

Chapter 4

SNMP Overview

The Simple Network Management Protocol (SNMP) enables the monitoring of network devices from a central location. This chapter provides an overview of SNMP and describes how SNMP is implemented in the JUNOS software.

This chapter covers the following topics:

SNMP Architecture on page 18

SNMP Standards on page 19

JUNOS SNMP Agent Features on page 22

System Logging Severity Levels for SNMP Traps on page 23

SNMP Architecture

The SNMP agent exchanges network management information with SNMP manager software running on a network management system (NMS), or host. The agent responds to requests for information and actions from the manager. The agent also controls access to the agent's Management Information Base (MIB), the collection of objects that can be viewed or changed by the SNMP manager.

The SNMP manager collects information on network connectivity, activity, and events by polling managed devices.

Communication between the agent and the manager occurs in one of the following forms:

Get, GetBulk, and GetNext requests—The manager requests information from the agent; the agent returns the information in a Get response message.

Set requests—The manager changes the value of a MIB object controlled by the agent; the agent indicates status in a Set response message.

Traps notification—The agent sends traps to notify the manager of significant events that occur on the network device.

Management Information Base

A MIB, or Management Information Base, is a hierarchy of information used to define managed objects in a network device. The MIB structure is based on a tree structure, which defines a grouping of objects into related sets. Each object in the MIB is associated with an object identifier (OID), which names the object. The “leaf” in the tree structure is the actual managed object instance, which represents a resource, event, or activity that occurs in your network device.

MIBs are either standard or enterprise-specific. Standard MIBs are created by the IETF and documented in various RFCs. Depending on the vendor, many standard MIBs are delivered with the NMS software. You can also download the standard MIBs from the IETF Web site, <http://www.ietf.org>, and compile them into your NMS if necessary.

For a list of standard supported MIBs, see “SNMP Standards” on page 19.

Enterprise-specific MIBs are developed and supported by a specific equipment manufacturer. If your network contains devices that have enterprise-specific MIBs, you must obtain them from the manufacturer and compile them into your network management software.

For a list of Juniper Networks enterprise-specific supported MIBs, see “Juniper Networks Enterprise-Specific MIBs” on page 101.

SNMP Traps

A trap reports significant events occurring on a network device, most often errors or failures.

SNMP traps are defined in either standard or enterprise-specific MIBs. Standard traps are created by the IETF and documented in various RFCs. The standard traps are compiled into the network management software. You can also download the standard traps from the IETF Web site, <http://www.ietf.org>.

For more information on standard traps supported by the JUNOS software, see “Standard SNMP Traps” on page 115.

Enterprise-specific traps are developed and supported by a specific equipment manufacturer. If your network contains devices that have enterprise-specific traps, you must obtain them from the manufacturer and compile them into your network management software.

For more information on enterprise-specific traps supported by the JUNOS software, see “Juniper Networks Enterprise-Specific SNMP Traps” on page 107.

For information on system logging severity levels for SNMP traps, see “System Logging Severity Levels for SNMP Traps” on page 23.

SNMP Standards

The following standards documents define SNMP and the standard MIBs supported by the JUNOS software. RFCs can be found at <http://www.ietf.org>.

IEEE, 802.3ad, *Aggregation of Multiple Link Segments*

Only the following are supported:

dot3adAggPortTable, dot3adAggPortListTable, dot3adAggTable, and dot3adAggPortStatsTable

dot3adAggPortDebugTable (only dot3adAggPortDebugRxState, dot3adAggPortDebugMuxState, dot3adAggPortDebugActorSyncTransitionCount, dot3adAggPortDebugPartnerSyncTransitionCount, dot3adAggPortDebugActorChangeCount, and dot3adAggPortDebugPartnerChangeCount)

dot3adTablesLastChanged

RFC 1155, *Structure and Identification of Management Information for TCP/IP-based Internets*

RFC 1157, *A Simple Network Management Protocol (SNMP)*

RFC 1213, *Management Information Base for Network Management of TCP/IP-based Internets: MIB-II* (except for ipRouteTable, which has been replaced by ipCidrRouteTable [RFC 2096])

RFC 1215, *A Convention for Defining Traps for use with the SNMP* (only MIB II SNMP version 1 traps and version 2 notifications)

RFC 1657, *Definitions of Managed Objects for the Fourth Version of the Border Gateway Protocol (BGP-4) using SMIV2*

RFC 1850, *OSPF Version 2 Management Information Base* (except for the ospfOriginateNewLsas and ospfRxNewLsas objects, the Host Table, and the traps ospfOriginateLSA, ospfLsdbOverflow, and ospfLsdbApproachingOverflow)

RFC 1901, *Introduction to Community-based SNMPv2*

RFC 1905, *Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)*

RFC 1907, *Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)*

RFC 2011, *SNMPv2 Management Information Base for the Internet Protocol using SMIV2*

RFC 2012, *SNMPv2 Management Information Base for the Transmission Control Protocol using SMIV2*

RFC 2013, *SNMPv2 Management Information Base for the User Datagram Protocol using SMIV2*

RFC 2096, *IP Forwarding Table MIB*

RFC 2115, *Management Information Base for Frame Relay DTEs Using SMIV2*

RFC 2287, *Definitions of System-Level Managed Objects for Applications* (only sysAppInstallPkgTable, sysAppInstallElmtTable, sysAppElmtRunTable, and sysAppMapTable)

RFC 2465, *Management Information Base for IP Version 6: Textual Conventions and General Group* (except for IPv6 interface statistics)

RFC 2495, *Definitions of Managed Objects for the DS1, E1, DS2, and E2 Interface Types* (except for dsx1FarEndConfigTable, dsx1FarEndCurrentTable, dsx1FarEndIntervalTable, dsx1FarEndTotalTable, and dsx1FracTable)

RFC 2496, *Definitions of Managed Objects for the DS3/E3 Interface Type* (except dsx3FarEndConfigTable, dsx3FarEndCurrentTable, dsx3FarEndIntervalTable, dsx3FarEndTotalTable, and dsx3FracTable)

RFC 2515, *Definitions of Managed Objects for ATM Management* (except atmVpCrossConnectTable, atmVcCrossConnectTable, and aal5VccTable)

RFC 2558, *Definitions of Managed Objects for the SONET/SDH Interface Type*

RFC 2570, *Introduction to Version 3 of the Internet-standard Network Management Framework*

RFC 2571, *An Architecture for Describing SNMP Management Frameworks* (read-only access)

RFC 2572, *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)* (read-only access)

RFC 2576, *Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework*

RFC 2578, *Structure of Management Information Version 2 (SMIPv2)*

RFC 2579, *Textual Conventions for SMIPv2*

RFC 2665, *Definitions of Managed Objects for the Ethernet-like Interface Types*

RFC 2787, *Definitions of Managed Objects for the Virtual Router Redundancy Protocol*

RFC 2790, *Host Resources MIB*

Only the hrStorageTable. The file systems /, /config, /var, and /tmp will always return the same index number. When SNMP restarts, the index numbers for the remaining file systems might change.

Only the objects of the hrSystem and hrSWInstalled groups.

RFC 2819, *Remote Network Monitoring Management Information Base* (the etherStatsTable for Ethernet interfaces only and the objects alarmTable, eventTable, and logTable)

RFC 2863, *The Interfaces Group MIB*

RFC 2925, *Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations* (only the objects pingCtlTable, pingResultsTable, pingProbeHistoryTable, pingMaxConcurrentRequests, traceRouteCtlTable, traceRouteResultsTable, traceRouteProbeHistoryTable, and traceRouteHopsTable)

RFC 2932, *IPv4 Multicast Routing MIB*

RFC 3413, *Simple Network Management Protocol (SNMP) Applications* (except for the proxy MIB)

RFC 3414, *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*

RFC 3415, *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*

Internet draft draft-blumenthal-aes-usm-08.txt, *The AES Cipher Algorithm in the SNMP User-based Security Model*

Internet draft draft-ietf-idr-bgp4-mibv2-03.txt, *Definitions of Managed Objects for the Fourth Version of Border Gateway Protocol (BGP-4), Second Version* (only jnxBgpM2PrefixInPrefixes, jnxBgpM2PrefixInPrefixesAccepted, and jnxBgpM2PrefixInPrefixesRejected objects)

Internet draft draft-reeder-snmpv3-usm-3desede-00.txt, *Extension to the User-Based Security Model (USM) to Support Triple-DES EDE in 'Outside' CBC Mode*

Internet draft draft-ietf-atommib-sonetaps-mib-10.txt, *Definitions of Managed Objects for SONET Linear APS architectures* (as defined under the Juniper Networks enterprise branch only)

Internet draft draft-ietf-idmr-igmp-mib-13.txt, *Internet Group Management Protocol (IGMP) MIB*

Internet Assigned Numbers Authority, *IANAiftype Textual Convention MIB* (referenced by RFC 2233, available at <ftp://ftp.isi.edu/mib/ianaiftype.mib>)

Internet draft draft-ietf-isis-wg-mib-07.txt, *Management Information Base for IS-IS*, (only isisISAdjTable, isisISAdjAreaAddrTable, isisISAdjIPAddrTable, and isisISAdjProtSuppTable)

Internet draft draft-ietf-ppvpn-mpls-vpn-mib-04.txt, *MPLS/BGP Virtual Private Network Management Information Base Using SMIv2* (only mplsVpnScalars, mplsVpnVrfTable, mplsVpnPerTable, and mplsVpnVrfRouteTargetTable)

Internet draft draft-ietf-msdp-mib-07.txt, *Multicast Source Discovery protocol MIB* (except msdpEstablished, msdpBackwardTransition, and msdpRequestsTable)

Internet draft draft-ietf-idmr-pim-mib-09.txt, *Protocol Independent Multicast (PIM) MIB*

ESO Consortium MIB, which can be found at <http://www.snmp.com/eso/>.

JUNOS SNMP Agent Features

The JUNOS SNMP agent software consists of an SNMP master agent that delegates all SNMP requests to subagents. Each subagent is responsible for the support of a specific set of MIBs.

The JUNOS software supports the following versions of SNMP:

SNMPv1—The initial implementation of SNMP that defines the architecture and framework for SNMP.

SNMPv2c—The revised protocol, with improvements to performance and manager-to-manager communications. Specifically, SNMPv2c implements community strings, which act as passwords when determining who, what, and how the SNMP clients can access the data in the SNMP agent. The community string is contained in SNMP Get, GetBulk, GetNext, and Set requests. The agent may require a different community string for Get, GetBulk, and GetNext requests (read-only access) than it does for Set requests (read-write access).

SNMPv3—The most up-to-date protocol focuses on security. SNMPv3 defines a security model, user-based security model (USM), and a view-based access control model (VACM). SNMPv3 USM provides data integrity, data origin authentication, message replay protection, and protection against disclosure of the message payload. SNMPv3 VACM provides access control to determine whether a specific type of access (read or write) to the management information is allowed.

In addition, the JUNOS SNMP agent software accepts IPv4 and IPv6 addresses for transport over IPv4 and IPv6. For IPv6, the JUNOS software supports the following IPv6 over SNMP:

- SNMP data over IPv6 networks

- IPv6-specific MIB data

- SNMP agents for IPv6

System Logging Severity Levels for SNMP Traps

For some traps, when a trap condition occurs, regardless of whether the SNMP agent sends a trap to an NMS, the trap is logged if the system logging is configured to log an event with that system logging severity level. For more information about system logging severity levels, see the *JUNOS System Basics Configuration Guide*.

For more information on system logging severity levels for standard traps, see “Standard SNMP Traps” on page 115. For more information on system logging severity levels for enterprise-specific traps, see “Juniper Networks Enterprise-Specific SNMP Traps” on page 107.

