

DHCPv4, DDNS Retries Failed

Operating Instructions



Contents

1	Introduction	1
1.1	Alarm Description	1
1.2	Prerequisites	2
2	Procedure	5
2.1	Checking file "resolv.conf"	5
2.2	Checking DDNS Configuration	5



DHCPv4, DDNS Retries Failed



1 Introduction

This instruction concerns alarm handling.

1.1 Alarm Description

The alarm is issued when the counter *ipworksDhcpv4DDNSRetryFail* exceeds the threshold (defined by attribute *thresholdHigh*) in a given time interval (defined by attribute *granularityPeriod*)

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

Table 1 Alarm Causes

Alarm Cause	Description	Fault Reason	Fault Location	Impact	Solution
Configuration error.	When DHCPv4 server failed to get respond from DNS server for DDNS update request, it resends the request. When the resend times exceed the predefined threshold, this alarm raises.	The DNS server is not configured in <code>/etc/resolv.conf</code> .	DHCPv4 server	DDNS update is partially failed.	See Section 2.1 Checking file "resolv.conf" on page 5
		The configuration of DNS server is incorrect.	DNS server		See Section 2.2 Checking DDNS Configuration on page 5

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

The alarm attributes are listed and explained in Page 1.

Table 2 Alarm Attributes

Attribute Name	Attribute Value
Major Type	193



Attribute Name	Attribute Value
Minor Type	872451
Managed Object Class	IpworksDhcpv4
Source	ManagedElement=<Node Name>,SystemFunctions=1,Pm=1,PmJob=<PM Job name, default job is DHCPv4DefaultPmThresholdJob>,MeasurementReader=<Default is DDNSRetryFailMr>:<hostname>
Specific Problem	DHCPv4, DDNS Retries Failed
Event Type	qualityOfServiceAlarm(11)
Probable Cause	x733RetransmissionRateExcessive(345)
Additional Text	This alarm is raised after a number of retries have been made by the DHCPv4 server without receiving any acknowledgement regarding the status of the update.;uuid:<Product_UUID> ⁽¹⁾
Perceived Severity	Warning

(1) <Product_UUID> is the universally unique identifier (UUID) of machine that generates the alarm. The value can be fetched from `/sys/devices/virtual/dmi/id/product_uuid` on the PL node.

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 you have read the following documents:

- *System Safety Information*
- *Personal Health and Safety Information*
- *Fault Management*

1.2.2 Tools

No tools are required.



1.2.3

Conditions

No conditions.



DHCPv4, DDNS Retries Failed



2 Procedure

This section describes the procedure to clear this alarm.

2.1 Checking file "resolv.conf"

Do the following:

1. Edit the file `/etc/resolv.conf`. Replace the IP for nameserver with the IP for DNS server, from which DDNS determines to be updated.
2. Restart DHCPv4 server. For example:


```
# ipw-ctr restart dhcp <PL hostname>
```
3. This alarm is automatically cleared when the DDNS update retry failed times falls below the predefined threshold in the given time interval (defined by the related MO *PmJob*, the default value is 60s).
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.

2.2 Checking DDNS Configuration

Do the following:

1. Ensure the DNS server configuration is correct.

For more information about how to configure DDNS, refer to *Configure DHCP*.
2. This alarm is automatically cleared when the DDNS update retry failed times falls below the predefined threshold in the given time interval (defined by the related MO *PmJob*, the default value is 60s).
3. 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.