Application Note

The Miranda SNMP Option

Introduction

Simple Network Management Protocol (SNMP) was historically rooted in the development of Simple Gateway Management Protocol (SGMP) in the late 1980s by the Internet Engineering Task Force (IETF). The IETF recognized that total chaos was imminent unless some standards were established for the Internet including monitoring applications. In 1992, SNMP version 1 (SNMPv1) was born.

Currently, SNMP is available in three versions. The SNMP option is “trilingual” in that it is compatible with SNMPv1, v2, and v3.

During the 1990s, SNMP became popular as a monitoring and control tool in large data centers and network control facilities. Starting around 2000, SNMP has gradually been adopted in the broadcast industry. Currently, with the rapid implementation of network-based technology in broadcast facilities, interest in SNMP has increased sharply.

This document contains:

- A basic SNMP system overview.
- How the Miranda SNMP option fits into the system architecture.
- The main features of the Miranda SNMP option.

Basic SNMP System Overview

There are three fundamental components found in a SNMP system:

- SNMP manager(s).
- SNMP agent(s).
- Management Information Bases (MIBs).

Relationship of Managers, Agents, and MIBs

Suppose you are involved with a job interview as the job applicant. Your role would be similar to that of an SNMP agent because you know who you are and base your communication on items found in your resume. The interviewer is like an SNMP manager and queries you based on information found in your resume which, in the case of SNMP, would represent an MIB that has been compiled into an SNMP manager.

There could also be the case where you have more than one resume (one for technical, one for administrative, etc.) that represent different MIBs and are presented through your (master agent) based on subsets of your skill sets (or sub-agents).

Miranda SNMP

Miranda SNMP comprises a master agent, two sub-agents and three MIBs. Miranda SNMP does not include an SNMP manager but can communicate with any third-party SNMP manager that is SNMPv1, v2, or v3 compliant.

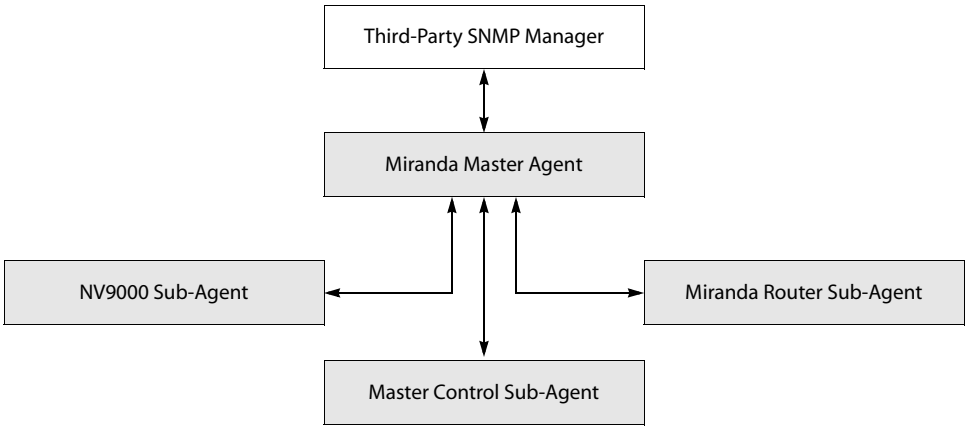

Figure 1. Manager, Master Agent and Sub-Agent Relationships

Miranda Agents

Miranda Master Agent

The Miranda master agent can be thought of as a gateway application. For example, the master agent can process ‘Get’ requests from the manager by directing the request to the appropriate sub-agent whose response passes through the master agent and back to the manager. Other parameters such as security settings reside in the master agent as well.

NV9000 Sub-Agent

The NV9000 sub-agent provides general router information from the NV9000 control server. Information on third-party routers under NV9000 control can be reported as well.

In the case of a redundant NV9000 control system, the Miranda SNMP option is installed on the primary system controller.

Miranda Router Sub-Agent

The Miranda router sub-agent can reside on a NV9000 system controller or a standalone Windows XP proxy platform. It is different from the NV9000 sub-agent because it communicates directly with Miranda router frames, enabling a more detailed level of information than the NV9000 sub-agent.

The Miranda router sub-agent does not look at third-party router frames.

Miranda Master Control Sub-Agent

The Miranda master control sub-agent can reside on a NV9000 system controller. It communicates directly with Miranda MCPMs and MCEs (master control’s transition processors).

The Miranda master control sub-agent does not look at third-party master control devices.

Windows SNMP Agent

The Miranda SNMP agent currently runs under the Microsoft Windows operating system. A customer can enable the Windows native SNMP agent to get information about the operating system and/or hardware. The Windows SNMP agent can run concurrently with the Miranda SNMP agent without conflict. However, each SNMP agent must be configured to “listen” on a unique port for an incoming request from a manager. The NV9000 SNMP proxy agent does not provide any Windows specific hardware or software information because it is already available from the Windows native agent.

Miranda MIBs

A MIB (Management Information Base) is a text file that is written to conform to a universal MIB standard using ASN.1. A common assumption is that MIBs reside in agents. This is not true. Actually, they are compiled into SNMP managers. Agents are written in such a way that they already understand the MIB parameters.

When compiled, MIBs add branches and leaves to the MIB tree that currently resides in the SNMP manager. This information becomes the basis for all manager/agent communication within the managed network.

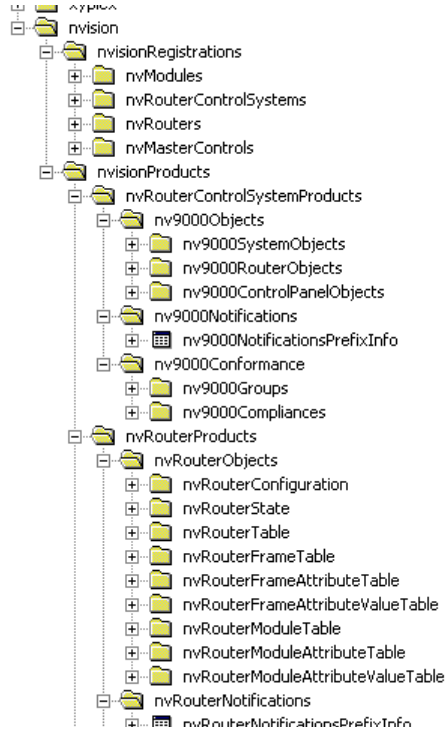

Figure 2. MIB Browser Display

Figure 2 shows an SNMP manager’s MIB browser display of the tree after the Miranda MIBS have been compiled into the manager.

Currently, there are four Miranda MIBs:

- NVISION-Registrations-MIB.mi2

  One can view the registrations MIB as a “header” function: it primarily provides definitions for the product-specific MIBs. Registrations MIB definitions are imported by all Miranda product MIBs.

- NVISION-NV9000-MIB.mi2

  The NV9000 MIB contains data for the control system, routers, and control panels. These objects include items such as configuration, operational status, and error information.

- NVISION-Router-MIB.mi2

  The NVISION router MIB contains data for the frames on a router subnet. Data associated with attributes such as frame ID, control card and power supply status, and the state of a fan or module can be reported.

- NVISION-MasterControl-MIB.mi2

  The Master Control MIB is for monitoring MCEs and MCPMs in master control frames.

Figure 3 shows them in the SNMP Manager:

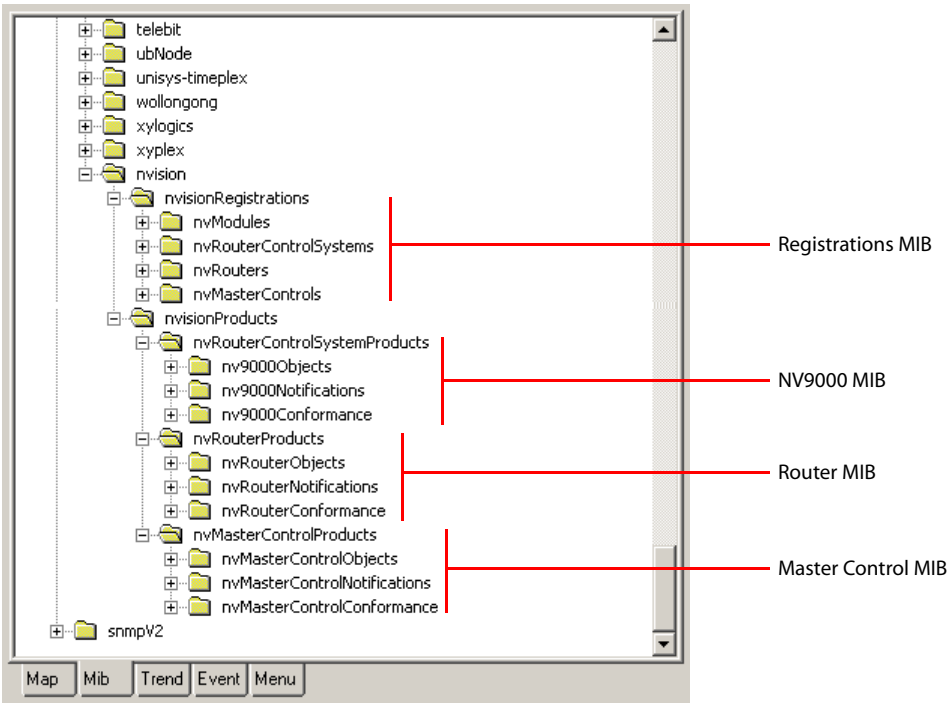

Figure 3. Miranda MIB Locations

Figure 4 shows the basic elements of the SNMP system:

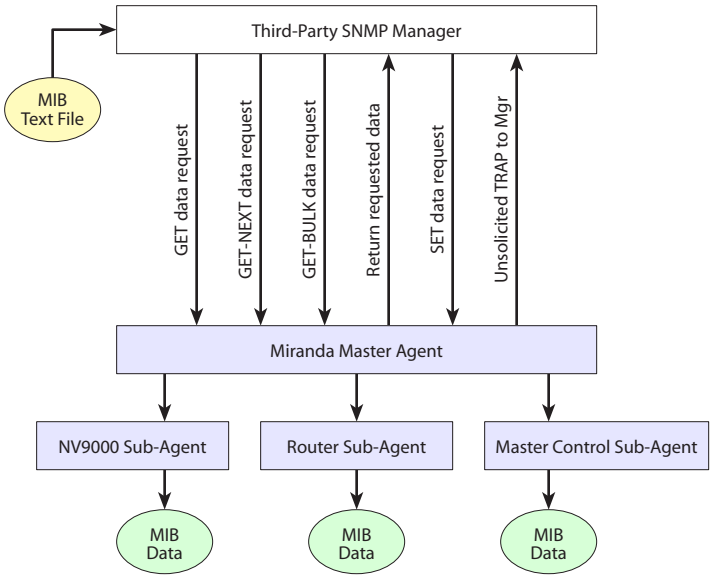

Figure 4. Manager, Agent and MIB Interaction

The following points apply:

- The MIB text file(s) are compiled into the manager using the manager's compiler.
- The MIB tree is now updated to reflect the addition of the Miranda Product MIB.
- Data requests from the manager can occur in three basic modes; GET, GET-NEXT and GET-BULK.
- An agent will respond to a request by an SNMP manager.
- A manager can set data in the agent using the SET data command if the agent permits a particular leaf, or data object, within its tree to accept a SET.
- Unsolicited TRAP information is sent from the agent to the manager.
- The Miranda sub-agents express, or realize, the data objects which each of the MIBs associated with an Miranda product. The leaves of the directory tree conform to the MIB format that was compiled in the Manager.
- The actual Miranda product data is sent through the sub-agents to the master agent where it is finally sent to the manager.

SNMP Traps

A trap (or notification) is an asynchronous message sent from an SNMP agent to an SNMP manager to indicate that a state change has taken place in the device the agent is monitoring.

Miranda traps are symmetrical because for every critical indication or warning issued, an informational trap is sent when the state of the given system value falls back into compliance. For example, a trap will be sent for an overheated power supply and will be followed by another trap when that the supply has cooled to within a safe temperature range.

Miranda Traps

There are three sets of Miranda traps:

- NV9000 traps
- Router traps
- Master control traps

NV9000 Traps

System Traps

- NV9000 System-Is-Running Trap: This trap is true if NvMaster is running on either the primary or secondary NV9000 configuration server.
- NV9000 System Health Trap: This trap is issued for a variety of state changes within the NV9000, whether they are warnings, critical, or merely informational. The specifics of why a state change has taken place can be found in the NV9000 system logs.

Router Traps

- The router is considered 'healthy' when it is on-line, active on the primary host, and all the communication links are operational.
- The agent issues a 'critical' trap when the router goes off-line.
- A 'warn' trap is issued in all other cases not covered by the 'healthy' and 'critical' traps.

Control Panel Traps

- When a control panel has an error, that panel will appear in the Nv9000CpErrTable with specific information about that panel and the accompanying error.

When a trap occurs for any one of these categories, a message will appear in the NV9000 logs if the log is configured for it. Log messages are not SNMP messages. Rather, they are the internal messages generated by the NV9000 system itself.

Router Traps

- Connection health.

  The agent sends a notification if any one of the connections for a given frame changes; that is, if a connection can suddenly be established, or if a connection is lost, it sends a notification.

- Frame attribute health.

  A determination of this attribute's health is based upon changes in its state.

- Module health.

  The health of the module based upon the unique criteria for this particular module.

- Module attribute health.

  A determination of this attribute's health is based upon changes in its state.

Master Control Traps

- Connection health.

  The agent sends a notification if any one of the connections for a given MCPM or MCE changes; that is, if a connection can suddenly be established, or if a connection is lost, it sends a notification.

- MCPM/MCE health.

  A determination of this module's health is based upon changes in its state.

- Attribute health.

  A determination of an attribute's health is based upon changes in its state.

Frame Attribute Trap Determination

Informational Notification

If the attribute value moves back into a compliant range or an element (such as a fan) reappears, this notification is sent. The following conditions result in an informational notification:

- An alarm is off.
- The video, AES, TDM, power supply, temperature, fan, and control card health alarms are off.
- A power supply is present.
- A power supply's temperature is nominal.
- A fan is operational.
- If applicable, the video, AES, and TDM references are present.

'Warn' Notification

A 'warn' notification is generally sent when a redundant subsystem is either not present or not operational. For example, an NV8256 router has four redundant power supplies. If one power supply is missing or non-operational in one of the redundant slots, a warning will be issued. The same holds true for the reference signals. If an AES reference for a router which requires it is present, but a second reference cannot be detected, the agent will issue a warning for the missing redundant reference.

The control cards are the exception to this rule because they contain the Ethernet connection hardware. If an IP address has not been specified for either the primary or secondary card, a warning for a “non-present” control card or connection will not be invoked.

‘Critical’ Notification

A ‘critical’ notification is sent when an attribute falls out of a safe operational range, or when one of the elements (such as a fan) disappears or stops functioning. The following conditions result in a ‘critical’ notification:

- An alarm is on.
- A power supply is missing when both power supplies in a redundant pair are missing.
- A power supply has exceeded a safe operating temperature.
- A fan is missing or non-operational.
- All references of a given type, such as a TDM sync or AES reference, are missing when the frame’s configuration requires them.

Alarms

The following are alarm conditions:

- Major alarm.

  Both video references are missing.

  Both AES references are missing in AES synchronous routers.

  Two or more fans are missing.

  Temperature of any power supply exceeds specification.

  Both TDM cards are missing in an NV5256 router.
- Minor alarm.

  A minor alarm is set if either the power supplies, video references, AES references, TDM sync, fan, temperature, or control card health alarms are on.
- Power supply and TDM sync alarm.

  This (combined) alarm is set if any power supply is missing or if any TDM card is missing from an NV5256 frame.
- Video reference.

  This alarm is set when either video reference 1 or 2 is missing.
- AES reference.

  This alarm is set when either AES reference 1 or 2 is missing on a frame requiring synchronous audio.
- Fan and temperature alarm.

  This (combined) alarm is set for any fan failure or when the temperature exceeds specification.
- Control card health

  This alarm is set for the following conditions:
  - Missing video reference 1 or 2.
  - Missing AES reference in a frame configured for synchronous audio.
  - Missing TDM sync in an NV5256.
  - 10-Base2 terminators missing.
  - Specific critical application tasks not running on the host control card.

Conclusion

A large number of broadcast devices, including Miranda's NVISION series routers, are capable of connecting to, and communicating over, Ethernet networks. As a result, SNMP network management systems are becoming increasingly attractive to broadcasters.

Miranda has developed an SNMP option that supports monitoring from third-party SNMP management systems.

SNMP implementation can be complicated and can be challenging to those who have never installed and configured an SNMP network management system.

If you have questions regarding this paper, contact Don Morgan at Miranda's Grass Valley (CA) office (530)-265-1000.