

MRF H.248 Link Unavailable

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 H.248 Link Unavailable Alarm Description	1
2	Procedure	4
2.1	Analyze the Alarm	4
2.2	Clear an Alarm when SCTP Association Is Down	4
2.3	Clear an Alarm when No ServiceChange Response Is Received from MTAS	8
2.4	Clear an Alarm when Protocol Negotiation Failed	9
2.5	Clear an Alarm when IP Address Collision Occurred	9
2.6	Perform Concluding Routines	11



MRF H.248 Link Unavailable



1 Overview

This instruction concerns alarm handling.

1.1 MRF H.248 Link Unavailable Alarm Description

The alarm is a primary alarm. The alarm is issued either by the `MrfH248Interface` Managed Object (MO), or the `SctpEndpoint` MO. The severity of the alarm is Major.

An alarm is issued when the H.248 control link signaling between MTAS and vMRF has failed to function.

Note: The alarm can also be issued if there are no free signaling IP addresses in the `SignalingIpPool` MO. In this case, the alarm is raised simultaneously with the MRF Signaling IP Interface Configuration Failure alarm. To cease both alarms, follow the instructions in the MRF Signaling IP Interface Configuration Failure alarm OPI.

In case an already established SCTP transport link loss is detected, a 30-second timer is started. If the link recovers before the timer expires, the MRF H.248 Link Recovered after Temporary Outage event is reported, and the timer is cancelled. If the link does not recover before the timer ends, the alarm is raised.

If the fault is at the local endpoint and no SCTP connection can be opened towards MTAS, the alarm is issued by the `SctpEndpoint`. If the SCTP connection is established and the fault is in the network or in MTAS, the alarm is issued by the `MrfH248Interface` MO. Traffic is impacted on each VM that is connected to the faulty MTAS.

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

Table 1 Alarm Causes

Alarm Cause	Description	Fault Reason ⁽¹⁾	Fault Location	Impact
SCTP association is down	SCTP transport layer cannot transfer the H.248 messages	SCTP transport unavailable	vMRF Network MTAS	No new sessions can be set up on the affected link or links while the alarm is active. Ongoing calls are not impacted.
No ServiceChange response is received from MTAS	H.248 layer connectivity failure between MTAS and vMRF	Timeout for ServiceChange transaction reply	MTAS	



Alarm Cause	Description	Fault Reason ⁽¹⁾	Fault Location	Impact
Protocol negotiation failed	There is a functional incompatibility between MTAS and vMRF	H.248 profile mismatch, or H.248 version mismatch, or H.248 error code received from MTAS	MTAS vMRF	
IP address collision	Another IP host is using the same address as the vMRF	SCTP transport unavailable	vMRF or peer IP interface	
Incomplete configuration	The administrative state attribute of the MrfH248Interface MO is UNLOCKED, but no IP pool configured for signaling	SCTP transport unavailable	vMRF	

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

Note: The H.248 protocol negotiation failure can occur as a result of the maintenance activity.

If the alarm is not solved, all H.248 communication between MTAS and vMRF stays down. The alarm is ceased automatically if it was raised due to timeout while waiting for ServiceChange reply and ServiceChange reply is received from MTAS, or if the MrfH248Interface MO is locked during the procedure, in which case all traffic towards the MTAS will stop.

The alarm attributes are listed and explained in [Table 2](#).

Table 2 Alarm Attributes

Attribute Name	Attribute Value
Major Type	193
Minor Type	5308419
Managed Object Class	MrfH248Interface or SctpEndpoint



Attribute Name	Attribute Value
Managed Object Instance	ManagedElement=1,MediaResourceFunction=1,MrfH248Control=1,MrfH248Interface= <MrfH248InterfaceId> or ManagedElement=1,Transport=1,SctpEndpoint=<SctpEndpointId>
Specific Problem	MRF H.248 Link Unavailable
Event Type	communicationsAlarms (2)
Probable Cause	CommunicationsProtocolError (305)
Additional Text	<reason> ⁽¹⁾ ; uuid:<uuid> ⁽²⁾
Perceived Severity	major (4)

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

(2) If the alarm is issued by the SctpEndpoint MO, <uuid> is the identity of the Virtual Machine from which the alarm is issued.



2 Procedure

The following procedure describes how to cease an MRF H.248 Link Unavailable alarm.

2.1 Analyze the Alarm

Steps

1. See details for the alarm vMRF H.248 Link Unavailable. Check the additional info field of the alarm.
 - If the additional info includes Sctp transport unavailable, continue to [Clear an Alarm when Sctp Association Is Down](#) on page 4.
 - If the additional info includes Timeout for ServiceChange transaction reply, continue to [Clear an Alarm when No ServiceChange Response Is Received from MTAS](#) on page 8.
 - If the additional info includes H.248 version mismatch, H.248 profile mismatch, or Error code received from MTAS, continue to [Clear an Alarm when Protocol Negotiation Failed](#) on page 9.

2.2 Clear an Alarm when Sctp Association Is Down

1. Identify the issuing MO of the alarm.
 - If the alarm is issued by the SctpEndpoint MO, continue to [Local Endpoint Configuration Fault](#) on page 5.
 - If the alarm is issued by the MrfH248Interface MO, continue with the next step
2. Run the `verify_vmrf_node_status.py` command and check the command printout.

If the printout contains NO IPv4 ADDRESS (CONFIGURATION NEEDED) on the eth2 interface in any of the VMs, continue with [Resolve Missing Configuration Fault](#) on page 6, otherwise continue with the next step.

3. Ping the local IP address from another VM and check the MAC address using the following command:

```
arp -n
```

If the MAC matches the one in the printout of the `ifconfig` command issued on the faulty VM, continue to [Remote Endpoint Configuration Fault](#) on page



5, otherwise continue to [Clear an Alarm when IP Address Collision Occurred](#) on page 9.

2.2.1 Local Endpoint Configuration Fault

1. Check the `localPortNumber` attribute of the `MrfH248Control` MO. The value specifies the local SCTP port used towards MTAS for every `SctpEndpoint` MO.
 2. Reconfigure the `localPortNumber` attribute of the `MrfH248Control` MO if needed. To do this, lock all the associated `MrfH248Interface` MOs. The value specifies the MOs before the procedure, by setting the value of the attribute, `administrativeState` to `LOCKED`. Unlock them after the reconfiguration, by setting the value of the attribute, `administrativeState` to `UNLOCKED`.
 - If the alarm has ceased, continue to [Perform Concluding Routines](#) on page 11.
 - If the alarm is still active, continue with the next step.
- Note:** By locking the `MrfH248Interface` MO, the alarm is automatically ceased and all traffic towards the MTAS stops.
3. If the alarm remains, consult the next level of maintenance support. Further actions are outside the scope of this instruction. Continue to [Perform Concluding Routines](#) on page 11.

2.2.2 Remote Endpoint Configuration Fault

Steps

1. Check the `remotePortNumber` and `remoteIpAddress` attributes of the `MrfH248Interface` MO. These are restricted values and cannot be reconfigured without deleting and recreating the MO.
2. Ensure that the IP address and port defined in the vMRF VNF match with IP address and port defined in the MTAS. If the alarm has ceased, continue to [Perform Concluding Routines](#) on page 11.
3. To reconfigure the attributes mentioned in [Step 1](#), the `MrfH248Interface` MO must be locked, deleted, and created again. If the alarm has ceased, continue to [Perform Concluding Routines](#) on page 11.

Note: By locking the `MrfH248Interface` MO, the alarm is automatically ceased and all traffic towards MTAS stops.



4. If the alarm is issued again, consult the next level of maintenance support. Further actions are outside the scope of this instruction. Continue to [Perform Concluding Routines](#) on page 11.

2.2.3 Resolve Missing Configuration Fault

The printout of the `verify_vmrf_node_status.py` contains `NO IPv4 ADDRESS (CONFIGURATION NEEDED)` on the `eth2` interface of the VMs of the cluster, which means that there is no signaling IP address pool configured for the VNF. The alarm can be ceased by configuring a `SignalingIpPool` MO. If the `MrfNetworkIpPool` MO has not been configured at this point, it must be configured as well.

The MRF H.248 Link Unavailable alarm can be active with the MRF Signaling IP Interface Configuration Failure alarm simultaneously. In this case, the MRF H.248 Link Unavailable alarm is raised because of missing signaling IP pool configuration. To cease the alarm, configure the `SignalingIpPool` MO.

Prerequisites

- The `MrfH248Interface` MO has been configured and its `administrativeState` is `UNLOCKED`.

Steps

1. Check if the media IP pool is configured in the `MrfNetworkIpPool` MO.
 - If the `MrfNetworkIpPool` MO is already configured, continue with [Step 11](#).
 - If the `MrfNetworkIpPool` MO is not configured yet, continue with the next step.
2. In the MOM, navigate to `ManagedElement=1,MediaResourceFunction=1,MrfConfiguration=1`, enter Config mode, and create a `MrfNetworkIpPool` MO:

```
>ManagedElement=1,MediaResourceFunction=1,MrfConfiguration=1  
(ManagedElement=1,MediaResourceFunction=1,MrfConfiguration=1)>  
configure  
(config-  
ManagedElement=1,MediaResourceFunction=1,MrfConfiguration=1)>M  
rfNetworkIpPool=1
```
3. Navigate to the `ManagedElement=1,MediaResourceFunction=1,MrfConfiguration=1,MrfNetworkIpPool=1` MO and enter Config mode:



```
ManagedElement=1,MediaResourceFunction=1,MrfConfiguration=1,MrfNetworkIpPool=1
```

```
(ManagedElement=1,MediaResourceFunction=1,MrfConfiguration=1,MrfNetworkIpPool=1)>configure
```

4. Define the starting value of the IP pool range:

```
(config-ManagedElement=1,MediaResourceFunction=1,MrfConfiguration=1,MrfNetworkIpPool=1)>ipPoolRangeStart=<IP_pool_start_address>
```

Note: The IP pool range starting value can be an IPv4 or an IPv6 address.

5. Define the ending value of the IP pool range:

```
(config-ManagedElement=1,MediaResourceFunction=1,MrfConfiguration=1,MrfNetworkIpPool=1)>ipPoolRangeEnd=<IP_pool_end_address>
```

Note: The IP pool range ending value can be an IPv4 or an IPv6 address.

6. Set the value of the ipPoolState attribute:

```
(config-ManagedElement=1,MediaResourceFunction=1,MrfConfiguration=1,MrfNetworkIpPool=1)>ipPoolState=<value>
```

7. Set the value of the nextHopAddress attribute:

```
(config-ManagedElement=1,MediaResourceFunction=1,MrfConfiguration=1,MrfNetworkIpPool=1)>nextHopAddress=<IPv4_or_IPv6_nexthop_address>
```

8. Set the value of the subnetMaskLength attribute:

```
(config-ManagedElement=1,MediaResourceFunction=1,MrfConfiguration=1,MrfNetworkIpPool=1)>subnetMaskLength=<subnet_mask_length_value>
```

9. Commit the changes:

```
(config-ManagedElement=1,MediaResourceFunction=1,MrfConfiguration=1,MrfNetworkIpPool=1)>commit
```

10. Check if the alarm is still active.

- If the alarm is still active, continue with the next step.
- If the alarm has ceased, continue to [Perform Concluding Routines](#) on page 11.

11. In the MOM, navigate to ManagedElement=1, Transport=1:



```
>ManagedElement=1,Transport=1
```

12. Enter Config mode:

```
(ManagedElement=1,Transport=1)>configure
```

13. Create a SignalingIpPool MO for the signaling network:

```
(config-ManagedElement=1,Transport=1)>SignalingIpPool=1
```

14. Define the starting value of the IP pool range:

```
(config-ManagedElement=1,Transport=1,SignalingIpPool=1)>ipPoolRangeStart=<IP_Pool_Start_Address>
```

Note: The IP pool range starting value can only be an IPv4 address.

15. Define the ending value of the IP pool range:

```
(config-ManagedElement=1,Transport=1,SignalingIpPool=1)>ipPoolRangeEnd=<IP_Pool_End_Address>
```

Note: The IP pool range ending value can only be an IPv4 address.

16. Add values for the following attributes of the SignalingIpPool MO:

- gatewayAddress
- ipPoolState
- subnetMaskLength

17. Commit the changes:

```
(config-ManagedElement=1,Transport=1,SignalingIpPool=1)>commit
```

18. Continue to [Perform Concluding Routines](#) on page 11.

2.3 Clear an Alarm when No ServiceChange Response Is Received from MTAS

Steps

1. Ensure that the IP address and port defined in the vMRF VNF match with IP address and port defined in MTAS. If the alarm has ceased, continue to [Perform Concluding Routines](#) on page 11.



2. If the alarm remains, consult the next level of maintenance support. Further actions are outside the scope of this instruction. Continue to [Perform Concluding Routines](#) on page 11.

2.4 Clear an Alarm when Protocol Negotiation Failed

Steps

1. If the additional info indicated a H.248 profile or version mismatch, confirm that the MTAS has the correct H.248 version.
2. If the additional info described a H.248 error code received from MTAS, contact the MTAS operators with the error code.
3. After all possible procedures on MTAS side are done, view the currently active alarms in the alarm list.
4. If the alarm is still active, lock the `MrfH248Interface` MO that issued the alarm. To do this, select the MO and set the value of the attribute, `administrativeState` to `LOCKED`.
5. Unlock the `MrfH248Interface` MO. To do this, select the MO and set the value of the attribute, `administrativeState` to `UNLOCKED`. Continue to [Perform Concluding Routines](#) on page 11.

Note: By locking the `MrfH248Interface` MO, the alarm will be automatically ceased and all traffic towards MTAS will stop.

6. If the alarm is raised again, consult the next level of maintenance support. Further actions are outside the scope of this instruction. Continue to [Perform Concluding Routines](#) on page 11.

2.5 Clear an Alarm when IP Address Collision Occurred

This procedure describes how to cease an MRF H.248 Link Unavailable alarm if the alarm was raised because of IP address collision.

Steps

1. Continue with one of the following procedures, depending on the interface that needs to be reconfigured:

Interface to be reconfigured	Procedure
MRF signaling IP interface	— In the case of VMware-based deployment using an OVF file for deployment with manual IP address allocation, continue with



Interface to be reconfigured	Procedure
	Resolve IP Address Collision in Deployments with Manual IP Allocation on page 11. — In the case of MO-based IP pool allocation deployments, continue with Step 2 .
Peer IP interface	Resolve IP Address Collision by Reconfiguring Peer IP Interface on page 11 Note: This procedure is applicable independently from the IP address allocation method used in vMRF.

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

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

Note: For example, in the MtasMrfpNode MO in vMTAS.
- Scale-out the vMRF VNF with a new VM.

Result: The signaling IP interface IP address is assigned from the new signaling IP pool.

After This Task

If the original signaling IP pool is needed back in service (after it was modified to exclude the faulty IP address), then the vMRF VNF needs to be migrated to use signaling addresses only from the new pool. This is performed by locking and scaling-in the VMs using the old signaling pool, and extending the VNF with new VMs.

Once the ipAddressesInUseList attribute of the old signaling pool is empty, and its ipPoolState attribute is LOCKED, it can be deleted, and reconfigured without the IP address or addresses causing IP address collision.



2.5.1 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 11.

2.5.2 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 11.

2.6 Perform Concluding Routines

Steps

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