# SNMP

## 简介：

简单网络管理协议（SNMP），由一组网络管理的标准组成，包含一个应用层协议（application layer protocol）、数据库模型（database schema）和一组资源对象。该协议能够支持网络管理系统，用以监测连接到网络上的设备是否有任何引起管理上关注的情况。

## 背景：

SNMP的基本思想：为不同种类的设备、不同厂家生产的设备、不同型号的设备，定义为一个统一的接口和协议，使得管理员可以是使用统一的外观面对这些需要管理的网络设备进行管理。通过网络，管理员可以管理位于不同物理空间的设备，从而大大提高网络管理的效率，简化网络管理员的工作。

## 历史：

SNMP共有v1，v2，v3这三个版本：

* v1和v2都具有基本的读、写MIB功能。
* v2增加了警报、批量数据获取、管理站和管理站通信能力。
* v3在v2的基础上增加了USM，使用加密的数据和用户验证技术，提高了安全性

## 应用模型：

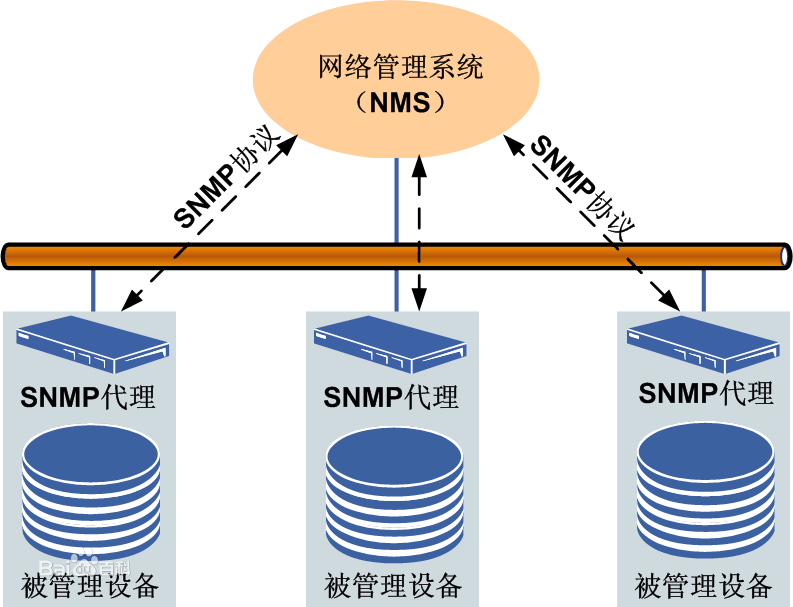
SNMP是基于TCP/IP协议族的网络管理标准，是一种在IP网络中管理网络节点（如服务器、工作站、路由器、交换机等）的标准协议。SNMP能够使网络管理员提高网络管理效能，及时发现并解决网络问题以及规划网络的增长。网络管理员还可以通过SNMP接收网络节点的通知消息以及告警事件报告等来获知网络出现的问题。

SNMP管理的网络主要由三部分组成：

被管理的设备

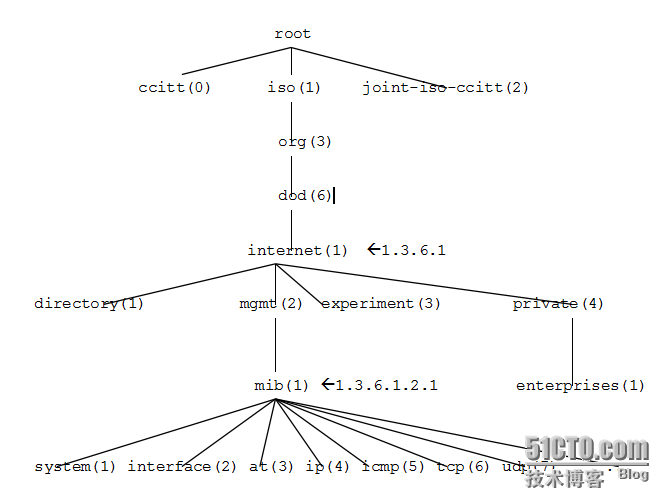
SNMP代理

网络管理系统（NMS）

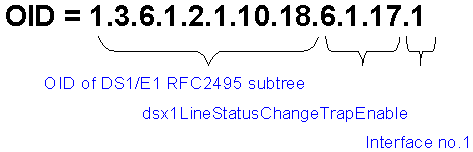


## 详解MIB：

IETF规定的管理信息库MIB（由中定义了可访问的网络设备及其属性，由对象识别符（OID：Object Identifier）唯一指定。MIB是一个树形结构，SNMP协议消息通过遍历MIB树形目录中的节点来访问网络中的设备。下图给出了NMS系统中SNMP可访问网络设备的对象识别树（OID：Object Identifier）结构。



下图给出了对一个DS1线路状态进行查询的OID设置例子。



MIB查询网址：http://www.mibdepot.com/cgi-bin/xsearch\_index3.cgi?id=173033

## 风险：

由于SNMP的效果实在太好了，所以网络硬件厂商开始把SNMP加入到它们制造的每一台设备。今天，各种网络设备上都可以看到默认启用的SNMP服务，从交换机到路由器，从防火墙到网络打印机，无一例外。

仅仅是分布广泛还不足以造成威胁，问题是许多厂商安装的SNMP都采用了默认的通信字符串（例如密码），这些通信字符串是程序获取设备信息和修改配置必不可少的。采用默认通信字符串的好处是网络上的软件可以直接访问设备，无需经过复杂的配置。

通信字符串主要包含两类命令：GET命令，SET命令。GET命令从设备读取数据，这些数据通常是操作参数，例如连接状态、接口名称等。SET命令允许设置设备的某些参数，这类功能一般有限制，例如关闭某个网络接口、修改路由器参数等功能。但很显然，GET、SET命令都可能被用于拒绝服务攻击（DoS）和恶意修改网络参数。

## SNMP术语列表：

* SNMP：Simple Network Management Protocol(简单网络管理协议)，是一个标准的用于管理基于IP网络上设备的协议。
* MIB：Management Information Base(管理信息库)，定义代理进程中所有可被查询和修改的参数。
* SMI：Structure of Management Information(管理信息结构)，SMI定义了SNMP中使用到的ASN.1类型、语法，并定义了SNMP中使用到的类型、宏、符号等。SMI用于后续协议的描述和MIB的定义。每个版本的SNMP都可能定义自己的SMI。
* PDU： Protocol Data Unit(协议数据单元)，它是网络中传送的数据包。每一种SNMP操作，物理上都对应一个PDU。
* NMS： Network Management System，网络管理系统，又名网络管理站，简称“管理站”。它是SNMP的总控机，提供统一的用户界面访问支持SNMP的设备，一般提供UI界面，并有统计、分析等功能，是网管系统的总控制台。NMS是网络管理操作的发起者。
* Agent： 是SNMP的访问代理，简称“代理”，为设备提供SNMP能力，负责设备与NMS的通信。
* Proxy： 代理服务器，对实现不同协议的设备进行协议转换，使非IP协议的设备也能被管理。
* Trap： 是由设备主动发出的报警数据，用于提示重要的状态的改变。