SNMP Protocol for Easy Network Management

Contents

- Introduction
- How to Set Up SNMP
- SNMP Trap
- What Information Does ACTi SNMP Offer
- The Theory of SNMP
- Reference

Introduction

Have you ever met difficulties in managing network devices?

When the number of video cameras in the site grows bigger, there is a need for easy and organized network management by software.

In such cases, if your customer tells you the network management server is full of traffic load and some cameras on site have unstable video quality, you don’t have to go there to check lots of cameras one-by-one and try to bring it back to connection. You just need to use SNMP (Simple Network Management Protocol) management software to connect to cameras to get fast and accurate analysis, such as network traffic load, the number of delivery/receive/error packets and logs on third party connections to cameras. This makes finding out the root cause much easier and helps to speed up problem resolution.

SNMP provides an easy way to manage network devices. The main features are:

1. Monitoring device uptime.
2. System detail description. (Ex: model name, model description and firmware version.)
3. Collect interface information. (Ex: MAC address, interface speed, local port.)
To use SNMP, just enable SNMP function in ACTi devices (SNMP agents) and run SNMP management software in server (NMS: Network Management Station) to connect with the devices. In the next section, we will introduce the step-by-step procedure to set up the basic SNMP support.

*About NMS and SNMP agent, please refer The Theory of SNMP for detail.

How to Set Up SNMP

Search ACTi Devices
You can use the IP-Utility to find out and connect the cameras to your local network. The IP-Utility tool program can be downloaded from ACTi website. As an example, a TCM-7011 is listed here with the IP address 10.1.1.125. Click on it to launch the Web Configurator.

After login, follow the steps below to set up SNMP function. There are two product lines for ACTi, ACM and TCM series. We will first show you how to enable SNMP then guide you through its detail settings.

Enable SNMP for ACTi Devices
- ACM series/ACD-2100 (Firmware version V3.12.15 or above)
  Go to “Setup” → SNMP Setting → Enable
  Selecting SNMP versions will be described in later sections.

---

About NMS and SNMP agent, please refer The Theory of SNMP for detail.
• TCM series/TCD-2100/TCD-2500 (Firmware version V4.07.15 or above)
  Go to “Setup” → Network → SNMP Setting → Enable
  Selecting SNMP versions will be described in later sections.

Configuring SNMP Setting
ACTi’s SNMP agent supports versions V1, V2 and V3. SNMP V1 is the initial implementation of SNMP. SNMP V2 is proposed to enhance the performance of management, such as the communication of server and devices, the confirmation of information delivery and receipt. Primary additions in SNMP V3 concern security and remote configuration enhancements.

• SNMP V1/V2:
  SNMP V1/V2 uses “Community” name as password to authenticate identity. “Read Community” is the password for server to get information from devices. “Write Community” is the password for server to edit values on devices. The default is “public” for Read Community and “write” for Write Community. Of course, you can set any other password as your read/write community.

You can enable V1, V2 or both. Click “Apply” after you’ve completed setup.
SNMP V3:
The security method of SNMP V3 uses account/password for authentication. “Security Name” is the account name to be used with your “Password”. The default security name is “public” and the password must be at least 8 characters long. You also can set any other security name or password. Click “Apply” after you’ve completed setup.

SNMP function is now enabled. Next, we will install and run the SNMP management software on computer server.

SNMP Management Software
In this sample we use a SNMP management software called “iReasoning” to demonstrate how to manage your network via SNMP.

Go to [http://www.ireasoning.com/downloadmibbrowserlicense.shtml](http://www.ireasoning.com/downloadmibbrowserlicense.shtml) for download. In browser and press “I Accept” after reading the agreement. You will be automatically redirected to download page.
Download the “setup.exe” for Windows and install it.

After installation, you can see the icon on windows desktop.

Double Click the icon to show the user interface.

ACTi SNMP support MIBII* (Management Information Base) standard, which is defined by RFC-1213*. After loading RFC1213-MIB into the management software, MIBII information groups** will show in SNMP MIB Tree. Please see next page for detailed steps.

*About MIBII and RFC-1213, please refer The Theory of SNMP and Reference for detail.
** MIBII uses different groups to define different information. About MIBII information groups, please refer [What Information Does ACTi SNMP Offer](#) for detail.

File → Load MIBs → RFC1213-MIB.
Type the IP address of ACTi device and press “Advanced” to set the advanced setting.

Type the “Read/Write Community” and choose SNMP Version as same as the SNMP setting in ACTi devices. (Default is “public” for read and “write” for write on version1 and version2). Then, press OK.

Press “Go” in main page to connect with ACTi devices. It will show the simple system description in result table once the connection is successful.
We have now completed management software setup.
Go to “Get Subtree” of these MIB groups to see the detailed information of ACTi devices via SNMP.

**SNMP Trap**

SNMP traps enable notifications from devices. Devices may send message to the management server whenever significant events occur such as cold start, warm start and authentication failure. The manager will get the information immediately and take action if necessary.

**Cold start** means device reboot by power disconnection. **Warm start** means device reboot by firmware without power disconnection. If there other parties attempt to connect to the device with wrong security password under SNMP V1, V2 or V3 setting, the device will send an **authentication failure** message to the management server.

To enable SNMP Trap function in ACTi devices, type the IP address of the computer running the SNMP management software and type trap community as password to allow server to get trap message from device (Default is public). Select available traps and click “Apply”.

![SNMP Trap Configuration](image)
Steps to use SNMP trap from the management server:

In iReasoning MIB Browser, Tools → Trap Receiver

While ACTi devices encounter cold starts, warm starts or authentication failures, SNMP management software will get notification message in the Trap Receiver table.
**What Information Does ACTi SNMP Offer**

ACTi SNMP supports MIBII standard as defined by RFC1213. MIBII uses different groups to define different information. Available information types are shown in the table below following MIB II standard.

*About MIBII and RFC-1213, please refer [The Theory of SNMP](#) and [Reference](#) for detail.*

<table>
<thead>
<tr>
<th>Group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>Provide general information about the managed device.</td>
</tr>
<tr>
<td></td>
<td><em>Ex: system description, system name.</em></td>
</tr>
<tr>
<td>Interface</td>
<td>Provide general information from the physical interfaces.</td>
</tr>
<tr>
<td></td>
<td><em>Ex: interface speed, MAC address.</em></td>
</tr>
<tr>
<td>Address-Translation</td>
<td>Provide information about the mapping between network addresses and physical addresses for each physical interface</td>
</tr>
<tr>
<td></td>
<td><em>Ex: The IP/MAC addresses to connect to the managed device.</em></td>
</tr>
<tr>
<td>IP</td>
<td>Provide the status and operation of Network Layer (Layer 3).</td>
</tr>
<tr>
<td></td>
<td><em>Ex: the information and traffic flow of received/delivered package.</em></td>
</tr>
<tr>
<td>ICMP</td>
<td>Provide the status and statistics of ICMP.</td>
</tr>
<tr>
<td></td>
<td><em>Ex: amount of receive/error message of ICMP.</em></td>
</tr>
<tr>
<td>TCP</td>
<td>Provide the status and operation of Transport Layer (Layer 4) using TCP protocol.</td>
</tr>
<tr>
<td></td>
<td><em>Ex: TCP Local Port, incoming/outgoing TCP segments.</em></td>
</tr>
<tr>
<td>UDP</td>
<td>Provide the status and operation of Transport Layer (Layer 4) using UDP protocol.</td>
</tr>
<tr>
<td></td>
<td><em>Ex: UDP Local Port, in/out datagram.</em></td>
</tr>
<tr>
<td>SNMP</td>
<td>Provide the related statistics through SNMP</td>
</tr>
</tbody>
</table>
The Theory of SNMP

**SNMP (Simple Network Management Protocol)** is a UDP-based network protocol. It is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention. SNMP is a component of the Internet Protocol Suite as defined by the Internet Engineering Task Force (IETF). It consists of a set of standards for network management, including an application layer protocol, a database schema, and a set of data objects. SNMP exposes management data in the form of variables on the managed systems, which describe the system configuration. These variables can then be queried (and sometimes set) by managing applications. (Wikipedia)

A Network managed via SNMP is made of two groups of softwrae, **NMS (Network Management Station)** and **SNMP Agent**. NMS runs on management servers while Agent funs on the managed devices. Variables available for management are described by **MIB (Management Information Base)**.

MIB is a virtual database that is hierarchical and may be depicted as a tree with a nameless root, the levels of which are assigned by different organizations. The top level MIB OIDs belong to different standards organizations, while lower level IDs are allocated by associated organizations. The managed data variable is called “Object”. The **Object Identifier (OID)** uniquely identifies a managed object in the MIB hierarchy. Each OID identifies a variable that can be read or set via SNMP.

For example, OID: .1.3.6.1.2.1.1.1.0 as shown in SNMP management software is the system description of this particular managed variable.
Reference

- **SNMP (Simple Network Management Protocol)**

- **MIB (Management Information Base)**

- **OID (Object Identifier)**