

CSCF ICMP Protocol Not Operational

Call Session Control Function

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	3
2	Procedure	5
2.1	Analyze the Alarm	5
2.2	Actions to Clear the Alarm	5



CSCF ICMP Protocol Not Operational



1 Introduction

This instruction concerns alarm handling.

1.1 Alarm Description

The alarm is issued when the Internet Control Message Protocol (ICMP) functionality is not working for a port. This happens when the assigned port is already in use by another application. This error prevents the affected application from getting immediate information about problems that are normally sent using the ICMP protocol.

The possible alarm causes and the corresponding fault reasons, fault locations, and impacts are described in Table 1.

Table 1 Alarm Causes

Alarm Cause	Description	Fault Reason	Fault Location	Impact
The enabling of ICMP has failed.	The port assigned for ICMP is already used by another application.	Configuration error.	The ICMP port to be used by the CSCF application, indicated in the alarm, is used by another application, or the port does not exist.	The ICMP being enabled is not operational for the indicated CSCF application. If the reason is because another application is using the same port, the ICMP, as such, is enabled, but not from the indicated SIP interface.

Note: The alarm can appear as a result of maintenance activity.

The alarm attributes are listed and explained in Table 2.



Table 2 Alarm Attributes

Attribute Name	Attribute Value
Major Type	193
Minor Type	6684691
Managed Object Class	<ul style="list-style-type: none">• IcsfNetworkInterface or• PcsfNetworkInterface or• ScsfNetworkInterface or• BcfNetworkInterface or• EcsfNetworkInterface or• EatfNetworkInterfaceEntry
Managed Object Instance	<p>ManagedElement=<node_name>,C scfFunction=1,CSCF-Applicat ion=CSCF,CscfNwIfContainer= 0,XNwIfs=0,XNetworkInterfac e=<protocol>:<IP-address>:<po rt>⁽¹⁾⁽²⁾</p> <p>OR</p> <p>ManagedElement=<node_name>,C scfFunction=1,CSCF-Applicat ion=CSCF,CscfNwIfContainer= 0,EatfNwIfs=0,EatfNetworkIn terfaceEntry=<protocol>:<IP- address>:<port></p>
Specific Problem	CSCF ICMP Protocol Not Operational
Event Type	processingErrorAlarm (4)
Probable Cause	x733ConfigurationOrCustomization Error (307)



Attribute Name	Attribute Value
Additional Text	<p>Potential conflict of XNetworkInterface with other interface or application using the port ⁽³⁾⁽⁴⁾ <code><protocol>: <IP-address>: <port></code></p> <p>OR</p> <p>Potential conflict of EatfNetworkInterfaceEntry with other interface or application using the port <code><protocol>: <IP-address>: <port></code></p>
Perceived Severity	minor (5)

(1) X represents *lscsf*, *Pcscf*, *Scscf*, *Bcf*, or *Ecscf*

(2) Example: `ManagedElement=CSCF,CscfFunction=1,CSCF-Application=CSCF,CscfNwIfContainer=0,lscsfNwIfs=0,lscsfNetworkInterface=UDP:192.168.10.201:5060`

(3) X represents *lscsf*, *Pcscf*, *Scscf*, *Ecscf*, or *Bcf*

(4) Example: Potential conflict of *lscsfNetworkInterface* with other interface or application using the port `UDP:192.168.10.201:5060`

1.2 Prerequisites

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

1.2.1 Documents

This instruction references the following documents:

- *Managed Object Model (MOM)*

1.2.2 Tools

No tools are required.

1.2.3 Conditions

No conditions.





2 Procedure

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

2.1 Analyze the Alarm

Do the following:

1. Check if there is a reconfiguration planned on the node requiring that the node must be taken out of service. If so, ignore this alarm until the reconfiguration has been completed.
2. Check if there are any other active alarms for the CSCF application network interfaces.

2.2 Actions to Clear the Alarm

Do the following:

1. Check the Additional Text information of the issued alarm to find which CSCF application network interface failed to enable ICMP, and check if other existing interfaces or applications have the same address configured to identify the faulty interface.
2. Correct the faulty interface configuration using the latest site configuration information.
3. Confirm that the alarm ceases after the interface configuration is corrected. If not, repeat Step 1 and Step 2. Check for more missing parameters, or check that the parameters were configured correctly.
4. Confirm that the alarm has ceased. If the alarm remains, consult the next level of maintenance support. Further actions are outside the scope of this instruction.
5. Job is completed.