使用 MP管理及配置cisco交换机 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/260/2021_2022__E4_BD_BF_E7_94_A8_MP_E7_c101_260890.htm SNMP版本 Cisco IOS支持SNMP协议的下列版本： SNMPv1 C 简单网络管理协议：一个完全的互联网标准，定义在STD15/RFC1157（RFC1157文档替代了早期的RFC1098和RFC1067文档）和 STD16/RFC1155，RFC1212文档中。安全机制采用基于团体字符串（Community String）认证方式。 SNMPv2c C 基于团体字符串认证管理框架的简单网络管理协议版本2.SNMPv2c（c代表Community）是一个互联网实验标准，具体技术规范定义在 RFC1901，RFC1905和RFC1906文档。SNMPv2c在SNMPv2p（SNMPv2 Classic）基础上定义了协议操作和数据类型的更新，安全机制延续了SNMPv1的基于团体字符串认证方式。 SNMPv3 C 简单网络管理协议版本3，2002年3月被IESG（Internet Engineering Steering Group）批准为完全的互联网标准。SNMPv3是一个具有互操作性的标准协议，核心规范定义在STD62/RFC3411到RFC3418文档中。 SNMPv3提供了设备安全访问机制，是由认证和网络传输中数据包加密的组合方式实现的。 SNMPv3提供的安全特性包括： 报文完整性 C 确保数据包在传输过程中没有被篡改 认证 C 确定报文是由正确信息源发送来的 加密 C 对报文内容进行加密，防止其被未经授权的读取 SNMPv1和SNMPv2c都利用了基于“ 团体（Community）”形式的安全认证机制。能够访问SNMP代理MIB数据的管理者“ 团体 ”通过一个IP地址访问控制列表和口令进行定义。 SNMPv2c还增加了对大批量数据读取机制的

支持和向管理工作站更加详细的错误消息汇报机制。支持对大批量数据的读取机制能够用来对整个MIB数据表格和大量的信息进行快速读取，减少请求/应答的往复数量。SNMPv2c增强的错误处理机制包括扩展的错误代码，用于区别不同的错误状况。错误返回代码现在将包括错误类型。 SNMPv3重点强调增强协议的安全认证/加密，授权/访问控制以及远程配置管理等功能，而在其它方面沿用了部分SNMPv2原有的技术规范。 SNMPv3提供了一个安全模型。这个安全模型中可以为用户/用户组定义不同的安全认证策略；而安全级别是指SNMPv3安全模型中被允许的安全等级。安全模型和安全等级的组合将会决定在处理一个SNMP数据包时采用的安全机制。 如果想了解SNMPv3的额外信息，可以参阅RFC3410文档《Introduction and Applicability Statements for Internet Standard Management Framework》 