When Running HSRP, "Duplicate IP Address" Messages Appear in HP OpenView NNM Event Browser

Document ID: 13432

Introduction

When Hot Standby Router Protocol (HSRP) is run, "Duplicate IP Address" messages may appear in (and sometimes flood) the Hewlett−Packard (HP) OpenView Network Node Manager (NNM) event browser. For example, this problem could appear when you have two Route Switch Modules (RSMs) with HSRP enabled. One message displays in the event browser for each IP address configured on the RSMs. This document provides a workaround for this problem.

Note: This document originated from HP technical support. If you would like more information or have further questions on this issue, you may wish to contact HP .

Note: This workaround causes HP OpenView to poll the Hot Standby routers with an incorrect community string. If configured, these routers could potentially flood your management station with Authorization Failure traps. An unsupported method by which to work around this problem is to create a file called **netmon.noDiscover** in the /etc/opt/OV/share/conf directory. Include in the file all of the Hot Standby IP addresses. This causes the HP OpenView discovery mechanism to disregard these addresses before it begins to poll them.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on the HP OpenView NNM event browser.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

For more information on document conventions, refer to Cisco Technical Tips Conventions.

Workaround

This is an HP−recommended procedure that allows HP OpenView NNM to operate correctly in an environment with Cisco routers that support HSRP:

1. Obtain a list of all Hot Standby addresses in the management domain. These are the IP addresses that migrate from one physical router to another when one router goes down.
2. Choose **Options > SNMP Configuration** from the menu to add an entry for each Hot Standby address. In each entry, enter the IP address in the **Target** field, and an *incorrect* community name in the **Community** field. The incorrect name causes all SNMP access to the Hot Standby address to fail.
3. Make sure that none of the Hot Standby addresses resolve to the same hostname as any of the real routers in the /etc/hosts file or the nameserver.
4. If the **I** flag has been added to the /etc/opt/OV/share/conf/oid_to_type file in an attempt to fix the HSRP problem, it can be safely removed at this time.
5. Issue the **ovstop netmon** command to stop network monitoring.
6. Find all instances of the Hot Standby addresses in your map and delete any interface that contains these addresses. This step may need to be repeated for all maps, if you have multiple OVW maps.
7. If any of the routers in the map look incorrect (that is, they have incorrect addresses or interfaces associated with them), delete these routers as well. They should be rediscovered later.
8. Issue the **xnmsnmpconf −clearCache** command to clear the IP address−to−name mapping cache.
9. Issue the **ovstart netmon** command to restart network monitoring.

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- **IP Application Services Configuration Examples**
- **Technical Support − Cisco Systems**

Updated: Oct 26, 2005 Document ID: 13432