

Ethernet Port Fault

Cloud Execution Environment

OPERATING INSTRUCTIONS

Copyright

© Ericsson AB 2016. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Trademark List

All trademarks mentioned herein are the property of their respective owners. These are shown in the document Trademark Information.



Contents

1	Introduction	1
1.1	Alarm Description	1
1.2	Prerequisites	2
2	Procedure	3
2.1	Analyzing the Alarm	3
2.2	Troubleshooting the Server	5
2.3	Troubleshooting the Switch	5





1 Introduction

This instruction concerns alarm handling.

1.1 Alarm Description

The alarm is issued by the Managed Object (MO) `EthernetPort`.

The severity of the alarm is `MAJOR`.

The alarm is issued when a physical network port on a server loses connectivity with the related network. The alarm remains active as long as the connectivity is missing. It is possible that the underlying fault requires site visit.

The possible alarm causes and fault locations are explained in Table 1.

Table 1 Alarm Causes

Alarm Cause	Description	Fault Reason	Fault Location	Impact
Link is down	The connectivity with the network through the reported physical port is lost. It is possible that the connection with the network is still maintained by another network port.	<ul style="list-style-type: none">• Hardware fault• Network fault• Switch infrastructure reboot	<ul style="list-style-type: none">• Server• Ethernet network• Switch infrastructure	<ul style="list-style-type: none">• Network connectivity is lost on the reported physical port.• Network link redundancy is lost.

The following are the consequences for the server if the alarm is not solved:

- The link redundancy on the affected network is lost.

The alarm attributes are listed in Table 2.

Table 2 Alarm Attributes

Attribute Name	Attribute Value
Major Type	193
Minor Type	2031681
Managed Object Class	<code>EthernetPort</code>



Attribute Name	Attribute Value
Managed Object Instance	Region=<name_of_the_region>, CeeFunction=1, Node=<hostname_of_the_node>, Network=<network>, Aggregator=<aggr>, EthernetPort=<port>
Specific Problem	Ethernet Port Fault
Event Type	communicationsAlarm (2)
Probable Cause	m3100LossOfSignal (8)
Additional Information	Name of the physical network port
Additional Text	Network=<network>,Aggregator=<aggr>, EthernetPort=<port>;uuid=<HW_UUID_of_cor responding_server> ⁽¹⁾
Severity	MAJOR (4)

(1) The format of this field is expected to change in CEE R6.

1.2 Prerequisites

This section provides information on the documents, tools, and conditions that apply to the procedure.

1.2.1 Documents

Before starting this procedure, ensure that the following documents were read:

- *System Safety Information*
- *Personal Health and Safety Information*
- Documentation for the used server management tool

1.2.2 Tools

The following tool is needed:

- Management tool for the server configuration

1.2.3 Conditions

Before starting this procedure, ensure that the following conditions are met:

- No hardware reconfiguration is in progress.



- No system update is in progress.
- The site network plan is available.

2 Procedure

This section describes the procedure to follow when this alarm is received.

2.1 Analyzing the Alarm

Do the following at the maintenance center:

1. With the help of the information contained by the alarm and by using Table 3, identify the affected network, the Ethernet port for which the alarm raised, and the possible related Ethernet port aggregator.

Table 3 Ethernet Ports and Aggregators

Network	Aggregator	Ethernet Port	Text in the Additional Information Field of the Alarm
Control	control	1 ⁽¹⁾	Name of the physical network port ⁽²⁾
		2 ⁽¹⁾	Name of the physical network port ⁽²⁾
Traffic	traffic	1 ⁽¹⁾	Name of the physical network port ⁽³⁾
		2 ⁽¹⁾	Name of the physical network port ⁽³⁾
Storage	storage	1 ⁽¹⁾	Name of the physical network port ⁽²⁾
		2 ⁽¹⁾	Name of the physical network port ⁽²⁾



Network	Aggregator	Ethernet Port	Text in the <i>Additional Information</i> Field of the Alarm
SR-IOV ⁽⁴⁾	sriov	1 ⁽⁵⁾	Name of the physical network port ⁽²⁾
		2 ⁽⁵⁾	Name of the physical network port ⁽²⁾
		3 ⁽⁵⁾	Name of the physical network port ⁽²⁾
		4 ⁽⁵⁾	Name of the physical network port ⁽²⁾

(1) If two ports of two different servers have the same *Ethernet port* values, we say that these ports are on the same “network side”. Due to the consequent port numbering, if two ports are on the same *network side*, then they are also on the same network. **1** means the left, and **2** means the right side.

(2) The name of the physical port must match *eth[0–9]*.

(3) The name of the physical port must be *dpdk0* or *dpdk1*.

(4) Only applicable if one or two additional Network Interface Controllers (NICs) for SR-IOV are installed, providing two or four ports.

(5) For SR-IOV, left and right network sides are not distinguished.

2. Check the alarm list and continue with the relevant step:

- If the *Ethernet Port Aggregator Fault* alarm is active for the relevant aggregator, continue with Step 3. For more information, refer to *Ethernet Port Aggregator Fault*.
- Otherwise continue with Step 6.

3. Check the alarm list and perform the relevant action:

- If the *Ethernet Port Fault* alarm is active for the other Ethernet port belonging to the same aggregator, then continue with Step 5.
- Otherwise, continue with Step 9.

4. If *Ethernet Port Fault* alarms are also raised for physical network ports on other servers, proceed to Step 6. If other servers are not affected, then it is possible that the server having the *Ethernet Port Fault* alarm is faulty, continue with Section 2.2 on page 5.

5. Continue with the relevant step:

- If the *Ethernet Port Fault* alarm also raised for physical network ports on other servers, proceed to Step 6.
- If other servers are not affected, then it is possible that the server having the *Ethernet Port Fault* alarm is faulty. Continue with Section 2.2 on page 5.



6. Check to which side the reported physical network port is connected. See the table note about network sides in Table 3.
7. Perform the relevant action:
 - If all faulty physical network ports are on the same side, proceed to Step 8.
 - Otherwise, continue with Step 9.
8. Perform the relevant action:
 - If all faulty physical network ports are connected to the same switch, then it is possible that the switch board or external switch is faulty. Continue with Section 2.3 on page 5 to troubleshoot the switch.
 - If the faulty physical network ports are connected to different switches, continue with Step 9.
9. Collect troubleshooting data as described in the *Data Collection Guideline*. For alarm-specific logs, refer to the Table *Data Collection for Alarms and Alerts* in the *Data Collection Guideline*.
10. Consult the next level of maintenance support. Further actions are outside the scope of this instruction.
11. The job is completed.

2.2 Troubleshooting the Server

In case of a possibly faulty server, do the following:

1. Collect troubleshooting data as described in the *Data Collection Guideline*. For alarm-specific logs, refer to the table *Data Collection for Alarms and Alerts* in the *Data Collection Guideline*.
2. Consult the next level of maintenance support. Further actions are outside the scope of this instruction.
3. The job is completed.

2.3 Troubleshooting the Switch

In case of a possibly faulty switch, do the following:

1. Troubleshoot the switch board or external switch by using its own documentation.
2. Perform the relevant action:
 - If the switch problem is solved and the alarm ceases, exit this procedure.



- Or continue with Step 3 in the following cases:
 - The switch board or external switch turns out not to be faulty.
 - Or the *Ethernet Port Fault* alarm is still active when the switch problem is solved.
- 3. Collect troubleshooting data as described in the *Data Collection Guideline*. For alarm-specific logs, refer to the Table *Data Collection for Alarms and Alerts* in the *Data Collection Guideline*.
- 4. Consult the next level of maintenance support. Further actions are outside the scope of this instruction.
- 5. The job is completed.