**3GPP TSG-SA3 Meeting #114e ad-hoc *S3-240106***

**Electronic meeting, online, 22 - 26 January 2024**

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

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

|  |
| --- |
|  |
| ***Title:***  | Processing of ICMPv4 and ICMPv6 packets |
|  |  |
| ***Source to WG:*** | Ericsson |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | \_5G\_Ph3 |  | ***Date:*** | 2024-01-15 |
|  |  |  |  |  |
| ***Category:*** | **F** |  | ***Release:*** | Rel-18 |
|  | *Use one of the following categories:****F*** *(correction)****A*** *(mirror corresponding to a change in an earlier release)****B*** *(addition of feature),* ***C*** *(functional modification of feature)****D*** *(editorial modification)*Detailed explanations of the above categories canbe found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | *Use one of the following releases:Rel-8 (Release 8)Rel-9 (Release 9)Rel-10 (Release 10)Rel-11 (Release 11)…Rel-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** | Correction to remove “by appropriate means” and change “The tester knows whether the network product supports IPv4 and/or IPv6.” to “The vendor provides documentation whether the network product supports IPv4 and/or IPv6” to clarify pre-condition. |
|  |  |
| ***Summary of change:*** | Correction to test case 4.2.4.1.1.2 to remove subjectivity and clarify pre-condition. |
|  |  |
| ***Consequences if not approved:*** | Test case is subjective. |
|  |  |
| ***Clauses affected:*** | 4.2.4.1.1.2 |
|  |  |
|  | **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:*** |  |

\*\*\* 1st CHANGE \*\*\*

4.2.4.1.1.2 Handling of ICMP

*Requirement Name*: Processing of ICMPv4 and ICMPv6 packets

*Requirement Reference:* In accordance with industry best practice

*Requirement Description*:

Processing of ICMPv4 and ICMPv6 packets which are not required for operation shall be disabled on the network product. In particular, there are certain types of ICMP4 and ICMPv6 that are not used in most networks, but represent a risk.

ICMP message types which on receipt lead to responses or to configuration changes are not mentioned in this requirement, but they may be necessary to support relevant and specified networking features. Those shall be documented.

Certain ICMP types are generally permitted and do not need to be specifically documented. Those are marked as "Permitted" in below table.

The network product shall not send certain ICMP types by default, but it may support the option to enable utilization of these types (e.g. for debugging). This is marked as "Optional" in below table.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Type (IPv4) | Type (IPv6) | Description | Send | Respond to |
| 0  | 128 | Echo Reply | Optional(i.e. as automatic reply to "Echo Request") | N/A |
| 3 | 1 | Destination Unreachable | Permitted | N/A |
| 8 | 129 | Echo Request | Permitted | Optional |
| 11 | 3 | Time Exceeded | Optional | N/A |
| 12 | 4 | Parameter Problem | Permitted | N/A |
| N/A | 2 | Packet Too Big | Permitted | N/A |
| N/A | 135 | Neigbor Solicitation | Permitted | Permitted |
| N/A | 136 | Neighbor Advertisement | Permitted | N/A |

The network product shall not respond to, or process (i.e. do changes to configuration), under any circumstances certain ICMP message types as marked in below table.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Type (IPv4) | Type (IPv6) | Description | Send | Respond to | Process (i.e. do changes to configuration) |
| 5 | 137 | Redirect | N/A | N/A | Not Permitted |
| 13 | N/A | Timestamp | N/A | Not Permitted | N/A |
| 14 | N/A | Timestamp Reply | Not Permitted (i.e. as automatic reply to "Timestamp") | N/A | N/A |
| N/A | 133 | Router Solicitation | N/A | Not Permitted | Not Permitted |
| N/A | 134 | Router Advertisement | N/A | N/A | Not Permitted |

*Threat Reference*: TR 33.926 [4]

*Test Case*:

The test for this requirement can be carried out using a suitable tool or manually by performing the steps described below. If a tool is used then the tester needs to provide evidence, e.g. by referring to the documentation of the tool, that the tool actually provides functionality equivalent to the steps described below.

**Test Name:** TC\_HANDLING\_OF\_ICMP

**Purpose:**

To verify that the network product does not reply to certain ICMP types in accordance with the requirement. To verify that the network product does not send 'Time Exceeded'.

To verify that the network product does not process the following ICMPv4 and ICMPv6 types:

- "Redirect (5)"

- Router Solicitation

- Router Advertisement

**Procedure and execution steps:**

**Pre-Conditions:**

- The vendor provides documentation whether the network product supports IPv4 and/or IPv6.

- If applicable, the tester has the needed system privileges for confirming that the ICMP messages with types "Not Permitted" to process are indeed not leading to configuration changes.

- If applicable, the tester has the needed system privileges for confirming that certain ICMP message types are dropped by the network product on receipt.

- A tester machine is available and equipped with a suitable ICMP packets generator tool.

**Execution Steps**

The following needs to be done for all IP protocol versions (IPv4 and/or IPv6) supported by the network element.

For verifying that the network product does not reply to ICMP messages with types where this is not permitted: The tester sends samples of the applicable ICMP messages from the tester machine to the network product and verifies that

- the messages are dropped on receipt by the network product (e.g. by means of appropriate firewall rules),

- or no response is sent out towards the test machine,

- or there are other means ensuring that the ICMP messages cannot trigger a response.

For verifying that the network product does not change its configuration due to receiving ICMP messages with types where this is not permitted: The tester sends samples of the applicable ICMP messages from the tester machine to the network product and verifies that

- the messages are dropped on receipt by the network product (e.g. by means of appropriate firewall rules),

- or the network product's applicable system configuration remains unchanged upon receipt of the messages,

- or there are other means ensuring that the ICMP messages cannot lead to configuration changes.

The tester verifies consistency between the documentation in regard to ICMP and the network product.

**Expected Results:**

The ICMP messages which are "Not Permitted" to generate a response from the network product do not generate a response.

The ICMP messages which are "Not Permitted" to change the configuration of the network element do not change the configuration.

ICMP message types which lead to responses or to configuration changes on receipt, if neither mentioned in the requirement nor in the documentation, are not enabled.

**Expected format of evidence:**

The following information needs to be retained and included into the report as appropriate:

- Tools used and their configuration

- Tool output

- Test result (Passed or not)

\*\*\* END OF CHANGES \*\*\*