MANAGEMENT PROTOCOL
Elkaf Rahmawan Pramudya, M.Kom

Competencies

- Name the most common management protocols
- Understand how they are positioned and what their most important distinguishing characteristics are
- Explain management primitives and protocol message structure used with SNMP
- Grasp the reasons for the enormous popularity of the command-line interface (CLI), while appreciating some of the challenges faced by management applications that use it
- Understand how syslog works
- Explain the use of Netflow and IP Flow Information Export (IPFIX)
- Describe the latest trend in management protocols, Netconf

SNMP
Simple Network Management Protocol

- SNMP, an application layer protocol, facilitates the exchange of management information among network devices, such as nodes and routers. It comprises part of the TCP/IP suite. System administrators can remotely manage network performance, find and solve network problems, and plan for network growth by using SNMP

- Devices that typically support SNMP include routers, switches, servers, workstations, printers, modem racks and more.
- Used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention.
- Consists of a set of standards for network management, including an application layer protocol, a database schema, and a set of data objects.
SNMP Simple Network Management Protocol

SNMP Basic Commands

- **Read**: monitor managed devices
- **Write**: control (change variable value of) managed devices
- **Trap**: asynchronously report events to the NMS.
  - when types of events occur, agent device sends a trap NMS
- **Traversal operations**: determine which variables a managed device supports
  - sequentially gather information in variable tables, eg: routing table.

SNMP versions

<table>
<thead>
<tr>
<th>Function</th>
<th>SNMPv1</th>
<th>SNMPv2c</th>
<th>SNMPv3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trap</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>GET</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SET</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Inform</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Secure Encryption</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

SNMPv1
- lacking in security and delivery guarantees
- easy to implement

SNMPv2c
- lacking in security
- Inform command. Unlike Traps, which are simply received by a manager, Informs are positively acknowledged with a response message. If a manager does not reply to an Inform, the SNMP agent will resend the Inform.
- improved error handling
- improved SET commands

SNMP V3
- Authentication—Verifying that the request comes from a genuine source.
- Privacy—Encrypting data.
- Authorization—Verifying that the user allows the requested operation.
- Access control—Verifying that the user has access to the objects that are requested.
SNMP: Simple Network Management Protocol

SNMP operations format

<table>
<thead>
<tr>
<th>Operation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>get-request</td>
<td>Retrieve a value from a specific variable.</td>
</tr>
<tr>
<td>.next request</td>
<td>Retrieve the value following the named variable. Often used to retrieve variables from within a table. This operation is an SNMP manager's request to get the name of the named variable from the MIB.</td>
</tr>
</tbody>
</table>
| Get-response  | Reply to a get-request, .next request, get-bulk request, and set-request that can result in.
| Get-bulk request | Fill the get-response with up to max-repetition number of get-next interactions, similar to get-next-request. |
| Set-request   | Store a value in a specific variable.            |
| Traps         | Sent by an SNMP agent to an SNMP manager to indicate that some event occurred. |

How SNMP works

SNMP is an IETF UDP based network protocol to manage network attached devices, formally named managed devices, from remote network management systems (NMS).

- Managed device software component, supporting the protocol, formally called agent, is public through UDP port 161 and allows NMSs:
  - Setting data to managed devices.
  - Getting data from managed devices.
  - Receiving events from managed devices.
SNMP uses one or more administrative computers, managers, have the task of monitoring or managing a group of hosts or devices on a computer network. Each managed system executes, at all times, a software component called an agent which reports information via SNMP to the manager.

There are two ways to convey MIB info, commands:
- request/response mode
- trap mode
Alternative Protocol

CLI (Command Line Interface)

- Help functions (typing a ? behind a command to display the list of available command options)
- Auto-completion (needing to type only the first few characters of a command or option that make it unique, and using the Tab key to tell the system to fill in the rest)
- Prompts (enabling you to enter different command modes, and reminding you of that mode by the form that the prompt takes)

Example CLI: Configuring an Interface

Linux

```
# mode: hw/sysconfig/network-scripts/ifcfg-eth0
# Intel Corporation 82573EB Gigabit Ethernet Controller (Copper)
DEVICE=eth0
BOOTPROTO=static
DHCPCLASS=default
ONBOOT=1
IPADDR=192.168.1.10
NETMASK=255.255.255.0
DEFAULT=eth0
```
Use of CLI as a Management Protocol

CLI is not a management protocol at all. It is a command-line interface. However, management applications face the problem of how to access certain management functionality at the device. In many cases, not all features are covered through SNMP or other management interfaces. This requires applications (as well as operator-defined management scripts, subsumed in our discussion under management applications) to fall back on what is available, which is generally CLI.

show Management Information Displayed in Table Format

**syslog Overview**

**syslog** - to write system messages to a log file

example of a syslog message:

172.16.209.130 000024: *Apr 12 18:01:55.643: % ENV_MON-1-SHUTDOWN: Environmental monitor initiated shutdown

01:14:11: %IPPHONE-6-REG_ALARM: 25: Name=SEP003094C38724 Load=3.2(2.9) Last=Initialized

**syslog Message Structure According to IETF**

<table>
<thead>
<tr>
<th>Header</th>
<th>Structured Data</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>Message Type</td>
<td>Time Sync</td>
</tr>
<tr>
<td>ID</td>
<td>Format</td>
<td>Length</td>
</tr>
</tbody>
</table>
syslog

Summarizing

Bibliography

- Alexander Clemm, Ph.D., *Network Management Fundamentals*, Copyright© 2007 Cisco Systems, Inc., Cisco Press 800 East 96th Street Indianapolis, IN 46240 USA
- http://monitoringtt.blogspot.com/2010/05/snmp-for-dummies-protocol.html
- http://medusa.sisdu.edu/network/CCS96Lectures/1b23_SNMP.pdf