Introduction

- Designed in 1987 by Internet Engineering Task Force (IETF) to send and receive management and status information across networks
- Most widely used network management protocol on IP networks
- Designed to be simple, easy to implement and consume minimal processor and network resources.
Overview

- Request/response protocol, management information moves between "SNMP managers" and "SNMP agents"
- Information defined by a set of managed objects: "Management Information Base" (MIB).
- Network Management Station (NMS) application collects status, configuration, and performance information from "Network Elements" with "SNMP agents"
- Example: HP openView on a server (NMS) collects performance information from a Crisco router (agent)
- SNMP Versions 1, 2c, 3
PDU: Protocol Data Unit, used by SNMP when transferring data between two protocol stacks.

Port n, m: Where n or m is typically port 161: However this is a user definable value. Note that port 162 is the default port for a network management station to receive traps.
Use UDP

- Faster than TCP, no need to initiate connection before sending data.
- Minimal use of network bandwidth: no re-send, no polling of destination address
- Less reliable
# SNMP Commands

<table>
<thead>
<tr>
<th>Operation</th>
<th>PDU</th>
<th>Comment</th>
<th>Flow</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get</td>
<td>GetRequest</td>
<td>Contains the values of the requested object instances.</td>
<td>M-&gt;A</td>
</tr>
<tr>
<td></td>
<td>GetResponse</td>
<td>Retrieves a variable on an SNMP agent.</td>
<td>A-&gt;M</td>
</tr>
<tr>
<td>Set</td>
<td>SetRequest</td>
<td>Sets a variable on an SNMP agent.</td>
<td>M-&gt;A</td>
</tr>
<tr>
<td></td>
<td>GetResponse</td>
<td>Contains the error status of SetRequest.</td>
<td>A-&gt;M</td>
</tr>
<tr>
<td>Trap</td>
<td>Trap</td>
<td>Signals the occurrence of an unexpected event.</td>
<td>A-&gt;M</td>
</tr>
<tr>
<td>Getnext</td>
<td>GetNextRequest</td>
<td>Retrieves object instances.</td>
<td>M-&gt;A</td>
</tr>
<tr>
<td></td>
<td>GetResponse</td>
<td>Contains the values of object instances.</td>
<td>M-&gt;A</td>
</tr>
</tbody>
</table>

get-bulk (SNMPv2 and SNMPv3)
"Structure of Management Information" SMI

• The name - object identifier (OID), uniquely defines a managed object.
• The type - defined using Abstract Syntax Notation One (ASN.1) : INTEGER, "OCTET STRING" , TimeTicks etc.
The MIB tree

Online SNMP Object Navigator from Cisco

MIB Variables

- Scalar - an object with a single representation

- Tabular - an object with multiple representations depending on "index"
A closer look on one variable

Name: wmtsChassisDescr

Object IDentifier / OID: 1.3.6.1.4.1.3066.2.2.2.1.1.1.1.1

Full path:


Base syntax: OCTET STRING

Max access: read-only

Description: A textual description of the chassis.
# MIB-II (RFC 1213)

<table>
<thead>
<tr>
<th>Subtree Name</th>
<th>OID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>system</td>
<td>1.3.6.1.2.1.1</td>
<td>Defines a list of objects that pertain to system operation, such as the system uptime, system contact, and system name.</td>
</tr>
<tr>
<td>interfaces</td>
<td>1.3.6.1.2.1.2</td>
<td>Keeps track of the status of each interface on a managed entity. The <em>interfaces</em> group monitors which interfaces are up or down and tracks such things as octets sent and received, errors and discards, etc.</td>
</tr>
</tbody>
</table>

See example: [RFC1213-MIB.txt]( RFC1213-MIB.txt)
SNMP Walk

Start at the root and walk down walk_example.txt
SNMP Set

• Change the value of one or more variables
• Requires “Set Community”
• Configuring devices using SNMP is hard
• Complex device configuration is typically done using CLI or configuration files
• Emerging IETF standard for configuration uses “Web-Services” NETCONF

http://www.ops.ietf.org/netconf/
Traps / Notifications

- Initiated by the agent (Network Element)
- Unusually to port 162
- Example:

  Name: wmtsWmuRegistrationComplete
  Type: NOTIFICATION-TYPE
  OID: 1.3.6.1.4.1.3066.2.2.1.2.0.31
  Module: VYYO-WMTS21-30-MIB
  Objects: 1: trapText
  2: docsIfCmtsCmStatusIndex
  3: docsIfCmtsCmStatusMacAddress
  4: docsIfCmtsCmStatusIpAddress
  Description: WMU registration successfully completed.
NET-SNMP

- Used to be UCD SNMP
- Included in most Linux distributions
- snmpget
- snmpwalk
- snmpset
- More: http://www.net-snmp.org/
NET-SNMP snmpget, snmpset

[root@nmsLinux zeev]# snmpget -v 1 -c zzzzzzzzzz 10.200.1.100 system.sysContact.0
SNMPv2-MIB::sysContact.0 = STRING: Sys Admin
[root@nmsLinux zeev]# snmpset -v 1 -c zzzzzzzzzz 10.200.1.100 system.sysContact.0 s "Zeev Home"
SNMPv2-MIB::sysContact.0 = STRING: Zeev Home
[root@nmsLinux zeev]# snmpget -v 1 -c zzzzzzzzzz 10.200.1.100 system.sysContact.0
SNMPv2-MIB::sysContact.0 = STRING: Zeev Home
NET-SNMP snmpwalk

[root@nmsLinux zeev]# snmpwalk -v 1 -c zzzzzzzzz 10.200.1.100 1.3.6.1.2.1.10.127.1.3.1
SNMPv2-SMI::transmission.127.1.3.3.1.1.2.1 = Hex-STRING: 00 10 3D 12 7D FA
SNMPv2-SMI::transmission.127.1.3.3.1.3.1 = IpAddress: 0.0.0.0
SNMPv2-SMI::transmission.127.1.3.3.1.4.1 = INTEGER: 2
SNMPv2-SMI::transmission.127.1.3.3.1.5.1 = INTEGER: 34
SNMPv2-SMI::transmission.127.1.3.3.1.6.1 = INTEGER: 0
SNMPv2-SMI::transmission.127.1.3.3.1.7.1 = Gauge32: 0
SNMPv2-SMI::transmission.127.1.3.3.1.8.1 = ""
SNMPv2-SMI::transmission.127.1.3.3.1.9.1 = INTEGER: 4
snmpd

Steps (RedHat)

1. Create /etc/snmp/snmpd.conf using snmpconf
   
   rwuser zeev
   rwcommunity zeev
   disk / 1000
   agentaddress 161
   syscontact Zeev Halevi

2. service snmpd restart
Example: Monitor disk usage

```
[root@nmsLinux snmp]# snmptable -v 1 -c zeev localhost hrStorageTable
SNMP table: HOST-RESOURCES-MIB::hrStorageTable

<table>
<thead>
<tr>
<th>hrStorageIndex</th>
<th>hrStorageType</th>
<th>hrStorageDescr</th>
<th>hrStorageSize</th>
<th>hrStorageUsed</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>HOST-RESOURCES-TYPES::hrStorageFixedDisk</td>
<td>/</td>
<td>4747707</td>
<td>1497931</td>
</tr>
<tr>
<td>2</td>
<td>HOST-RESOURCES-TYPES::hrStorageFixedDisk</td>
<td>/proc/bus/usb</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>HOST-RESOURCES-TYPES::hrStorageFixedDisk</td>
<td>/boot</td>
<td>101089</td>
<td>9380</td>
</tr>
<tr>
<td>4</td>
<td>HOST-RESOURCES-TYPES::hrStorageFixedDisk</td>
<td>/dev/pts</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>HOST-RESOURCES-TYPES::hrStorageFixedDisk</td>
<td>/dev/shm</td>
<td>64241</td>
<td>0</td>
</tr>
<tr>
<td>101</td>
<td>HOST-RESOURCES-TYPES::hrStorageRam</td>
<td>Real Memory</td>
<td>513932</td>
<td>396632</td>
</tr>
<tr>
<td>102</td>
<td>HOST-RESOURCES-TYPES::hrStorageVirtualMemory</td>
<td>Swap Space</td>
<td>522104</td>
<td>0</td>
</tr>
<tr>
<td>103</td>
<td>HOST-RESOURCES-TYPES::hrStorageOther</td>
<td>Memory Buffers</td>
<td>?</td>
<td>?</td>
</tr>
</tbody>
</table>
```
MRTG

- "Multi Router Traffic Grapher" (MRTG) - monitor traffic load on network-links.
- MRTG generates trend-analysis HTML pages with live visual representation of this traffic.
- Using Perl, GNU license.
- http://people.ee.ethz.ch/~oetiker/webtools/mrtg/
- Example: mrtg_example.htm
- Interface types are defined in MIB-II (RFV 1213)
RRDTool

- From MRTG a new project was born: RRDTool, a tool that maintains "round robin databases" (RRDs) for time-series data.
  - example 1 weather monitoring
  - Example 2 laptop monitoring
  - http://people.ee.ethz.ch/~oetiker/webtools/rrdtool/
Other tools

• MIB Browser: tkmib from NET-SNMP
• libsmi, an open source MIB parser library: http://www.ibr.cs.tu-bs.de/projects/libsmi/
Security considerations

- SNMPv1 and SNMPv2 use "communities"
- SNMPv3 added cryptographic security
- Vulnerabilities in Many Implementations of SNMP:
  http://www.cert.org/advisories/CA-2002-03.html
Other Service Monitoring tools

• Nagios: host, service and network monitoring  http://www.nagios.org/

• Sysmon - service monitoring
  http://www.sysmon.org/
Measurement/Monitoring tools

• CAIDA Measurement and Analysis Tools
  • http://www.caida.org/tools/measurement/
• Network Monitoring Tools
  • http://www.slac.stanford.edu/xorg/nmtf/nmtf-tools.html
Standards

• Apparently SNMP is not so simple – see the list of related RFCs snmp_rfc.txt