

MRF IP Auto-Configuration Failure

Virtual Multimedia Resource Function

Operating Instructions

Copyright

© Ericsson AB 2016, 2017. 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.



Contents

1	Overview	1
1.1	MRF IP Auto-Configuration Failure Alarm Description	1
2	Cease the MRF IP Auto-Configuration Failure Alarm	5
2.1	Perform Concluding Routines	5





1 Overview

This instruction concerns alarm handling.

1.1 MRF IP Auto-Configuration Failure Alarm Description

The alarm is a primary alarm. The severity of the alarm is Major. The alarm is issued by the *MrfMediaInterface* MO.

The alarm is raised when IP auto-configuration of a media IP address in a VM fails, for example, if the DHCP client cannot obtain, renew, or rebind an IP address, or if the lease time of the IP address ends.

The possible alarm causes and fault locations are explained in [Table 1](#).

Table 1 Alarm Causes

Alarm Cause	Description	Fault Reason ⁽¹⁾	Fault Location	Impact
DHCP server not responding	Connectivity failure between DHCP server and client	DHCP Discover sent, and no accepted Offer received	DHCP server or Network or Cloud environment	No user plane traffic is possible on the media interface. If all media interfaces are down, MTAS is instructed not to offer new sessions to the VM connected to the media interface while the problem persists.
		DHCP IPV6 Solicit sent, and no accepted Advertise received		
		DHCP REQUEST sent, and no accepted ACK received		
		DHCP IPV6 REQUEST sent, and no accepted ACK received		
Invalid response	No valid configuration	DHCP ACK rejected		



Alarm Cause	Description	Fault Reason ⁽¹⁾	Fault Location	Impact
from DHCP server	answer from server	DHCP <code>IPV6</code> <code>Reply</code> discarded		
IP address confirmation failed	The server indicates that the client network address is incorrect or client IP address lease has expired	DHCP <code>NAK</code> received for <code>REQUEST</code>		
Unsuccessful IP address lifetime extension	The server indicates that the client network address is incorrect or client IP address lease has expired	DHCP <code>NAK</code> in <code>RENEW</code> state		
		DHCP <code>NAK</code> in <code>REBIND</code> state		
	IP address lease has expired	DHCP <code>LEASE</code> expired		
		DHCP <code>IPV6</code> <code>LEASE</code> expired		

(1) Fault reason is described in the `additionalText` field of the alarm and it is used when analyzing the alarm.

The alarm is ceased in the following case:

- The DHCP client receives a valid IP address for a media interface.

The DHCP client is continuously trying to obtain IP addresses after the alarm is raised, therefore no manual actions are needed in the VM after the DHCP-related issues are solved.

The following is the consequence for the VM if the alarm is not solved:

- No user plane traffic is possible on the media interface.

DHCP client states are listed and explained in [Table 2](#).



Table 2 DHCP Client States

DHCP Client State	Description
INIT	Initialization state, the client starts requesting an IP address lease. Also, it is the state after failed lease or when lease ends.
SELECTING	The client is waiting to receive <code>DHCPOFFER</code> messages from one or more DHCP servers.
REQUESTING	The client is waiting for reply from the server to which it sent <code>DHCPREQUEST</code> .
BOUND	The client has a valid lease and is in normal operational state.
RENEWING	The client is trying to renew its lease. It regularly sends <code>DHCPREQUEST</code> messages with the server that gave it its current lease and waits for a reply.
REBINDING	The client has failed to renew its lease with the selected server, and now seeks a lease extension with any server. The client periodically sends <code>DHCPREQUEST</code> messages with no server specified until it receives a reply or the lease ends.

The alarm attributes are listed and explained in [Table 3](#).

Table 3 Alarm Attributes

Attribute Name	Attribute Value
Major Type	193
Minor Type	5308426
Managed Object Class	<i>MrfMediaInterface</i>
Managed Object Instance	ManagedElement=1,MediaResourceFunction=1,MrfResource=1, , MrfInstance=<MrfInstanceId> ,MrfMediaInterface=<MrfMediaInterfaceId>
Specific Problem	MRF IP Auto-Configuration Failure
Event Type	communicationsAlarms (2)
Probable Cause	CommunicationsProtocolError (305)



Attribute Name	Attribute Value
Additional Text	DHCP Server <IP address>, <cause> ⁽¹⁾ , State: <state> ⁽²⁾ ; uuid: <uuid> ⁽³⁾
Perceived Severity	major (4)

(1) <cause> is one of the fault reasons from [Table 1](#).

(2) <state> is one of the states from [Table 2](#).

(3) <uuid> is the identity of the Virtual Machine from which the alarm is issued.



2 Cease the MRF IP Auto-Configuration Failure Alarm

The following procedure describes how to cease an MRF IP Auto-Configuration Failure alarm.

Prerequisites

You have logged into the node.

Steps

1. Check from the cloud environment, or, if in use, from the external DHCP server, whether DHCP server is enabled for the instance. If the server is disabled, enable it.
2. Check the DHCP server configuration. One possible scenario is to run out of IP addresses in the subnet.
 - If only one VM has the active alarm, lock and restart the VM.
 - If all VMs have DHCP problem, restart the DHCP service in the cloud environment.
3. If the alarm does not cease, consult the next level of maintenance support. Further actions are outside the scope of this instruction.

2.1 Perform Concluding Routines

Steps

1. Make a report.
2. The job is completed.