

MRF IP Address Collision

Virtual Multimedia Resource Function

Operating Instructions

Copyright

© Ericsson AB 2016–2019. 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	Overview	1
1.1	MRF IP Address Collision Alarm Description	1
2	Procedure	3
2.1	Resolve IP Address Collision in Deployments with Manual IP Allocation	3
2.2	Resolve IP Address Collision in Deployments with MO-based Automatic IP Allocation	4
2.3	Resolve IP Address Collision by Reconfiguring Peer IP Interface	4
2.4	Perform Concluding Routines	5





1 Overview

This instruction concerns alarm handling.

1.1 MRF IP Address Collision Alarm Description

This alarm is a primary alarm. The alarm is issued by the `MrfMediaInterface` Managed Object (MO). The severity of the alarm is Major.

The MRF IP Address Collision alarm indicates that the IP address allocated to a MRF IP interface is already used in the network. The MRF IP interface that issued the alarm cannot be used while the alarm is active. The collision can occur in the following cases:

- A MRF media IP interface is activated with an IP address already used in the network.
- The IP interface of another host in the network is activated with the IP address already used by a MRF media IP interface.

The possible alarm cause and alarm locations are explained in the table below.

Table 1 Alarm Causes

Cause	Description	Reason	Location	Impact
MRF IP Address Collision, media IP interface	An IP address collision on the MRF media IP interface is detected.	Configuration error	IP pool, vMRF deployment parameter	The MTAS is notified about the situation and it releases all ongoing calls on the MRF media IP interface (IPv4 or IPv6) the collision occurred on. The interface cannot be used for traffic while the alarm is active.
			Peer IP interface	

The alarm is ceased in the following case:

- The alarm is ceased when the IP address of either the MRF media IP interface or the peer IP interface is reconfigured, and no address collision is detected with the new IP address.

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



- While the alarm is active, MRF capacity is degraded since the affected VM cannot be used for either IPv4 or IPv6 traffic depending on the type of the interface that raised the alarm. The MTAS is notified about the situation.

Table 2 Alarm Attributes

Attribute Name	Attribute Value
Major Type	193
Minor Type	5308417
Managed Object Class	MrfMediaInterface
Managed Object Instance	ManagedElement=<node_name>,MediaResourceFunction=1,MrfResource=1,MrfInstance=<mrif_instance>,MrfMediaInterface=<mrif_media_ip_interface>
Specific Problem	MRF IP Address Collision
Event Type	communicationsAlarm (2)
Probable Cause	configurationOrCustomisationError (159)
Additional Text	Detected IP address collision in MRF media IP interface; uuid: <uuid> ⁽¹⁾
Perceived Severity	major (4)

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



2 Procedure

The following procedures describe how to cease a MRF IP Address Collision alarm.

- If the MRF media IP interface needs to be reconfigured, continue with one of the following procedures, depending on the IP allocation method:
 - In the case of VMware® based deployment using an OVF file for deployment with manual IP address allocation, continue with [Resolve IP Address Collision in Deployments with Manual IP Allocation](#) on page 3.
 - In the case of MO-based IP allocation deployments, continue with [Resolve IP Address Collision in Deployments with MO-based Automatic IP Allocation](#) on page 4.
- If the peer IP interface needs to be reconfigured, continue with the following procedure:
 - [Resolve IP Address Collision by Reconfiguring Peer IP Interface](#) on page 4

Note: This procedure is applicable independently from the IP address allocation method used in vMRF.

2.1 Resolve IP Address Collision in Deployments with Manual IP Allocation

1. Power off the VM.

For more information, see the relevant VMware documentation.

Note: Shutting down a VM can impact the traffic.

To minimize the traffic impact, lock the VM to be deleted from the cluster. Lock the `MrfInstance` MO that represents the VM.

2. Correct the colliding IP addresses in VM Guest Properties.
3. Power on the VM.
4. If the alarm has ceased, continue with [Perform Concluding Routines](#) on page 5.



2.2 Resolve IP Address Collision in Deployments with MO-based Automatic IP Allocation

This procedure describes how to cease an MRF IP Address Collision alarm in MO-based IP allocation deployments.

Prerequisites

- An Ericsson Command-Line Interface (ECLI) session in Exec mode is in progress.

Steps

1. Set the `administrativeState` attribute of the affected `MrfInstance` MO to LOCKED.
2. Scale-in the VM with the faulty IP address using the following command:

```
/usr/bin/scale_in_node.sh <UUID_of_the_faulty_VM>
```
3. Set the `ipPoolState` attribute of the faulty `MrfNetworkIpPool` to LOCKED.
4. Configure a new `MrfNetworkIpPool` MO with a new IP address range.
5. Define the new VM using the new addresses in the node communicating with the vMRF, if needed.

Note: For example, in the `mtasMrfpNode` in vMTAS.

6. Scale-out the vMRF VNF with a new VM.
7. If the alarm has ceased, continue with [Perform Concluding Routines](#) on page 5.

2.3 Resolve IP Address Collision by Reconfiguring Peer IP Interface

The alarm is ceased if the colliding IP address is removed from a peer IP interface in the network. A typical scenario for this remedy is that the IP address has been used without collision for some time in vMRF before the alarm was issued.

Steps

1. Provide the unit responsible for the other network element with the information needed to reconfigure IP address on the peer IP interface.

Make sure that no static IP address is reserved by other peers on the network and the vMRF IP address pool at the same time.



2. Wait until the new IP address is recognized as unique in the network, and the alarm is ceased. Continue with [Perform Concluding Routines](#) on page 5.

2.4 Perform Concluding Routines

Steps

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