

通过CLI在交换机上配置SNMP组

目标

简单网络管理协议(SNMP)是一种网络管理协议，可帮助记录、存储和共享有关网络中设备的信息。这有助于管理员解决网络问题。SNMP使用管理信息库(MIB)以分层方式存储可用信息。SNMP组用于根据访问权限和对MIB中不同SNMP视图的授权来组合SNMP用户。每个SNMP组由组名称和安全级别的组合唯一标识。

本文档说明如何使用交换机的命令行界面创建和配置SNMP组。它假设已为设备配置了SNMP视图。

SNMP组也可以通过交换机的基于Web的实用程序进行配置。有关说明，请参阅[在交换机上配置简单网络管理协议\(SNMP\)组](#)。

适用设备

- Sx350 系列
- SG350X 系列
- Sx500系列
- Sx550X 系列

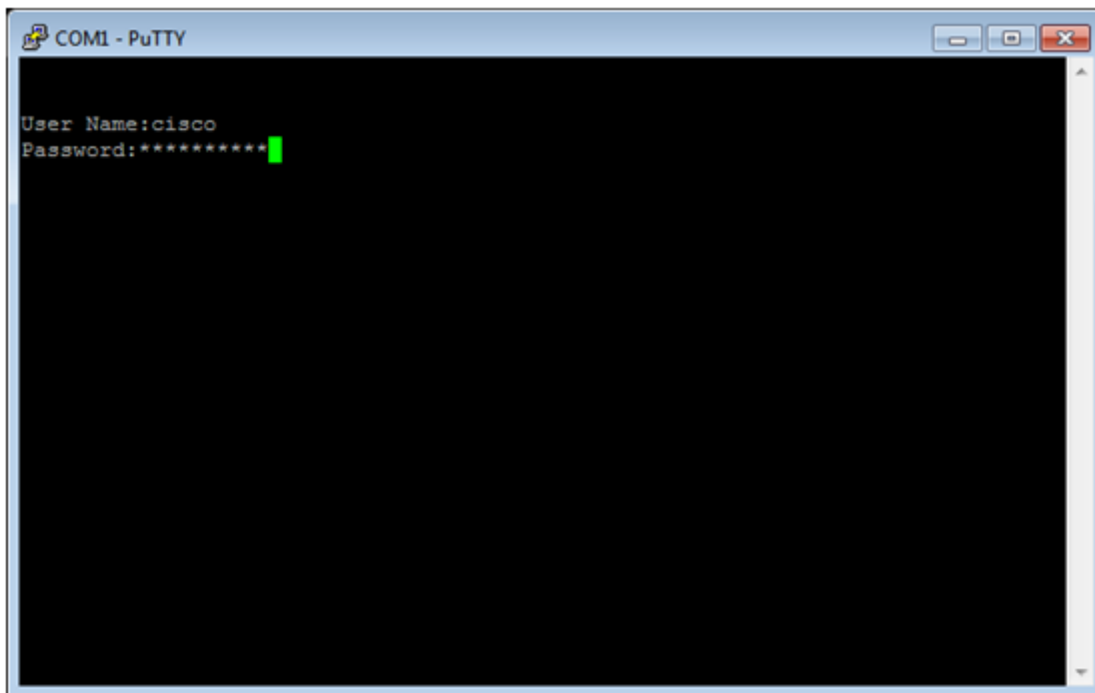
软件版本

- 1.4.7.05 - Sx300、Sx500
- 2.2.8.04 - Sx250、Sx350、SG350X、Sx550X

在交换机上配置SNMP组

第 1 步

访问交换机的CLI。



在本例中，PuTTY是用于访问交换机CLI的应用。默认用户名和密码为cisco/cisco。如果已自定义凭据，请使用用户名和密码。

步骤 2

通过输入以下命令切换到全局配置模式：

```
Switch350X#configure terminal
```

步骤 3

使用以下语法创建SNMP组：

```
snmp-server group groupname {{v1/v2/v3 {{noauth/auth/priv}}[notify notifyview]}}[read readview]  
[write writeview]。
```

其中：

- group *groupname* — 在此可以指定组的名称。组名长度可以是1到30个字符。
- v1 — 此选项使用SNMP第1版安全模型。
- v2 — 此选项使用SNMP第2版安全模型
- v3 — 此选项使用SNMP第3版安全模型。
- noauth — 此选项指定不执行数据包身份验证。此选项仅适用于SNMPv3安全模型。
- auth — 此选项指定将执行不加密的数据包身份验证。此选项仅适用于SNMPv3安全模型。
- priv — 此选项指定将执行加密数据包身份验证。此选项仅适用于SNMPv3安全模型。
- notify *notifyview* — （可选）此选项指定启用生成通知或陷阱的视图名称。通知是需要确认的陷阱。此选项仅在SNMPv3安全模型上可用。
- read *readview* — （可选）此选项指定仅启用查看的视图名称。视图名称的长度可以介于1到30个字符之间。
- write *writeview* — （可选）此选项指定启用配置代理的视图名称。视图名称可以是1到30个字符。

```
Switch350X#snmp-server group CiscoTestUsers v3 auth notify Cisco1234$ read
```

在本示例中，输入snmp-server group CiscoTestUsers v3 auth notify Cisco1234\$ read。

步骤 4

使用以下命令检验SNMP组：

```
Switch350X#show snmp groups
```

您现在应该已通过交换机的CLI配置SNMP组设置。