

IPWorks Alarm List for DL380 Gen9 Host Management

LIST

PRELIMINARY

Copyright

© Ericsson AB 2017, 2018. 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.

PRELIMINARY



Contents

1	Introduction	1
1.1	Related Information	1
1.2	Fetching SNMP Statistics Using SNMP Commands	1
1.2.1	SNMPGET	2
1.2.2	SNMPWALK	2
2	Overview	5
3	Alarms for Platform	7
3.1	Disk Utilization Monitoring	7
3.1.1	Alarm Description	7
3.1.2	Procedure	8
3.2	Memory Monitoring	9
3.2.1	Alarm Description	9
3.2.2	Procedure	9
3.3	Swap Space Monitoring	10
3.3.1	Alarm Description	10
3.3.2	Procedure	11
3.4	System Load Monitoring	12
3.4.1	Alarm Description	12
3.4.2	Procedure	13
3.5	Network Traffic Utilization Monitoring	14
3.5.1	Alarm Description	14
3.5.2	Procedure	15
3.6	Link Down	15
3.6.1	Alarm Description	15
3.6.2	Procedure	17
3.7	Temperature Monitoring	22
3.7.1	Alarm Description	22
3.7.2	Procedure	23
3.8	Power Supply Monitoring	24
3.8.1	Alarm Description	24
3.8.2	Procedure	24
3.9	Fan Status Monitoring	25
3.9.1	Alarm Description	25
3.9.2	Procedure	26
	Reference List	29



PRELIMINARY



1 Introduction

This document gives an overview of the IPWorks alarms for G9 platform.

Scope

For each alarm, the following topics are covered:

- Alarm description
- Procedure.

Note: For alarms with the `cleared` severity, no actions are provided because these alarms are used to clear the associated alarms.

Target Groups

This document is intended for personnel handling alarms. This includes network administrators and system administrators.

1.1 Related Information

Trademark information, typographic conventions, and definition and explanation of abbreviations and terminology can be found in the following documents:

- *Trademark Information*, Reference [1]
- *Typographic Conventions*, Reference [2]
- *Glossary of Terms and Acronyms*, Reference [3]

1.2 Fetching SNMP Statistics Using SNMP Commands

This section guides users how to fetch the Performance Management (PM) using SNMP Commands.

IPWorks supports fetching SNMP statistics from all protocol servers and EM SS component by using SNMP commands: `snmpget`, `snmpgetnext`, `snmpbulkget`, `snmpwalk`, `snmpbulkwalk`. Only `snmpget` and `snmpwalk` are described in details here. For more information about the other SNMP commands, see the online help by using the `man` command.

Note: For the counters belonging to the `Table Counter` group, only the commands `snmpwalk` and `snmpbulkwalk` are applicable for users to fetch the SNMP statistics.



1.2.1 SNMPGET

`snmpget` is an SNMP application that uses the `GET` request to query for information on a network entity. Any specific counter can be retrieved using the `snmpget` command.

An example is shown for the `ipworksDnsServQuerySuccess` counter. The command requires the exact name or the OID of the counter followed by “.0”. In the following example, the output shows that the value for the counter is “0”:

```
# snmpget -v 2c -c public localhost ipworksDnsServQuerySuccess.0
```

or

```
# snmpget -v 2c -c public localhost .1.3.6.1.4.1.193.113.1.1.1.1.2.1.0
```

The output:

```
.1.3.6.1.4.1.193.113.1.1.1.1.2.1.0 = Counter32: 0
```

Where

- `snmpget` indicates the SNMPGET Operation to be performed.
- `-v` indicates the protocol version in which the request is to be sent. The supported versions are SNMPv1, SNMPv2c, and SNMPv3. If SNMPv3 is used, SNMPv3 must be configured beforehand. Refer to *IPWorks Fault Management Guide for DL380 Gen9 Platform*, Reference [4] for more information.
- `-c` indicates the community of the Agent. In this case, we specify `public`.
- `ipworksDnsServQuerySuccess` is the name of the counter. It can also be the corresponding OID.
- `.0` indicates the instance for the scalar variable.

1.2.2 SNMPWALK

`snmpwalk` is an SNMP application that uses the `GET NEXT` requests to query for a tree of information about a network entity. All the child objects of a parent object can be retrieved using the `snmpwalk` command.

An example is shown for the `ipworksDnsServQuery` group. The output is a list of the counters in that group and their values. In the example below, the `ipworksDnsServQuerySuccess` counter starts the list and has a value of “0”:

```
# snmpwalk -v 2c -c public localhost ipworksDnsServQuery
```

or



```
# snmpwalk -v 2c -c public localhost .1.3.6.1.4.1.193.113.1.1.1.1.2
```

The output:

```
.1.3.6.1.4.1.193.113.1.1.1.1.2.1.0 = Counter32: 0  
.1.3.6.1.4.1.193.113.1.1.1.1.2.2.0 = Counter32: 0  
.1.3.6.1.4.1.193.113.1.1.1.1.2.3.0 = Counter32: 0  
.1.3.6.1.4.1.193.113.1.1.1.1.2.4.0 = Counter32: 0  
.1.3.6.1.4.1.193.113.1.1.1.1.2.5.0 = Counter32: 0  
.1.3.6.1.4.1.193.113.1.1.1.1.2.6.0 = Counter32: 0
```

- `snmpwalk` indicates the SNMPWALK Operation to be performed.
- `-v` indicates the protocol version in which the request is to be sent. The supported versions are SNMPv1, SNMPv2c, and SNMPv3. If SNMPv3 is used, SNMPv3 must be configured beforehand. Refer to *IPWorks Fault Management Guide for DL380 Gen9 Platform*, Reference [4] for more information.
- `-c` indicates the community of the Agent. In this case, we specify “public”.
- `ipworksDnsServQuery` is the name of the parent object. It can also be the corresponding OID.



PRELIMINARY



2 Overview

IPWorks supports alarm reporting according to the ERICSSON-ALARM-IRP-MIB standard. For more information about the standard attributes, see Table 1.

IPWorks maintains an active alarm table for the generated alarms. The active alarm table contains a list of alarms that are currently occurring on a system. It is intended that the table should be queried upon device discovery and rediscovery to determine which alarms are currently active on the device. This allows the network management station to find out any problem that may have occurred before it starts to manage, or while it is out of contact with, a particular network element. Only one active alarm is reported for a problem, that is to say, if an alarm is reported previously and is in active state, a new alarm will not be reported for the same problem.

An alarm is usually cleared automatically as soon as the condition that triggers the alarm is not existing. Alternatively it can also be cleared from the table manually. However, certain alarms can only be cleared manually.

To receive the alarms from the IPWorks SNMP Agent, an SNMP manager must register itself with the IPWorks SNMP Agent. As part of the registration process, the manager can specify a port as a destination for all traps. If there is no port specified, the agent sends all traps to port 162 on the manager.

Table 1 Standard Attributes and Descriptions

Standard Attributes	Description
Notification ID	It represents the unique identifier generated by the SNMP Agent. It increases every time a new notification is sent.
Alarm ID	It uniquely identifies an entry in the Alarm Table. It increases every time a new alarm occurs.
Managed Object Class	It identifies the class of network resources to which the subject alarm is related.
Managed Object Instance	It identifies the instance (of a class) of network resource to which the subject alarm is related.
Event Time	It represents the time of occurrence of the subject alarm. The format complies with the standard DateAndTime which is defined in the SNMPv2-TC. The DISPLAY-HINT format for DateAndTime is "2d-1d-1d,1d:1d:1d,1a1d:1d" For example: 2009-12-31,16:6:39.0,+8:0.
Event Type	It specifies the type of alarm raised.
Probable Cause	It gives the probable cause identification code for the alarm according to ITU recommendations X.733/X.736/M.3100.
Perceived Severity	It gives the perceived severity of the alarm raised.



Standard Attributes	Description
Specific Problem	It provides a textual description of the active alarm. ⁽¹⁾
Additional Text	It represents arbitrary additional text for the subject alarm. Some additional texts contain %s in this document. It is a string variable that is displayed with different contents depending on the context.

(1) In real environment, the specific problem displays only in one line. However, due to this document layout, the message can be chopped.

PRELIMINARY



3 Alarms for Platform

This section describes the alarms defined in the ERICSSON-ALARM-IRP-MIB and LM-SENSORS-MIB.

Disclaimer

For the alarm Swap Space Monitoring, regarding the Specific Problem description, ignore the deviation between CPI and the actual information in the raised alarm. Do take the CPI as the right reference.

3.1 Disk Utilization Monitoring

3.1.1 Alarm Description

This alarm is defined in the ERICSSON-ALARM-IRP-MIB.

This alarm is issued when the available disk space falls below a specific percentage.

TIP: The threshold of minimum available disk space is defined in the file `/etc/ipworks/common/snmp/snmpd.conf`. For details about how to configure the threshold, see *IPWorks Fault Management Guide for DL380 Gen9 Platform*, Reference [4].

The following is a list of the alarm attributes:

Table 2 Alarm attributes for Disk Utilization Monitoring

Standard Attributes	Node Attributes	Attribute Value
-	OID	.1.3.6.1.4.1.3881.2.2.0.1
Notification ID	-	<Integer>
Alarm ID	-	<Integer>
Managed Object Class	-	"ipworksDisman"
Managed Object Instance	-	"DN_prefix:DC=ipworks.com,g3SubNetwork=US,Node_Distinguished_Name=<hostname>,Mounted on <path>"
Event Time	-	DISPLAY-HINT "2d-1d-1d,1d:1d:1d,1a1d:1d" For example: 2009-12-31,16:6:39.0,+8:0.
Event Type	-	equipmentAlarm(4)
Probable Cause	-	x733ThresholdCrossed(351)
Perceived Severity	-	Major



Standard Attributes	Node Attributes	Attribute Value
Specific Problem	-	"Disk Utilization Threshold Reached"
Additional Text	-	"dskTable threshold limit exceeded."

Possible Causes

- The log files occupy a large amount of disk space so that the available disk space is less than the minimum percentage threshold.
- The core files occupy a large amount of disk space so that the available disk space is less than the minimum percentage threshold.

3.1.2

Procedure

To clear the alarm:

1. Check which mounted device occupies a large amount of disk space by using the following command:

```
#df -l
```

The disk usage of all mounted devices appear.

For example, the command output may be as follows:

```
Filesystem      1K-blocks  Used  Available Use% Mounted on
/dev/cciss/c0d0p1 52426492 8979312 43447180 18% /
devtmpfs         12300124   172   12299952  1% /dev
tmpfs            12300124   3676   12296448  1% /dev/shm
/dev/cciss/c0d0p3 52426492 410888  52015604  1% /var
/dev/mapper/ipwdg-ipwvol
52428800 2200264 50228536  5% /global/ipworks
```

TIP: Focus on the Use% column. For example, for the device /dev/cciss/c0d0p1, the disk usage percentage is 18%, so the available disk space percentage is 72%. Compare current available disk space percentage with the predefined threshold. If the current available disk space percentage is less than the threshold, a large amount of disk space is occupied.

2. If a large amount of disk space is occupied, try to find the specific reason. If you fail to identify the reason, consult the next level of maintenance support for help.



3.2 Memory Monitoring

3.2.1 Alarm Description

This alarm is defined in the ERICSSON-ALARM-IRP-MIB.

This alarm is issued when the memory usage of any process exceeds the specified threshold.

TIP: The threshold value is defined in the file `/etc/ipworks/common/snmp/snmpd.conf`. For details about the threshold configuration, see *IPWorks Fault Management Guide for DL380 Gen9 Platform*, Reference [4].

The following is a list of the alarm attributes:

Table 3 Alarm Attributes for Memory Monitoring

Standard Attributes	Node Attributes	Attribute Value
-	OID	.1.3.6.1.4.1.3881.2.2.0.1
Notification ID	-	<Integer>
Alarm ID	-	<Integer>
Managed Object Class	-	"ipworksDisman"
Managed Object Instance	-	"DN_prefix:DC=ipworks.com,g3SubNetwork=US,Node_Distinguished_Name=<hostname>,pid:<pid>,process:<process name>"
Event Time	-	DISPLAY-HINT "2d-1d-1d,1d:1d:1d.1d,1a1d:1d" For example: 2009-12-31,16:6:39.0,+8:0.
Event Type	-	qualityOfService(11)
Probable Cause	-	x733ThresholdCrossed(351)
Perceived Severity	-	Major
Specific Problem	-	"Memory Utilization Threshold Reached"
Additional Text	-	"%s process memory threshold limit exceeded"

Possible Causes

- The process has memory leak.

3.2.2 Procedure

To clear the alarm:

1. Check the threshold (default value is 10, 000 MB) of the memory usage.



2. Check what process consumes a lot of memory and the memory usage exceeds the threshold by using the following command:

```
#top
```

The memory usages of all processes appear. Take the following command output as example. Check the **RES** value that indicates the used memory volume of a specific process.

```
top - 01:01:53 up 6 days, 23:11, 7 users,
load average: 0.31, 0.22, 0.25
Tasks: 225 total, 2 running, 223 sleeping, 0 stopped, 0 zombie
Cpu(s): 0.2%us, 0.2%sy, 0.0%ni, 99.6%id, 0.0%wa, 0.0%hi, 0.0%si, 0.0%st
Mem: 24019M total, 7465M used, 16553M free, 701M buffers
Swap: 8189M total, 0M used, 8189M free, 3948M cached
```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
26139	root	20	0	1548m	1.4g	7216	S	3	6.1	36:15.08	ndbmttd
14822	root	20	0	304m	33m	3176	S	1	0.1	11:07.30	named
27298	mysql	20	0	206m	33m	6332	S	1	0.1	5:23.97	mysqld
18085	root	20	0	54236	47m	2228	S	1	0.2	1:06.66	be
26020	root	20	0	107m	6648	1244	S	1	0.0	5:37.83	ndb_mgmd
772	root	20	0	0	0	0	S	0	0.0	0:00.52	kworker/2:1

3. Compare the memory usage of a specific process with the minimum threshold.

If the memory usage exceeds the threshold, try to locate the reason. If you fail to identify the reason, consult the next level of maintenance support for help.

3.3 Swap Space Monitoring

3.3.1 Alarm Description

This alarm is defined in the `ERICSSON-ALARM-IRP-MIB`.

This alarm is issued when the available swap space falls below the specified threshold.

TIP: The threshold value is configured in the file `/etc/ipworks/common/snmp/snmpd.conf`. The default value is 1000 MB. For details about the threshold configuration, see *IPWorks Fault Management Guide for DL380 Gen9 Platform*, Reference [4].

The following is a list of the alarm attributes:



Table 4 Alarm attributes for Swap Space Monitoring

Standard Attributes	Node Attributes	Attribute Value
-	OID	.1.3.6.1.4.1.3881.2.2.0.1
Notification ID	-	<Integer>
Alarm ID	-	<Integer>
Managed Object Class	-	"ipworksDisman"
Managed Object Instance	-	"DN_prefix:DC=ipworks.com,g3SubNetwork=US,Node_Distinguished_Name=<hostname>"
Event Time	-	DISPLAY-HINT "2d-1d-1d,1d:1d:1d,1a1d:1d" For example: 2009-12-31,16:6:39.0,+8:0.
Event Type	-	qualityOfService(11)
Probable Cause	-	x733ThresholdCrossed(351)
Perceived Severity	-	Major
Specific Problem	-	"The available swap space falls below the specified threshold (MIN Kb)"
Additional Text	-	"Swap threshold limit exceeded"

Possible Causes

- The process has memory leak, which consumes all available physical memory, so that a lot of swap space is occupied.
- Sometimes much swap space is in use even though a lot of physical memory is still available. For instance, at one point, memory has to swap data so that a lot of swap space is occupied. Later a big process occupying much of the physical memory terminates and frees its occupied memory; however the swapped-out data is not automatically swapped back to memory until the data is needed to be accessed. In this case, the physical memory keeps much free space for a long time; however the swap space is used a lot.

3.3.2

Procedure

To clear the alarm:

1. Check the threshold of available swap space.

The threshold value is configured in file `/etc/ipworks/common/snmp/snmpd.conf`. For details about the threshold configuration, see *IPWorks Fault Management Guide for DL380 Gen9 Platform*, Reference [4].

2. Check the free physical memory and available swap space by using command `top`.



#top

The memory and swap usages of all processes appear. Take the following command output as example. Check the Swap row. The 8189M free indicates the free swap space.

```
top - 01:01:53 up 6 days, 23:11, 7 users,
load average: 0.31, 0.22, 0.25
Tasks: 225 total, 2 running, 223 sleeping, 0 stopped, 0 zombie
Cpu(s): 0.2%us, 0.2%sy, 0.0%ni, 99.6%id, 0.0%wa, 0.0%hi, 0.0%si, 0.0%st
Mem: 24019M total, 7465M used, 16553M free, 701M buffers
Swap: 8189M total, 0M used, 8189M free, 3948M cached

  PID USER PR NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
 26139 root  20   0 1548m 1.4g 7216 S   3   6.1 36:15.08 ndbmttd
 14822 root  20   0  304m  33m 3176 S   1   0.1 11:07.30 named
 27298 mysql 20   0  206m  33m 6332 S   1   0.1  5:23.97 mysqld
 18085 root  20   0 54236  47m 2228 S   1   0.2  1:06.66 be
 26020 root  20   0  107m 6648 1244 S   1   0.0  5:37.83 ndb_mgmd
   772 root  20   0     0     0   0 S   0   0.0  0:00.52 kworker/2:1
```

- If the free swap space is less than the threshold, try to locate the reason. If you fail to identify the reason, consult the next level of maintenance support for help.

3.4 System Load Monitoring

3.4.1 Alarm Description

This alarm is defined in the ERICSSON-ALARM-IRP-MIB.

The IPWorks SNMP Master Agent monitors the average load of the local system, specifying thresholds for the 1-minute, 5-minute, and 15-minute granularity period. If any of these loads exceed the associated maximum value, the alarm is raised.

TIP: The maximum threshold value is configured in the file `/etc/ipworks/common/snmp/snmpd.conf`. The user can configure the load average value. For details about the threshold configuration, see *IPWorks Fault Management Guide for DL380 Gen9 Platform*, Reference [4].

The following is a list of the alarm attributes:

Table 5 Alarm attributes for System Load Monitoring

Standard Attributes	Node Attributes	Attribute Value
-	OID	.1.3.6.1.4.1.3881.2.2.0.1
Notification ID	-	<Integer>
Alarm ID	-	<Integer>



Standard Attributes	Node Attributes	Attribute Value
Managed Object Class	-	"ipworksDisman"
Managed Object Instance	-	"DN_prefix:DC=ipworks.com,g3SubNetwork=US,Node_Distinguished_Name=<hostname>,Type:<Load Type>"
Event Time	-	DISPLAY-HINT "2d-1d-1d,1d:1d:1d,1a1d:1d" For example: 2009-12-31,16:6:39.0,+8:0.
Event Type	-	qualityOfService(11)
Probable Cause	-	x733ThresholdCrossed(351)
Perceived Severity	-	<ul style="list-style-type: none"> • 1 min: Minor • 5 min: Major • 15 min: Critical
Specific Problem	-	<ul style="list-style-type: none"> • 1min: "System Load Threshold Reached, 1 min Load Average too high" • 5 min: "System Load Threshold Reached, 5 min Load Average too high" • 15 min: "System Load Threshold Reached, 15 min Load Average too high"
Additional Text	-	"System Load threshold limit exceeded"

Possible Cause

- Some processes are suspended, occupying large CPU load.

3.4.2

Procedure

To clear the alarm:

1. Check the processes that consume most of the CPU time by using the following command:

```
#top
```

The CPU load status appear. Take the following command output as example. Check the top row. The load average: 0.31, 0.22, 0.25 indicates the CPU average load for 1-minute, 5-minute, and 15-minute granularity period respectively.

```
top - 01:01:53 up 6 days, 23:11, 7 users, \
load average: 0.31, 0.22, 0.25
Tasks: 225 total, 2 running, 223 sleeping, 0 stopped, 0 zombie
Cpu(s): 0.2%us, 0.2%sy, 0.0%ni, 99.6%id, 0.0%wa, 0.0%hi, 0.0%si, 0.0%st
Mem: 24019M total, 7465M used, 16553M free, 701M buffers
```



Swap: 8189M total, 0M used, 8189M free, 3948M cached

```

PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
26139 root 20 0 1548m 1.4g 7216 S 3 6.1 36:15.08 ndbmttd
14822 root 20 0 304m 33m 3176 S 1 0.1 11:07.30 named
27298 mysql 20 0 206m 33m 6332 S 1 0.1 5:23.97 mysqld
18085 root 20 0 54236 47m 2228 S 1 0.2 1:06.66 be
26020 root 20 0 107m 6648 1244 S 1 0.0 5:37.83 ndb_mgmd
772 root 20 0 0 0 0 S 0 0.0 0:00.52 kworker/2:1

```

2. If any of the CPI average loads exceed the associated maximum value, try to locate the reason. If you fail to identify the reason, consult the next level of maintenance support for help.

3.5 Network Traffic Utilization Monitoring

3.5.1 Alarm Description

This alarm is defined in the ERICSSON-ALARM-IRP-MIB.

This alarm is issued when the utilization of network exceeds the predefined fluctuation range.

TIP: Objects that could potentially fluctuate around the specified level are better monitored using a threshold monitor entry. The specified level is configured in the file `/etc/ipworks/common/snmp/snmpd.conf`. For details about the specified level configuration, see *IPWorks Fault Management Guide for DL380 Gen9 Platform*, Reference [4].

The following is a list of the alarm attributes:

Table 6 Alarm Attributes for Network Traffic Utilization Monitoring

Standard Attributes	Node Attributes	Attribute Value
-	OID	.1.3.6.1.4.1.3881.2.2.0.1
Notification ID	-	<Integer>
Alarm ID	-	<Integer>
Managed Object Class	-	"ipworksDisman"
Managed Object Instance	-	"DN_prefix:DC=ipworks.com,g3SubNetwork=US,Node_Distinguished_Name=<hostname>,interface:<network interface>"
Event Time	-	DISPLAY-HINT "2d-1d-1d,1d:1d:1d.1d,1a1d:1d" For example: 2009-12-31,16:6:39.0,+8:0.
Event Type	-	communicationsAlarm(2)
Probable Cause	-	x733ThresholdCrossed(351)



Standard Attributes	Node Attributes	Attribute Value
Perceived Severity	-	Major
Specific Problem	-	"Network Traffic Utilization Threshold Reached"
Additional Text	-	"%s network traffic threshold limit exceeded"

Possible Cause

- The incoming traffic rises too high.

3.5.2

Procedure

To clear the alarm:

1. Monitor the traffic on the network.

For details, refer to *IPWorks Fault Management Guide for DL380 Gen9 Platform*, Reference [4].

2. If the incoming traffic rises too high, try to locate the reason. If you fail to identify the reason, consult the next level of maintenance support for help.

3.6

Link Down

3.6.1

Alarm Description

This alarm is defined in the ERICSSON-ALARM-IRP-MIB.

This alarm is issued when the network interfaces is down.

The following is a list of the alarm attributes:

Table 7 Alarm attributes for Link Down

Standard Attributes	Node Attributes	Attribute Value
-	OID	.1.3.6.1.4.1.3881.2.2.0.1
Notification ID	-	<Integer>
Alarm ID	-	<Integer>
Managed Object Class	-	"ipworksDisman"
Managed Object Instance	-	"DN_prefix:DC=ipworks.com,g3SubNetwork=US,NodeDistinguished Name=<hostname>, interface=<ifNumber>"



Standard Attributes	Node Attributes	Attribute Value
Event Time	-	DISPLAY-HINT "2d-1d-1d,1d:1d:1d,1a1d:1d" For example: 2009-12-31,16:6:39.0,+8:0.
Event Type	-	communicationsAlarm(2)
Probable Cause	-	x733CommunicationsProtocolError(305)
Perceived Severity	-	Major
Specific Problem	-	"linkDown,communication link failure"
Additional Text	-	"An interface is down"

(1) *ifNumber* represents the row position of the interface entry in *iftable*. For more information about *iftable*, see Page 16.

Possible Cause

- The network card is unavailable.
- The network cable of the interfaces is plugged out.

IfEntry

The following syntax defines the `IfEntry` structure. The `IfEntry` records the status of all network interfaces. In the following example, the `IfEntry` defines 22 attributes for each network interface. The `iftable` is the output of `IfEntry`, where each attribute of all network interfaces appears as a group.

TIP: The `ifNumber` retrieved from the raised alarm corresponds to the `ifIndex` in `IfEntry`. Each `ifIndex` has an associated `ifDescr` that indicates the interface name.

```

IfEntry ::=
    SEQUENCE {
1      ifIndex          InterfaceIndex,
2      ifDescr          DisplayString,
3      ifType           IANAifType,
4      ifMtu            Integer32,
5      ifSpeed          Gauge32,
6      ifPhysAddress    PhysAddress,
7      ifAdminStatus    INTEGER,
8      ifOperStatus     INTEGER,
9      ifLastChange     TimeTicks,
10     ifInOctets        Counter32,
11     ifInUcastPkts     Counter32,
12     ifInNUcastPkts   Counter32, -- deprecated
13     ifInDiscards     Counter32,
14     ifInErrors        Counter32,
15     ifInUnknownProtos Counter32,

```



```

16         ifOutOctets          Counter32,
17         ifOutUcastPkts       Counter32,
18         ifOutNUcastPkts      Counter32,  -- deprecated
19         ifOutDiscards        Counter32,
20         ifOutErrors          Counter32,
21         ifOutQLen            Gauge32,    -- deprecated
22         ifSpecific            OBJECT IDENTIFIER -- deprecated
    }

```

3.6.2 Procedure

To clear the alarm:

1. From the information of the raised alarm (see the previous table), get the `ifNumber` value.

For example, the `ifNumber` is 5.

For more information about `ifNumber`, see Section `IfEntry`.

2. Print the `iftable` by using `snmpwalk -v 2c localhost 1.3.6.1.2.1.2.2.1`.

Take the following command output only as example. Each attribute of all network interfaces appears as a group and each group consists of ten items. If the `ifNumber` is 5, the `ifIndex` is 5. Therefore, focus on the fifth row of each group (see the bold highlight in the output) and find out what specific interface issues the alarm. For example, the **.1.3.6.1.2.1.2.2.1.2.5 = STRING: eth3** indicates that the network interface `eth3` is down and triggers the alarm.

```

registered debug token dump, 1
.1.3.6.1.2.1.2.2.1.1.1 = INTEGER: 1
.1.3.6.1.2.1.2.2.1.1.2 = INTEGER: 2
.1.3.6.1.2.1.2.2.1.1.3 = INTEGER: 3
.1.3.6.1.2.1.2.2.1.1.4 = INTEGER: 4
.1.3.6.1.2.1.2.2.1.1.5 = INTEGER: 5
.1.3.6.1.2.1.2.2.1.1.6 = INTEGER: 6
.1.3.6.1.2.1.2.2.1.1.7 = INTEGER: 7
.1.3.6.1.2.1.2.2.1.1.8 = INTEGER: 8
.1.3.6.1.2.1.2.2.1.1.9 = INTEGER: 9
.1.3.6.1.2.1.2.2.1.1.10 = INTEGER: 10
.1.3.6.1.2.1.2.2.1.2.1 = STRING: lo
.1.3.6.1.2.1.2.2.1.2.2 = STRING: eth0
.1.3.6.1.2.1.2.2.1.2.3 = STRING: eth1
.1.3.6.1.2.1.2.2.1.2.4 = STRING: eth2
.1.3.6.1.2.1.2.2.1.2.5 = STRING: eth3
.1.3.6.1.2.1.2.2.1.2.6 = STRING: eth4
.1.3.6.1.2.1.2.2.1.2.7 = STRING: eth5
.1.3.6.1.2.1.2.2.1.2.8 = STRING: eth6
.1.3.6.1.2.1.2.2.1.2.9 = STRING: eth7

```



.1.3.6.1.2.1.2.2.1.2.10 = STRING: sit0
.1.3.6.1.2.1.2.2.1.3.1 = INTEGER: softwareLoopback(24)
.1.3.6.1.2.1.2.2.1.3.2 = INTEGER: ethernetCsmacd(6)
.1.3.6.1.2.1.2.2.1.3.3 = INTEGER: ethernetCsmacd(6)
.1.3.6.1.2.1.2.2.1.3.4 = INTEGER: ethernetCsmacd(6)
.1.3.6.1.2.1.2.2.1.3.5 = INTEGER: ethernetCsmacd(6)
.1.3.6.1.2.1.2.2.1.3.6 = INTEGER: ethernetCsmacd(6)
.1.3.6.1.2.1.2.2.1.3.7 = INTEGER: ethernetCsmacd(6)
.1.3.6.1.2.1.2.2.1.3.8 = INTEGER: ethernetCsmacd(6)
.1.3.6.1.2.1.2.2.1.3.9 = INTEGER: ethernetCsmacd(6)
.1.3.6.1.2.1.2.2.1.3.10 = INTEGER: tunnel(131)
.1.3.6.1.2.1.2.2.1.4.1 = INTEGER: 16436
.1.3.6.1.2.1.2.2.1.4.2 = INTEGER: 1500
.1.3.6.1.2.1.2.2.1.4.3 = INTEGER: 1500
.1.3.6.1.2.1.2.2.1.4.4 = INTEGER: 1500
.1.3.6.1.2.1.2.2.1.4.5 = INTEGER: 1500
.1.3.6.1.2.1.2.2.1.4.6 = INTEGER: 1500
.1.3.6.1.2.1.2.2.1.4.7 = INTEGER: 1500
.1.3.6.1.2.1.2.2.1.4.8 = INTEGER: 1500
.1.3.6.1.2.1.2.2.1.4.9 = INTEGER: 1500
.1.3.6.1.2.1.2.2.1.4.10 = INTEGER: 1480
.1.3.6.1.2.1.2.2.1.5.1 = Gauge32: 10000000
.1.3.6.1.2.1.2.2.1.5.2 = Gauge32: 100000000
.1.3.6.1.2.1.2.2.1.5.3 = Gauge32: 10000000
.1.3.6.1.2.1.2.2.1.5.4 = Gauge32: 10000000
.1.3.6.1.2.1.2.2.1.5.5 = Gauge32: 10000000
.1.3.6.1.2.1.2.2.1.5.6 = Gauge32: 1000000000
.1.3.6.1.2.1.2.2.1.5.7 = Gauge32: 1000000000
.1.3.6.1.2.1.2.2.1.5.8 = Gauge32: 10000000
.1.3.6.1.2.1.2.2.1.5.9 = Gauge32: 1000000000
.1.3.6.1.2.1.2.2.1.5.10 = Gauge32: 0
.1.3.6.1.2.1.2.2.1.6.1 = STRING:
.1.3.6.1.2.1.2.2.1.6.2 = STRING: 0:1f:29:5f:86:51
.1.3.6.1.2.1.2.2.1.6.3 = STRING: 0:1f:29:5f:86:50
.1.3.6.1.2.1.2.2.1.6.4 = STRING: 0:1f:29:5f:86:53
.1.3.6.1.2.1.2.2.1.6.5 = STRING: 0:1f:29:5f:86:52
.1.3.6.1.2.1.2.2.1.6.6 = STRING: 0:25:b3:21:69:b8
.1.3.6.1.2.1.2.2.1.6.7 = STRING: 0:25:b3:21:69:ba
.1.3.6.1.2.1.2.2.1.6.8 = STRING: 0:25:b3:21:69:bc
.1.3.6.1.2.1.2.2.1.6.9 = STRING: 0:25:b3:21:69:be
.1.3.6.1.2.1.2.2.1.6.10 = STRING:
.1.3.6.1.2.1.2.2.1.7.1 = INTEGER: up(1)
.1.3.6.1.2.1.2.2.1.7.2 = INTEGER: up(1)
.1.3.6.1.2.1.2.2.1.7.3 = INTEGER: down(2)
.1.3.6.1.2.1.2.2.1.7.4 = INTEGER: down(2)
.1.3.6.1.2.1.2.2.1.7.5 = INTEGER: down(2)
.1.3.6.1.2.1.2.2.1.7.6 = INTEGER: up(1)
.1.3.6.1.2.1.2.2.1.7.7 = INTEGER: up(1)
.1.3.6.1.2.1.2.2.1.7.8 = INTEGER: down(2)
.1.3.6.1.2.1.2.2.1.7.9 = INTEGER: up(1)
.1.3.6.1.2.1.2.2.1.7.10 = INTEGER: down(2)



```

.1.3.6.1.2.1.2.2.1.8.1 = INTEGER: up(1)
.1.3.6.1.2.1.2.2.1.8.2 = INTEGER: up(1)
.1.3.6.1.2.1.2.2.1.8.3 = INTEGER: down(2)
.1.3.6.1.2.1.2.2.1.8.4 = INTEGER: down(2)
.1.3.6.1.2.1.2.2.1.8.5 = INTEGER: down(2)
.1.3.6.1.2.1.2.2.1.8.6 = INTEGER: up(1)
.1.3.6.1.2.1.2.2.1.8.7 = INTEGER: up(1)
.1.3.6.1.2.1.2.2.1.8.8 = INTEGER: down(2)
.1.3.6.1.2.1.2.2.1.8.9 = INTEGER: up(1)
.1.3.6.1.2.1.2.2.1.8.10 = INTEGER: down(2)
.1.3.6.1.2.1.2.2.1.9.1 = Timeticks: (0) 0:00:00.00
.1.3.6.1.2.1.2.2.1.9.2 = Timeticks: (0) 0:00:00.00
.1.3.6.1.2.1.2.2.1.9.3 = Timeticks: (0) 0:00:00.00
.1.3.6.1.2.1.2.2.1.9.4 = Timeticks: (0) 0:00:00.00
.1.3.6.1.2.1.2.2.1.9.5 = Timeticks: (0) 0:00:00.00
.1.3.6.1.2.1.2.2.1.9.6 = Timeticks: (0) 0:00:00.00
.1.3.6.1.2.1.2.2.1.9.7 = Timeticks: (0) 0:00:00.00
.1.3.6.1.2.1.2.2.1.9.8 = Timeticks: (0) 0:00:00.00
.1.3.6.1.2.1.2.2.1.9.9 = Timeticks: (0) 0:00:00.00
.1.3.6.1.2.1.2.2.1.9.10 = Timeticks: (0) 0:00:00.00
.1.3.6.1.2.1.2.2.1.10.1 = Counter32: 63234758
.1.3.6.1.2.1.2.2.1.10.2 = Counter32: 144492868
.1.3.6.1.2.1.2.2.1.10.3 = Counter32: 0
.1.3.6.1.2.1.2.2.1.10.4 = Counter32: 0
.1.3.6.1.2.1.2.2.1.10.5 = Counter32: 0
.1.3.6.1.2.1.2.2.1.10.6 = Counter32: 103988327
.1.3.6.1.2.1.2.2.1.10.7 = Counter32: 4385190
.1.3.6.1.2.1.2.2.1.10.8 = Counter32: 0
.1.3.6.1.2.1.2.2.1.10.9 = Counter32: 4385188
.1.3.6.1.2.1.2.2.1.10.10 = Counter32: 0
.1.3.6.1.2.1.2.2.1.11.1 = Counter32: 41648
.1.3.6.1.2.1.2.2.1.11.2 = Counter32: 134245
.1.3.6.1.2.1.2.2.1.11.3 = Counter32: 0
.1.3.6.1.2.1.2.2.1.11.4 = Counter32: 0
.1.3.6.1.2.1.2.2.1.11.5 = Counter32: 0
.1.3.6.1.2.1.2.2.1.11.6 = Counter32: 125152
.1.3.6.1.2.1.2.2.1.11.7 = Counter32: 18933
.1.3.6.1.2.1.2.2.1.11.8 = Counter32: 0
.1.3.6.1.2.1.2.2.1.11.9 = Counter32: 18933
.1.3.6.1.2.1.2.2.1.11.10 = Counter32: 0
.1.3.6.1.2.1.2.2.1.12.1 = Counter32: 0
.1.3.6.1.2.1.2.2.1.12.2 = Counter32: 0
.1.3.6.1.2.1.2.2.1.12.3 = Counter32: 0
.1.3.6.1.2.1.2.2.1.12.4 = Counter32: 0
.1.3.6.1.2.1.2.2.1.12.5 = Counter32: 0
.1.3.6.1.2.1.2.2.1.12.6 = Counter32: 0
.1.3.6.1.2.1.2.2.1.12.7 = Counter32: 0
.1.3.6.1.2.1.2.2.1.12.8 = Counter32: 0
.1.3.6.1.2.1.2.2.1.12.9 = Counter32: 0
.1.3.6.1.2.1.2.2.1.12.10 = Counter32: 0
.1.3.6.1.2.1.2.2.1.13.1 = Counter32: 0

```



.1.3.6.1.2.1.2.2.1.13.2 = Counter32: 0
.1.3.6.1.2.1.2.2.1.13.3 = Counter32: 0
.1.3.6.1.2.1.2.2.1.13.4 = Counter32: 0
.1.3.6.1.2.1.2.2.1.13.5 = Counter32: 0
.1.3.6.1.2.1.2.2.1.13.6 = Counter32: 0
.1.3.6.1.2.1.2.2.1.13.7 = Counter32: 0
.1.3.6.1.2.1.2.2.1.13.8 = Counter32: 0
.1.3.6.1.2.1.2.2.1.13.9 = Counter32: 0
.1.3.6.1.2.1.2.2.1.13.10 = Counter32: 0
.1.3.6.1.2.1.2.2.1.14.1 = Counter32: 0
.1.3.6.1.2.1.2.2.1.14.2 = Counter32: 0
.1.3.6.1.2.1.2.2.1.14.3 = Counter32: 0
.1.3.6.1.2.1.2.2.1.14.4 = Counter32: 0
.1.3.6.1.2.1.2.2.1.14.5 = Counter32: 0
.1.3.6.1.2.1.2.2.1.14.6 = Counter32: 0
.1.3.6.1.2.1.2.2.1.14.7 = Counter32: 0
.1.3.6.1.2.1.2.2.1.14.8 = Counter32: 0
.1.3.6.1.2.1.2.2.1.14.9 = Counter32: 0
.1.3.6.1.2.1.2.2.1.14.10 = Counter32: 0
.1.3.6.1.2.1.2.2.1.15.1 = Counter32: 0
.1.3.6.1.2.1.2.2.1.15.2 = Counter32: 0
.1.3.6.1.2.1.2.2.1.15.3 = Counter32: 0
.1.3.6.1.2.1.2.2.1.15.4 = Counter32: 0
.1.3.6.1.2.1.2.2.1.15.5 = Counter32: 0
.1.3.6.1.2.1.2.2.1.15.6 = Counter32: 0
.1.3.6.1.2.1.2.2.1.15.7 = Counter32: 0
.1.3.6.1.2.1.2.2.1.15.8 = Counter32: 0
.1.3.6.1.2.1.2.2.1.15.9 = Counter32: 0
.1.3.6.1.2.1.2.2.1.15.10 = Counter32: 0
.1.3.6.1.2.1.2.2.1.16.1 = Counter32: 63234758
.1.3.6.1.2.1.2.2.1.16.2 = Counter32: 83449274
.1.3.6.1.2.1.2.2.1.16.3 = Counter32: 0
.1.3.6.1.2.1.2.2.1.16.4 = Counter32: 0
.1.3.6.1.2.1.2.2.1.16.5 = Counter32: 0
.1.3.6.1.2.1.2.2.1.16.6 = Counter32: 34880250
.1.3.6.1.2.1.2.2.1.16.7 = Counter32: 4937411
.1.3.6.1.2.1.2.2.1.16.8 = Counter32: 0
.1.3.6.1.2.1.2.2.1.16.9 = Counter32: 4939041
.1.3.6.1.2.1.2.2.1.16.10 = Counter32: 0
.1.3.6.1.2.1.2.2.1.17.1 = Counter32: 41648
.1.3.6.1.2.1.2.2.1.17.2 = Counter32: 117295
.1.3.6.1.2.1.2.2.1.17.3 = Counter32: 0
.1.3.6.1.2.1.2.2.1.17.4 = Counter32: 0
.1.3.6.1.2.1.2.2.1.17.5 = Counter32: 0
.1.3.6.1.2.1.2.2.1.17.6 = Counter32: 57755
.1.3.6.1.2.1.2.2.1.17.7 = Counter32: 19662
.1.3.6.1.2.1.2.2.1.17.8 = Counter32: 0
.1.3.6.1.2.1.2.2.1.17.9 = Counter32: 19664
.1.3.6.1.2.1.2.2.1.17.10 = Counter32: 0
.1.3.6.1.2.1.2.2.1.18.1 = Counter32: 0
.1.3.6.1.2.1.2.2.1.18.2 = Counter32: 0



```

.1.3.6.1.2.1.2.2.1.18.3 = Counter32: 0
.1.3.6.1.2.1.2.2.1.18.4 = Counter32: 0
.1.3.6.1.2.1.2.2.1.18.5 = Counter32: 0
.1.3.6.1.2.1.2.2.1.18.6 = Counter32: 0
.1.3.6.1.2.1.2.2.1.18.7 = Counter32: 0
.1.3.6.1.2.1.2.2.1.18.8 = Counter32: 0
.1.3.6.1.2.1.2.2.1.18.9 = Counter32: 0
.1.3.6.1.2.1.2.2.1.18.10 = Counter32: 0
.1.3.6.1.2.1.2.2.1.19.1 = Counter32: 0
.1.3.6.1.2.1.2.2.1.19.2 = Counter32: 0
.1.3.6.1.2.1.2.2.1.19.3 = Counter32: 0
.1.3.6.1.2.1.2.2.1.19.4 = Counter32: 0
.1.3.6.1.2.1.2.2.1.19.5 = Counter32: 0
.1.3.6.1.2.1.2.2.1.19.6 = Counter32: 0
.1.3.6.1.2.1.2.2.1.19.7 = Counter32: 0
.1.3.6.1.2.1.2.2.1.19.8 = Counter32: 0
.1.3.6.1.2.1.2.2.1.19.9 = Counter32: 0
.1.3.6.1.2.1.2.2.1.19.10 = Counter32: 0
.1.3.6.1.2.1.2.2.1.20.1 = Counter32: 0
.1.3.6.1.2.1.2.2.1.20.2 = Counter32: 0
.1.3.6.1.2.1.2.2.1.20.3 = Counter32: 0
.1.3.6.1.2.1.2.2.1.20.4 = Counter32: 0
.1.3.6.1.2.1.2.2.1.20.5 = Counter32: 0
.1.3.6.1.2.1.2.2.1.20.6 = Counter32: 0
.1.3.6.1.2.1.2.2.1.20.7 = Counter32: 0
.1.3.6.1.2.1.2.2.1.20.8 = Counter32: 0
.1.3.6.1.2.1.2.2.1.20.9 = Counter32: 0
.1.3.6.1.2.1.2.2.1.20.10 = Counter32: 0
.1.3.6.1.2.1.2.2.1.21.1 = Gauge32: 0
.1.3.6.1.2.1.2.2.1.21.2 = Gauge32: 0
.1.3.6.1.2.1.2.2.1.21.3 = Gauge32: 0
.1.3.6.1.2.1.2.2.1.21.4 = Gauge32: 0
.1.3.6.1.2.1.2.2.1.21.5 = Gauge32: 0
.1.3.6.1.2.1.2.2.1.21.6 = Gauge32: 0
.1.3.6.1.2.1.2.2.1.21.7 = Gauge32: 0
.1.3.6.1.2.1.2.2.1.21.8 = Gauge32: 0
.1.3.6.1.2.1.2.2.1.21.9 = Gauge32: 0
.1.3.6.1.2.1.2.2.1.21.10 = Gauge32: 0
.1.3.6.1.2.1.2.2.1.22.1 = OID: .0.0
.1.3.6.1.2.1.2.2.1.22.2 = OID: .0.0
.1.3.6.1.2.1.2.2.1.22.3 = OID: .0.0
.1.3.6.1.2.1.2.2.1.22.4 = OID: .0.0
.1.3.6.1.2.1.2.2.1.22.5 = OID: .0.0
.1.3.6.1.2.1.2.2.1.22.6 = OID: .0.0
.1.3.6.1.2.1.2.2.1.22.7 = OID: .0.0
.1.3.6.1.2.1.2.2.1.22.8 = OID: .0.0
.1.3.6.1.2.1.2.2.1.22.9 = OID: .0.0
.1.3.6.1.2.1.2.2.1.22.10 = OID: .0.0

```

3. Check whether the interface that triggers the alarm is configured.



#ifconfig -a

- If the interface that triggers the alarm is not configured at all, follow the substeps:

- a Ignore the alarm or clear the alarm manually.

For more information, refer to *IPWorks Fault Management Guide for DL380 Gen9 Platform*, Reference [4].

- b Clear the notification in OSS.

For details about how to clear the notification in OSS, contact the OSS support.

- If the interface that triggers the alarm is configured, bring up the interface.

3.7 Temperature Monitoring

3.7.1 Alarm Description

The alarm is defined in the ERICSSON-ALARM-IRP-MIB.

This alarm is issued when the temperature level exceeds the predefined threshold.

TIP: The threshold value is configured in the file `/etc/ipworks/common/snmp/snmpd.conf`. The user is allowed to configure the threshold. For details about the threshold configuration, see *IPWorks Fault Management Guide for DL380 Gen9 Platform*, Reference [4].

The following is a list of the alarm attributes:

Table 8 Alarm Attributes for Temperature Monitoring

Standard Attributes	Node Attributes	Attribute Value
-	OID	.1.3.6.1.4.1.3881.2.2.0.1
Notification ID	-	<Integer>
Alarm ID	-	<Integer>
Managed Object Class	-	"ipworksDisman"
Managed Object Instance	-	"DN_prefix:DC=ipworks.com,g3SubNetwork=US,Node_Distinguished_Name=<hostname>,<SensorInfo>"
Event Time	-	DISPLAY-HINT "2d-1d-1d,1d:1d:1d,1a1d:1d" For example: 2009-12-31,16:6:39.0,+8:0.



Standard Attributes	Node Attributes	Attribute Value
Event Type	-	environmentalAlarm(3)
Probable Cause	-	x733ThresholdCrossed(351)
Perceived Severity	-	Major
Specific Problem	-	"Temperature Level Threshold Reached"
Additional Text	-	"lmTempSensorsValue.<Sensor Number> threshold limit exceeded"

Possible Cause

- CPU temperature is too high.

3.7.2

Procedure

To clear the alarm:

1. Start the IPMI utility firstly.

```
# systemctl start ipmi
```

2. Check the temperature value of the corresponding sensor by running the following command:

```
#ipmitool -v sdr type Temperature
```

The current temperature of the sensor indicated by the **Sensor Reading** appears in the following command output (only an example).

```
Sensor ID           : Temp 1 (0xd)
Entity ID           : 39.1 (External Environment)
Sensor Type (Analog) : Temperature
Sensor Reading      : 20 (+/- 0) degrees C
Status              : ok
Positive Hysteresis  : Unspecified
Negative Hysteresis  : Unspecified
Minimum sensor range : -127.000
Maximum sensor range : Unspecified
Event Message Control : Entire Sensor Only
Readable Thresholds  : ucr unr
Settable Thresholds  :
Threshold Read Mask  : ucr unr
```

3. If the current temperature of the sensor is higher than the predefined temperature threshold, try to locate the reason. If you fail to identify the reason, consult the next level of maintenance support for help.



3.8 Power Supply Monitoring

3.8.1 Alarm Description

This alarm is defined in the ERICSSON-ALARM-IRP-MIB.

This alarm is issued when the power supply is not in the range between the minimum and maximum threshold.

TIP: Both minimum and maximum threshold value is configured in the file `/etc/ipworks/common/snmp/snmpd.conf`. The user is allowed to configure the threshold. For details about the threshold configuration, see *IPWorks Fault Management Guide for DL380 Gen9 Platform*, Reference [4].

The following is a list of the alarm attributes:

Table 9 Alarm Attributes for Power Supply Monitoring

Standard Attributes	Node Attributes	Attribute Value
-	OID	.1.3.6.1.4.1.3881.2.2.0.1
Notification ID	-	<Integer>
Alarm ID	-	<Integer>
Managed Object Class	-	"ipworksDisman"
Managed Object Instance	-	"DN_prefix:DC=ipworks.com,g3SubNetwork=US,Node_Distinguished_Name=<hostname>,<Sensor_Info>"
Event Time	-	DISPLAY-HINT "2d-1d-1d,1d:1d:1d,1a1d:1d" For example: 2009-12-31,16:6:39.0,+8:0.
Event Type	-	environmentalAlarm(3)
Probable Cause	-	x733ThresholdCrossed(351)
Perceived Severity	-	Major
Specific Problem	-	"Power Supply Level Threshold Reached"
Additional Text	-	"1mPSSensorsValue.<Sensor Number> threshold limit exceeded"

Possible Cause

- Power supply may have problem.

3.8.2 Procedure

To clear the alarm:



1. Start the IPMI utility firstly.

```
# systemctl start ipmi
```

2. Check the current of power supply by running the following command:

```
#ipmitool -v sdr type 'Power Supply'
```

The current power supply indicated by the **Sensor Reading** appears in the following command output (only an example).

```
ipwm10ps-01:~ # ipmitool -v sdr type 'Power Supply'
Sensor ID           : Power Supply 1 (0x3)
Entity ID           : 10.1 (Power Supply)
Sensor Type (Analog) : Power Supply
Sensor Reading      : 70 (+/- 0) Watts
Status              : Lower Non-Critical
Positive Hysteresis  : Unspecified
Negative Hysteresis  : Unspecified
Minimum sensor range : Unspecified
Maximum sensor range : Unspecified
Event Message Control : Entire Sensor Only
Readable Thresholds  : No Thresholds
Settable Thresholds  : No Thresholds
```

3. If the power is out of the range between the minimum and maximum threshold, try to locate the reason. If you fail to identify the reason, consult the next level of maintenance support for help.

3.9 Fan Status Monitoring

3.9.1 Alarm Description

It is defined in the ERICSSON-ALARM-IRP-MIB.

This alarm is issued when the fan status level exceeds the predefined threshold.

TIP: The threshold value is configured in the file `/etc/ipworks/common/snmp/snmpd.conf`. The user is allowed to configure the threshold. For details about the threshold configuration, see *IPWorks Fault Management Guide for DL380 Gen9 Platform*, Reference [4].

The following is a list of the alarm attributes:

Table 10 Alarm Attributes for Fan Status Monitoring

Standard Attributes	Node Attributes	Attribute Value
-	OID	.1.3.6.1.4.1.3881.2.2.0.1



Standard Attributes	Node Attributes	Attribute Value
Notification ID	-	<Integer>
Alarm ID	-	<Integer>
Managed Object Class	-	"ipworksDisman"
Managed Object Instance	-	"DN_prefix:DC=ipworks.com,g3 SubNetwork=US,Node_Distinguished_Name=<hostname>,<Sensor Info>"
Event Time	-	DISPLAY-HINT "2d-1d-1d,1d:1d:1d.1 d,1a1d:1d" For example: 2009-12-31,16:6:39 .0,+8:0.
Event Type	-	environmentalAlarm(3)
Probable Cause	-	x733ThresholdCrossed(351)
Perceived Severity	-	Major
Specific Problem	-	"Fan Status Level Threshold Reached"
Additional Text	-	"lmFanSensorsValue.<Sensor Number> threshold limit exceeded"

Possible Cause

- The fan may be damaged.

3.9.2

Procedure

To clear the alarm:

1. Start the IPMI utility firstly.

```
#systemctl start ipmi
```

2. Check the current fan status by running the following command:

```
#ipmitool -v sdr type Fan
```

The current fan status indicated by the **Status** appears in the following command output (only an example).

```
ipwm10ps-01:~ # ipmitool -v sdr type Fan
Sensor ID : Fan 1 (0x6)
Entity ID : 7.1 (System Board)
Sensor Type (Analog) : Fan
Sensor Reading : 13.720 (+/- 0) unspecified
Status : ok
Positive Hysteresis : Unspecified
Negative Hysteresis : Unspecified
Minimum sensor range : Unspecified
```



Maximum sensor range : Unspecified
Event Message Control : Entire Sensor Only
Readable Thresholds : No Thresholds
Settable Thresholds : No Thresholds

3. If the fan status level exceeds the predefined threshold, try to locate the reason. If you fail to identify the reason, consult the next level of maintenance support for help.

PRELIMINARY



PRELIMINARY



Reference List

Ericsson Documents

- [1] *Trademark Information*
- [2] *Typographic Conventions*
- [3] *Glossary of Terms and Acronyms*
- [4] *IPWorks Fault Management Guide for DL380 Gen9 Platform*
- [5] *IPWorks Troubleshooting Guideline*

PRELIMINARY