explanations of the above categories can be found in 3GPP TR 21.900. | | | | | | | | *Use one of the following releases: Rel-8 (Release 8) Rel-9 (Release 9) Rel-10 (Release 10) Rel-11 (Release 11) Rel-12 (Release 12) Rel-13 (Release 13) Rel-14 (Release 14) Rel-15 (Release 15) Rel-16 (Release 16)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | SA2 has agreed to the use of static filtering entries in the FS\_IIoT study which needs to be captured in normative text. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Clarify that UPF uses the static filtering entry to achieve routing in all direction, and clarify that it is up to implementation how this is achieved. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Agreement of the FS\_IIoT study is not captured in the specifications. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 5.6.10.2, 5.8.2.5.3, 5.28.3.1 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | |  | **X** | Other core specifications | | | | TS/TR ... CR ... | | |
| ***affected:*** | |  | **X** | Test specifications | | | | TS/TR ... CR ... | | |
| ***(show related CRs)*** | |  | **X** | O&M Specifications | | | | TS/TR ... CR ... | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | |  | | | | | | | | |

**\* \* \* \* Start of Change \* \* \* \***

#### 5.6.10.2 Support of Ethernet PDU Session type

For a PDU Session set up with the Ethernet PDU Session type, the SMF and the UPF acting as PDU Session Anchor (PSA) can support specific behaviours related with the fact the PDU Session carries Ethernet frames.

Depending on operator configuration related with the DNN, different configurations for how Ethernet traffic is handled on N6 may apply, for example:

- Configurations with a 1-1 relationship between a PDU Session and a N6 interface possibly corresponding to a dedicated tunnel established over N6. In this case the UPF acting as PSA transparently forwards Ethernet frames between the PDU Session and its corresponding N6 interface, and it does not need to be aware of MAC addresses used by the UE in order to route down-link traffic.

- Configurations, where more than one PDU Session to the same DNN (e.g. for more than one UE) corresponds to the same N6 interface. In this case the UPF acting as PSA needs to be aware of MAC addresses used by the UE in the PDU Session in order to map down-link Ethernet frames received over N6 to the appropriate PDU Session. Alternatively the UPF may also apply static filtering entries when they are provided as specified in clause 5.8.2.5.3. Forwarding behaviour of the UPF acting as PSA is managed by SMF as specified in clause 5.8.2.5.

NOTE 1: The "MAC addresses used by the UE" correspond to any MAC address used by the UE or any device locally connected to the UE and using the PDU Session to communicate with the DN.

Based on operator configuration, the SMF may request the UPF acting as the PDU Session Anchor to respond to ARP/IPv6 Neighbour Solicitation requests based on local cache information, i.e. the mapping between the UE MAC address to the UE IP address, and the DN where the PDU Session is connected to, or to redirect the ARP traffic from the UPF to the SMF. Responding to ARP/IPv6 ND based on local cache information applies to ARP/IPv6 ND received in both UL and DL directions.

NOTE 2: Responding to ARP/ND from a local cache assumes the UE or the devices behind the UE acquire their IP address via in-band mechanisms that the SMF/UPF can detect and by this link the IP address to the MAC address.

NOTE 3: This mechanism is intended to avoid broadcasting or multicasting the ARP/IPv6 ND to every UE.

Ethernet Preamble and Start of Frame delimiter are not sent over 5GS:

- For UL traffic the UE strips the preamble and frame check sequence (FCS) from the Ethernet frame.

- For DL traffic the PDU Session Anchor strips the preamble and frame check sequence (FCS) from the Ethernet frame.

Neither a MAC nor an IP address is allocated by the 5GC to the UE for a PDU Session.

The PSA shall store the MAC addresses received from the UE, and associate those with the appropriate PDU Session.

The SMF may receive a list of allowed VLAN tags from DN-AAA (for a maximum of 16 VLAN tags) or may be locally configured with allowed VLAN tags values. The SMF may also be configured with instructions on VLAN handling (e.g., the VLAN tag to be inserted or removed, S-TAG to be inserted or removed). Taking this into account, the SMF determines the VLAN handling for the PDU Session, and instructs the UPF to accept or discard the UE traffic based on the allowed VLAN tags, as well as to handle VLAN tags (addition/removal) via PDR (Outer header removal) and FAR (UPF applying Outer header creation of a Forwarding policy). For example:

- The UPF may insert (for uplink traffic) and remove (for downlink traffic) a S-TAG on N6 or N19 or internal interface ("5G VN internal") for the traffic from and to the UE.

- The UPF may insert (for uplink traffic) and remove (for downlink traffic) a VLAN tag on the N6 interface while there is no VLAN in the traffic to and from the UE.

- The UPF may discard any UE traffic that does not contain any allowed VLAN tag when the UPF handles the UE uplink or downlink traffic.

NOTE 4: This can be used for traffic steering to N6-LAN but also for N6-based traffic forwarding related with 5G-VN service described in clause 5.29.4

Apart from specific conditions related to the support of PDU sessions over W-5GAN defined in TS 23.316 [84], the UPF shall not remove VLAN tags sent by the UE and the UPF shall not insert VLAN tags for the traffic sent to the UE.

PDU(s) containing a VLAN tag shall be switched only within the same VLAN by a PDU Session Anchor.

The UE may acquire from the SMF, at PDU Session Establishment, the MTU of the Ethernet frames' payload that the UE shall consider, see clause 5.6.10.4.

NOTE 5: The UE may operate in bridge mode with regard to a LAN it is connecting to the 5GS, thus different MAC addresses may be used as source address of different frames sent UL over a single PDU Session (and destination MAC address of different frames sent DL over the same PDU Session).

NOTE 6: Entities on the LAN connected to the 5GS by the UE may have an IP address allocated by the DN but the IP layer is considered as an application layer which is not part of the Ethernet PDU Session.

NOTE 7: In this Release of the specification, only the UE connected to the 5GS is authenticated, not the devices behind such UE.

NOTE 8: 5GS does not support the scenario where a MAC address or if VLAN applies a (MAC address, VLAN) combination is used on more than one PDU Session for the same DNN and S-NSSAI.

NOTE 9: This Release of the specification does not guarantee that the Ethernet network remains loop-free. Deployments need to be verified on an individual basis that loops in the Ethernet network are avoided.

NOTE 10: This Release of the specification does not guarantee that the Ethernet network properly and quickly reacts to topology changes. Deployments need to be verified on an individual basis how they react to topology changes.

Different Frames exchanged on a PDU Session of Ethernet type may be served with different QoS over the 5GS. Thus, the SMF may provide to the UPF Ethernet Packet Filter Set and forwarding rule(s) based on the Ethernet frame structure and UE MAC address(es). The UPF detects and forwards Ethernet frames based on the Ethernet Packet Filter Set and forwarding rule(s) received from the SMF. This is further defined in clauses 5.7 and 5.8.2.

When a PDU Session of Ethernet PDU type is authorized by a DN as described in clause 5.6.6, the DN-AAA server may, as part of authorization data, provide the SMF with a list of allowed MAC addresses for this PDU Session; the list is limited to a maximum of 16 MAC addresses. When the list has been provided for a PDU Session, the SMF sets corresponding filtering rules in the UPF(s) acting as PDU Session Anchor for the PDU Session. The UPF discards any UL traffic that does not contain one of these MAC addresses as a source address if the list of allowed MAC addresses is provided.

In this Release of specification, the PDU Session of Ethernet PDU Session type is restricted to SSC mode 1 and SSC mode 2.

For a PDU Session established with the Ethernet PDU Session type, the SMF may, upon PCF request, need to ensure reporting to the PCF of all Ethernet MAC addresses used as UE address in a PDU Session. In this case, as defined in clause 5.8.2.12, the SMF controls the UPF to report the different MAC addresses used as source address of frames sent UL by the UE in the PDU Session.

NOTE 11: This relates to whether AF control on a per MAC address is allowed on the PDU Session as defined in TS 23.503 [45] clause 6.1.1.2.

The PCF may activate or deactivate the reporting of the UE MAC address using the "UE MAC address change" Policy Control Request Trigger as defined in Table 6.1.3.5-1 of TS 23.503 [45].

The SMF may relocate the UPF acting as the PDU Session Anchor for an Ethernet PDU Session as defined in clause 4.3.5.8 of TS 23.502 [3]. The relocation may be triggered by a mobility event such as a handover, or may be triggered independent of UE mobility, e.g. due to load balancing reasons. In order to relocate the PSA UPF, the reporting of the UE MAC addresses needs to be activated by the SMF.

**\* \* \* \* Next Change \* \* \* \***

##### 5.8.2.5.3 Support of Ethernet PDU Session type

When configuring an UPF acting as PSA for an Ethernet PDU Session Type, the SMF may instruct the UPF to route the traffic based on detected MAC addresses as follows.

- The UPF learns the MAC address(es) connected via N6 based on the source MAC addresses of the DL traffic received on a N6 Network Instance.

- The UPF learns the MAC address(es) of UE(s) and devices connected behind, if any, based on the source MAC address contained within the UL traffic received on a PDU Session (N3/N9 interface).

- The UPF forwards DL unicast traffic (with a known destination address) on a PDU Session determined based on the source MAC address(es) used by the UE for the UL traffic.

- The UPF forwards UL unicast traffic (with a known destination address) on a port (PDU Session or N6 interface) determined based on the source MAC address(es) learned beforehand.

- In the case of multicast and broadcast traffic (if the destination MAC address is a broadcast or multicast address):

- for DL traffic received by UPF on a N6 Network Instance the UPF should forward the traffic to every DL PDU Session (corresponding to any N4 Session) associated with this Network Instance

- for uplink traffic received by UPF over a PDU session on a N3/N9 interface, the UPF should forward the traffic to the N6 interface and downlink to every PDU session (except toward the one of the incoming traffic) associated with the same N6 Network Instance

- for uplink and downlink unicast traffic received by UPF, if the destination MAC has not been learnt, the UPF should forward the traffic to every PDU session associated with the same N6 Network Instance and towards the N6 interface. In any case the traffic is not replicated on the PDU Session or the N6 interface of the incoming traffic.

NOTE 1: The UPF can consider a PDU Session or a N6 interface to be active or inactive in order to avoid forwarding loops. User data traffic is not sent on inactive PDU sessions or inactive N6 interface. This release of the specification does not further specify how the UPF determines whether a PDU Session or N6 interface is considered active or inactive.

NOTE 2: This release of the specification supports only a single N6 interface in a UPF associated with the N6 Network Instance.

- if the traffic is received with a VLAN ID, the above criteria apply only towards the N6 interface or PDU session matching the same VLAN ID, unless the UPF is instructed to remove the VLAN ID in the incoming traffic.

NOTE 3: This release of the specification supports Independent VLAN Learning (IVL) and does not support Shared VLAN Learning (SVL), as described in IEEE Std 802.1Q [98].

- if the destination MAC address of traffic refers to the same N6 interface or PDU session on which the traffic has been received, the frame shall be dropped.

In order to handle scenarios where a device behind a UE is moved from one UE to another UE, a MAC address is considered as no longer associated with a UPF interface when the MAC address has not been detected as Source MAC address in UL traffic for a pre-defined period of time or it has been detected under a different interface (PDU Session or N6).

When static filtering entries are provided to the UPF/NW-TT as described in clause 5.28.3, the UPF/NW-TT shall apply static filtering entries for the specified destination address, VLAN ID pairs rather than MAC learning as described above. The use of static filtering entries are described in IEEE Std. 802.1Q [98] clause 8.8.1.

NOTE 4: How the UPF uses the static filtering entry to achieve routing in all direction is up to UPF implementation. The externally-observable behaviour of 5GS Bridge needs to comply with IEEE Std 802.1Q.

For ARP/IPv6 Neighbour Solicitation traffic, a SMF's request to respond to ARP/IPv6 Neighbour Solicitation based on local cache information or to redirect such traffic from the UPF to the SMF overrules the traffic forwarding rules described above.

NOTE 5: Local policies in UPF associated with the Network Instance can prevent local traffic switching in the UPF between PDU Sessions either for unicast traffic only or for any traffic. In the case where UPF policies prevent local traffic switching for any traffic (thus for broadcast/multicast traffic) some mechanism such as responding to ARP/ND based on local cache information or local multicast group handling is needed to ensure that upper layer protocol can run on the Ethernet PDU sessions.

The SMF may ask to get notified with the source MAC addresses used by the UE.

In order to request the UPF to act as defined above, the SMF may, for each PDU Session corresponding to a Network Instance, set an Ethernet PDU Session Information in a DL PDR that identifies all (DL) Ethernet packets matching the PDU session. Alternatively, for unicast traffic the SMF may provide UPF with dedicated forwarding rules related with MAC addresses notified by the UPF.

**\* \* \* \* Next Change \* \* \* \***

### 5.28.3 Port and bridge management information exchange in 5GS

#### 5.28.3.1 General

Port and bridge management information is exchanged between CNC and TSN AF. The port management information, is related to Ethernet ports located in DS-TT or NW-TT.

5GS shall support transfer of standardized and deployment-specific port management information transparently between TSN AF and DS-TT or NW-TT, respectively inside a Port Management Information Container. NW-TT may support one or more ports. In this case, each port uses separate Port Management Information Container. 5GS shall also support transfer of standardized and deployment-specific bridge management information transparently between TSN AF and NW-TT, respectively inside a Bridge Management Information Container. Table 5.28.3.1-1 and Table 5.28.3.1-2 list standardized port management information and bridge management information, respectively.

Table 5.28.3.1-1: Standardized port management information

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Port management information | Applicability (see NOTE 6) | | Supported operations by TSN AF | Reference |
|  | DS-TT | NW-TT | (see NOTE 1) |  |
| **General** |  |  |  |  |
| Port management capabilities (see NOTE 2) | X | X | R |  |
| **Bridge delay related information** |  |  |  |  |
| txPropagationDelay | X | X | R | IEEE Std 802.1Qcc [95] clause 12.32.2.1 |
| **Traffic class related information** |  |  |  |  |
| Traffic class table | X | X | RW | IEEE Std 802.1Q [98] clause 12.6.3 and clause 8.6.6. |
| **Gate control information** |  |  |  |  |
| GateEnabled | X | X | RW | IEEE Std 802.1Q [98] Table 12-29 |
| AdminBaseTime | X | X | RW | IEEE Std 802.1Q [98] Table 12-29 |
| AdminControlList | X | X | RW | IEEE Std 802.1Q [98] Table 12-29 |
| AdminCycleTime (see NOTE 3) | X | X | RW | IEEE Std 802.1Q [98] Table 12-29 |
| AdminControlListLength (see NOTE 3) | X | X | RW | IEEE Std 802.1Q [98] Table 12-28 |
| Tick granularity | X | X | R | IEEE Std 802.1Q [98] Table 12-29 |
| **General Neighbor discovery configuration**  **(NOTE 4)** |  |  |  |  |
| adminStatus | D | X | RW | IEEE Std 802.1AB [97] clause 9.2.5.1 |
| lldpV2LocChassisIdSubtype | D | X | RW | IEEE Std 802.1AB [97] Table 11-2 |
| lldpV2LocChassisId | D | X | RW | IEEE Std 802.1AB [97] Table 11-2 |
| lldpV2MessageTxInterval | D | X | RW | IEEE Std 802.1AB [97] Table 11-2 |
| lldpV2MessageTxHoldMultiplier | D | X | RW | IEEE Std 802.1AB [97] Table 11-2 |
| **NW-TT port neighbor discovery configuration** |  |  |  |  |
| lldpV2LocPortIdSubtype |  | X | RW | IEEE Std 802.1AB [97] Table 11-2 |
| lldpV2LocPortId |  | X | RW | IEEE Std 802.1AB [97] Table 11-2 |
| **DS-TT port neighbor discovery configuration** |  |  |  |  |
| lldpV2LocPortIdSubtype | D |  | RW | IEEE Std 802.1AB [97] Table 11-2 |
| lldpV2LocPortId | D |  | RW | IEEE Std 802.1AB [97] Table 11-2 |
| **Neighbor discovery information for each discovered neighbor of NW-TT** |  |  |  |  |
| lldpV2RemChassisIdSubtype |  | X | R | IEEE Std 802.1AB [97] Table 11-2 |
| lldpV2RemChassisId |  | X | R | IEEE Std 802.1AB [97] Table 11-2 |
| lldpV2RemPortIdSubtype |  | X | R | IEEE Std 802.1AB [97] Table 11-2 |
| lldpV2RemPortId |  | X | R | IEEE Std 802.1AB [97] Table 11-2 |
| TTL |  | X | R | IEEE Std 802.1AB [97] clause 8.5.4 |
| **Neighbor discovery information for each discovered neighbor of DS-TT**  **(NOTE 5)** |  |  |  |  |
| lldpV2RemChassisIdSubtype | D |  | R | IEEE Std 802.1AB [97] Table 11-2 |
| lldpV2RemChassisId | D |  | R | IEEE Std 802.1AB [97] Table 11-2 |
| lldpV2RemPortIdSubtype | D |  | R | IEEE Std 802.1AB [97] Table 11-2 |
| lldpV2RemPortId | D |  | R | IEEE Std 802.1AB [97] Table 11-2 |
| TTL | D |  | R | IEEE Std 802.1AB [97] clause 8.5.4.1 |
| **Stream Parameters**  **(NOTE 11)** |  |  |  |  |
| MaxStreamFilterInstances | X |  | R | IEEE Std 802.1Q [98]  clause 12.31.1.1 |
| MaxStreamGateInstances | X |  | R | IEEE Std 802.1Q [98]  clause 12.31.1.2 |
| MaxFlowMeterInstances | X |  | R | IEEE Std 802.1Q [98]  clause 12.31.1.3 |
| SupportedListMax | X |  | R | IEEE Std 802.1Q [98]  clause 12.31.1.4 |
| **Per-Stream Filtering and Policing information**  (NOTE 10) |  |  |  |  |
| Stream Filter Instance Table  (NOTE 8) |  |  |  | IEEE Std 802.1Q [98] Table 12-32 |
| > Stream Identification type | X | X | RW | IEEE 802.1CB [83] clause 9.1.1.6 |
| > Stream Identification Controlling Parameters | X | X | RW | IEEE 802.1CB [83] clauses 9.1.2, 9.1.3, 9.1.4  (NOTE 12) |
| > PrioritySpec | X | X | RW | IEEE Std 802.1Q [98] Table 12-32 |
| > StreamGateInstanceID | X | X | RW | IEEE Std 802.1Q [98] Table 12-32 |
| Stream Gate Instance Table  (NOTE 9) |  |  |  | IEEE Std 802.1Q [98] Table 12-33 |
| StreamGateInstance | X | X | R | IEEE Std 802.1Q [98] Table 12-33 |
| PSFPAdminBaseTime | X | X | RW | IEEE Std 802.1Q [98] Table 12-33 |
| PSFPAdminControlList | X | X | RW | IEEE Std 802.1Q [98] Table 12-33 |
| PSFPAdminCycleTime | X | X | RW | IEEE Std 802.1Q [98] Table 12-33 |
| PSFPTickGranularity | X | X | R | IEEE Std 802.1Q [98] Table 12-33 |
| NOTE 1: R = Read only access; RW = Read/Write access.  NOTE 2: Indicates which standardized and deployment-specific port management information is supported by DS-TT or NW-TT.  NOTE 3: AdminCycleTime and AdminControlListLength are optional for gate control information.  NOTE 4: If DS-TT supports neighbor discovery, then TSN AF sends the general neighbor discovery configuration for DS-TT Ethernet ports to DS-TT. If DS-TT does not support neighbor discovery, then TSN AF sends the general neighbor discovery configuration for DS-TT Ethernet ports to NW-TT using the Bridge Management Information Container (refer to Table 5.28.3.1-2) and NW-TT performs neighbor discovery on behalf on DS-TT. When a parameter in this group is changed, it is necessary to provide the change to every DS-TT and the NW-TT that belongs to the 5GS TSN bridge. It is mandatory that the general neighbor discovery configuration is identical for all DS-TTs and the NW-TTs that belongs to the bridge.  NOTE 5: If DS-TT supports neighbor discovery, then TSN AF retrieves neighbor discovery information for DS-TT Ethernet ports from DS-TT. If DS-TT does not support neighbor discovery, then TSN AF retrieves neighbor discovery information for DS-TT Ethernet ports from NW-TT, using the Bridge Management Information Container (refer to Table 5.28.3.1-2), the NW-TT performing neighbor discovery on behalf on DS-TT.  NOTE 6: X = applicable; D = applicable when validation and generation of LLDP frames is processed at the DS-TT.  NOTE 7: Void.  NOTE 8: There is a Stream Filter Instance Table per Stream.  NOTE 9: There is a Stream Gate Instance Table per Gate.  NOTE 10: TSN AF indicates the support for PSFP to the CNC only if each DS-TT and NW-TT of the 5GS bridge has indicated support of PSFP. DS-TT indicates support of PSFP using port management capabilities, i.e. by indicating support for the Per-Stream Filtering and Policing information and by setting higher than zero values for MaxStreamFilterInstances, MaxStreamGateInstances, MaxFlowMeterInstances, SupportedListMax parameters. When available, TSN AF uses the PSFP information for determination of the traffic pattern information as described in Annex I. The PSFP information can be used at the DS-TT (if supported) and at the NW-TT (if supported) for the purpose of per-stream filtering and policing as defined in IEEE Std 802.1Q [98] clause 8.6.5.1.  NOTE 11: TSN AF composes a Stream Parameter Table towards the CNC. It is up to TSN AF how it composes the Stream Parameter Table based on the numerical values as received from DS-TT and NW-TT port(s) and for the bridge for each individual parameter.  NOTE 12: The set of Stream Identification Controlling Parameters depends on the Stream Identification type value as defined in IEEE Std 802.1CB [83] Table 9-1 and clauses 9.1.2, 9.1.3, 9.1.4. | | | | |

Table 5.28.3.1-2: Standardized bridge management information

|  |  |  |
| --- | --- | --- |
| Bridge management information | Supported operations by TSN AF  (see NOTE 1) | Reference |
| **Information for 5GS Bridge** |  |  |
| Bridge Address | R |  |
| Bridge ID | R |  |
| NW-TT port numbers | R |  |
| **Traffic forwarding information** |  |  |
| Static Filtering Entry (NOTE 3) | RW | IEEE Std 802.1Q [98] clause 8.8.1 |
| **General Neighbor discovery configuration**  **(NOTE 2)** |  |  |
| adminStatus | RW | IEEE Std 802.1AB [97] clause 9.2.5.1 |
| lldpV2LocChassisIdSubtype | RW | IEEE Std 802.1AB [97] Table 11-2 |
| lldpV2LocChassisId | RW | IEEE Std 802.1AB [97] Table 11-2 |
| lldpV2MessageTxInterval | RW | IEEE Std 802.1AB [97] Table 11-2 |
| lldpV2MessageTxHoldMultiplier | RW | IEEE Std 802.1AB [97] Table 11-2 |
| **DS-TT port neighbor discovery configuration for DS-TT ports (NOTE 4)** |  |  |
| **>DS-TT port neighbor discovery configuration for each DS-TT port** |  |  |
| >> DS-TT port number | RW |  |
| >> lldpV2LocPortIdSubtype | RW | IEEE Std 802.1AB [97] Table 11-2 |
| >> lldpV2LocPortId | RW | IEEE Std 802.1AB [97] Table 11-2 |
| **Discovered neighbor information for DS-TT ports**  **(NOTE 4)** |  |  |
| **>Discovered neighbor information for each DS-TT port**  **(NOTE 4)** |  |  |
| >> DS-TT port number | R |  |
| >> lldpV2RemChassisIdSubtype | R | IEEE Std 802.1AB [97] Table 11-2 |
| >> lldpV2RemChassisId | R | IEEE Std 802.1AB [97] Table 11-2 |
| >> lldpV2RemPortIdSubtype | R | IEEE Std 802.1AB [97] Table 11-2 |
| >> lldpV2RemPortId | R | IEEE Std 802.1AB [97] Table 11-2 |
| >> TTL | R | IEEE Std 802.1AB [97] clause 8.5.4.1 |
| **Stream Parameters (NOTE 5)** |  |  |
| MaxStreamFilterInstances | R | IEEE Std 802.1Q [98] |
| MaxStreamGateInstances | R | IEEE Std 802.1Q [98] |
| MaxFlowMeterInstances | R | IEEE Std 802.1Q [98] |
| SupportedListMax | R | IEEE Std 802.1Q [98] |
| NOTE 1: R = Read only access; RW = Read/Write access.  NOTE 2: General neighbor discovery information is included only when NW-TT performs neighbor discovery on behalf of DS-TT. When a parameter in this group is changed, it is necessary to provide the change to every DS-TT and the NW-TT that belongs to the 5GS TSN bridge.  NOTE 3: If the Static Filtering Entry information is present, UPF/NW-TT uses Static Filtering Entry information to determine the NW-TT or DS-TT egress port. If the Static Filtering Entry information is not present, then the forwarding information as in clause 5.8.2.5.3 applies.  NOTE 4: DS-TT discovery configuration and DS-TT discovery information are used only when DS-TT does not support LLDP and NW-TT performs neighbor discovery on behalf of DS-TT.  NOTE 5: TSN AF indicates the support for PSFP to the CNC only if each DS-TT and NW-TT of the 5GS bridge have indicated support of PSFP. The support of PSFP at the NW-TT ports is expressed by setting higher than zero values for MaxStreamFilterInstances, MaxStreamGateInstances, MaxFlowMeterInstances, SupportedListMax parameters. | | |

Exchange of port and bridge management information between TSN AF and NW-TT or DS-TT allows TSN AF to:

1) retrieve port management information for a DS-TT or NW-TT Ethernet port or bridge management information for a 5GS TSN bridge;

2) send port management information for a DS-TT or NW-TT Ethernet port or bridge management information for a 5GS TSN bridge;

3) subscribe to and receive notifications if specific port management information for a DS-TT or NW-TT Ethernet port changes or bridge management information changes.

Exchange of port management information between TSN AF and NW-TT or DS-TT is initiated by DS-TT or NW-TT to:

- notify TSN AF if port management information has changed that TSN AF has subscribed for.

Exchange of bridge management information between TSN AF and NW-TT is initiated by NW-TT to:

- notify TSN AF if bridge management information has changed that TSN AF has subscribed for.

Exchange of port management information is initiated by DS-TT to:

- provide port management capabilities, i.e. provide information indicating which standardized and deployment-specific port management information is supported by DS-TT.

TSN AF indicates inside the Port Management Information Container or Bridge Management Information Container whether it wants to retrieve or send port or bridge management information or intends to (un-)subscribe for notifications.

**\* \* \* \* End of Change \* \* \* \***