How To Configure SNMP on IP Appliances

18 May 2011
Important Information

Latest Software
We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.

Latest Documentation
The latest version of this document is at:
http://supportcontent.checkpoint.com/documentation_download?ID=12193
For additional technical information, visit the Check Point Support Center (http://supportcenter.checkpoint.com).

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>25 January 2011</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>

Feedback
Check Point is engaged in a continuous effort to improve its documentation.
Please help us by sending your comments (mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on How To Configure SNMP on IP Appliances).
## Contents

Important Information ................................................................. 3  
How To Configure SNMP on IP Appliances .................................. 5  
   Objective ............................................................................. 5  
   Supported Versions .............................................................. 5  
   Supported OS ...................................................................... 5  
   Supported Appliances ........................................................... 5  
   Related Documentation and Assumed Knowledge ...................... 5  
   Impact on the Environment and Warnings ............................... 5  
SNMP Overview ....................................................................... 6  
   SNMP Terms: ...................................................................... 6  
Enabling and Configuring SNMP .............................................. 7  
Completing the Procedure ....................................................... 14  
Verifying .................................................................................. 15
How To Configure SNMP on IP Appliances

Objective
This guide describes the Check Point IPSO implementation of Simple Network Management Protocol (SNMP) and how to configure it on your IP Appliance system.

Supported Versions
- IPSO 4.2
- IPSO 6.2

Supported OS
- IPSO 4.2
- IPSO 6.2

Supported Appliances
- IP150
- IP260/IP265 (IPSO 4.2 only)
- IP290
- IP390
- IP560
- IP690
- IP1220/IP1260 (IPSO 4.2 only)
- IP1280
- IP2250/IP2255 (IPSO 4.2 only)
- IP2450

Related Documentation and Assumed Knowledge
- IPSO 4.2 and IPSO 6.2 Voyager Reference Guides and Help menu.

Impact on the Environment and Warnings
- n/a.
SNMP Overview

The Simple Network Management Protocol (SNMP) is the Internet standard protocol used to exchange management information between network devices. It is defined by RFC 1157. SNMP works by sending messages, called protocol data units (PDUs), to different parts of a network. SNMP-compliant devices, called agents, store data about themselves in Management Information Bases (MIBs) and return this data to the SNMP requesters.

SNMP operates in the Application Layer of the Internet Protocol Suite (Layer 7 of the OSI model). The SNMP agent receives requests on UDP port 161. The manager may send requests from any available source port to port 161 in the agent. The agent response will be sent back to the source port on the manager. The manager receives notifications (Traps and InformRequests) on port 162. The agent may generate notifications from any available port.

SNMP, as implemented on IPSO platforms, supports the following:

- GetRequest, GetNextRequest, GetBulkRequest, and a select number of traps. The Check Point implementation also supports SetRequest for three attributes only: sysContact, sysLocation, and sysName. You must configure a read-write community string to enable set operations.
- SNMP v1, v2, and v3:
  - Version 1: Initial implementation of the SNMP protocol. Very simple
  - Version 2: Improvements in the areas of performance, security, confidentiality, and manager-to-manager communications
  - Version 3: Primarily added security and remote configuration enhancements to SNMP
    Note - The IPSO implementation of SNMPv3 does not yet support SNMPv3 traps.
- Other public and proprietary MIBs. Both the proprietary MIBs and the public MIBs are supplied with the system. MIBs are text files, and values of MIB data objects are the topic of conversation between Managers and Agents. These files are normally loaded into the SNMP Managers for translations. IPSO uses MIBs that start with .1.3.6.1.4.1.94. To view more detailed information about the MIBs, see the /etc/snmp/mibs directory.

SNMP Terms:

- **Trap**: Notification of an event sent out from a managed device (Agent) when certain types of events occur.
- **MIB**: Stands for Management Information Base and is a collection of information organized hierarchically in a tree structure.
- **OID**: Object Identifiers uniquely identify managed objects in a MIB hierarchy.
- **Community**: An SNMP community is the group that devices and management stations running SNMP belong to. The community name is used to identify the group. A SNMP device or agent may belong to more than one SNMP community. It will not respond to requests from management stations that do not belong to one of its communities. SNMP default communities are:
  - Read-only community string = Public
  - Read-write community string = Private
- **Agent**: SNMP-compliant device that stores data about itself in Management Information Bases (MIBs) and return this data to the SNMP requesters. The SNMP agent implemented in IPSO enables an SNMP manager to monitor the device and to modify the sysName, sysContact and sysLocation objects only.
Enabling and Configuring SNMP

The SNMP daemon is enabled by default. If you choose to use SNMP, configure it according to your network and security requirements. It is recommended disabling SNMP if you do not plan to use it to manage the network.

To enable or disable SNMP:

1. Select SNMP under Configuration in the tree view. Configuration > System Configuration > SNMP
2. Check or uncheck Enable SNMP Daemon checkbox, click Apply. The SNMP configuration options appear.
3. Select the SNMP version to run from the SNMP version drop-down list. You can choose to use all versions of SNMP (v1, v2, and v3) on your system. If your management station supports v3, select to use only v3 on your IPSO system.
   • SNMPv1/v2/v3: Select this option if your management station does not support SNMPv3.
   • SNMPv3: Select this option if your management station supports v3. SNMPv3 provides a higher level of security than v1 or v2.
4. If you selected v1/v2/v3, enter a new read-only community string under Community Strings. This is a basic security precaution that you should always take.
5. Set a read-write community string only if you have reason to enable set operations, only if you enabled SNMPv3 (not v1/v2/v3), and if your network is secure.
6. Click Apply, then click Save to make the changes permanent.

To set an agent address:

An agent address is a specific IP address at which the SNMP agent listens and responds to requests. If you specify one or more agent addresses, the system SNMP agent listens and responds only on those interfaces. If no agent addresses are specified, the SNMP protocol responds to requests from all interfaces. You can use the agent address as another way to limit SNMP access.

1. Select SNMP under Configuration in the tree view.
2. Enter the valid IP address of a configured interface in the Agent New Address field. You can use the IP address of any existing and valid interface.
3. Click Apply and Save. The IP address and a corresponding Delete check box appear.
To configure traps:

Managed devices (Agents) use trap messages to report events to the network management station (NMS). When certain types of events occur, the platform sends a trap to the management station.

Traps or MIBs are defined in text files located in the /etc/snmp/mibs directory:

```bash
IP2450A[admin]# ls /etc/snmp/mibs
AGENTX-MIB.txt
DIAL-CONTROL-MIB.txt
DISMAN-SCHEDULE-MIB.txt
DISMAN-SCRIPT-MIB.txt
ENTITY-MIB.txt
EtherLike-MIB.txt
FRAME-RELAY-DTE-MIB.txt
HCNUM-TC.txt
HOST-RESOURCES-MIB.txt
HOST-RESOURCES-TYPES.txt
IANA-ADDRESS-FAMILY-NUMBERS-MIB.txt
IANA-LANGUAGE-MIB.txt
IANA-RTPROTO-MIB.txt
IANAifType-MIB.txt
IF-INVERTED-STACK-MIB.txt
IF-MIB.txt
INET-ADDRESS-MIB.txt
IP-FORWARD-MIB.txt
IP-MIB.txt
IPV6-ICMP-MIB.txt
IPV6-MIB.txt
IPV6-TC.txt
IPV6-TCP-MIB.txt
IPV6-UDP-MIB.txt
ISDN-MIB.txt
NET-SNMP-AGENT-MIB.txt
NET-SNMP-EXAMPLES-MIB.txt
NET-SNMP-EXTEND-MIB.txt
NET-SNMP-MIB.txt
NET-SNMP-TC.txt
NOKIA-COMMON-MIB-OID-REGISTRATION-MIB.txt
NOKIA-COMMON-NE-ROLE-MIB.txt
NOKIA-ENHANCED-SNMP-SOLUTION-SUITE-ALARM-IRP.txt
NOKIA-ENHANCED-SNMP-SOLUTION-SUITE-COMMON-DEFINITION.txt
NOKIA-ENHANCED-SNMP-SOLUTION-SUITE-PM-COMMON-DEFINITION.txt
NOKIA-ENHANCED-SNMP-SOLUTION-SUITE-PM-IRP.txt
NOKIA-HWM-MIB.txt
NOKIA-IPSO-LBCLUSTER-MIB.txt
NOKIA-IPSO-LINKAGGREGATION-MIB.txt
NOKIA-IPSO-REGISTRATION-MIB.txt
NOKIA-IPSO-SYSTEM-MIB.txt
NOKIA-NE3S-REGISTRATION-MIB.txt
NOKIA-NTP-MIB.txt
NOKIA-OID-REGISTRATION-MIB.txt
NOKIA-RATESHAPE-MIB.txt
NOKIA-UNITTYPES-MIB.txt
NOTIFICATION-LOG-MIB.txt
RFC-1215.txt
RFC1155-SMI.txt
RFC1213-MIB.txt
RIPv2-MIB.txt
RMON-MIB.txt
SMUX-MIB.txt
SNMP-COMMUNITY-MIB.txt
SNMP-FRAMEWORK-MIB.txt
SNMP-MPD-MIB.txt
SNMP-NOTIFICATION-MIB.txt
```
SNMP-PROXY-MIB.txt
SNMP-TARGET-MIB.txt
SNMP-USER-BASED-SM-MIB.txt
SNMP-USM-AES-MIB.txt
SNMP-USM-DH-OBJECTS-MIB.txt
SNMP-VIEW-BASED-ACM-MIB.txt
SNMPv2-CONF.txt
SNMPv2-MIB.txt
SNMPv2-SMI.txt
SNMPv2-TC.txt
SNMPv2-TM.txt
TCP-MIB.txt
TOKENRING-MIB.txt
TRANSPORT-ADDRESS-MIB.txt
TUNNEL-MIB.txt
UDP-MIB.txt
VRRP-MIB.txt

IPSO uses MIBS that start with .1.3.6.1.4.1.94.

Below is a list of types of SNMPv1 and SNMPv2 traps which IPSO supports:

You can click on the Help button to view more detailed information about the traps.

- Enable coldStart traps: A coldStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself and that its configuration might have been altered.
  * Default: Checked.

- Enable linkUp/linkDown traps: Enables/Disables notification that one of the links, which is administratively up, either has come up or been lost.
  * Default: Checked.

- Enable Link Aggregation member active traps: Enables/Disables notification that a link aggregation group member has become active.
  * Default: Unchecked.

- Enable Link Aggregation member inactive traps: Enables/Disables notification that a link aggregation group member has become inactive.
  * Default: Unchecked.

- Enable Authentication traps: Enables/Disables notification that the SNMP message received from the sending entity is not properly authenticated.
  * Default: Unchecked.

- Enable vrrpTrapNewMaster traps: Enables/Disables notification of the VRRP New Master trap.
  * Default: Unchecked.

- Enable vrrpTrapAuthFailure traps: Enables/Disables notification of the VRRP Authentication Failure trap.
  * Default: Unchecked.

- Enable systemTrapConfigurationChange traps: Enables/Disables notification of the System Configuration Change trap.
  * Default: Unchecked.

- Enable systemTrapConfigurationFileChange traps: Enables/Disables notification of the System Configuration File Change trap.
  * Default: Unchecked.

- Enable systemConfigurationSaveChange traps: Enables/Disables notification of the System Configuration Save Change trap.
  * Default: Unchecked.
- Enable systemTrapLowDiskSpace traps: Enables/Disables notification of the System Low Disk Space trap. This trap is sent when the disk utilization, as seen by a non-superuser, in any of the local file systems exceeds 80%. The trap is initially sent within the scan interval (currently 30 seconds), and subsequently at preset intervals, of 15 minutes, until the disk utilization falls below 80%.
  * Default: Unchecked.

- Enable systemTrapNoDiskSpace traps: Enables/Disables notification of the System No Disk Space trap. This trap is sent when the disk utilization, as seen by a non-superuser, in any of the local file systems exceeds 98%. The trap is initially sent within the scan interval (currently 30 seconds), and subsequently at preset intervals, of 15 minutes, until the disk utilization falls below 98%.
  * Default: Unchecked.

- Enable systemTrapDiskFailure traps: Enables/Disables notification of the System Disk Failure trap. This trap is sent when a particular disk drive has failed, that is, there is no response from the disk for read/write operations.
  * Default: Unchecked.

- Enable systemTrapDiskMirrorSetCreate traps: Enables/Disables notification of the System Disk Mirror Set Create trap. This trap is sent when a particular mirror set has been created on the system.
  * Default: Unchecked.

- Enable systemTrapDiskMirrorSetDelete traps: Enables/Disables notification of the System Disk Mirror Set Delete trap. This trap is sent when a particular mirror set has been deleted from the system.
  * Default: Unchecked.

- Enable systemTrapDiskMirrorSyncSuccess traps: Enables/Disables notification of the System Disk Mirror Sync Success trap. This trap is sent when a particular mirror set has been successfully synced.
  * Default: Unchecked.

- Enable clusterMemberReject traps: Enables/Disables notification of a join request rejected by the cluster. This trap is sent when a node is trying to join and is rejected by the cluster.
  * Default: Unchecked.

- Enable clusterMemberJoin traps: Enables/Disables notification of a node joining the cluster. This trap is sent when a node joins the cluster.
  * Default: Unchecked.

- Enable clusterMemberLeft traps: Enables/Disables notification of a member leaving the cluster. This trap is sent when a member leaves the cluster.
  * Default: Unchecked.

- Enable clusterNewMaster traps: Enables/Disables notification of a new master elected by the cluster. This trap is sent when a new master is elected in the cluster.
  * Default: Unchecked.

  * Default: Unchecked.

- Enable systemPowerSupplyFailure traps: This trap is sent at an interval of 60 seconds when a power supply for the system fails. For the 2250, this trap is also sent if one of the power supplies is switched off. This trap includes the power supply index and is supported only on platforms with two power supplies installed and running.
  * Default: Unchecked.

- Enable systemFanFailure traps: This trap is sent at an interval of 60 seconds when a CPU or chassis fan fails. This trap includes the fan index.
  * Default: Unchecked.

- Enable systemOverTemperature traps: This trap is sent at an interval of 60 seconds when the temperature sensor detects that the temperature of the system has exceeded the threshold.
  * Default: Unchecked.
- Enable systemSnmpProcessShutdown traps: This trap is sent for notification of snmp process shutdown.
  * Default: Unchecked.

- Enable systemLowVoltage traps: This trap is sent at an interval of 60 seconds when the voltage sensor detects that the voltage of the system has fallen below low limit.
  * Default: Unchecked.

- Enable systemHighVoltage traps: This trap is sent at an interval of 60 seconds when the voltage sensor detects that the voltage of the system has exceeded the maximum limit.
  * Default: Unchecked.

**To enable or disable traps:**

1. Select SNMP under Configuration in the tree view.
2. To enable any type of trap, place a check next to the name of the trap and click Apply.
3. To disable any type of trap, uncheck the name of the trap and click Apply.
4. Click Save to make the changes permanent.

**To configure trap receivers:**

You must specify the network management station (NMS) that accepts traps from your appliance, and the community string used on your management station (receiver) to control access.

1. Select SNMP under Configuration in the tree view.
2. Enter the IP address (or the hostname if DNS is set) of a receiver in the Add New Trap Receiver text field.
3. Enter the community string for the specified receiver in the Community String for new Trap Receiver field.
4. Select the Trap SNMP Version for the trap receiver in the drop-down menu.
5. Click Apply and Save.

To set the Trap PDU Agent Address

1. Select SNMP under Configuration in the tree view.
2. To specify the IP address to be used for sent trap PDU, enter the IP address in the Trap PDU Agent Address field.
3. Click Apply and Save to make your changes permanent.
Completing the Procedure

Your IPSO appliance is now configured for SNMP. As an option, you may configure location and contact information to provide information to the management system about where your device is located and who to contact about it.

To configure location and contact information

1. Select SNMP under Configuration in the tree view.
2. In the SNMP Location String text field, enter the actual location of the device. Click Apply.
3. In the SNMP Contact String text field, enter the name of department or person who has administrative responsibility for the device.
4. Click Apply and Save to make your changes permanent.
Verifying

- To verify SNMP is running on your IPSO platform, the snmpd process should be running:

  ```
  IP2450A[admin]# ps auxw | grep snmpd
  root 27169  0.0  0.2  7636  5288  ??  Ss    6:18PM   0:01.22 /bin/snmpd –f
  ```

- To verify the IP appliance is sending the appropriate trap to the management station when a type of event occurs, you can run tcpdump capture on the specified Agent Address interface:

  ```
  IP2450A[admin]# tcpdump -v -i eth-s4p1c0 -s 256 -l udp and port 162
  tcpdump: listening on eth-s4p1c0, link-type EN10MB (Ethernet), capture size 256 bytes
  10:29:56.081885  O IP (tos 0x0, ttl  64, id 7202, offset 0, flags [none], proto: UDP (17), length: 150) IP2450A.63021 > 172.26.127.99.snmptrap: { SNMPv2c { V2Trap(107) R=1161396139 system.sysUpTime.0=307062 S:1.1.4.1.0=E:nokia.1.21.1.8.0 S:1.1.4.1.0=E:nokia.1.21.1.0.13 E:nokia.1.21.3.1.1.1.2=2 } }
  10:30:56.317446  O IP (tos 0x0, ttl  64, id 7310, offset 0, flags [none], proto: UDP (17), length: 150) IP2450A.63021 > 172.26.127.99.snmptrap: { SNMPv2c { V2Trap(107) R=1161396140 system.sysUpTime.0=313085 S:1.1.4.1.0=E:nokia.1.21.1.8.0 S:1.1.4.1.0=E:nokia.1.21.1.0.13 E:nokia.1.21.3.1.1.1.2=2 } }
  10:31:56.481701  O IP (tos 0x0, ttl  64, id 7420, offset 0, flags [none], proto: UDP (17), length: 150) IP2450A.63021 > 172.26.127.99.snmptrap: { SNMPv2c { V2Trap(107) R=1161396141 system.sysUpTime.0=319101 S:1.1.4.1.0=E:nokia.1.21.1.8.0 S:1.1.4.1.0=E:nokia.1.21.1.0.13 E:nokia.1.21.3.1.1.1.2=2 } }
  10:32:56.564580  O IP (tos 0x0, ttl  64, id 7530, offset 0, flags [none], proto: UDP (17), length: 150) IP2450A.63021 > 172.26.127.99.snmptrap: { SNMPv2c { V2Trap(107) R=1161396142 system.sysUpTime.0=325109 S:1.1.4.1.0=E:nokia.1.21.1.8.0 S:1.1.4.1.0=E:nokia.1.21.1.0.13 E:nokia.1.21.3.1.1.1.2=2 } }
  10:33:56.583095  O IP (tos 0x0, ttl  64, id 7638, offset 0, flags [none], proto: UDP (17), length: 150) IP2450A.63021 > 172.26.127.99.snmptrap: { SNMPv2c { V2Trap(107) R=1161396143 system.sysUpTime.0=331111 S:1.1.4.1.0=E:nokia.1.21.1.8.0 S:1.1.4.1.0=E:nokia.1.21.1.0.13 E:nokia.1.21.3.1.1.1.2=2 } }
  10:34:56.952555  O IP (tos 0x0, ttl  64, id 7744, offset 0, flags [none], proto: UDP (17), length: 150) IP2450A.63021 > 172.26.127.99.snmptrap: { SNMPv2c { V2Trap(107) R=1161396144 system.sysUpTime.0=337148 S:1.1.4.1.0=E:nokia.1.21.1.8.0 S:1.1.4.1.0=E:nokia.1.21.1.0.13 E:nokia.1.21.3.1.1.1.2=2 } }
  10:35:57.277279  O IP (tos 0x0, ttl  64, id 7852, offset 0, flags [none], proto: UDP (17), length: 150) IP2450A.63021 > 172.26.127.99.snmptrap: { SNMPv2c { V2Trap(107) R=1161396145 system.sysUpTime.0=343181 S:1.1.4.1.0=E:nokia.1.21.1.8.0 S:1.1.4.1.0=E:nokia.1.21.1.0.13 E:nokia.1.21.3.1.1.1.2=2 } }
  10:36:57.552318  O IP (tos 0x0, ttl  64, id 7963, offset 0, flags [none], proto: UDP (17), length: 150) IP2450A.63021 > 172.26.127.99.snmptrap: { SNMPv2c { V2Trap(107) R=1161396146 system.sysUpTime.0=349208 S:1.1.4.1.0=E:nokia.1.21.1.8.0 S:1.1.4.1.0=E:nokia.1.21.1.0.13 E:nokia.1.21.3.1.1.1.2=2 } }
  10:37:57.771046  O IP (tos 0x0, ttl  64, id 8065, offset 0, flags [none], proto: UDP (17), length: 150) IP2450A.63021 > 172.26.127.99.snmptrap: { SNMPv2c { V2Trap(107) R=1161396147 system.sysUpTime.0=355230 S:1.1.4.1.0=E:nokia.1.21.1.8.0 S:1.1.4.1.0=E:nokia.1.21.1.0.13 E:nokia.1.21.3.1.1.1.2=2 } }
  ```

  In the above example, we have verified the IP2450 appliance (with dual power supplies) is sending power supply failure trap every 60 seconds to NMS server 172.26.127.99 after we enabled systemPowerSupplyFailure trap and unplugged Power Supply B as a test.

  `nokia.1.21.1.3.1.1.1` is the oid address for ipsoPowerSupplyIndex

- Use the command 'snmpwalk' to query the agent for a tree of information about a network entity.

  A variable may also be given on the command line. This variable specifies which portion of the object identifier space will be searched using GET NEXT requests. All variables in the subtree below the given variable are queried and their values presented to the user. Each variable name is given in the format specified in variables.
Example for System details that includes uptime:

```
ip260[admin]# snmpwalk localhost public .1.3.6.1.2.1.25.1
host.hrSystem.hrSystemUptime.0 = Timeticks: (155953200) 18 days, 1:12:12.00
host.hrSystem.hrSystemDate.0 = 2010-5-4,13:14:25.0,+0:0
host.hrSystem.hrSystemInitialLoadDevice.0 = 3
host.hrSystem.hrSystemInitialLoadParameters.0 = "/config/active"
host.hrSystem.hrSystemNumUsers.0 = Gauge: 3
host.hrSystem.hrSystemProcesses.0 = Gauge: 64
host.hrSystem.hrSystemMaxProcesses.0 = 2048
```

You can choose to be more granular on the OID:

```
ip260[admin]# snmpwalk localhost public .1.3.6.1.2.1.25.1.1
host.hrSystem.hrSystemUptime.0 = Timeticks: (155955600) 18 days, 1:12:36.00
```

You can see that the appliance has been up for 18 days.

- **snmpget** is an SNMP command that uses the GET request to query for information on a network entity. One or more fully qualified object identifiers may be given as arguments on the command line.

```
ip260[admin]# snmpget localhost public .1.3.6.1.2.1.1.1.0
system.sysDescr.0 = IP260 rev 1, IPSO ip260 4.2-BUILD110 releng 1515 04.07.2010-182037 i386
```

- **snmpbulkwalk** is an SNMP application that uses BULK Requests to query for a tree of information about a network entity. As its name implies, snmpbulkwalk utilizes the SNMP GETBULK message, which is not available in SNMPv1.

A variable may also be given on the command line. This variable specifies which portion of the object identifier space will be searched using BULK requests. All variables in the subtree below the given variable are queried as a single request and their values presented to the user. Each variable name is given in the format specified in variables.

If the OID argument is not present, snmpbulkwalk will search MIB-2.

```
ip260[admin]# snmpbulkwalk -v 2c localhost public system
```

```
system.sysOrTable.sysOEntry.sysORDescr.3 = The MIB for Message Processing and Dispatching.
system.sysOrTable.sysOEntry.sysORDescr.4 = The management information definitions for the SNMP User-based Security Model.
system.sysOrTable.sysOEntry.sysORDescr.5 = View-based Access Control Model for SNMP.
system.sysOrTable.sysOEntry.sysORUpTime.1 = Timeticks: (3) 0:00:00.03
system.sysOrTable.sysOEntry.sysORUpTime.2 = Timeticks: (3) 0:00:00.03
system.sysOrTable.sysOEntry.sysORUpTime.3 = Timeticks: (3) 0:00:00.03
system.sysOrTable.sysOEntry.sysORUpTime.4 = Timeticks: (3) 0:00:00.03
system.sysOrTable.sysOEntry.sysORUpTime.5 = Timeticks: (332) 0:00:03.32
```

- **snmptranslate** is an SNMP application that uses to translate OID values to meaningful textual names and sensible format values. This is the one tool which can be used standalone, simply displays information drawn from the MIB files themselves.

In its simplest form, snmptranslate takes a numeric OID and displays the corresponding textual MIB name. This uses the -On flag:

```
ip260[admin]# snmptranslate -On .1.3.6.1.2.1.1.3.0
system.sysUpTime.0
```

It can also perform the reverse translation, taking the textual MIB name and displaying the numeric OID.

```
ip260[admin]# snmptranslate SNMPv2-MIB::sysUpTime.0 .1.3.6.1.2.1.1.3.0
```