

# **HP OpenView**

## **Network Node Manager / Route Analytics Management System Integration Module**

### **User's Guide**

**Software Version: 4.0**



**Manufacturing Part Number : BA129-90017**

**May 2006**

© Copyright 2006 Hewlett-Packard Development Company, L.P.

---

## Legal Notices

### **Warranty.**

*Hewlett-Packard makes no warranty of any kind with regard to this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.*

A copy of the specific warranty terms applicable to your Hewlett-Packard product can be obtained from your local Sales and Service Office.

### **Restricted Rights Legend.**

Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause in DFARS 252.227-7013.

Hewlett-Packard Company, United States of America

Rights for non-DOD U.S. Government Departments and Agencies are as set forth in FAR 52.227-19(c)(1,2).

### **Copyright Notices.**

©Copyright 2006 Hewlett-Packard Development Company, L.P.

No part of this document may be copied, reproduced, or translated to another language without the prior written consent of Hewlett-Packard Company. The information contained in this material is subject to change without notice.

Contains software from Packet Design, Inc.

©Copyright 2006 Packet Design, Inc.

### **Trademark Notices.**

Linux is a U.S. registered trademark of Linus Torvalds.

Microsoft<sup>®</sup>, Windows<sup>®</sup>, and MS Windows<sup>®</sup> are U.S. registered trademarks of Microsoft Corporation.

Netscape<sup>™</sup> and Netscape Navigator<sup>™</sup> are U.S. trademarks of Netscape Communications Corporation.

**1. Overview****2. NNM/RAMS Integration Module Usage****3. Protocol Diagnosis**

GRE Tunnel Health . . . . .	15
SNMP MIBs . . . . .	16
Disable Protocol Diagnosis and Tunnel Health Monitoring . . . . .	17

**4. RAMS Views****5. RAMS Reports****6. Route Analytics Alarms**

Alarms From the RAMS Appliance. . . . .	25
Configure Alarms From the RAMS Appliance . . . . .	25
Watch Lists . . . . .	26
Watch List Operation of the Adjacency Lost Alarm . . . . .	27
RAMS Adjacency Lost Alarm. . . . .	27
RAMS Adjacency Established Alarm. . . . .	28
RAMS Route Change Alarm . . . . .	28
RAMS Adjacency Flap Alarm. . . . .	29
RAMS Prefix Origination Change Alarm . . . . .	29
RAMS Prefix Change Alarm . . . . .	30
RAMS Routing Event Alarm . . . . .	30
RAMS Excess Net Churn Alarm . . . . .	31
RAMS Peering Change Alarm . . . . .	31
RAMS Prefix Flap Alarm . . . . .	31
RAMS BGP Prefix Drought Alarm . . . . .	32
RAMS BGP Prefix Flood Alarm. . . . .	32
RAMS BGP Route Flap Alarm. . . . .	33
RAMS BGP Lost Redundancy Alarm . . . . .	33
RAMS MPLS/VPN Lost Router Reachability Alarm . . . . .	34
RAMS MPLS/VPN Lost Customer Reachability Alarm . . . . .	34
RAMS MPLS/VPN Customer Privacy Alarm . . . . .	35
RAMS MPLS/VPN Router Intrusion Alarm . . . . .	35
RAMS BGP Acquired Redundancy Alarm. . . . .	36
RAMS BGP Peer Lost Alarm . . . . .	36

---

# Contents

RAMS BGP AS Path Longer Alarm . . . . .	36
RAMS BGP Down to One Path Alarm . . . . .	37
RAMS BGP Down to Zero Paths Alarm . . . . .	37
RAMS BGP Peer Established Alarm . . . . .	38
Alarms From the NNM/RAMS Integration Module . . . . .	39
Router Misconfiguration Alarm . . . . .	39
Duplicate Router ID Alarm . . . . .	39
OSPF is Disabled Alarm . . . . .	40
<OSPF   EIGRP   ISIS> Tunnel Down Alarm . . . . .	40
<OSPF   EIGRP   ISIS> Tunnel Up Alarm . . . . .	41

## 7. RAMS Correlators

Trigger APA Polling . . . . .	45
Trigger APA Polling for MPLS BGP Alarms . . . . .	46
Correlate APA Root Cause Alarms Under RAMS Alarms . . . . .	47
Change Parent/Child Alarm Hierarchy . . . . .	47
Correlate State Change Alarms Under RAMS Adjacency Alarms . . . . .	49
Cleanup Correlation Composer Queue . . . . .	51
Set Correlator Parameters . . . . .	52
Correlator Fact Store Files . . . . .	53
Troubleshoot Correlation Composer . . . . .	54

<b>Index . . . . .</b>	<b>55</b>
------------------------	-----------

---

## Support

You can visit the HP OpenView support web site at:

**<http://www.hp.com/managementsoftware/support>**

This web site provides contact information and details about the products, services, and support that HP OpenView offers.

HP OpenView online software support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest
- Submit enhancement requests online
- Download software patches
- Submit and track progress on support cases
- Manage a support contract
- Look up HP support contacts
- Review information about available services
- Enter discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and log in. Many also require a support contract.

To find more information about access levels, go to:

**[http://www.hp.com/managementsoftware/access\\_level](http://www.hp.com/managementsoftware/access_level)**

To register for an HP Passport ID, go to:

**<http://www.managementsoftware.hp.com/passport-registration.html>**



---

# 1 Overview

The integration of NNM Advanced Edition (NNM AE) with the HP OpenView Route Analytics Management System (RAMS) gives you a powerful tool to pinpoint, analyze, and prevent problems in your OSPF, EIGRP, ISIS, BGP, and MP-BGP routing protocols.

The NNM/RAMS Integration Module provides the following values in your networking experience:

- The combination of layer 2 topology information from NNM and layer 3 routing expertise from RAMS gives you real-time and historical perspectives on important changes in your IP network.
- Maps and tables are built from real-time routing protocol data to help you visualize your routing environment. These views are accessible from the NNM Home Base and the Alarm Browsers.
- RAMS alarms are fed into the root cause analysis of NNM AE. As a result, you receive real-time notification of changes in your routing environment, enhanced with layer 2 data to help you understand the source and impact of these changes.
- Protocol diagnosis allows you to pinpoint router protocol misconfigurations that cause adjacency loss between neighbor routers. You receive real-time notification of changes in your routing environment as well as a description of the logical misconfiguration.
- GRE tunnels to the RAMS appliance are monitored. This allows you to know when visibility into part of your network is down or restored.
- Monitor key routes in your network and get immediate correlation between layer 2 faults and their layer 3 impact.

Use the integration of NNM AE and RAMS to keep up with your routers as they adapt to network changes.





- **Expand Layer 2 Connectivity Between Layer 3 Peers**  
Select a node in the IGP view, and use the right-click menu to expand connecting neighbors. This action displays layer 2 connectivity, giving you a more in-depth view of your layer 3 connectivity.
- **Launch a Neighbor View from an IGP View**  
Cross-launch a Neighbor view from an IGP view to show both layer 2 and layer 3 information. With this information, you can identify devices that are not reachable.
- **Launch a Path History View from an IGP View**  
Cross-launch a Path History view from an IGP view to show the layer 2 connections for the path between the two selected nodes. This action allows you to inspect the physical path and identify problems.
- **Launch a Path History View from a Route Change Alarm**  
From a Route Change alarm in the Route Analytics Alarm Browser, cross-launch the Path History view to see how the path changes over time. For failover scenarios, you can see which path is chosen. You might see multiple paths or no path. This information helps you know what actions you need to take to restore your network to full connectivity.
- **Launch Router Reports from Views and Alarms**  
From any dynamic view or the Route Analytics Alarm Browser, you can view reports on a specific router if it is monitored by RAMS. The reports give you summary information about the router specified.
- **Correlate Routing Failures to Layer 2 Failures**  
Correlate routing failures to layer 2 failures that are reported by APA in NNM AE. This action allows you to quickly identify the root cause and reduce your mean time to repair.
- **Detect Layer 3 Logical Causes for Routing Failures**  
NNM and RAMS alarms help you detect layer 3 logical protocol misconfiguration errors that lead to routing failures. This allows you to quickly identify the root cause and reduces your mean time to repair.
- **Monitor the Health of GRE Tunnels**

GRE tunnels provide visibility from the RAMS appliance into parts of your network. You can receive alarms when GRE tunnels go down or are restored. The alarms contain information about layer 2 failures or layer 3 logical misconfiguration errors that lead to the tunnel down status.

- Focus on Critical Routes

Isolate critical routes and network destinations so you can easily see potential problems. Use SNMP alarm watch lists to focus monitoring on critical routes and important servers as well as prefix changes, origination changes, and flaps.



---

## **3** Protocol Diagnosis

Network outages often result from router misconfigurations rather than hardware failures. NNM detects the physical hardware failures that can effect routing failures. The RAMS Integration Module protocol diagnosis

feature adds the ability to diagnose routing failures caused by protocol misconfiguration on routers. Supported protocols are OSPF, EIGRP, and ISIS.

When you set up the RAMS Integration Module, a new OpenView process starts. This process is called `ovramsd`. The `ovramsd` process listens to alarms from the RAMS appliance. Based on the alarms received, `ovramsd` issues SNMP queries to specific MIB entries to initiate additional protocol diagnosis. The protocol diagnosis feature defines a probable root cause for neighbor adjacency failures.

The following steps define a scenario in which protocol diagnosis plays a troubleshooting role:

1. The hello-interval on one adjacent endpoint is incorrectly changed from 30 to 40, creating a mismatch between two adjacent endpoints.
2. `ovramsd` receives a RAMS Adjacency Lost alarm with regard to the two previously adjacent routers.
3. `ovramsd` issues SNMP queries to the adjacent endpoint routers and analyzes the results for misconfiguration errors.
4. `ovramsd` generates a Router Misconfiguration alarm with the misconfiguration information.
5. The RAMS Adjacency Lost alarm is correlated under the Router Misconfiguration alarm.
6. When the hello-interval is correctly set to 30, adjacency is restored, and `ovramsd` receives a RAMS Adjacency Established alarm.
7. Based on the RAMS Adjacency Established alarm, `ovramsd` cancels the Router Misconfiguration alarm.

---

**NOTE**

`ovramsd` uses NNM 7.5 Extended Topology information to more quickly access router information. If router information is not available in Extended Topology, the analysis will not proceed. Make sure you have discovered the NNM Extended Topology network devices that are monitored by your RAMS appliance.

---

## GRE Tunnel Health

In addition to performing protocol diagnosis, ovransd listens for alarms from the RAMS appliance that indicate a tunnel health issue. The tunnel can be an OSPF, EIGRP, or ISIS tunnel.

When ovransd receives a RAMS alarm that indicates a tunnel health issue, it issues SNMP queries to specific MIB entries in the tunnel router to determine if the tunnel configuration is correct. ovransd then generates a tunnel alarm and correlates the RAMS alarm under it. If there is a misconfiguration, the ovransd tunnel alarm contains a description of the probable configuration error; otherwise, the description indicates “no probable logical cause.” If there is a physical layer 2 failure, the tunnel alarm detects and contains a description of the tunnel router down or the physical interface for the disabled tunnel.

The RAMS appliance detects and sends alarms to the connected NNM management station on health changes for tunnels that are configured on the management station. The RAMS appliance may not always send an alarm to the NNM management station with regard to tunnel health changes on a peer RAMS box in the network. ovransd supports both cases if it receives the correct notification.

The following steps define a tunnel health monitoring scenario:

1. A tunnel IP address is accidentally removed from the tunnel configuration statement.
2. ovransd receives a RAMS Peering Change alarm.
3. ovransd determines that the event is related to a tunnel.
4. ovransd issues SNMP queries to the tunnel router and analyzes the results for configuration errors.
5. ovransd generates a Tunnel Down alarm and provides a configuration error description.
6. The RAMS Peering Change event is correlated under the Tunnel Down alarm.
7. When the tunnel is restored, ovransd receives a RAMS Peering Change alarm.
8. ovransd generates a Tunnel Up alarm which cancels the Tunnel Down alarm.

## SNMP MIBs

Following are the MIB tables that contain specific entries queried by the ovransd process. ovransd does not query an entire table but only specific attributes for a given table.

- .iso.org.dod.internet.mgmt.mib-2.interfaces
- .iso.org.dod.internet.mgmt.mib-2.ip.ipAddrTable
- .iso.org.dod.internet.mgmt.mib-2.ifMIB.ifMIBObjects.ifXTable
- .iso.org.dod.internet.mgmt.mib-2.ospf.ospfGeneralGroup
- .iso.org.dod.internet.mgmt.mib-2.ospf.ospfIfTable



## Disable Protocol Diagnosis and Tunnel Health Monitoring

You can disable protocol diagnosis and tunnel health monitoring by stopping the `ovramsd` process. To stop the `ovramsd` process, issue the following command at a command prompt:

*UNIX:*

```
$OV_BIN/ovstop ovramsd
```

*Windows:*

```
%OV_BIN%\ovstop ovramsd
```

To start the `ovramsd` process again, issue the following command at a command prompt:

*UNIX:*

```
$OV_BIN/ovstart ovramsd
```

*Windows:*

```
%OV_BIN%\ovstart ovramsd
```

You can check the running status of `ovramsd` when you issue the following command at a command prompt:

*UNIX:*

```
$OV_BIN/ovstatus -c ovramsd
```

*Windows:*

```
%OV_BIN%\ovstatus -c ovramsd
```

---

### NOTE

To get additional information on the running state, use the following command: `ovstatus -v ovramsd`.

This information is useful if you suspect that `ovramsd` is not functioning correctly.

---

Protocol Diagnosis

**Disable Protocol Diagnosis and Tunnel Health Monitoring**

---

## **4** **RAMS Views**

The NNM/RAMS Integration Module provides the following dynamic views:

- The RAMS Path History view lets you see and compare current and historical routing topologies in your network.
- The RAMS IGP (Internal Gateway Protocol) view offers detailed OSPF, EIGRP, or ISIS information.

RAMS views can be accessed from the NNM Home Base. You will find more information about the views in the online help for each view.

---

## 5 **RAMS Reports**

RAMS provides IGP and BGP reports to give you information about specific routers. To access these reports, right click a router in a view. From the drop-down menu, select RAMS, and choose IGP or BGP. From the expanded drop-down menu, choose the specific report you want to

see.

The reports available include the following:

- IGP Reports
  - Summary
  - Events
  - Flapping Links
  - Changed Metrics
  - New Prefixes
  - Prefixes Withdrawn
- BGP Reports
  - Summary
  - Route Distribution
  - Route Flap

For more information on RAMS reports, see the *RAMS User's Guide*.

---

**NOTE**

Specific reports are also available in the NNM Alarm Browser. To view reports for a specific alarm, select the alarm and then find the report in the Views→Actions menu. This access provides quick information on the router that is specific to a particular alarm.

---

---

## **6** **Route Analytics Alarms**

RAMS alarms can come from two sources:

1. The RAMS appliance.
2. The NNM/RAMS Integration Module.





## Alarms From the RAMS Appliance

After you configure communications between NNM and the RAMS appliance, alarms from the RAMS appliance can help you troubleshoot your routing environment. When you configure the Integration Module to use alarms from the RAMS appliance, there are changes in NNM that allow NNM to respond to these new alarms:

- A Route Analytics Alarms category is added to the Alarm Browser tab of Home Base.
- RAMS alarms appear in the Route Analytics category with the Advanced Problem Analyzer (APA) alarms correlated under them.
- APA performs root cause analysis on incoming RAMS alarms to find the root cause of the RAMS alarm.

If NNM determines the root cause of a RAMS alarm, the APA alarm appears in the Status alarm category.

RAMS alarms are found in the Route Analytics Alarms category of the Alarms Browser where they are correlated to a root cause.

## Configure Alarms From the RAMS Appliance

**To configure a RAMS alarm, complete the following steps:**

1. Launch your web browser, and load the Extended Topology web-based configuration utility with the following URL:  
`http://<nnm_mgmt_station>:7510/topology/etconfig`
2. Click the RAMS tab, and within that tab, click the Rams Event Configuration link.
3. Refer to the *HP OpenView Route Analytics Management System User's Guide* chapter on Alerts for detailed configuration instructions.

### Watch Lists

A Watch List is essentially a filter on an alarm. It is a way to ensure that the only alarms sent are those that meet the criteria of the Watch List. For performance reasons, you may want to limit your number of entries in a Watch List to approximately 100.

Some alarms require that you configure a Watch List; for other alarms, a Watch List is optional. When a Watch List is optional for an alarm and it is not set, all alarms of that type are sent. In this case, if you do not configure a Watch List, you can be overwhelmed with irrelevant alarms. As soon as a Watch List is configured, RAMS sends only alarms that match the Watch List.

For example, if you do not configure a Watch List for the Adjacency Lost alarm, then all Adjacency Lost alarms are sent to NNM. However, if you configure one entry in the Watch List for the Adjacency Lost alarm, then NNM will get alarms for only that adjacency. Therefore, you should either configure the Watch List to specify all the adjacencies of interest or configure no Watch List at all.

There are two kinds of Watch Lists:

- Node-Based**      A node-based Watch List filters the alarms based on specific nodes. For example, the Adjacency Lost alarm uses a node-based Watch List to specify which routers have an adjacency of interest. For Route Change alarms, you can configure the Watch List using hostnames or IP addresses. All other Watch Lists are configured using IP addresses.
  
- Network-Based**      A network-based Watch List filters the alarms based on prefixes (or networks) and masks. For example the Prefix Origination Change alarm uses a network based Watch List. The alarm is triggered by a change in the prefix advertisement, which is not specific to a router.

**Watch List Operation of the Adjacency Lost Alarm** The Watch List for the Adjacency Lost alarm includes an Operation field. This sets conditions for when the alarm is issued, as follows:

**Table 6-1**      **Operation in Watch List**

Operation	Meaning
and	The <code>and</code> operation indicates that an alarm should be sent when the adjacency from the Source router to the Destination router is lost. You must specify both the Source and Destination.
or	<p>The <code>or</code> operation provides a compact way to specify multiple adjacencies of interest. It indicates that an alarm should be sent if either of the following occurs:</p> <ul style="list-style-type: none"> <li>• An outbound adjacency from the specified Source router to any other router is lost.</li> <li>• An inbound adjacency from any router to the specified Destination router is lost.</li> </ul> <p>You must specify both Source and Destination. You can use the same router in both fields to watch all adjacencies involving that router.</p>
none	<p>The <code>none</code> operation is exactly like the <code>or</code> operation except that it requires you to specify either the Source or Destination but not both.</p> <p>Cases where the <code>none</code> operation is more effective is when you want to monitor a limited set of adjacencies (inbound or outbound) on one router.</p>

## RAMS Adjacency Lost Alarm

The RAMS Adjacency Lost alarm is generated by the RAMS appliance when it detects that a previously known adjacency no longer exists. The Adjacency Lost alarm triggers a layer 3 misconfiguration diagnosis as a probable cause for the adjacency alarm.

If a watch list is configured and enabled, only routers that fall within the list are considered.

The information fields for this alarm are as follows:

1. source IP address
2. source node type - 0 router, 1 pseudonode
3. destination IP address
4. destination node type - 0 router, 1 pseudonode
5. time stamp

The SNMP event object ID for this alarm is .1.3.6.1.4.1.8083.1.1.9.1

### **RAMS Adjacency Established Alarm**

The RAMS Adjacency Established alarm is generated by the RAMS appliance when it detects that a new adjacency has been established.

If a watch list is configured and enabled, only routers that fall within the list are considered.

The information fields for this alarm are as follows:

1. source IP address
2. source node type - 0 router, 1 pseudonode
3. destination IP address
4. destination node type - 0 router, 1 pseudonode
5. time stamp
6. topology instance

The SNMP event object ID for this alarm is .1.3.6.1.4.1.8083.1.1.9.2

### **RAMS Route Change Alarm**

The RAMS Route Change alarm is generated by the RAMS appliance when a route from a source to a destination changes. A watch list must be configured for this alarm or it will not work.

When a watch list is configured and enabled, only routes that fall within the list are considered.

The information fields for this alarm are as follows:

1. source IP address
2. destination IP address

3. metric of a route before it changes
4. metric of a route after it changes
5. time stamp
6. topology instance

The SNMP event object ID for this alarm is .1.3.6.1.4.1.8083.1.1.9.3

### **RAMS Adjacency Flap Alarm**

The RAMS Adjacency Flap alarm is generated by the RAMS appliance when a link generates events at a rate higher than the RAMS router flap threshold.

If a watch list is configured and enabled, only routers that fall within the list are considered.

The information fields for this alarm are as follows:

1. destination IP address
2. hostname of the destination node
3. hostname of the source node
4. source node type - 0 router, 1 pseudonode
5. time stamp
6. topology instance

The SNMP event object ID for this alarm is .1.3.6.1.4.1.8083.1.1.9.4

### **RAMS Prefix Origination Change Alarm**

The RAMS Prefix Origination Change alarm is generated by the RAMS appliance when a prefix originates or is withdrawn. Route flaps can cause these alarms.

If a watch list is configured and enabled, only prefixes that fall within the list are considered.

The information fields for this alarm are as follows:

1. network number of the target of the prefix route
2. network mask of the target of the prefix route
3. type of prefix

4. IP address (or router id) of the originator of this prefix
5. time stamp
6. topology instance

The SNMP event object ID for this alarm is .1.3.6.1.4.1.8083.1.1.9.5

### **RAMS Prefix Change Alarm**

The RAMS Prefix Change alarm is generated by the RAMS appliance when a prefix attribute changes.

If a watch list is configured and enabled, only prefixes that fall within the list are considered.

The information fields for this alarm are as follows:

1. network number of the target of the prefix route
2. network mask of the target of the prefix route
3. type of prefix
4. IP address (or router id) of the originator of this prefix
5. time stamp
6. topology instance

The SNMP event object ID for this alarm is .1.3.6.1.4.1.8083.1.1.9.6

### **RAMS Routing Event Alarm**

The RAMS Routing Event alarm is generated by the RAMS appliance when a routing event occurs after a configured quiet period. This alarm is very chatty. Only turn it on if you need to know if alarms are behaving correctly.

If a hold time is configured and enabled, a routing event is triggered if it is received after the designated quiet period.

The information fields for this alarm are as follows:

1. time stamp

The SNMP event object ID for this alarm is .1.3.6.1.4.1.8083.1.1.9.7

## **RAMS Excess Net Churn Alarm**

The RAMS Excess Net Churn alarm is generated by the RAMS appliance when the current network churn is higher than the configured net churn threshold.

If an excess churn threshold is configured and enabled, an excess churn alarm is triggered only after this threshold is exceeded.

The information fields for this alarm are as follows:

1. current network churn number
2. time stamp
3. topology instance

The SNMP event object ID for this alarm is .1.3.6.1.4.1.8083.1.1.9.8

## **RAMS Peering Change Alarm**

The RAMS Peering Change alarm is generated by the RAMS appliance when one of the Route Explorer peers goes down or becomes adjacent to a new router.

If you want to monitor GRE tunnels, you must turn on this alarm.

The information fields for this alarm are as follows:

1. source IP address
2. GRE tunnel IP address on the router if tunnel peering
3. GRE tunnel IP address on the RAMS appliance if tunnel peering
4. status of the GRE tunnel
5. topology instance
6. time stamp

The SNMP event object ID for this alarm is .1.3.6.1.4.1.8083.1.1.9.9

## **RAMS Prefix Flap Alarm**

The RAMS Prefix Flap alarm is generated by the RAMS appliance when a prefix is flapping at a specified rate.

If a watch list is configured and enabled, only prefixes that fall within the list are considered.

The information fields for this alarm are as follows:

1. network number of the target of the prefix route
2. network mask of the target of the prefix route
3. time stamp
4. topology instance

The SNMP event object ID for this alarm is .1.3.6.1.4.1.8083.1.1.9.10

### **RAMS BGP Prefix Drought Alarm**

The RAMS BGP Prefix Drought alarm is generated by the RAMS appliance when a particular peer RIB drops significantly below the configured baseline size.

The information fields for this alarm are as follows:

1. peer IP address
2. number of days used for baselining
3. number of peer routes in the baseline
4. current RIB size
5. percent change in the size of the current peer RIB from the baseline peer RIB
6. time stamp
7. topology instance

The SNMP event object ID for this alarm is .1.3.6.1.4.1.8083.1.1.9.12

### **RAMS BGP Prefix Flood Alarm**

The RAMS BGP Prefix Flood alarm is generated by the RAMS appliance when a particular peer RIB increases significantly above the configured baseline size.

The information fields for this alarm are as follows:

1. peer IP address
2. number of days used for baselining
3. number of peer routes in the baseline



4. current RIB size
5. percent change in the size of the current peer RIB from the baseline peer RIB
6. time stamp
7. topology instance

The SNMP event object ID for this alarm is .1.3.6.1.4.1.8083.1.1.9.13

### **RAMS BGP Route Flap Alarm**

The RAMS BGP Route Flap alarm is generated by the RAMS appliance when a particular route is flapping at a rate higher than the configured threshold.

If a watch list is configured and enabled, only networks that fall within the list are considered.

The information fields for this alarm are as follows:

1. peer IP address
2. prefix IP address
3. prefix mask
4. peer AS number
5. next hop IP
6. next hop AS
7. route status
8. time stamp
9. topology instance

The SNMP event object ID for this alarm is .1.3.6.1.4.1.8083.1.1.9.14

### **RAMS BGP Lost Redundancy Alarm**

The RAMS BGP Lost Redundancy alarm is generated by the RAMS appliance when a prefix that was previously reachable redundantly has now lost this redundancy.

If a watch list is configured and enabled, only networks that fall within the list are considered.

The information fields for this alarm are as follows:

1. peer IP address
2. prefix IP address
3. prefix mask
4. route source AS
5. baseline number of next hops
6. current number of next hops
7. time stamp
8. topology instance

The SNMP event object ID for this alarm is .1.3.6.1.4.1.8083.1.1.9.15

### **RAMS MPLS/VPN Lost Router Reachability Alarm**

The RAMS MPLS/VPN Lost Router Reachability alarm is generated by the RAMS appliance when a PE router that was previously reachable is no longer reachable.

The information fields for this alarm are as follows:

1. route target
2. ID of the PE Router
3. time stamp
4. topology instance

The SNMP event object ID for this alarm is .1.3.6.1.4.1.8083.1.1.9.16

### **RAMS MPLS/VPN Lost Customer Reachability Alarm**

The RAMS MPLS/VPN Lost Customer Reachability alarm is generated by the RAMS appliance when prefixes associated with RTs for a customer fall below the configured threshold. This customer is no longer reachable.

The information fields for this alarm are as follows:

1. VPN customer name
2. time stamp

3. topology instance

The SNMP event object ID for this alarm is .1.3.6.1.4.1.8083.1.1.9.17

### **RAMS MPLS/VPN Customer Privacy Alarm**

The RAMS MPLS/VPN Customer Privacy alarm is generated by the RAMS appliance when the number of PEs participating in a VPN has falls below the configured threshold.

If a watch list is configured and enabled, only routers that fall within the list are considered.

The information fields for this alarm are as follows:

1. VPN customer name
2. time stamp
3. topology instance

The SNMP event object ID for this alarm is .1.3.6.1.4.1.8083.1.1.9.18

### **RAMS MPLS/VPN Router Intrusion Alarm**

The RAMS MPLS/VPN Router Intrusion alarm is generated by the RAMS appliance when a new PE enters a customer's VPN network or a PE that was previously a part of the baseline VPN is no longer present.

If a watch list is configured and enabled, only routers that fall within the list are considered.

The information fields for this alarm are as follows:

1. route target
2. ID of the PE Router
3. time stamp
4. topology instance

The SNMP event object ID for this alarm is .1.3.6.1.4.1.8083.1.1.9.19

## **RAMS BGP Acquired Redundancy Alarm**

The RAMS BGP Acquired Redundancy alarm is generated by the RAMS appliance when a prefix acquires more next hops than the number configured.

The information fields for this alarm are as follows:

1. peer IP address
2. prefix IP address
3. prefix mask
4. route source AS
5. baseline number of next hops
6. current number of next hops
7. time stamp
8. topology instance

The SNMP event object ID for this alarm is .1.3.6.1.4.1.8083.1.1.9.20

## **RAMS BGP Peer Lost Alarm**

The RAMS BGP Peer Lost alarm is generated by the RAMS appliance when the BGP adjacency to a peer is dropped or otherwise lost.

The information fields for this alarm are as follows:

1. peer IP address
2. time stamp
3. topology instance

The SNMP event object ID for this alarm is .1.3.6.1.4.1.8083.1.1.9.21

## **RAMS BGP AS Path Longer Alarm**

The RAMS BGP AS Path Longer alarm is generated by the RAMS appliance when the AS Path for a BGP prefix increases in length.

The information fields for this alarm are as follows:

1. peer IP address
2. prefix IP address

3. prefix mask
4. time stamp
5. topology instance

The SNMP event object ID for this alarm is .1.3.6.1.4.1.8083.1.1.9.22

### **RAMS BGP Down to One Path Alarm**

The RAMS BGP Down To One Path alarm is generated by the RAMS appliance when a prefix has only one path remaining. When only one path is available, there is no redundancy.

The information fields for this alarm are as follows:

1. peer IP address
2. prefix IP address
3. prefix mask
4. time stamp
5. topology instance

The SNMP event object ID for this alarm is .1.3.6.1.4.1.8083.1.1.9.23

### **RAMS BGP Down to Zero Paths Alarm**

The RAMS BGP Down To Zero Paths alarm is generated by the RAMS appliance when a prefix has no paths. When a path is not available, the route is down.

The information fields for this alarm are as follows:

1. peer IP address
2. prefix IP address
3. prefix mask
4. time stamp
5. topology instance

The SNMP event object ID for this alarm is .1.3.6.1.4.1.8083.1.1.9.24

## **RAMS BGP Peer Established Alarm**

The RAMS BGP Peer Established alarm is generated by the RAMS appliance when the BGP adjacency to a peer is established.

The information fields for this alarm are as follows:

1. peer IP address
2. time stamp
3. topology instance

The SNMP event object ID for this alarm is .1.3.6.1.4.1.8083.1.1.9.26

## Alarms From the NNM/RAMS Integration Module

The NNM/RAMS Integration Module generates alarms as a part of the protocol diagnosis process. The following sections describe the alarms that are generated by the Integration Module.

### Router Misconfiguration Alarm

The Router Misconfiguration alarm is generated by the RAMS Integration Module when it detects a protocol misconfiguration in a router that participates in an adjacency or peer relationship for the particular routing protocol called out.

The Router Misconfiguration alarm provides information about what is misconfigured to cause the adjacency to be lost.

The information fields for this alarm are as follows:

1. routing protocol
2. misconfigured attributes
3. source router address
4. source router attribute values
5. destination router address
6. destination router attribute values
7. time stamp

The SNMP event object ID for this alarm is  
.1.3.6.1.4.1.11.2.17.1.0.59000000

### Duplicate Router ID Alarm

The Duplicate Router ID alarm is generated by the RAMS Integration Module when it detects that endpoints have duplicate router IDs in your OSPF network.

This alarm tells you why an adjacency has been lost.

The information fields for this alarm are as follows:

1. routing protocol
2. misconfigured attributes
3. source router address
4. source router attribute values
5. destination router address
6. destination router attribute values
7. time stamp

The SNMP event object ID for this alarm is  
.1.3.6.1.4.1.11.2.17.1.0.59000001

### **OSPF is Disabled Alarm**

The OSPF is Disabled alarm is generated by the RAMS Integration Module when an OSPF Adjacency has been dropped.

This alarm identifies the IP address that has been disabled or removed from the OSPF process.

The information fields for this alarm are as follows:

1. specifies if the source or destination IP is disabled
2. disabled IP address
3. time stamp

The SNMP event object ID for this alarm is  
.1.3.6.1.4.1.11.2.17.1.0.59000002

### **<OSPF | EIGRP | ISIS> Tunnel Down Alarm**

The Tunnel Down alarm is generated by the RAMS Integration Module when it detects that a tunnel to the RAMS appliance is down.

This alarm identifies the tunnel that is down and, if possible, the probable cause.

The information fields for this alarm are as follows:

1. tunnel interface name description and RAMS appliance name
2. probable cause for the down tunnel
3. tunnel router IP address



4. logical tunnel IP address on the router (OSPF and EIGRP) or the logical tunnel IP address on the RAMS appliance (ISIS)

The SNMP event object ID for this alarm is  
.1.3.6.1.4.1.11.2.17.1.0.59000003

### **<OSPF | EIGRP | ISIS> Tunnel Up Alarm**

The Tunnel Up alarm is generated by the RAMS Integration Module when it detects that a tunnel to the RAMS appliance is up.

This alarm notifies you that a tunnel has come up.

The information fields for this alarm are as follows:

1. tunnel interface name description and RAMS appliance name
2. tunnel router IP address
3. logical tunnel IP address on the router (OSPF and EIGRP) or the logical tunnel IP address on the RAMS appliance (ISIS)

The SNMP event object ID for this alarm is  
.1.3.6.1.4.1.11.2.17.1.0.59000004

Route Analytics Alarms  
**Alarms From the NNM/RAMS Integration Module**



correlators and NNM, see *Managing Your Network with NNM*.

RAMS correlators are contained in the following namespaces:

- The `OV_RAM`s namespace correlators listen for RAMS alarms. These correlators perform additional processing on the alarms and then release them to the NNM Alarm browser. Since the incoming RAMS alarms are protocol-independent, the correlators operate across all supported protocols.
- The `OV_RAM`s\_BGP namespace correlators process BGP alarms from the RAMS appliance.
- The `OV_RAM`s\_2547 (MPLS over BGP, rfc2547) namespace correlators process MPLS/VPN alarms from the RAMS appliance. There are two correlators, and they work in concert. Both must be enabled or both must be disabled. Only the second of the two correlators, `OVRAMS_POLL_VPN_2`, can be modified.
- The `OV_OSPF` namespace correlators process OSPF IF State Change alarms (.1.3.6.1.2.1.14.16.2.0.16) and OSPF NBR State Change alarms (.1.3.6.1.2.1.14.16.2.2) from network devices. These alarms are correlated to RAMS Adjacency Lost and RAMS Adjacency Established alarms.

The RAMS correlators perform several main functions, which are discussed in the following sections.

## Trigger APA Polling

APA is configured to receive some alarms immediately, but when adjacency lost and route change alarms are received, a new alarm is generated that contains the corresponding router IP address. This new log-only alarm causes APA to begin analysis on the specified router IP address.

Correlators that process the alarms and generate an appropriate poll trigger request are as follows:

- OV\_RAMs\_TRIGGER\_POLL\_ADJ\_LOST
- OV\_RAMs\_TRIGGER\_POLL\_ROUTE\_CHANGE

No parameters for these correlators are configurable.

These correlators are enabled when you install and configure the integration module.

## Trigger APA Polling for MPLS BGP Alarms

These correlators trigger an APA Poll of an MPLS PE Router when a VPN loss alarm is received. This alarm is defined as the Customer Reachability by PE alarm in the RAMS VPN Explorer.

Following are the correlators that perform additional processing and generate an appropriate poll trigger request:

- OVRAMS\_POLL\_VPN\_LOST\_1
- OVRAMS\_POLL\_VPN\_LOST\_2

The Window Period parameter is configurable.

These correlators are enabled when you install and configure the integration module.

---

## Correlate APA Root Cause Alarms Under RAMS Alarms

These correlators perform two functions:

- Listen for RAMS route change, adjacency, prefix, and BGP alarms and store the UUID, router address, and subnet mask values in a queue for two minutes.
- Correlate the RAMS alarms in the queue with the appropriate APA root cause alarm when it is received.

APA alarms and RAMS alarms can arrive in any order. Within the time window, RAMS alarms are evaluated to determine if an incoming APA alarm is the root cause of the RAMS alarm. If a match is made, the APA alarm is nested under the RAMS alarm in the Route Analytics Alarm Browser. The APA alarm is also listed in the Status Alarm Browser.

The correlators that relate root cause APA alarms to the RAMS alarms are as follows:

- OV\_RAMs\_QUEUE\_ROUTE
- OV\_RAMs\_QUEUE\_ADJ
- OV\_RAMs\_QUEUE\_PREFIX
- OV\_RAMs\_QUEUE\_BGP
- OV\_RAMs\_APA\_1
- OV\_RAMs\_APA\_2

No parameters for these correlators are configurable.

These correlators are enabled when you install and configure the integration module.

### Change Parent/Child Alarm Hierarchy

By default, when RAMS and APA alarms are correlated, the APA alarms are correlated under the RAMS alarms, making the RAMS alarms the parent alarms. You can access the APA alarm by drilling down into the RAMS alarm. This action allows you to see the root cause for the protocol problem identified by RAMS.

If you would prefer that the APA alarms be the parent alarms in these correlations, you can change the relationship hierarchy.

**To change the parent/child alarm correlation hierarchy for RAMS and APA alarms, complete the following steps:**

1. Create the following file:

*UNIX:*

```
$OV_CONF/.rams_apa_parent
```

*Windows:*

```
%OV_CONF%\.rams_apa_parent
```

2. Stop the NNM processes by executing the following command at a command prompt:

*UNIX:*

```
$OV_BIN/ovstop
```

*Windows:*

```
%OV_BIN%\ovstop
```

3. Start the NNM processes by executing the following command at a command prompt:

*UNIX:*

```
$OV_BIN/ovstart
```

*Windows:*

```
%OV_BIN%\ovstart
```

This change will take effect when the NNM processes are started again. It will not change previous correlations.



## Correlate State Change Alarms Under RAMS Adjacency Alarms

If you have enabled OSPF state change alarms in your network, you can enable the RAMS IM correlators. These correlators nest OSPF state change alarms under RAMS Adjacency Lost and Established alarms.

Correlators that relate state change alarms to adjacency alarms are as follows:

- OV\_QUEUE\_EST\_NBR\_CHANGE
- OV\_QUEUE\_EST\_STATE\_CHANGE
- OV\_QUEUE\_EST\_STATE\_CHANGE\_IFINDEX
- OV\_QUEUE\_LOST\_NBR\_CHANGE
- OV\_QUEUE\_LOST\_STATE\_CHANGE
- OV\_QUEUE\_LOST\_STATE\_CHANGE\_IFINDEX
- OV\_RAM\_ADJ\_EST\_DST
- OV\_RAM\_ADJ\_EST\_SRC
- OV\_RAM\_ADJ\_LOST\_DST
- OV\_RAM\_ADJ\_LOST\_SRC

No parameters for these correlators are configurable.

These correlators are not enabled when you install and configure the integration module.

### To enable the RAMS IM correlators, complete the following steps:

1. Run the following command at a command prompt to open the Correlation Composer user interface:

```
$OV_BIN/ovcomposer -m d
```

2. Select File→Open and open the following file:

```
$OV_CONF/ecs/CIB/OSPF.fs
```

3. Enable each correlator by clicking its check box in the Enabled column.

**Correlate State Change Alarms Under RAMS Adjacency Alarms**

4. Select Correlations→Deploy to activate the correlators.
5. Exit the Correlation Composer user interface.

## Cleanup Correlation Composer Queue

These correlators make up an internal utility that prevents the Correlation Composer queue from growing too large. The queue is erased after a threshold is reached. The default is 50 alarms.

Following are the internal utility correlators that prevent the queue from growing too large:

- OV\_RAMs\_CLEANUP
- OV\_RAMs\_CLEANUP2

No parameters for these correlators are configurable.

These correlators are enabled when you install and configure the integration module.

## Set Correlator Parameters

Complete the following steps to review parameter definitions or modify parameters contained within a Correlation Composer correlator.

**To review or modify correlator parameters, complete the following steps:**

1. From any view, select Options→Event Configuration to launch the Event Configuration window.
2. From the Event Configuration window, select Edit→Event Correlation to launch the ECS Configuration window.
3. From the ECS Configuration window, select the default stream, highlight `Composer` in the correlation table, and select `Modify`. The Correlation Composer window appears in your web browser.
4. In the Correlation Composer window, select the `OV_RAMs` namespace from the `NameSpace` table. Its correlators display in the Correlator Store.
5. Double-click the correlator to display the `Description` tab.
6. Review the configurable parameters listed on the `Description` tab.
7. Click the `Definition` tab to access the configurable parameter setting. Click `Help` for information about each field.
8. After making changes, click `OK` to close the correlator configuration window and return to the Correlation Composer main window.
9. Save your change by clicking `File→Save`. This updates the correlator fact store file associated with the namespace.
10. To activate your change, click `File→Close` and then click `Correlations→Deploy`.
11. Exit the Correlation Composer main window.

## Correlator Fact Store Files

The RAMS correlator fact store files for the namespaces are located in the following directory:

UNIX                    `$OV_CONF/ecs/CIB/`

Windows                `<install_dir>\ecs\CIB\`

If you want to make experimental changes to the correlator parameter settings, it is good to create a backup of the fact store file before you proceed.

---

## Troubleshoot Correlation Composer

For troubleshooting information relating to the HP OpenView Correlation Composer or NNM correlators, see the *HP OpenView Correlation Composer's Guide* or *Managing Your Network with NNM*.

## C

configure

  RAMS alarms, 25

Correlation Composer

  setting parameters, 52

correlators, 44

  deploy, 52

  setting parameters, 52

## F

factstore file, 53

## N

namespace, 52

  RAMS enabled correlators, 44

## O

overview, 7

## P

parameters, 52

## R

RAMS alarms

  configure, 25

  screen, 26

RAMS.fs, 53

## T

troubleshoot, 54

## W

watch lists, 26

---

# Index