网络管理系统：最佳实践白皮书

目录

简介
网络管理
故障管理
网络管理平台
基础设施故障排除
故障检测和通知
前摄故障监视和通知
配置管理
配置标准
配置文件管理
Inventory Management
软件管理
性能管理
服务级别协议
性能监视、评定和报告
性能分析和调整
安全管理
身份验证
授权
记账
SNMP 安全
记帐管理
网流激活和数据收集策略
配置 IP 计费

简介

国际标准化组织 (ISO) 网络管理模型定义了网络管理的五个功能区域。本文档介绍了所有这些功能区域。本文的整体目的是要在每个功能区域提供实用的推荐标准，增加当前管理工具和运作的整体效果。同时还提供了针对未来实施网络管理工具和技术的设计指导原则。

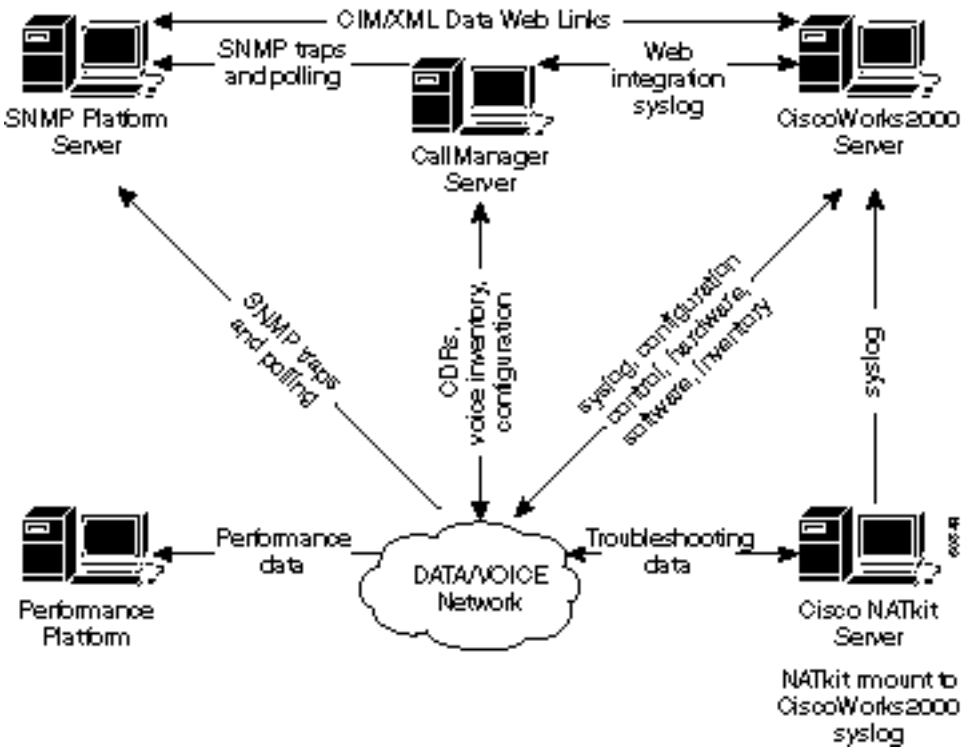
网络管理

ISO 网络管理模型的 5 个功能区域具体如下。

- 故障管理 – 对网络中的故障进行检测、隔离、通知和更正。
- 配置管理 – 与网络设备的配置相关的管理工作，例如配置文件管理、资产管理和软件管理。
- 性能管理——监控和测量各个方面的性能，以便将整体性能维持在可接受的水平上。
- 安全管理 – 向授权人员提供对网络设备和公司资源的访问权限。
- 计费管理 – 网络资源的使用信息。

下列图表显示Cisco系统相信的参考体系结构应该是管理数据网的最小解决方案。此体系结构包括适

用于管理基于 IP 的语音传输 (VoIP) 的 Cisco CallManager 服务器：图中展示了如何将 CallManager 服务器集成到 NMS 拓扑。



网络管理体系结构包括以下组件：

- 简单网络管理协议 (SNMP) 平台，用于故障管理
- 性能监控平台，用于长期性能管理和趋势分析
- CiscoWorks2000 服务器，用于配置管理、系统日志收集，以及硬件和软件资产管理

运用公用信息模块/可扩展标记语言(CIM/XML)法，一些SNMP平台能与CiscoWorks2000服务器直接共享数据。CIM是与实施无关的方案的普通数据模型，用来描述网络或企业环境的整体管理信息。CIM 由规格和计划两部分组成。规格详细定义了与其他管理模型，如SNMP MIB或桌面管理工作组管理信息文件(DMTF MIF)的集成，而计划则提供了实际模式的说明。

XML 是一种用于以文本格式呈现结构化数据的标记语言。XML的一个特定目标是保持SGML的大多数描述功能，尽可能减少复杂性。XML概念上类似于HTML，HTML用于表示文件的图形信息，XML则表示文件中的结构化数据。

思科高级服务客户还将获得思科的 NATkit 服务器，从而能够使用额外的主动监控和故障排除功能。NATkit服务器拥有远程磁盘配置(rmount)或文件传输协议（FTP）权限访问位于CiscoWorks2000服务器的数据。

如需了解更多网络管理基础知识，请参阅*《互联网技术概述》的*网络管理基础知识一章。

故障管理

故障管理的目标是检测、记录、通知用户和自动修复（可能程度上）网络问题，保持网络高效运行。由于故障可能导致停机或不能接受的网络性能下降，因此故障管理也许是实施最广泛的ISO网络管理要素。

网络管理平台

企业中部署的网络管理平台用于管理由多供应商网络元素构成的基础设施。这类平台会接收并处理来自各种网络元素的事件。来自服务器和其他关键资源的事件也可以转发到管理平台。标准管理平台通常包括以下常见功能：

- 网络发现
- 网络元素拓扑映射
- 事件处理程序
- 性能数据收集器和绘图器
- 管理数据浏览器

在检查基础设施的故障时，网络管理平台可以被视作网络操作的主要控制台。因此，具备在任何网络中快速发现问题的能力至关重要。网络操作人员可以依赖图形网络映射，显示重要网元的操作状态，例如路由器和交换机。

诸如 HP OpenView、Computer Associates Unicenter 和 SUN Solstice 等网络管理平台都能执行网络设备发现操作。在网络管理平台的控制台中，每个网络设备都用一个图形元素表示。图形元素的各种颜色表示网络设备的当前工作状态。通过配置网络设备，可以使其向网络管理平台发送通知（调用的 SNMP 陷阱）。在接收通知时，根据接收到的通知的严重性，表示网络设备的图形要素将变成不同颜色。通知（通常称为“事件”）会被储存到一个日志文件。尤其重要的是最当前的Cisco管理信息库(MIB)文件应装载到SNMP平台上，以确保来自Cisco设备的不同告警能被正确解释。

思科发布了多种 MIB 文件，用于管理各种网络设备。Cisco MIB文件位于cisco.com网站，包括以下信息：

- 以 SNMPv1 格式发布的 MIB 文件
- 以 SNMPv2 格式发布的 MIB 文件
- 思科设备上支持的 SNMP 陷阱
- 用于思科当前 SNMP MIB 对象的 OID

许多网络管理平台都能用于管理分散在不同地理位置的多个站点。这是通过各远程站点的管理控制台的和主站点管理站之间的管理数据交换而实现的。分布式体系结构的主要优点是它减少管理数据流量，从而更有效地使用带宽。借助分布式体系结构，IT 人员可以在远程站点使用网络管理系统本地执行网络管理操作。

作为最近推出的一项增强功能，管理平台现在可以通过 Web 界面远程管理网络元素。这样一来，单个用户工作站上无需安装特定的客户端软件，即可访问管理平台。

典型的企业网络由各种各样的网络元素组成。通常，每个管理设备上需要单独安装供应商特定的网络元素管理系统，才能有效管理网络元素。因此，可能会出现多个管理工作站重复轮询网络元素，获取相同信息的情形。不同系统收集的数据分别保存在独立的数据库中，用户因此产生了更多管理开销。此限制提示网络和软件供应商采用诸如Common Object Request Broker Architecture (CORBA)和集成计算机制造(CIM)等标准，促进管理平台和网元管理系统之间的管理数据交换。随着供应商采用标准管理系统开发，用户有望在部署和管理基础设施中实现互用性和成本节约。

CORBA指定能够提供异构分布式环境对象之间的互操作性的系统，指定方式对程序员是透明的。其设计以对象管理组 (OMG) 对象模型为基础。

基础设施故障排除

简单文件传输协议(TFTP)和系统日志(syslog) 服务器是网络操作中的故障排除基础设施的关键组件。TFTP 服务器主要用于存储网络设备的配置文件和软件映像。路由器和交换机可以将系统日志消息发送到系统日志服务器。这些消息有助于在出现问题时进行故障排除。有时，思科支持人员需要使用系统日志消息来执行根本原因分析。

CiscoWorks2000资源管理基础(精华)所具有的系统日志收集功能允许在远程站点部署几个UNIX或NT收集站，执行消息收集和过滤。过滤功能可用于指定要将哪些系统日志消息转发到主 Essentials 服务器。进行分布式收集的主要优点是转发到主要系统日志服务器的消息减少。

故障检测和通知

故障管理的目的是发现、隔离、通知和更正网络遇到的故障。当系统中发生故障时，网络设备可以向管理工作站发出警报。有效的故障管理系统由多个子系统组成。当设备发送SNMP陷阱消息、SNMP轮询、远程监控(RMON)阈值和系统日志消息时，故障检测便完成。在报告故障时，管理系统通知终端用户，采取纠正措施。

应始终在网络设备上启用陷阱。适用于路由器和交换机的新版 Cisco IOS 软件支持更多陷阱。请务必注意检查和更新配置文件，以确保陷阱能够正确解码。Cisco保证网络服务(ANS)团队定期检查配置陷阱，将保证网络中的有效故障检测。

下表列出了可以支持和监控故障状况、Cisco Catalyst局域网(LAN)交换机的CISCO-STACK-MIB陷阱。

陷阱	描述
moduleUp	代理实体检测到该MIB中的moduleStatus对象为它的的某个模块转成ok(2)状态。
moduleDown	代理实体检测到该MIB中的moduleStatus对象为它的的某个模块转出ok(2)状态。
chassisAlarmOn	代理实体检测到该MIB中的chassisTempAlarm、chassisMinorAlarm或chassisMajorAlarm对象已经转换到 on(2)状态。*chassisMajorAlarm 表示存在以下情形之一：* • 电压故障 • 同时出现温度和风扇故障 • 所有电源全部故障（双电源配置中的两个电源或单电源配置中的一个电源） • 电可擦除可编程只读存储器 (EEPROM) 故障 • 非易失性 RAM (NVRAM) 故障 • MCP 通信故障 • NMP 状态未知 chassisMinorAlarm 表示存在以下情形之一： • 温度告警 • 风扇故障 • 部分电源发生故障（双电源配置中的一个电源） • 两个电源类型不兼容
chassisAlarmOff	代理实体检测到该MIB中的chassisTempAlarm、chassisMinorAlarm或chassisMajorAlarm对象已经转换到off(1)状态。

环境监视器 (envmon) 陷阱在 CISCO-ENVMON-MIB 陷阱中定义。envmon 陷阱会在环境参数超出阈值时，发送思科企业特定环境监视器通知。使用envmon时，可以启用特定的环境陷阱类型，或者接收来自环境监控系统的所有陷阱类型。如果未指定任何选项，则默认启用所有环境类型。此陷阱可以设置为以下一个或多个值：

- 如果测量到的电压超过电压测试点的正常范围(例如警告、重要或关闭阶段)，则发送电压--A ciscoEnvMonVoltageNotification。
- 关闭--如果环境监控器发现测试点到达关键状态并且将起动关闭，则发送 ciscoEnvMonShutdownNotification。
- 电源 – 当冗余电源（如果有）发生故障时，发送 ciscoEnvMonRedundantSupplyNotification。
- 风扇-- 如果风扇阵列(现存的)的某个风扇出现故障，则发送ciscoEnvMonFanNotification。
- 如果测量到的温度超过温度测试点的正常范围(例如警告、重要或关闭阶段)，则发送温度--A ciscoEnvMonTemperatureNotification。

故障检测和网络元素监控可以从设备级别扩展到协议和接口级别。对于网络环境，故障监控可以包括虚拟局域网(VLAN)、异步传输模式（ATM）、物理接口上的故障指示等等。协议级别的故障管理可以借助 CiscoWorks2000 Campus Manager 等网元管理系统来实现。Campus Manager 中的 TrafficDirector 应用主要用于通过 Catalyst 交换机支持的 mini-RMON 功能执行交换机管理。

随着网元数量和网络问题复杂性的增加，可以考虑能够关联不同网元(系统日志、陷井、日志文件)的事件管理系统。这种存在于事件管理系统背后的体系结构好比是一种“管理器的管理器”(MOM) 系统。设计完美的事件管理系统，允许网络运营中心(NOC)的工作人员主动、有效地检测和诊断网络问题。事件优先级和抑制允许网络操作人员着重于关键网络事件，调查几大事件管理系统（包括Cisco信息中心），进行可行性分析，全面探究该系统的功能。有关更多信息，请访问思科信息中心。

前摄故障监视和通知

RMON 警报和事件是 RMON 规格中定义的两个组。管理站通常在网络设备上执行轮询，以确定某些变量的状态或值。例如，当值命中达到配置的阈值时，管理站轮询路由器查看中央处理器(CPU)利用率并生成事件。这种方法会浪费网络带宽，而且根据轮询间隔还可能会遗漏实际的阈值。

提供RMON告警和事件后，可以配置网络设备来监控自己，升高和降低阈值。在预定义的时间间隔内，网络设备将取样变量，并将它与阈值相比较。如果实际值超过或低于所配置的阈值，SNMP陷阱可能被发送到管理站。RMON 警报和事件组提供了一种对关键网络设备进行前摄式管理的方法。

思科系统公司建议对关键网络设备实施 RMON 警报和事件。被监控的变量包括CPU利用率、缓冲故障、输入-输出丢弃，或者所有整数类型的变量。从 Cisco IOS 软件版本 11.1(1) 起，所有路由器映像均支持 RMON 警报和事件组。

有关实现 RMON 警报和事件的详细信息，请参阅 RMON 警报和事件实现部分。

RMON 内存限制

RMON 内存使用率在所有交换机平台间是恒定的，与统计数据、历史记录、警报和事件有关。RMON使用所谓的时段，将历史记录和统计数据存储在RMON代理程序(此处指交换机)。 RMON探测器(SwitchProbe设备)或RMON应用程序(流量控制器工具)定义的桶容量，然后被发送到待设置交换机。

需要大约450 K的代码空间来支持微型RMON (例如，四个RMON组)：统计数据、历史记录、警报和事件。 RMON 的动态内存要求并不固定，而是取决于运行时配置。

下表列出了各个 mini-RMON 组的运行时 RMON 内存使用量信息。

RMON 组定义	DRAM 空间使用量	备注

统计信息	每个以太网/快速以太网交换端口 140 字节	每个端口
历史记录	50 个存储空间 3.6 K*	每增加一个存储空间，多占用 56 字节
警报和事件	每个警报及相应的事件条目 2.6 K	每个警报每个端口

RMON使用所谓的时段，将历史记录和统计数据存储在RMON代理程序(例如交换机)。

RMON 警报和事件实现

把RMON合并为故障管理解决方案的组成部分，用户可以在潜在问题发生之前主动监控网络。例如，如果接收到的广播包数量大幅增加，那么它可能导致CPU利用率增高。通过执行RMON告警和事件，用户可以设置阈值，监控收到的广播信息包的数量。如果达到配置阈值，则通过SNMP陷阱方式向SNMP平台发送警报。RMON告警和事件消除SNMP平台通常执行的额外轮询，用来完成相同目标。

配置 RMON 警报和事件有两种方法：

- 命令行界面 (CLI)
- SNMP SET

以下示例程序显示如何设置门限值监控接口上收到的广播包数量。上述程序所用的相同计数器显示在本部分结尾处的show interface命令示例中。

命令行界面示例

要使用 CLI 界面实现 RMON 警报和事件，请执行以下步骤：

1. 遍历 ifTable MIB，找到与 Ethernet 0 关联的接口索引。
```
interfaces.ifTable.ifEntry.ifDescr.1 = "Ethernet0"
interfaces.ifTable.ifEntry.ifDescr.2 = "Ethernet1"
interfaces.ifTable.ifEntry.ifDescr.3 = "FastEthernet0"
interfaces.ifTable.ifEntry.ifDescr.4 = "Fddi0"
```
2. 获取与所要监控的 CLI 字段关联的 OID。在本例中，“广播”的OID为1.3.6.1.2.1.2.1.12。特定MIB变量的Cisco OID可从cisco.com网站获取。
3. 确定以下参数，设置阈值和事件。阈值上限和下限采样类型（绝对值采样或变化值采样）采样间隔达到阈值时的操作为此示例，正在设置阈值以监控在Ethernet 0上接收的广播数据包数。如果在60秒采样之间接收的广播数据包数大于500，将生成陷阱。当使用的两个示例间的输入广播数量不再增加时，阈值将被重新激活。**注意：** 如需详细了解这些命令参数，请检查有关RMON警告的Cisco在线连接(CCO)说明文档和有关特殊Cisco IOS版本的事件命令。
4. 达到阈值时，使用以下CLI命令(Cisco IOS命令用粗体显示)指定已发送陷阱(RMON 事件)。**rmon event 1 trap gateway description "High Broadcast on Ethernet 0" owner ciscormon event 2 log description "normal broadcast received on ethernet 0" owner cisco**
5. 使用以下 CLI 命令指定阈值和相关参数（RMON 警报）：**rmon alarm 1 ifEntry.12.1 60 delta rising-threshold 500 1falling-threshold 0 2 owner cisco**
6. 使用 SNMP 轮询以下表格，确认是否在设备中设置了这些 eventTable 条目。
```
rmon.event.eventTable.eventEntry.eventIndex.1 = 1

rmon.event.eventTable.eventEntry.eventIndex.2 = 2

rmon.event.eventTable.eventEntry.eventDescription.1 =
```

```
"High Broadcast on Ethernet 0"

rmon.event.eventTable.eventEntry.eventDescription.2 =
"normal broadcast received on ethernet 0"

rmon.event.eventTable.eventEntry.eventType.1 = snmp-trap(3)

rmon.event.eventTable.eventEntry.eventType.2 = log(2)

rmon.event.eventTable.eventEntry.eventCommunity.1 = "gateway"

rmon.event.eventTable.eventEntry.eventCommunity.2 = ""

rmon.event.eventTable.eventEntry.eventLastTimeSent.1 =
Timeticks: (0) 0:00:00

rmon.event.eventTable.eventEntry.eventLastTimeSent.2 =
Timeticks: (0) 0:00:00

rmon.event.eventTable.eventEntry.eventOwner.1 = "cisco"

rmon.event.eventTable.eventEntry.eventOwner.2 = "cisco"

rmon.event.eventTable.eventEntry.eventStatus.1 = valid(1)

rmon.event.eventTable.eventEntry.eventStatus.2 = valid(1)
```

7. 使用 SNMP 轮询以下表格，确认是否设置了这些 alarmTable 条目。

```
rmon.alarm.alarmTable.alarmEntry.alarmIndex.1 = 1

rmon.alarm.alarmTable.alarmEntry.alarmInterval.1 = 60

rmon.alarm.alarmTable.alarmEntry.alarmVariable.1 = OID:
interfaces.ifTable.ifEntry.ifInNUcastPkts.2

rmon.alarm.alarmTable.alarmEntry.alarmSampleType.1 = absoluteValue(1)

rmon.alarm.alarmTable.alarmEntry.alarmValue.1 = 170183

rmon.alarm.alarmTable.alarmEntry.alarmStartupAlarm.1 =
risingOrFallingAlarm(3)

rmon.alarm.alarmTable.alarmEntry.alarmRisingThreshold.1 = 500

rmon.alarm.alarmTable.alarmEntry.alarmFallingThreshold.1 = 0

rmon.alarm.alarmTable.alarmEntry.alarmRisingEventIndex.1 = 1

rmon.alarm.alarmTable.alarmEntry.alarmFallingEventIndex.1 = 2

rmon.alarm.alarmTable.alarmEntry.alarmOwner.1 = "cisco"

rmon.alarm.alarmTable.alarmEntry.alarmStatus.1 = valid(1)
```

SNMP SET 示例

要使用 SNMP SET 操作实现 RMON 警报和事件，请完成以下步骤：

1. 使用以下SNMP SET操作，指定到达阈值时发送的陷阱(RMON事件)：

```
# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.9.1.1.2.1
  octetstring "High Broadcast on Ethernet 0"
  eventDescription.1 : DISPLAY STRING- (ascii): High Broadcast on Ethernet 0
```

```
# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.9.1.1.3.1
  integer 3 eventType.1 : INTEGER: SNMP-trap

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.9.1.1.4.1 octetstring "gateway"
  eventCommunity.1 : OCTET STRING- (ASCII): gateway

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.9.1.1.6.1
  octetstring "cisco" eventOwner.1 : OCTET STRING- (ASCII): cisco

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.9.1.1.7.1 integer 1
  eventStatus.1 : INTEGER: valid
```

2. 使用以下 SNMP SET 操作指定阈值和相关参数（RMON 警报）：

```
# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.9.1.1.2.2
  octetstring "normal broadcast received on ethernet 0"
  eventDescription.2 : DISPLAY STRING- (ASCII): normal broadcast
  received on ethernet 0

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.9.1.1.3.2 integer 2
  eventType.2 : INTEGER: log

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.9.1.1.6.2 octetstring "cisco"
  eventOwner.2 : OCTET STRING- (ASCII): cisco

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.9.1.1.7.2 integer 1
  eventStatus.2 : INTEGER: valid
```

3. 轮询以下表格，确认是否在设备中设置了这些 eventTable 条目。

```
% snmpwalk -v 1 172.16.97.132 private .1.3.6.1.2.1.16.9.1

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.3.1.1.2.1 integer 60
  alarmInterval.1 : INTEGER: 60

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.3.1.1.3.1
 objectidentifier .1.3.6.1.2.1.2.2.1.12.2
  alarmVariable.1 : OBJECT IDENTIFIER:
.iso.org.dod.internet.mgmt.mib2.interfaces.ifTable
  ifEntry.ifInNUcastPkts.2

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.3.1.1.4.1 integer 2

alarmSampleType.1 : INTEGER: deltaValue

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.3.1.1.7.1 integer 500
  alarmRisingThreshold.1 : INTEGER: 500

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.3.1.1.8.1 integer 0
  alarmFallingThreshold.1 : INTEGER: 0

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.3.1.1.9.1 integer 1
  alarmRisingEventIndex.1 : INTEGER: 1

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.3.1.1.10.1 integer 2
  alarmFallingEventIndex.1 : INTEGER: 2

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.3.1.1.11.1 octetstring
"cisco"
  alarmOwner.1 : OCTET STRING- (ASCII): cisco

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.3.1.1.12.1 integer 1
  alarmStatus.1 : INTEGER: valid
```

4. 轮询以下表格，确认是否设置了这些 alarmTable 条目。

```
% snmpwalk -v 1 172.16.97.132 private .1.3.6.1.2.1.16.3.1
```

show interface

下面的示例显示了 **show interface 命令的运行结果。**

gateway > **show interface ethernet 0**

```
Ethernet0 is up, line protocol is up
Hardware is Lance, address is 0000.0c38.1669 (bia 0000.0c38.1669)
Description: NMS workstation LAN
Internet address is 172.16.97.132/24
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
Encapsulation ARPA, loopback not set, keepalive set (10 sec)
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:00, output 00:00:00, output hang never
Last clearing of "show interface" counters never
Queueing strategy: fifo
Output queue 0/40, 27 drops; input queue 0/75, 0 drops
5 minute input rate 1000 bits/sec, 2 packets/sec
5 minute output rate 1000 bits/sec, 1 packets/sec
21337627 packets input, 3263376846 bytes, 0 no buffer

Received 7731303 broadcasts , 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 input packets with dribble condition detected
17328035 packets output, 2824522759 bytes, 0 underruns
174 output errors, 44368 collisions, 4 interface resets
0 babbles, 0 late collision, 104772 deferred
174 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
```

配置管理

配置管理的目标是监控网络和系统配置信息，以便追踪和管理各种版本的硬件和软件元件的网络操作受到的影响。

配置标准

由于配置的网络设备数量不断增长，能正确地识别网络设备的位置十分重要。当网络发生故障时，位置信息应像那些需要分配资源的人提供有意义的详细说明。如果网络发生问题，要加快找到解决方法，保证能够提供负责设备的人或部门的联系信息。联系人信息应包含相关人员/部门的电话号码和姓名/名称。

网络设备的命名规则，从设备名开始到单个接口等都应当作配置标准的一部分进行计划和实施。在进行网络故障排除时，一个定义得很好的命名规则可以为相关人员能提供准确的信息。按照惯例，命名设备可以使用地理位置名称、建筑名称、楼层等等。至于接口命名规则，它包括端口连接的分段、连接集线器的名字等等。在串行接口，它应该包括实际带宽、本地数据链路连接标识符(DLCI)编号(如帧中继)、目的地、电路ID或运营商提供的信息。

配置文件管理

在现有网络设备中添加所需的新配置命令时，必须在实际实现这些命令之前验证命令的完整性。网络设备配置不正确可能会对网络连接和网络性能造成灾难性影响。请务必仔细检查配置命令和参数，以免出现匹配性或兼容性问题。建议定期安排思科工程师进行全面的配置审查。

CiscoWorks2000 Essentials 在开通全部功能时，可以自动在路由器和 Cisco Catalyst 交换机上备份配置文件。您还可以使用 Essentials 的安全功能来验证配置更改。跟踪更改及个人发送更改的用户名可以获得更改审计日志。要更改多个设备的配置，有两个选项可以使用：当前版本的 CiscoWorks2000 Essentials 中的基于 Web 的 NetConfig 或 **cwconfig 脚本。**配置文件可以使用 CiscoWorks2000 Essentials进行下载和上载操作，该软件使用预定义或用户定义模板。

CiscoWorks2000 Essentials 的配置管理工具可以实现下列功能：

- 将配置文件从 Essentials 的配置存档推送到一个或多个设备
- 将配置从设备推送到 Essentials 存档
- 从存档提取最新的配置，并将其写入文件
- 从文件导入配置，并将其推送到设备
- 比较 Essentials 存档中最新的两个配置
- 从存档中删除比指定的日期或版本更早的配置
- 将启动配置复制到运行配置中

Inventory Management

多数网络管理平台的发现功能打算提供在网络中发现的设备动态列表。执行发现操作需要使用发现引擎（例如网络管理平台中实施的发现引擎）。

资产数据库可提供网络设备的具体配置信息，常见信息包括硬件型号、已安装的模块、软件映像、微代码级别等等。这些信息对于完成软件和硬件维护等任务而言至关重要。发现过程收集到的最新网络设备列表可以用作主列表，以便收集使用SNMP或脚本的库存信息。设备列表可以从 CiscoWorks2000 Campus Manager导入CiscoWorks2000 Essentials 的库存数据库，以获取Cisco Catalyst交换机的最新产品清单。

软件管理

网络设备上的Cisco IOS镜象的成功升级需要详细分析需求，如内存、引导程序ROM、微码级等等。这些需求被正常存档，并在Cisco网站上以版本说明和安装指南的形式提供。运行思科IOS的网络设备的升级进程包括从CCO下载正确的镜像，备份当前镜像，确定符合所有硬件需求，以及把新的镜像加载到设备。

对某些组织来说，执行设备维护的升级窗口相当有限。在一个资源有限的大型网络环境中，可能需要工作时间后再安排自动升级软件。这个程序的实现可以使用脚本语言（例如Expect）或特别为执行此任务编写的应用。

应该追踪网络设备中的软件变化，如Cisco IOS镜象和微码版本，以便当其他软件需要维护时为分析阶段提供帮助。如果已经提供更改过的历史记录报告，那么执行更新的人可以最大程度地降低向网络设备装载不兼容镜像或微码的风险。

性能管理

服务级别协议

服务级别协议(SLA)是服务提供商和其用户书面签署的网络服务的期望性能级别协议。SLA 包含供应商与客户之间达成一致的指标。对双方而言，设置为权值的值必须是可以实现的、有意义的和可以测量的。

通过从网络设备收集各种接口统计数据，可以衡量性能级别。这些统计数据可以作为指标纳入 SLA 中。诸如“输入队列丢包”、“输出队列丢包”和“已忽略的数据包”等统计数据对于诊断性能相关问题十分有用。

在设备级别，性能测量指标可以包括CPU利用率、缓冲分配(大缓冲区、中等缓冲区、错过率、命中率)和内存分配。特定网络协议的性能会直接影响网络设备缓冲区的可用性。测量设备级性能统计数据对于优化更高级协议的性能至关重要。

网络设备，例如路由器支持多种更高层协议，如数据链路交换工作组(DLSW)，远端 源 路由 桥接(RSRB)和AppleTalk等。广域网(WAN)技术性能统计数据包括帧中继、ATM、综合服业务数字网络(ISDN)和其他可以监控和收集的数据。

性能监视、评定和报告

接口、设备和协议级别的不同性能度量指标，应该使用SNMP进行定期收集。网络管理系统的轮询引擎可用于收集数据。大多数网络管理系统都能收集、存储和呈现轮询数据。

多种解决方案可在市场上使用，以满足企业环境的性能管理的需要。这些系统能从网络设备和服务器上收集、存储和提交数据。这类系统大多配备基于 Web 的界面，支持在企业的任何位置访问性能数据。一些常用的性能管理解决方案包括：

- InfoVista VistaView
- SAS IT Service Vision
- Trinagy TREND

上述产品的评估将确定它们是否符合不同用户的要求。一些供应商的解决方案支持与网络管理平台及系统管理平台集成。例如，InfoVista 支持使用 BMC Patrol Agent 提供来自应用服务器的关键性能统计数据。每种产品在基本报价下，定价模式和功能不尽相同。Cisco设备如NetFlow、RMON和Cisco IOS服务保证代理/响应时间报告程序(RTR/SAA CSAA/RTR)的性能管理功能支持，可以在某些解决方案上使用。Cisco的广域网交换机可以用来能使用收集和查看性能数据的技术支持。

思科IOS上的CSAA/RTR服务保证代理程序(SAA) /响应时间报告器(RTR)功能可以用来测量IP设备之间的响应时间。配置有CSAA的源路由器能够测量到目的地IP设备的响应时间，目的地IP设备可以是路由器或IP设备。可以测量路径上的每级跳在源地址和目的地之间的响应时间。通过配置 SNMP 陷阱，可以在响应时间超过预定义的阈值时向管理控制台发出警报。

在 Cisco IOS 最近的增强功能中，CSAA 增加了以下方面的测量功能：

- 超文本传输协议 (HTTP) 服务性能域名系统 (DNS) 查找传输控制协议 (TCP) 连接HTTP 事务时间
- IP 语音 (VoIP) 流量的数据包间延迟变化量（抖动）
- 特定服务质量 (QoS) 下，终端间的响应时间IP 服务类型 (ToS) 位
- 基于 CSAA 生成的数据包的丢包数

要在路由器上配置 CSAA 功能，可以使用 Cisco Internetwork Performance Monitor (IPM) 应用。许多路由器都内嵌 CSAA/RTR，但不一定具备 Cisco IOS 软件的全部功能。支持CSAA/RTR Cisco的IOS软件版本必须安装在IPM用于收集性能统计数据的设备上。欲知支持CSAA/RTR/IPM的Cisco IOS版本概要，参见“IPM常见问题”网站。

有关 IPM 的更多信息，请参阅：

- IPM 概述
- 服务保证代理

性能分析和调整

如今，用户流量显著增加，这就对网络资源提出了更高的要求。一般情况下，网络管理员无法完全掌握网络中存在的流量类型。但是，用户和应用流量分析功能可以帮助详细了解网络中存在的流量。收集流量分析信息有两种技术：RMON 探测器和 NetFlow。

RMON

RMON标准是设计为部署在分布式体系结构中，该结构中的代理(嵌入或位于独立探测器中)通过SNMP与中心站点(管理控制台)通信。RFC 1757 RMON标准组织监控功能到九个组中，以支持以太网拓扑；同时在RFC 1513中添加第十个组，以提供Token Ring-unique 参数。快速以太网链路监控在RFC 1757标准框架中提供，光纤分布式数据接口FDDI环监控则在RFC 1757和RFC 1513框架中提供。

新兴的RFC 2021 RMON规格在MAC控制（MAC）层到网络和应用层之外驱动远程监控标准。此设置可以让管理员分析和故障检测网络应用，如Web流量、NetWare、备注、电子邮件、数据库访问，网络文件系统(NFS)和其他。根据网络中应用层数据流的最重要流量，目前可以使用RMON告警、统计数据、历史记录、主机/会话组主动监控和维护网络可用性。利用 RMON2 标准，网络管理员可以像以前一样部署基于标准的监控解决方案，为基于服务器的任务关键型应用提供支持。

下表列出了各个 RMON 组的具体功能。

RMON 组 (RFC 1757)	功能
统计信息	网段中或端口上的数据包数、八位组数、广播数、错误数和 Offer 数。
历史记录	对统计数据组的计数定期采样和保存，以备日后检索。
主机	有关网段中或端口上的每个主机设备的统计数据。
排名前 N 的主机	用户定义的主机组子报告，按统计数据（计数）排列。通过仅返回此结果，可帮助减少管理流量。
流量矩阵	有关网络中主机间对话的统计数据。
警报	可针对关键 RMON 变量设置的阈值，用于实现前摄式管理。
事件	当超过警报组阈值时，系统会生成 SNMP 陷阱和日志条目。
数据包捕获	管理过滤器组捕获数据包（用于上传到管理控制台）所使用的缓冲区。
令牌环	环站 – 令牌环中各个工作站的详细统计数据；环站顺序 – 令牌环中现有工作站的顺序列表；环站配置 – 每个工作站的配置和插入/移除操作；源路由 – 源路由的统计数据，例如跳数等等。

RMON2	功能
协议目录	代理监控和维护统计数据所使用的协议。
协议分发	每个协议的统计数据。
网络层主机	网段中、令牌环中或端口上的每个网络层地址的统计数据。
网络层矩阵	网络层地址对的流量统计数据。
应用层主机	每个网络地址的应用层协议的统计数据。
应用层矩阵	网络层地址对的应用层协议的流量统计数据。
用户可定义的历史记录	扩展历史记录的范围，除 RMON1 链路层统计数据外，增加所有 RMON、RMON2、MIB-I 或 MIB-II 统计数据。
地址映射	MAC 与网络层地址的绑定。
配置组	代理的功能和配置。

Netflow

Cisco NetFlow功能使数据流的详细统计数据能被收集起来，提供容量规划、计费和故障排除功能。NetFlow可以在单个接口上配置，并提供通过这些接口的数据流信息。详细的流量统计数据中包括的部分信息举例如下：

- 源和目的 IP 地址
- 输入和输出接口编号
- TCP/UDP 源端口和目的端口
- 数据流中的字节数和数据包数
- 源和目的自治系统号
- IP 服务类型 (ToS)

网络设备上收集的 NetFlow 数据会导出到收集器设备。收集器执行功能，如减少数据量(过滤和聚合)，分级数据储存和文件系统管理。Cisco提供NetFlow收集器和NetFlow分析器应用程序，可以采集和分析路由器和Catalyst交换机的数据。也有一些共享软件工具，例如cflowd ，能收集Cisco NetFlow用户数据协议(UDP)的记录。

NetFlow 数据可使用三种不同格式的 UDP 数据包进行传输：

- 版本 1 – 初始 NetFlow 版本中支持的原始格式。
- 版本 5 – 后期增强版本，增加了边界网关协议 (BGP) 自治系统信息和数据流顺序号。
- 版本7---稍后的增强措施，为配备Netflow功能卡(NFFC)的Cisco Catalyst 5000系列交换机增加NetFlow交换技术支持功能。

版本2到4和版本6既不由FlowCollector发布，也不由它提供支持。在上述三个版本中，数据报由报头和一个或多个数据流记录组成。

有关更多信息，请参阅 NetFlow 服务解决方案指南白皮书。

下表列出了支持从路由器和 Catalyst 交换机收集 NetFlow 数据的 Cisco IOS 版本。

Cisco IO	支持的思科硬件平台	支持的

S 软件版本		NetFlow 导出版本
11.1 CA 和 11.1 CC	Cisco 7200、7500 和 RSP7000	V1 和 V5
11.2 和 11.2 P	Cisco 7200、7500 和 RSP7000	V1
11.2 P	思科路由交换模块 (RSM)	V1
11.3 和 11.3 T	Cisco 7200、7500 和 RSP7000	V1
12.0	Cisco 1720、2600、3600、4500、4700、AS5800、7200、uBR7200、7500、RSP7000 和 RSM	V1 和 V5
12.0 T	Cisco 1720、2600、3600、4500、4700、AS5800、7200、uBR7200、7500、RSP7000、RSM、MGX 8800 RPM 和 BPX 8600	V1 和 V5
12.0(3)T 及更高版本	Cisco 1600*、1720、2500**、2600、3600、4500、4700、AS5300*、AS5800、7200、uBR7200、7500、RSP7000、RSM、MGX8800 RPM 和 BPX 8650	V1、V5 和 V8
12.0(6)S	Cisco 12000	V1、V5 和 V8
—	带 NetFlow 功能卡 (NFFC) 的 Cisco Catalyst 5000***	V7

*Cisco 1600及2500平台上的NetFlow Export V1、V5和V8支持功能，目标是Cisco IOS软件版本12.0(T)。 如果使用 Cisco IOS 12.0 Mainline 版本，这些平台将不支持 NetFlow。

**AS5300平台上的NetFlow V1、V5和V8支持功能，目标是Cisco IOS软件版本12.06(T)。

*** 在 Catalyst 5000 系列管理引擎软件版本 4.1(1) 或更高版本中，可以支持 MLS 和 NetFlow 数据导出。

安全管理

安全管理的目标是根据本地指南控制网络资源使用，以便网络不被破坏(有意或无意) 。安全管理子系统，例如，能够监控用户注册到网络资源，拒绝代码输入不适当的访问。安全管理是一个内容十分广泛的主题，本文档中探讨的内容仅涉及与 SNMP 和基本设备访问安全性相关的主题。

有关高级安全的详细信息，请参阅：

- 提高 IP 网络的安全性
- 开放系统

良好的安全管理实践以全面的安全策略和到位的安全规程为基础。为所有路由器和交换机创建特定平台的最小配置标准至关重要，该标准需遵循安全和性能的行业最佳实践。

有多种方法可以控制对思科路由器和 Catalyst 交换机的访问，其中一些方法包括：

- 访问控制列表 (ACL)
- 设备本地的用户 ID 和密码
- 终端访问控制器访问控制系统 (TACACS)

TACACS是运行在网络客户端设备之间的依靠TACACS服务器的互联网工程任务组(RFC 1492)标准安全协议。TACACS是一种认证机制，用来验证寻找远程访问特权数据库设备的身份。TACACS 的变体包括 TACACS+，这是一种将身份验证、授权和计费功能相分离的 AAA 体系结构。

Cisco使用的TACACS+能够更好地控制谁能访问Cisco设备无论是以特权还是非特权的模式。可以出于容错的目的配置多个 TACACS+ 服务器。随着TACACS+的启用，路由器提示用户使用用户名和密码。身份验证不仅可用于实现登录控制，也可用于对单个命令进行身份验证。

身份验证

认证是识别用户的过程，包括登录和密码对话、挑战和响应，以及消息支持。允许访问路由器或交换机之前，需要通过认证，来识别用户。身份验证与授权之间存在一个基本的关联原则。用户被授予的授权权限越多，身份验证就应该越严格。

授权

授权可以为用户请求的每项服务提供远程访问控制，包括一次性认证和授权。在思科路由器上，用户的授权级别范围是0~15，其中0表示最低级别，15表示最高级别。

记账

记帐允许收集和发送用于计费、审计和报告的安全信息，如用户身份、开始和停止时间、所执行的命令。计帐能够让网络管理器追踪用户正在访问的服务，以及用户正在消耗的网络资源数量。

下面的表格列举了在Cisco路由器和Catalyst交换机上使用TACACS+、认证、授权和记帐的基本示例命令。有关更深入的命令，请参阅身份验证、授权和计费命令文档。

Cisco IOS 命令	目的
路由器	
aaa new-model	启用身份验证、授权和计费 (AAA) 作为主要的访问控制方法。
AAA accounting {*system|网络|连接|exec|命令级别*} {*start-stop|等待开始|仅停止*} {*tacacs+|radius*}	使用全局配置命令启用计费。
AAA authentication login default tacacs+	设置路由器，以便配有登录默认值的所有终端线路的连接可以使用TACACS+进行认证，如果由于任何原因没有通过认证，连接将失败。
AAA authoriz	请求TACACS+ 服务器，设置路由器来检查用户是否被允许运行EXEC Shell。

atio n exe c defa ult taca cs+ non e	
taca cs-serv er host *taca cs+ serv er ip addr ess*	使用全局配置命令指定用于执行身份验证的 TACACS+ 服务器。
taca cs-serv er key *shar ed-secr et*	指定由带全局配置命令的TACACS+服务器和 Cisco路由器知道的共享秘密。
Catalyst 交换机	
set auth enti cati on logi n taca cs ena ble [*all |控制台 | http | teln et*] [*主要*]	对常规登录模式启用 TACACS+ 身份验证。使用 console 或 telnet 关键字，仅对控制台端口或 Telnet 连接尝试启用 TACACS+。

set authorization exec enable {option} fallback option} [*console	telnet |两者*]	对常规登录模式启用授权。使用 console 或 telnet 关键字，仅对控制台端口或 Telnet 连接尝试启用授权。
Set tacacs-server key *shared-secret*	指定 TACACS+ 服务器和交换机已知的共享密钥。
Set tacacs-server host *tacacs+ server ip address*	使用全局配置命令指定用于执行身份验证的 TACACS+ 服务器。
Set accounting commands ena	使用配置命令启用计费。

ble {*config* | *all*} {*stop-only* } *tacacs+*	

如需详细了解如何配置 AAA 来监视和控制对 Catalyst 企业局域网交换机命令行界面的访问，请参阅使用身份验证、授权和计费控制对交换机的访问文档。

SNMP 安全

SNMP协议可以用来修改在路由器和Catalyst交换机配置，与CLI发送的修改内容类似。为了防止任何人通过 SNMP 进行未经授权的访问和更改，应在网络设备上配置适当的安全措施。使用社区字符串时，应遵循标准的密码指导原则（长度、字符和猜测难度）。请务必更改社区字符串，不要使用公共和专用默认值。

所有SNMP管理主机都应该具有静态IP地址，通过IP地址和访问控制表(ACL)预定义方式，明确授予这种网络设备的SNMP通信权。 Cisco IOS和Cisco Catalyst软件具有安全功能，能够保证只有授权管理站才允许在网络设备上执行更改。

路由器安全功能

SNMP 权限级别

此功能限制了管理站在路由器上提供的操作类型。路由器有两种权限级别：只读 (RO) 和读写 (RW)。 RO 级别仅允许管理工作站对路由器数据执行查询操作。它不允许配置命令，例如重新启动路由器和关闭要执行的接口等。要执行这些操作，必须拥有 RW 权限级别。

SNMP 访问控制列表 (ACL)

SNMP ACL功能可以与SNMP权限功能一起使用，用来限制特定管理站从路由器上请求管理信息。

SNMP 视图

此功能可限制管理工作站从路由器检索特定信息。它可以与SNMP权限级别和ACL特性一起使用，以通过管理控制台执行受限制的数据访问。有关 SNMP 视图的配置示例，请访问 snmp-server view。

SNMP 版本 3

SNMP 版本 3 (SNMPv3) 可用于在网络设备与管理工作站之间安全地交换管理数据。SNMPv3加密和认证功能确保在传输数据包时到管理控制台时具有很好的安全性。Cisco IOS 软件版本 12.0(3)T 及更高版本可支持 SNMPv3。有关 SNMPv3 的技术概述，请参阅 SNMPv3 文档。

接口上的访问控制列表 (ACL)

ACL 功能为防范 IP 欺骗等类型的攻击提供了安全措施。ACL 可以应用到路由器的传入或传出接口

。

Catalyst 局域网交换机的安全功能

IP 允许列表

ip permit列表功能限制从未授权的源IP地址到交换机的Inbound Telnet和SNMP访问。当发生违规或未经授权的访问时，支持系统日志消息和SNMP陷阱通知到管理系统。

您可以组合使用 Cisco IOS 的多种安全功能来管理路由器和 Catalyst 交换机。需要建立安全策略，以限制能够访问交换机和路由器的管理站的数量。

欲知如何增强IP网络安全的更多信息，参见“增强IP网络安全”。

记帐管理

记帐管理是测量网络利用率参数的程序，这样便可以适当调控网上的单个用户或群组用户，用于记帐或退款目的。适当记帐管理的第一步类似于性能管理，用来测量所有重要网络资源的利用率。利用 Cisco NetFlow 和 Cisco IP Accounting 功能即可测量网络资源的使用情况。通过分析利用这些功能收集到的数据，可以洞察当前的使用模式。

对任何服务级别协议 (SLA) 而言，基于使用情况的计费和记账系统都是必不可少的组成部分。 它提供在一个服务水平协议下定义义务的实用方法和水平协议条款之外的清晰的逻辑行为。

收集数据可以通过探测器或 Cisco NetFlow 来实现。Cisco提供NetFlow收集器和NetFlow分析器应用程序，可以采集和分析路由器和Catalyst交换机的数据。此外，cflowd 等共享软件应用也可用于收集 NetFlow 数据。资源使用的现行测量可以提供计费信息和信息平估计持续的公平资源和最佳资源。一些常用的计费管理解决方案包括：

- Evident Software

网流激活和数据收集策略

NetFlow(网络流)是一种输入端测量技术，允许获取所需数据，进行网络规划、监控和记帐应用。NetFlow应在边缘/聚合路由器接口上配置，供服务提供商或企业用户的广域网访问路由器接口使用。

思科系统公司建议精心规划 NetFlow 部署，从战略角度安设路由器并启用 NetFlow 服务。NetFlow可以递增式(逐个接口)和战略式(在精选路由器上)部署，而不必在网络的每一个路由器上部署。根据客户的数据流模式、网络拓扑和体系结构，思科工作人员与客户联合确认Netflow 应该在哪些重要路由器和重要接口上激活。

部署时的主要考虑事项包括：

- NetFlow 服务应该用作边缘测量和访问列表性能加速工具，而不应该在热核/骨干路由器或CPU利用率非常高的路由器上激活。
- 了解应用驱动的数据收集要求。记帐应用可能只需要始发和终接路由器流信息，因而监控应用程序可能要求一个更全面的(数据密集型)端到端视图。
- 了解网络拓扑和路由策略对流收集策略的影响。例如，通过激活关键聚合路由器上的NetFlow避免相同数据流集中。数据流在聚合路由器上生成或终止，而不是在骨干网路由器或中间路由器

上生成或终止。聚合路由器将提供相同数据流信息的重复视图。

- "服务提供商在提供运营商业务时(在他们的网络中传递数据流,既不开始又不终止数据流)，可以利用NetFlow输出数据，测量网络资源的传输数据流使用，达到记帐和计费目的。"

配置 IP 计费

思科 IP 计费支持可提供基本的 IP 计费功能。通过启用IP 记帐，用户可以根据源和目的地IP地址，查看通过Cisco IOS软件交换的字节数量和信息包数量。测量仅对出站传输 IP 流量执行。计费统计数据不包括软件生成的数据流、或在软件中终止的数据流。为确保计费合计值准确无误，软件使用两个计费数据库：活动数据库和检查点数据库。

思科 IP 计费支持还会提供信息来帮助确定违反 IP 访问列表的 IP 流量。通过确定违反 IP 访问列表的 IP 源地址，有助于发现试图侵害安全性的潜在尝试，同时也能表明 IP 访问列表配置需要验证。要使用户应用此功能，使用ip accounting access-violations命令启用访问列表侵害的IP计帐。用户然后可以显示单一来源发出的试图破坏安全性而访问列表的源目的地对的字节数和信息包数量。在默认情况下，ip 记帐显示已通过访问控制列表和被路由的信息包数量。

为了启用ip 记帐，请在接口配置模式中为每个接口提供下列命令之一：

命令	目的
ip accounting	启用基本的 IP 计费功能。
ip accounting access violations	启用可帮助确定违反 IP 访问列表的 IP 流量的 IP 计费功能。

如果要配置其他ip 记帐功能，请在全局配置模式中使用下面的一个或多个命令：

命令	目的
ip accounting-threshold threshold	设置所要创建的计费条目的最大数量。
ip accounting-list ip-address wildcard	筛选主机的计费信息。
ip accounting-transits count	控制将保存在IP记帐数据库的传输记录数量。

有关本文档中所用的规则信息，请参阅 Cisco Technical Tips Conventions 。