15.3 RELEASE NOTES

OVERVIEW

The release notes outline in broad terms some of the changes that have been made since release 15.2 of our products. Note that this list is not exhaustive for every product on every platform. If you have questions, please refer to the product-specific documentation or contact the support staff.

DOCUMENTATION

One of the major updates to SNMP products is the inclusion of electronic documentation. Software and hardware manuals for release 15.3 are included as files in Portable Document Format (PDF) on the accompanying CD-ROM. We recommend using Adobe Acrobat Reader® to view the manuals. The reader is freely available from www.adobe.com. The electronic manuals are accessible after software installation. The information given in the following sections describes how to access the manuals. (The following descriptions are based on installation of the software in the default directory. See product installation instructions for recommended default directory.)
CIAGENT

For CIAgent, the main manual is given in HTML and is accessible from the CIAgent interface. It can also be found in the /etc/srcconf/dr-web/doc/ciagent/manual directory and in the \etc\srcconf\dr-web\doc\ciagent\manual directory on Microsoft Windows. To access the manual from the manual directory, open the Table of Contents (toc.html) with a graphical Web browser. The CIAgent supplemental manuals (and a copy of the CIAgent main manual) are given in PDF and are not accessible through the CIAgent interface, but can be found in the /usr/local/CIAgent/manual directory and in the \Program Files\SNMPRI\CIAgent\manual directory on Microsoft Windows.

ENTERPOL

For EnterPol, the manual is given in PDF and is accessible from the EnterPol interface. It can also be found in the /opt/EnterPol/manual directory on solaris and in the /usr/local/EnterPol/manual directory on linux.

ALL OTHER PRODUCTS

For all other products, the manuals are given in PDF and are located in the /doc directory.

INTERNET STANDARDS

Since the release of version 15.2, several Internet standard documents have been published or updated by the Internet Engineering Task Force (IETF). SNMP Research has upgraded its products to meet these latest versions of the Internet standard documents (Requests For Comments, or RFCs). The latest additions and updates to IETF RFCs that affect SNMP Research products are as follows:

- RFC 2570: Introduction to SNMPv3
- RFC 2571: An Architecture for Describing SNMP Management Frameworks (obsoletes RFC 2271)
- RFC 2573: SNMP Applications (obsoletes RFC 2273)
- RFC 2575: View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP) (obsoletes RFC 2275)
- RFC 2576: Coexistence between Version 1, Version 2, and Version 3 of the Internet-Standard Network Management Framework
- RFC 2591: Definitions of Managed Objects for Scheduling Management Operations (DISMAN-SCHEDULE-MIB)
- RFC 2592: Definitions of Managed Objects for the Delegation of Management Scripts (DISMAN-SCRIPT-MIB)
- RFC 2790: Host Resources MIB (obsoletes RFC 1514)
- RFC 2981: The Event MIB

**OPERATING SYSTEMS**

SNMP Research’s products have been updated to support newer versions of existing supported platforms. For a current list of supported platforms, please visit our Web site at www.snmp.com.

**UPGRADES FOR CORE LIBRARIES**

Core Libraries are source code tools that provide the foundational routines used as the building blocks for other products. Core Libraries are written to support SNMPv1, SNMPv2, SNMPv3, and all MIB variables that conform to the Internet Standard Structure of Management Information (SMI). The following list of items reflects a brief overview of some of the more significant updates that affect SNMP Research’s core libraries.

- Added code to dynamically determine whether our code is running on a big endian or a little endian machine.
- Added pragmas where appropriate to suppress “line not reached” warnings in modules where these warnings are not relevant.
- Included miscellaneous casts, declarations, and include files to eliminate compiler warnings where feasible.
- Improved diagnostics to generate better system-dependent warning messages.
- Added several data initializations to reduce number of Purify™ warnings. These are in general controlled by the SR_CLEAR_MALLOC macro.
- Modified gettab to use new table routine.
- Repaired minor memory leaks in command-line tools.
- Fixed a command-line utility problem where the SNMP packet header error index was not correctly initialized on a getnext request.
- Changed mibs/common layout so that mib compiler output goes to an operating system specific directory.
- Fixed several problems causing DPRINTF to be called recursively.
- Addressed packet parsing routines in multiple locations to improve the handling of malformed received SNMP packets.
- Corrected localSnmpID parsing when entering initial manager configuration at the command line.
UPGRADES FOR AGENT PRODUCTS

SNMP Research provides agent products for end-users and Original Equipment Manufacturers (OEMs). Agent products are available for both open and embedded systems. SNMP Research’s agent products are built upon the world’s leading EMANATE® agent technology. We offer such options as Web accessibility to agent information, run-time extensibility, and compile-time extensibility. The following list of items reflects a brief overview of some of the more significant updates that affect SNMP Research’s agent products.

EMANATE AND EMANATE/Lite

EMANATE is a run-time extensible SNMP agent. The EMANATE system includes the world's leading subagent development kit, which automates subagent development. Based on a Master Agent/Subagent architecture, EMANATE allows subagents to be loaded and unloaded dynamically at run-time.

EMANATE/Lite is a monolithic agent, which includes an easy-to-use development toolkit for adding MIB extensions to the agent at compile time. EMANATE/Lite provides access to management information for each of the managed protocol layers within the network element. The upgrades for EMANATE, EMANATE/Lite, and other EMANATE-based agents include the items listed in the Core Libraries section, as well as the following items.

- Added configuration API that allows applications linked with EMANATE or EMANATE/Lite to alter agent configurations. The following may be configured via this API:
  - User-based Security Model (USM) MIB contents and SNMP Research additions
  - View-based Access Control Model (VACM) MIB contents
  - Target MIB (SNMP-TARGET-MIB) contents
- EMANATE, EMANATE/Lite: Added new routine called \texttt{SrAssignRequestIDToContextInfo()} to assign requestID to the ContextInfo structure as it is passed down to \texttt{get/test/set} method routines.
- Improved object registration time by deferring the rebuilding of the internal data structure in the EMANATE Master Agent until an event necessitating method routine access occurs. This is especially important when subagents that register large numbers of object/instances connect to the master agent.
- Changed usmUserTable row creation procedure to adhere more closely to the elements of procedure in RFC 2574.
- Changed tightly coupled subagent behavior to continue to work correctly with older master agent binaries. The EMANATE Master Agent and the tightly coupled subagent support library was modified to deliver additional symbol table information and to deliver the symbol table in a different order to tightly coupled subagents. This induced problems when using new tightly coupled subagents with older master agents. The tightly coupled subagent support library was modified to
check the version of the master agent to which the subagent is connecting, and to expect the old style symbol table if connecting to an older master agent.

- Removed call to `DiscardInvalidPdu()`. This removal resolved a race condition that could cause the master agent to fail when a subagent dies while multiple requests to the subagent are pending for multiple PDUs.

- Modified main event handling loop to process the next PDU thread before calling `GetSubagentEvent()`. This modification helps to avoid a possibly delay in processing the next PDU in the queue after the master agent finishes processing a `SET PDU`.

- Added check for “-” or `NULL` string to create zero length octet string for `usmTargetTag`.

- Added code in postmosy to print out the `#defines` that are needed when the `read-create` option is used in the command line.

- MIB-II: Modified the `mib2agt` that compiles on any 32-bit Solaris 2.x to run on any version of Solaris 2.x (32-bit or 64-bit).

- Replaced the `ConferenceRoom usmTargetTag` for the user “Guest” with “-” so SNMPv3 requests will succeed.

- Commented out the `snmpTargetAddrEntry` for `TrapSink` in the agent example configuration files.

- Added slight delay before mutex processing on HPUX11 to avoid a timing problem. This prevents the master agent from consuming large amounts of CPU time modification during getbulk processing.

- Modified the error severity on several diagnostics from `APERROR` to `APTRACE` to reduce the number of superfluous diagnostic messages.

- Corrected `snmpCommunityTable` implementation so that the table gets written back automatically to `nonVolatile` memory when a change is made.

- EMANATE (subagents): Modified processing of `GetVar()` and `SetVar()` requests to use a timer rather than a number of loop iterations for determining when to timeout `GetVar()` or `SetVar()` requests. The new code guarantees that requests will not timeout before 10 seconds.

- EMANATE with Proxy Option: Added call to `htons()` around the port specified in the `TransportInfo` structure for receiving traps. This addition resolves a problem that may cause the EMANATE agent with Proxy option to be unable to bind to trap port on little endian systems.

- Changed SNMPv2-trap to trap conversion to adhere more closely to RFC 2576 behavior.
CIAGENT

CIAgent, a member of the SecureIntelligence family, is a secure, intelligent, standards-based agent for open systems, such as mission-critical Web servers, DNS servers, file servers, and print servers. CIAgent combines the power of the EMANATE Master Agent with many standard and private MIB extensions to provide network-wide management of systems, applications, and services. The upgrades for CIAgent include the items listed in the EMANATE and DisMan Subagents sections, as well as the following items.

- Modified to register for the `SIGCHLD` signal so that child process terminations do not cause defunct processes.
- File Systems Monitor: Modified on Microsoft systems to reduce number of checks to the A: drive. The A: drive is now checked only on agent startup and on an SNMP request for information on that drive. This eliminates unnecessary periodic floppy drive activations.
- Host Resources MIB: Increased buffer size to improve performance.
- Host Resources MIB: Upgraded to run on Windows2000, in addition to Windows NT.

DISMAN SUBAGENTS

The Distributed Management (DisMan) MIB documents address the roles of distributed network managers. A distributed network manager is an application that acts as both a manager and an agent and can be controlled and observed remotely. SNMP Research offers implementations of the DisMan Schedule MIB, Script MIB, and Event MIB.

All of our DisMan MIBs are implemented as CIAgent subagents. The Schedule MIB Subagent defines standard MIB objects for scheduling SNMP set requests at periodic time intervals or at specific dates and times. The Script MIB Subagent can run interpreted script programs (get/set operations) autonomously without human intervention or console output. The Event MIB Subagent allows CIAgent to monitor MIB objects periodically and take action when a trigger condition is met. The upgrades to the DisMan subagents include the following items.

- Schedule MIB: Verified compliance to RFC 2591.
- Schedule MIB: Fixed problems that occurred when existing rows in the schedTable were modified.
- Schedule MIB: Modified the command-line option `-apuser` to print only those messages specifically related to scheduled events. (Note: Using the `-apall` command (without `-apuser`) may not print the messages generated by the Schedule MIB operations.)
- Schedule MIB: Modified the following items so that behavior unspecified in RFC 2591 would follow the clarifications in the recent draft of the standards-track revisions to RFC 2591 <draft-ietf-disman-schedule-mib-v2-03.txt>:
• Allow schedInterval and schedCalendarGroup objects to be modified regardless of the current value of schedRowStatus, schedAdminStatus, and schedOperStatus. This allows the events in the schedTable to be modified while the event is active and to take effect as soon as the event is modified. It is not necessary to deactivate the event or schedTable row before modifying the event characteristics.

• Mandate that schedOperStatus must be disabled while the schedRowStatus is inactive, i.e. inactive rows in the schedTable cannot specify active events.

• Mandate that schedRowStatus cannot be changed as long as the schedOperStatus is enabled, i.e. rows in the schedTable cannot be deactivated until the event has been deactivated.

• Script MIB: Made improvements to memory and suspended execution.

• Script MIB: Added a -notrap command-line option to prevent the DISMAN-SCRIPT-MIB from registering with BRASS to receive SNMP notifications. The BRASS server does not bind to UDP port 162 until a BRASS client wants to receive notifications. This feature allows the DISMAN-SCRIPT-MIB Subagent to run with another SNMP manager on the same host.

• Script MIB: Added the MLM_SET_VARS() function.

• Event MIB: Verified compliance to RFC 2981.

AGENT ADAPTERS

SNMP Research offers several SNMP agent adapters, including the Native Agent Adapter, the Native Subagent Adapter, and the new EMANATE Protocol Interface Component (EPIC) Subsystem. The Native Agent Adapter allows a user to easily integrate an EMANATE Master Agent into a system that already possesses an SNMP agent. The Native Subagent Adapter allows a user to easily integrate an EMANATE Master Agent into a system that already possesses an SNMP agent that is also based on the Master Agent/Subagent paradigm. The EPIC Subsystem allows applications using non-SNMP protocols to communicate with an SNMP agent. The upgrades to the agent adapters include the following items.

• Added EPIC Subsystem to our product line (available for purchase). The EPIC Subsystem provides a solution for interfacing non-UDP and non-SNMP protocols with our EMANATE and EMANATE/Lite Multilingual Agents (allowing the use of combinations of SNMPv1, SNMPv2, and SNMPv3).

• Native Agent Adapter: Added call to NormalizeVarBindList() before sending the varbind list received in the native agent’s responses. This addition corrects some common encoding errors that might be made by native agent.

• Native Agent Adapter: Put in check and diagnostic for our Microsoft Native Agent Adapter, because Microsoft extension agents have been known to return a different object than requested on get requests and the same object instance as requested on getnext requested.
UPGRADES FOR MANAGEMENT STATIONS AND APPLICATIONS

SNMP Research provides management stations and applications for end-users and Original Equipment Manufacturers (OEMs). Management stations and applications enable administrators to monitor and control networks, systems, and applications. Options, such as Web and java-based interfaces and policy-based management, are also available. The following list of items reflects a brief overview of some of the more significant updates that affect SNMP Research’s management stations and applications.

ARL

The Asynchronous Request Library (ARL) provides an API for building SNMP manager applications or for integrating SNMP manager capabilities into an existing application. The ARL makes it easy to write manager applications that take advantage of the SNMP management framework without requiring the developer to have SNMP expertise or programming capabilities. The upgrades for ARL and ARL-based management stations and applications include the items listed in the Core Libraries section, as well as the following items.

- Replaced table facility in ARL and BRASS with a facility better adapted to handling column holes and out-of-lexicographical-ordering agent errors.
- Fixed cleanup of ARL/BRASS requests that are deleted after submission but before response.
- Fixed code flow problem for ARL on Windows NT that would cause an uninitialized buffer to be used for snmpEngineID computation when the underlying host is misconfigured.
- Fixed the memory leak of a PDU when the Ar1V2GenerateTrap is called.
- Added support for receiving ICMP unreachable messages and passing the ICMP reason code back to the ARL application.
- Added code to save, then restore, the previous TTL for ICMP packets. This fixes a problem where setting the TTL once would cause the new TTL to apply permanently.
BRASS

The Bilingual Request and Security Subsystem (BRASS) is a Management Application Toolkit designed to provide facilities for creating SNMP management applications. It provides a C programming API that allows one or many management applications to access a single, shared SNMP stack and security database. BRASS optimizes the management station platform by providing full SNMP functionality, management application extensibility, support for SNMPv1, SNMPv2c, and SNMPv3, and simplified security configuration. BRASS also allows for efficient memory usage when there are multiple management applications. The upgrades for BRASS include the items listed in the ARL section, as well as the following items:

- Added general manager proxy capability to BRASS (as an optional product). This addition allows any network manager to use BRASS as a SNMPv3 proxy by putting all necessary information (username/passwords/context) in the community string of a SNMPv1 or SNMPv2 request.
- Modified the BRASS server to close the socket if it is unable to accept() the connection and effectively “slam the door” on a BRASS client that is attempting to connect. (The BRASS client will try to establish a connection a few times before it gives up).
- Improved checking in the ICMP response handler code. This resolves a problem where BRASS clients would receive NO_ERROR responses to ICMP echo or netmask requests from IP nodes that did not exist.
- Added support for DISPLAY_STRING_TYPE object to GetSizeSpecFromName() and GetSizeSpecFromOID().
- Removed duplicate freeing of varbind list contents by removing calls to FreeVarBindList in Ar1V1GenerateTrap() and Ar1V2GenerateTrap() because the varbind list is freed when entire trap PDU is freed.
- Modified ShutdownConnectionToServer() to convert length sent in packet to network byte order as expected by BRASS server. This addition resolves the problem with Ar1ShutdownApplication() on Windows, so that the shutdown message can correctly be sent to BRASS server.
EnterPol

EnterPol, a member of the SecureIntelligence family, offers policy-based tools for seamless management of networks, systems, applications, and services. EnterPol is an integrated collection of programs, processes, databases, and Java applications that forms a solid technological foundation for cooperating management applications. The upgrades for EnterPol include the items listed in the ARL section, as well as the following items.

- Added the following changes to the `snmpd.cnf` (v1c3.cnf) files to add more security and to allow EnterPol's Simple PolicyPro to configure SNMPv3 users:
  - SystemAdmin entries with `mgr` context for three SNMPv3 security levels have been added to the `vacmAccessTable` for manager configuration.
  - The `templateMD5 usmUserEntries` have been added so Simple PolicyPro can clone SNMPv3 users.
  - The `vacmAccessEntry for Anyone` has been changed to use the `CfgProt` views which restrict access to configuration tables.
  - The `CfgProt` view was added to the `vacmViewFamilyTree Table` to allow access to the MIB tree under `iso` but restrict views to configuration file tables.

- DR-Web Manager: Added extra command-line options for setting retries and timeouts (`-retries nn` and `-timeout nn`). (DR-Web Manager is also a stand-alone product. DR-Web Manager brings SNMP management to the Web by making it possible to talk to any SNMP agent using a Web browser.)

LT-301

The LATIN products (LT-301 and Mrs. Wright) are hardware-based products and management applications that provide SNMP interfaces between RS232 ports on legacy devices and SNMP management applications. The following list of items reflects a brief overview of some of the more significant updates that affect SNMP Research’s LT-301 products.

- Fixed a problem in OEM units with the `ping` command-line command. Previously, if you pinged a host that did not exist, all subsequent pings would fail, regardless of whether the host existed or not.
- Added checks to prevent the user from entering 0.0.0.0 as an IP address. This would cause problems that could only be fixed by erasing the FLASH memory with a FLASH programmer.
- Added additional error checking to ensure a domain name zone was entered. Entering an empty or blank domain name zone would cause problems that could only be fixed by erasing the FLASH memory with a FLASH programmer.
• Added code to read the LT-301 DIP switches and erase the IP FLASH sector at the earliest possible point in initialization processing so there would be very few things that could prevent the user from erasing the IP FLASH using the switch settings. This is intended to allow recovery from problems that previously required erasing the FLASH memory with a FLASH programmer.

• Added messages in the startup code to specify whether the LT-301 binary contains security level information that will help users know whether the LT-301 can be shipped outside of the U.S.

FOR MORE INFORMATION

For full descriptions of all of our products and their features, please visit our Web site at www.snmp.com. This version of the Release Notes for 15.3 is for in-house use only. A Release Notes Summary that would be appropriate for redistribution can be found on our Web site at www.snmp.com/products.