## **[Snmp学习总结(一)——Snmp的基本概念](https://www.cnblogs.com/xdp-gacl/p/3978825.html)**

## **一、SNMP简单概述**

### **1.1、什么是Snmp**

**SNMP**是英文"**Simple Network Management Protocol**"的缩写，中文意思是"**简单网络管理协议**"。**SNMP是一种简单网络管理协议，它属于TCP/IP五层协议中的应用层协议，用于网络管理的协议。SNMP主要用于网络设备的管理。由于SNMP协议简单可靠 ，受到了众多厂商的欢迎，成为了目前最为广泛的网管协议。**

　　SNMP协议主要由两大部分构成：SNMP管理站和SNMP代理。SNMP管理站是一个中心节点，负责收集维护各个SNMP元素的信息，并对这些信息进行处理，最后反馈给网络管理员；而SNMP代理是运行在各个被管理的网络节点之上，负责统计该节点的各项信息，并且负责与SNMP管理站交互，接收并执行管理站的命令，上传各种本地的网络信息。

　　SNMP管理站和SNMP代理之间是松散耦合。他们之间的通信是通过UDP协议完成的。一般情况下，SNMP管理站通过UDP协议向SNMP代理发送各种命令，当SNMP代理收到命令后，返回SNMP管理站需要的参数。但是当SNMP代理检测到网络元素异常的时候，也可以主动向SNMP管理站发送消息，通告当前异常状况。

**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。**

　　SNMP的工作方式：管理员需要向设备获取数据，所以SNMP提供了【读】操作；管理员需要向设备执行设置操作，所以SNMP提供了【写】操作；设备需要在重要状况改变的时候，向管理员通报事件的发生，所以SNMP提供了【Trap】操作。

### **1.2、SNMP 和 UDP**

　　SNMP采用UDP协议在管理端和agent之间传输信息。 SNMP采用UDP 161端口接收和发送请求，162端口接收trap，执行SNMP的设备缺省都必须采用这些端口。SNMP消息全部通过UDP端口161接收，只有Trap信息采用UDP端口162。

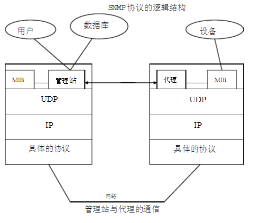
### **1.3、Snmp版本**

　　SNMP目前共有v1，v2，v3这三个版本：

* SNMP v1是SNMP协议的最初版本，不过依然是众多厂家实现SNMP基本方式。
* SNMP v2通常被指是基于community的SNMP V2。Community实质上就是密码。
* SNMP v3 是最新版本的SNMP。它对网络管理最大的贡献在于其安全性。增加了对认证和密文传输的支持。

## **二、Snmp的实现结构**

　　在具体实现上，SNMP为管理员提供了一个网管平台(NMS)，又称为【管理站】，负责网管命令的发出、数据存储、及数据分析。【被】监管的设备上运行一个SNMP代理(Agent))，代理实现设备与管理站的SNMP通信。

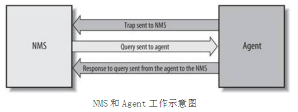


　　管理站与代理端通过MIB进行接口统一，MIB定义了设备中的被管理对象。管理站和代理都实现了相应的MIB对象，使得双方可以识别对方的数据，实现通信。管理站向代理申请MIB中定义的数据，代理识别后，将管理设备提供的相关状态或参数等数据转换为MIB定义的格式，应答给管理站，完成一次管理操作。

## **三、Snmp有关的基本概念**

### **3.1、**代理和管理站的模型****

　Snmp分2种角色：**SNMP管理站**（manager，我们的本机127.0.0.1）**和SNMP代理**（agent， 我们要操作的机器，比如 192.168.1.144）。管理站指的是运行了可以执行网络管理任务软件的服务器，通常被称作为网络管理工作站（NMS）,NMS负责采样网络中agent的信息，并接受agent的trap。代理是实际网络设备中用来实现SNMP功能的部分。代理在UDP的161端口接收NMS的读写请求消息，管理站在UDP的162端口接收代理的事件通告消息。所以，一旦获取设备的访问权限（community，默认为public），就可以访问设备信息、改写和配置设备参数。由于采用UDP协议，不需要在代理和管理站之间保持连接。



### **3.2、**SNMP的操作命令****

　　SNMP协议之所以易于使用，这是因为它对外提供了**三种用于控制MIB对象的基本操作命令**。它们是：**Get、Set 和 Trap**。

1. **Get**：管理站读取代理者处对象的值。它是SNMP协议中使用率最高的一个命令，因为该命令是从网络设备中获得管理信息的基本方式。
2. **Set**：管理站设置代理者处对象的值。它是一个特权命令，因为可以通过它来改动设备的配置或控制设备的运转状态。它可以设置设备的名称，关掉一个端口或清除一个地址解析表中的项等。
3. **Trap**： 代理者主动向管理站通报重要事件。它的功能就是在网络管理系统没有明确要求的前提下，由管理代理通知网络管理系统有一些特别的情况或问题 发生了。如果发生意外情况，客户会向服务器的162端口发送一个消息，告知服务器指定的变量值发生了变化。通常由服务器请求而获得的数据由服务器的161 端口接收。Trap 消息可以用来通知管理站线路的故障、连接的终端和恢复、认证失败等消息。管理站可相应的作出处理。

### **3.3、**SNMP的消息构成****

SNMP协议定义了数据包的格式，及网络管理员和管理代理之间的信息交换，它还控制着管理代理的MIB数据对象。因此，可用于处理管理代理定义的各种任务。  
    一条SNMP消息由"版本号"、"SNMP共同体名"和"协议数据单元(PDU)"构成，数据包的长度不是固定的。



* **版本识别符(version identifier)**：用于说明现在使用的是哪个版本的SNMP协议，确保SNMP代理使用相同的协议，每个SNMP代理都直接抛弃与自己协议版本不同的数据报。
* **团体名(Community Name)**：**团体（community）是基本的安全机制，用于实现SNMP网络管理员访问SNMP管理代理时的身份验证。类似于密码，默认值为 public。团体名（Community name）是管理代理的口令，管理员被允许访问数据对象的前提就是网络管理员知道网络代理的口令。**如果把配置管理代理成可以执行Trap命令，当网络管理 员用一个错误的分区名查询管理代理时，系统就发送一个autenticationFailure trap报文。
* **协议数据单元（PDU）**：**PDU** (协议数据单元)是SNMP消息中的数据区， 即Snmp通信时报文数据的载体。PDU指明了SNMP的消息类型及其相关参数

### ****3.4、PDU**(协议数据单元)**

PDU (协议数据单元)是SNMP消息中的数据区， 即Snmp通信时报文数据的载体。

### **3.5、**MIB(管理信息库)****

**管理信息(MIB)库可以理解成为agent维护的管理对象数据库，MIB中定义的大部分管理对象的状态和统计信息都可以被NMS访问。MIB是一个按照层次结构组织的树状结构，每个被管对象对应树形结构的一个叶子节点，称为一个object，拥有唯一的数字标识符**

　　MIB数据对象以一种树状分层结构进行组织，这个树状结构中的每个分枝都有一个专用的名字和一个数字形式的标识符。结构树的分枝实际表示的是数据对象的逻 辑分组。而树叶，有时候也叫节点（node），代表了各个数据对象。在结构树中使用子树表示增加的中间分枝和增加的树叶。   
    使用这个树状分层结构，MIB浏览器能够以一种方便而且简洁的方式访问整个MIB数据库。MIB浏览器是这样一种工具，它可以遍历整棵MIB结构树，通常 以图形显示的形式来表示各个分枝和树叶对象。可以通过其数字标识符来查找MIB中的数据对象，这个数字标识符号从结构树的顶部（或根部）开始，直到各个叶 子节点（即数据对象）为止。这种访问方式和文件系统的组织方式一致。两者的主要区别在于文件系统中的路径名可以以绝对也可以以相对方式表示，而MIB数据 对象只能以绝对方式表示，不能使用相对方式。  
    每一个节点都有一个对象标识符（OID）来唯一的标识，每个节点用数字和字符两种方式显示，其中对象标识符OID是由句点隔开的一组整数，也就是从根节点 通向它的路径。一个带标号节点可以拥有包含其它带标号节点为它的子树，如果没有子树它就是叶子节点，它包含一个值并被称为对象。比如网络设备名的oid 是.1.3.6.1.2.1.1.5.0，其值为设备名称的字符串。  
    网络资源被抽象为对象进行管理。但SNMP中的对象是表示被管资源某一方面的数据变量。对象被标准化为跨系统的类，对象的集合被组织为管理信息库 （MIB）。MIB作为设在代理者处的管理站访问点的集合，管理站通过读取MIB中对象的值来进行网络监控。管理站可以在代理者处产生动作，也可以通过修改变量值改变代理者处的配置。

### **3.6、OID(Object Identifier)**

　　每个管理对象都有自己的OID(Object Identifier)，管理对象通过树状结构进行组织，OID由树上的一系列整数组成，整数之间用点( . )分隔开，树的叶子节点才是真正能够被管理的对象。

## **四、Snmp的初步体验**

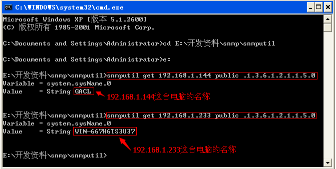
　　我们来做一个最简单的Snmp操作：获取一台IP为192.168.1.144的电脑的名称。  
     首先要给为192.168.1.144的电脑安装Snmp环境。Window组件的管理监视工具里包含Snmp，只需要安装一下就可以了。具体的安装步骤后面的博文会有详细的介绍，Snmp默认的通信端口是161/162

　　接下来需要一个能够进行Snmp通信的工具，比较简单的有snmputil，snmputil下载地址：[http://download.csdn.net/detail/aliang0708/4180259](http://download.csdn.net/detail/aliang0708/4180259" \o "Snmputil工具下载" \t "https://www.cnblogs.com/xdp-gacl/p/_blank)

　　将下载下来的【**snmputil.zip**】压缩包解压后就可以得到如下图所示的两个工具了，其中snmputil是我们要用来进行Snmp通信的工具。

  
　　**snmputil工具的命令规则是**：**snmputil [get|getnext|walk] agent community oid [oid ...]**  
**[get|getnext|walk]：**为消息类型，我们此次进行的操作是get  
**agent：**指Snmp代理即你想进行操作的网络设备的ip或名称，即192.168.1.144  
**community**：分区域，即密码，默认是public  
**oid**：想要操作的MIB数据对象号，设备名称对应的MIB对象号是.1.3.6.1.2.1.1.5.0

　　打开命令行窗口，进入snmputil所在路径，键入：**snmputil get 192.168.1.144 public .1.3.6.1.2.1.1.5.0**  
　　如果参数都正确，控制台就会显示出192.168.1.144的机器名。如下图所示：



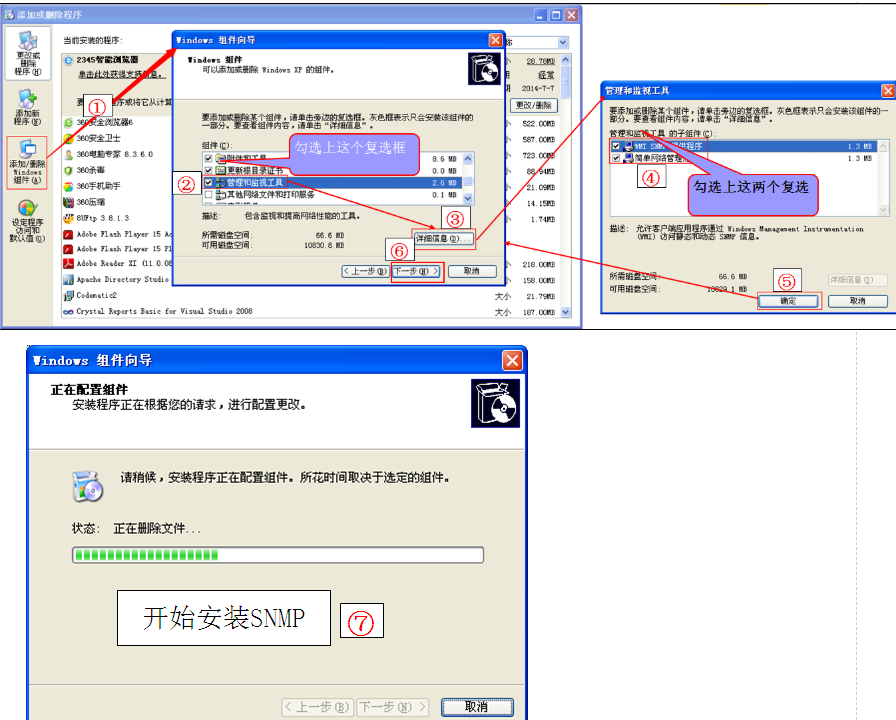
　　以上就是一些Snmp基本概念介绍和SNMP的初步体验，从下一篇博文开始，将重点介绍Window和Linux下Snmp协议的安装

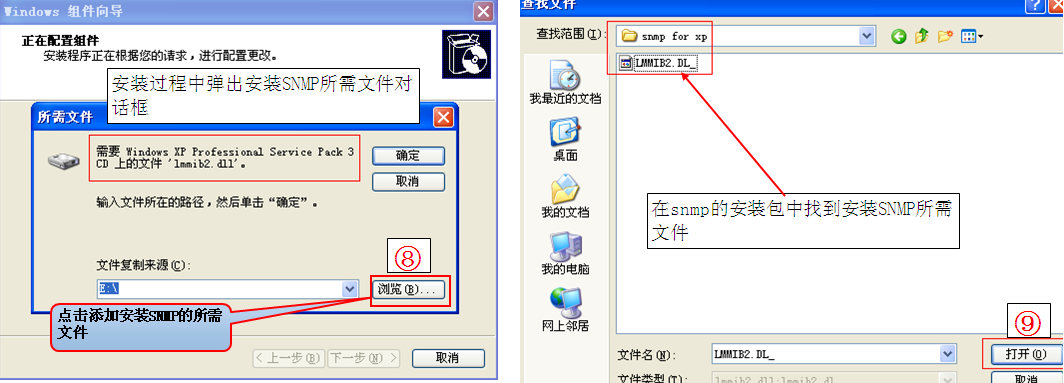
分类: [Snmp学习总结](https://www.cnblogs.com/xdp-gacl/category/613358.html" \t "https://www.cnblogs.com/xdp-gacl/p/_blank)

## **[Snmp学习总结(二)——WinXP安装和配置SNMP](https://www.cnblogs.com/xdp-gacl/p/4011771.html)**

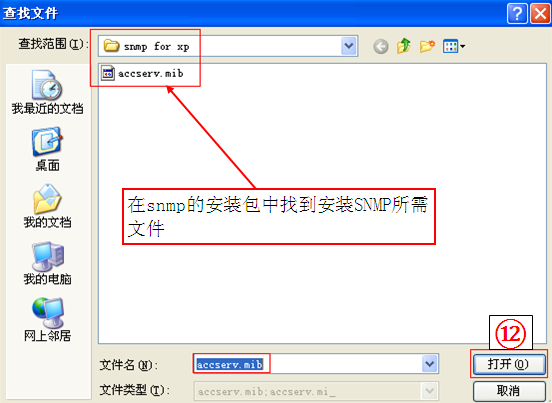
## **一、安装SNMP**

　　今天讲解一下在XP下安装SNMP协议，安装步骤如下：







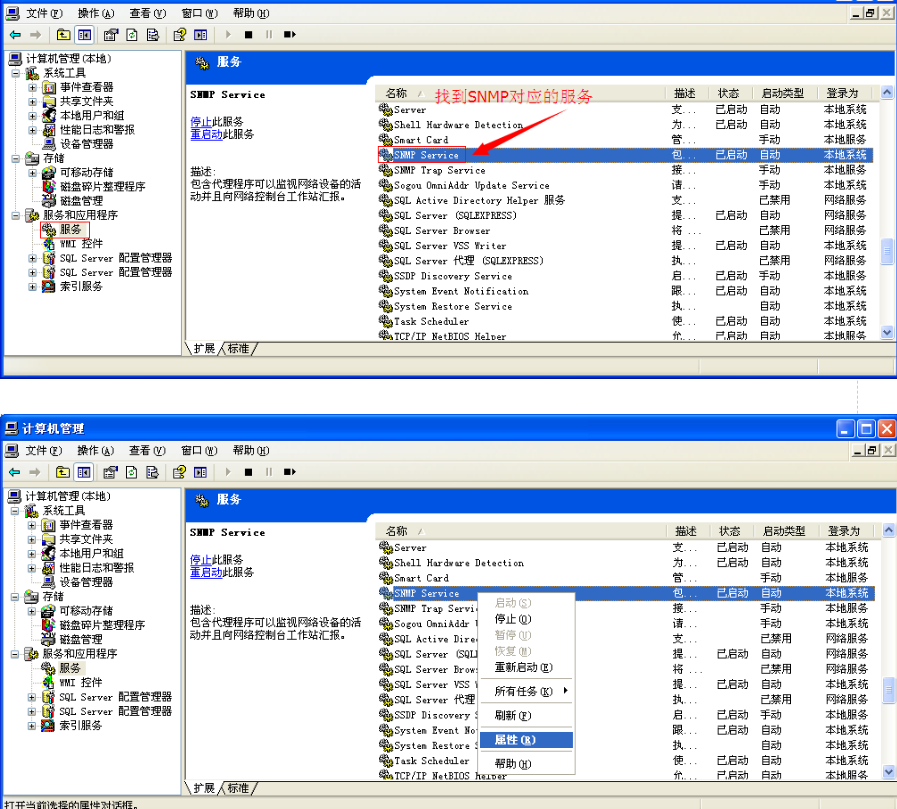


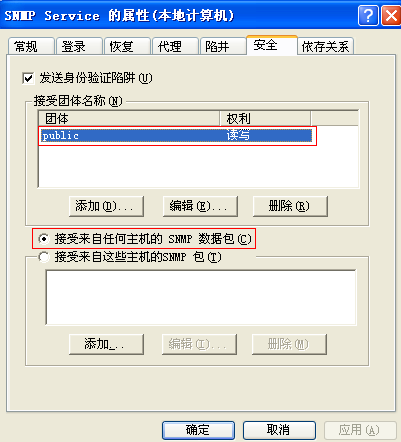
　　到此，XP系统下安装SNMP的工作就算是全部完成了。

## **二、配置SNMP**

　　安装好SNMP协议之后，还需要进行"团体名称"的配置，配置步骤如下：

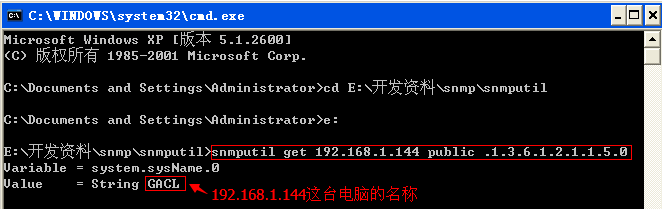
　　找到SNMP的服务，如下图所示：

　　点击【添加】按钮添加一个团体名称并设置访问权限，例如:public，访问权限是可读写，另外还需要指明可以接收来自哪些主机发送的SNMP数据包，可以使用具体的IP地址指明，这里为了方便演示，就使用"接受来自任何主机的SNMP数据包"。



　　到此，Snmp的配置工作就算是全部完成了。

## **三、测试Snmp**

　　XP下安装好Snmp之后，我们可以使用**snmputil**工具简单测试一下，打开命令行窗口，进入snmputil所在路径，键入：**snmputil get 192.168.1.144 public .1.3.6.1.2.1.1.5.0**  
　　如果参数都正确，控制台就会显示出192.168.1.144的机器名。如下图所示：　　

　　以上就是关于在XP下安装Snmp的过程，在实际的生产环境中肯定不会使用XP系统作为服务器的，因此在XP下安装Snmp了解一下即可。