网络管理系统：最佳实践白皮书

文档ID15114

已更新：七月11， 2007

 下载 pdf文档

 打印

反馈

相关产品

- Service Assurance Agent (SAA)
- CiscoWorks Resource Manager Essentials
- 高可用性
- 简单网络管理协议 (SNMP)
- 远程监控(RMON)

目录

简介

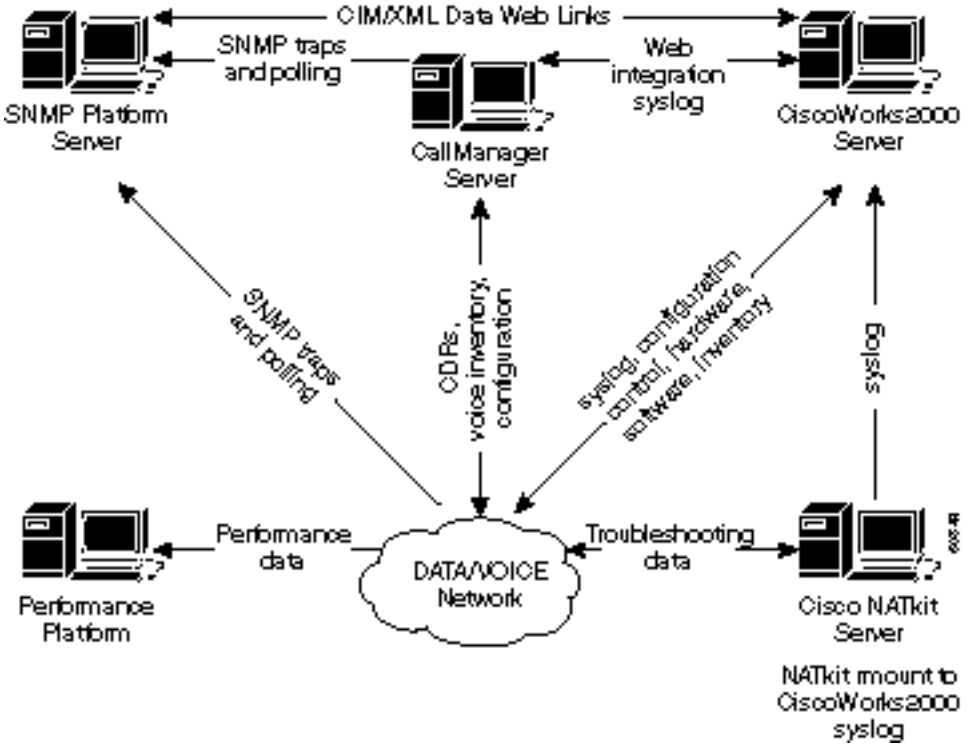
国际标准化组织(ISO)网络管理模型定义了网络管理五个功能区域。本文包括所有功能区域。本文的整体目的是要在每个功能区域提供实用的推荐标准，增加当前管理工具和运作的整体效果。同时还提供了针对未来实施网络管理工具和技术的设计指导原则。

网络管理

ISO网络管理模型的五个功能区域下面是列出的。

- 故障管理—检测，隔离，通知，并且更正在网络遇到的故障。
- 配置管理—网络设备的配置方面例如配置文件管理、库存管理和软件管理。
- 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—提供存取对于网络设备和公司资源给已授权个人。
- 记帐管理—网络资源使用信息。

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。此体系结构包括计划管理VoIP (VoIP)的那些人的一个Cisco CallManager服务器：图表显示您如何会集成CallManager服务器到NMS拓扑。



网络管理体系结构包括以下：

- 故障管理的简单网络管理协议(SNMP)平台
- 长期性能管理和趋向的性能监控平台
- CiscoWorks2000配置管理、系统日志收集和硬件和软件库存管理的服务器

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包括规格和模式。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是代表结构化数据使用的标记语言以文本形式。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。

思科的高级服务客户也包括另外的积极监控和故障排除的思科的NATkit服务器。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。

*互联网工作技术概述的*网络管理基础章节提供关于网络管理基础的更多详细概要。

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

在企业中部署的网络管理平台管理包括多厂商网络网络要素的基础设施。平台接收和处理事件从网元在网络。从服务器和其他重要资源的事件可能也转发到管理平台。以下普遍提供的功能在标准管理平台包括：

- 网络发现
- 网元结构拓扑图
- 事件处理程序
- 性能数据收集器和grapher
- 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。能力检测问题迅速在所有网络是关键。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。

网络管理平台这样HP OpenView、Computer Associates Unicenter和SUN Solstice可进行网络设备发现。每个网络设备由在管理平台的控制台的一个图形要素代表。在图形要素的不同的颜色代表当前网络设备的运行状态。网络设备可以配置发送通知，呼叫SNMP陷阱，到网络管理平台。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，通常呼叫事件，在日志文件安置。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。

思科发布管理的多种网络设备MIB文件。Cisco MIB文件位于cisco.com网站，包括以下信息：

- 在SNMPv1格式发布的MIB文件
- 在SNMPv2格式发布的MIB文件
- 在Cisco设备的支持的SNMP陷阱
- 思科当前SNMP MIB对象的OIDs

一定数量的网络管理平台能够管理多个地理分布式站点。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。分布式体系结构也允许人员本地管理他们的从远程站点的网络用系统。

使用Web接口，对管理平台的一种最近的增强功能远程是能力对管理网络网络要素。此增强排除需要对于在个人用户站的特殊客户端软件访问管理平台。

典型的企业包括不同的网元。然而，每个设备通常要求供应商专用的网元管理系统为了有效管理网元。所以，重复的管理站可能轮询网元对于同一信息。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。其设计根据对象管理组织(OMG)对象模型。

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 server使用主要存储配置文件和软件镜像网络设备的。路由器和交换机能够发送系统日志信息对系统日志服务器。当问题遇到时，消息实现故障排除功能。偶然地， Cisco支持人员需要系统消息执行根本原因分析。

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。过滤器能指定哪些系统消息将转发到主要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。当故障在系统时，发生网络设备能够警告管理站。有效的故障管理系统包括几个子系统。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。

在网络设备应该一致启用陷阱。另外的陷阱用路由器和交换机的新的Cisco IOS软件版本支持。检查和更新配置文件保证正确的解码陷阱是重要的。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	说明
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*表明任一个下列的条件存在： • 电压故障 • 同时出现温度和风扇故障 • 一百个百分比电源故障(两出于两或者一出于

	一个) • Electrically Erasable Programmable Read-Only Memory (EEPROM)失败 • 非易失性RAM (NVRAM)失败 • MCP通信故障 • NMP状态未知 chassisMinorAlarm表明任一个下列的条件存在： • 温度告警 • 风扇故障 • 部分电源故障(一出于两) • 两个电源不兼容类型
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。

环境监控器(envmon)陷阱在CISCO-ENVMON-MIB陷阱定义。当环境门限值被超出时， envmon陷阱发送Cisco企业特有环境监控器通知。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。如果选项没有指定，所有环境类型启用。它可以是一个或很多以下值：

- 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。
- 供应— ciscoEnvMonRedundantSupplyNotification发送，如果冗余电源(哪里现存)出故障。
- 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。协议级故障管理实施是可用的使用元素管理器系统例如CiscoWorks2000 Campus Manager。在Campus Manager的流量控制器应用着重利用微型RMON支持的交换机管理在Catalyst交换机。

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。在事件管理系统后的此体系结构与Manager of Managers (MOM)系统是可比较的。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。要得到更多信息，请去思科信息中心。

前摄故障监视和通知

RMON报警和事件是在RMON规格定义的两组。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。此方法浪费网络带宽，并且能根据轮询间隔也未命中实际阈值。

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报警和事件组提供管理重要网络设备主动手段。

Cisco系统推荐实现RMON报警和事件在重要网络设备。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。开始与Cisco IOS软件版本11.1(1)，所有路由器镜像支持RMON报警和事件组。

关于RMON警报和事件实现的详细信息，参考RMON警报和事件实现部分。

RMON内存约束

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。因为取决于运行时配置， RMON的动态内存需求变化。

下表定义了每微型RMON组的运行时RMON内存用量信息。

RMON组定义	使用的DRAM空间	备注
统计信息	每个交换以太网/快速以太网端口140个字节	每个端口
历史记录	3.6 50个桶的K *	每个另外的桶使用56个字节
报警和事件	2.6每报警和其对应的事件项的K	每报警每个端口

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。

两个方法从哪些是可得到配置RMON报警和事件：

- 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

使用CLI接口，要实现RMON报警和事件，请执行以下步骤：

1. 查找接口索引关联与Ethernet0通过走ifTable MIB。`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OID关联与CLI字段是受监视。对于此示例，‘广播的OID是1.3.6.1.2.1.2.2.1.12。特定MIB变量的思科OIDs从cisco.com网站是可得到。
3. 确定设置的阈值和事件以下参数。上升和降低阈值采样类型(绝对或Delta)采样间隔操作，当阈值达到为起到示例目的，设置阈值监控以Ethernet 0收到的广播包数量。如果在60秒示例之间收到的广播包数量大于500个，此时将生成陷阱。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事件1在以太网0"所有人Cisco的陷阱网关描述“高广播RMON事件2日志广播的说明“正常在以太网0"所有人Cisco接收**
5. 指定阈值和相关参数(RMON报警)使用以下CLI命令，：**RMON报警1 ifEntry.12.1 60 delta上升极限500 1下降极限0 2所有人Cisco**
6. 请使用SNMP轮询这些表验证事件表条目在设备被做了。

```
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. 请使用SNMP轮询这些表验证告警表条目设置。`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

为了实现RMON报警和事件与SNMP设置的操作，请完成这些步骤：

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. 指定阈值和相关参数(RMON报警)使用以下SNMP设置的操作，：`# 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. 轮询这些表验证事件表条目在设备被做了。`% 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. 轮询这些表验证告警表条目设置。`% snmpwalk -v 1 172.16.97.132 private .1.3.6.1.2.1.16.3.1`

show interface

此示例是结果**show interface命令**。

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。联系信息应该包括电话号码和人或部门的名称。

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。设备的命名规则能使用地理位置，建立名称，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

当您添加在现有的网络设备需要时的新的配置命令，您必须验证完整性的命令，在实际实施发生前。一个配置的网络设备能不正确地有对网络连通性和性能的一个灾难性影响。必须检查Configuration命令parameters避免不匹配或不兼容问题。经常安排配置详尽的回顾与Cisco工程师的是可行的。

功能完备的CiscoWorks2000精华允许自动备份在路由器和思科Catalyst交换机的配置文件。精华安全功能可以用于执行在配置更改的验证。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。对于在多个设备的配置更改，两个选项是可用的：在CiscoWorks2000精华或**cwconfig**脚本当前版本的基于Web的网络配置。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。

这些功能可以用在CiscoWorks2000精华的配置管理工具完成：

- 推送从精华配置存档的配置文件到设备或多个设备
- 请求从设备的配置到Essentials文档
- 解压缩从存档的新配置并且写它到文件
- 导入配置从文件并且推送配置到设备
- 在Essentials文档比较最后两配置
- 比一个指定的日期或版本删除配置旧从存档
- 复制启动配置对运行的配置

库存管理

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。应该使用发现引擎例如在网络管理平台实现的那些。

库存数据库在网络设备提供详细配置信息。普通的信息包括型号硬件，安装模块，软件镜像，微码级，等等。所有这些信息是关键的在完成任务例如软件和硬件维护。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。

完成设备维护的Upgrade窗口为一些组织相当被限制。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包括量度同意在供应商和其客户之间。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。

各种接口统计信息可以从网络设备收集测量性能级别。这些统计信息可以包括作为量度在SLA。统计信息例如输入队列丢弃、输出队列丢弃和已忽略的数据包为诊断与性能有关的问题是有用的。

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。某些网络协议性能与在网络设备的缓冲可用性直接地涉及。测量设备级性能统计数据是关键在优化更高级别性能的协议。

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。在网络管理系统的轮询引擎可以为数据收集目的使用。多数网络管理系统能够收集，存储和提交轮询数据。

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。在多数产品的基于Web的接口由任何地方企业使性能数据可访问。某些通常部署的性能管理解决方案包括：

- InfoVista VistaView
- SAS IT服务宣明会
- 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。一些供应商支持集成用网络管理和系统管理平台。例如， InfoVista支持BMC巡查代理提供从应用服务器的关键性能统计信息。每种产品有一个不同的定价模型和功能与基本提供。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。如果响应时间超出预定义的门限值， SNMP陷阱可以配置警告管理控制台。

对Cisco IOS的最近的增强功能扩大CSAA能力测量以下：

- 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事务处理时间
- 在IP (VoIP)流量的语音包间延迟差异(抖动)
- 端点之间的响应时间一特定服务质量(QoS)的IP服务类型(Tos)位
- 包丢失使用CSAA生成数据包

配置在路由器的CSAA功能可以是实现的使用Cisco互联网性能监控(IPM)应用程序。CSAA/RTR在许多，但是不是Cisco IOS软件的所有的特性组被嵌入。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。

关于IPM的其他信息包括：

- IPM概述
- Service Assurance Agent

性能分析和调整

用户数据流在网络资源显著增加和放置了更加高要求。网络管理器典型地有在运作的流量类型的一个有限视图在网络。用户和应用流量描出提供流量的详细信息在网络的。两技术、RMON探测器和Netflow，提供能力收集数据流配置文件。

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。RMON2使网络管理员继续他们的部署基于标准的监控解决方案支持任务关键型，基于服务器的应用。

下表列出RMON组的功能。

RMON组(RFC 1757)	功能
统	数据包、八位位组、广播、错误和提供的计数器在分

计信息	段或端口。
历史记录	周期地采样并且保存最新检索的统计组计数器。
主机	维护在每个主机设备的统计信息在分段或端口。
主机前N个	主机的用户定义子集报告分组，排序由统计计数器。通过返回仅结果，管理数据流最小化。
数据流表	保存在主机之间的会话统计数据在网络。
报警	在主动管理的重要RMON变量可以设置的阈值。
事件	当报警组阈值被超出时，生成SNMP陷阱和日志条目。
数据包捕获	管理上传的过滤器组捕获的数据包的缓冲区对管理控制台。
令牌环	环位置—在个人站点环位置顺序的详细统计—当前一个排好序的站列表在环环位置配置—配置和插入/删除每站点源路由统计数据在源路由，例如跳数和其他

RMON2	功能
协议目录	代理程序监控并且维护统计信息的协议。
协议分配	每份协议的统计信息。
网络层主机	每个网络层地址的统计信息在分段、环或者端口。
网络层一览表	对的流量统计网络层地址。
应用层主机	由应用层协议的统计信息每个网络地址的。
应用层一览表	由应用层协议的流量统计对的网络层地址。
用户可定义的历史记录	扩大在RMON1链路层统计之外的历史记录包括所有RMON， RMON2， MIB-I或者MIB-II统计信息。
地址映射	MAC到网络层地址绑定。
配置组	代理程序功能和配置。

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。信息的以下类型是详细的数据流统计的一部分：

- 源和目的 IP 地址
- 输入和输出接口号
- TCP/UDP源端口和目的地端口
- 字节数和数据包在流
- 源及目的地自治系统编号
- IP服务类型(Tos)

在网络设备收集的NetFlow数据导出对收集器计算机。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。

使用在三个不同的格式的UDP数据包NetFlow数据传输：

- 版本1 —支持初始NetFlow版本原始格式。
- 版本5 —一最新增强已添加边境网关协议(BGP)自控系统信息和流序号。
- 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。在所有三个版本中，数据包包括报头和一个或更多flow record。

欲知更多信息，参考NetFlow服务解决方案指南白皮书。

下表概述支持收集的NetFlow数据Cisco IOS版本从路由器和Catalyst交换机。

Cisco IOS软件版本	支持的Cisco硬件平台	支持的Netflow导出的版本
11.1 CA和11.1 CC	Cisco7200， 7500和RSP7000	V1和V5
11.2和11.2 P	Cisco7200， 7500和RSP7000	V1
11.2 P	Cisco路由交换模块(RSM)	V1
11.3和11.3 T	Cisco7200， 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、MGX8800 RPM和BPX 8600	V1和V5
12.0(3)T和	思科1600*， 1720，	V1、V5和V-8

以后	2500**， 2600， 3600，4500， 4700，AS5300*， AS5800，7200， uBR7200，7500， RSP7000、RSM、MGX8800 RPM和BPX 8650	
12.0(6)S	Cisco 12000	V1、V5和V-8
	有Netflow功能卡***的思科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)。这些平台的Netflow支持不是可用的在Cisco IOS 12.0主线版本。

**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)。

Catalyst 5000系列Supervisor Engine软件版本4.1(1)或以后支持*** MLS和NetFlow输出数据。

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。安全管理是非常广泛主题;因此本文的此区域只包括安全与SNMP和基本的设备访问安全性有关。

关于高级安全的详细信息包括：

- 增强IP网络安全
- 开放式系统

一次好安全管理实施从到位合理的安全策略和步骤开始。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。

有控制访问多种方法在Cisco路由器和Catalyst交换机的。其中一些方法包括：

- 访问控制列出(ACL)
- 用户ID和密码本地对设备
- 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的变化包括TACACS+，分离认证、授权和记帐功能的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。多个TACACS+服务器可以为容错配置。随着TACACS+的启用，路由器提示用户使用用户名和密码。验证能为登录控制配置或验证单个命令。

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。有认证和授权之间的一个基本关系。越多授权权限用户接收，越强验证应该。

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。

核算

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。参考更加详细的命令的认证、授权和记帐命令文档。

Cisco IOS 命令	**目的**
路由器	
aaa new-model	启用认证，授权，占(AAA)作为主要方法访问控制。
Aaa accounting {*系统|网络|连接|exec|指令水平***} {***开始-结束|等待开始|仅停止***} {***TACACS+|radius***}**	与全局配置命令的启用帐户。
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认证exec默认TACACS+无	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。
tacacs-server host *TACACS+服务器IP地址*	指定将使用验证用全局配置命令的TACACS+服务器。
tacacs-server key*共享密钥*	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 authentication login tacacs enable [*全部|控制台|http|telnet*] [primary]	正常登录模式的Enable (event) TACACS+认证。请使用控制台或Telnet关键字启用仅TACACS+控制台端口或Telnet连接测试的。
set authorization exec enable {option}{*回退选项*} [*控制台|telnet|两个*]	正常登录模式的Enable (event)授权。请使用控制台或Telnet关键字启用仅授权控制台端口或Telnet连接测试的。
设置 tacacs-server key*共享密钥*	指定由TACACS+服务器和交换机知道的共享机密。
设置 tacacs-server host *TACACS+服务器IP地址*	指定将使用验证用全局配置命令的TACACS+服务器。
Set accounting commands enable {*设置|所有*} {stop-only} *TACACS+*	配置命令启用帐户。

使用认证、授权和记帐文档，关于如何配置AAA的更多信息监控和控制对命令行界面的访问在Catalyst enterprise LAN交换机，参考控制访问到交换机。

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。在网络设备应该配置适当的安全措施通过SNMP防止未经授权的访问和更改。社区字符串应该遵从长度、字符

和困难的标准密码方针猜测。更改从他们的公共和专用默认值的社区字符串是重要的。

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。有权限级别的两种类型在路由器的：Read-Only(RO)和读写(RW)。RO级别只允许管理站查询路由器数据。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。仅RW权限级别可以用于执行这样操作。

SNMP访问控制表(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

此功能限制可以从路由器获取由管理站的特定信息。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。对于SNMP视图配置示例，请去snmp-server view。

SNMP 版本 3

管理数据SNMP版本3 (SNMPv3)提供安全交换在网络设备和管理站之间的。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及以上版本支持SNMPv3。对于SNMPv3技术概要，请去SNMPv3文档。

在接口的访问控制表(ACL)

ACL功能提供在防止攻击的安全措施例如IP伪装。ACL在路由器的流入或流出的接口可以应用。

Catalyst LAN交换机安全特性

IP Permit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。

Cisco IOS安全功能的组合可以用于管理路由器和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。使用Cisco NetFlow和思科IP记帐功能，网络资源使用率可以被测量。通过这些方法收集的数据的分析提供见解到当前使用模式。

一个基于用法的记帐和计费系统是重要部分其中任一服务级别协议。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。

数据可以通过探测器或Cisco NetFlow收集。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。共享件应用程序例如cflowd也用于收集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。一些通常部署的记帐管理解决方案包括：

- 明显的软件

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。

Cisco系统仔细推荐与在这些战略上查找的路由器启动的NetFlow服务的一个计划内的NetFlow部署。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。

关键部署注意事项包括：

- 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需求。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影响在流收集策略。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记帐

Cisco IP记帐支持提供基本IP记帐功能。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。仅转接IP数据流仅被测量和根据一个出站基本类型。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。要维护准确记帐总额，软件维护两个记帐数据库：激活和Checkpoint的数据。

Cisco IP记帐支持也提供识别IP数据流发生故障IP访问列表的信息。识别违犯IP访问列表的IP源地址发信号可能的尝试对破坏安全性。数据也表明应该验证IP访问控制列表配置。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记帐	Enable (event)基本IP记帐。

ip accounting access violations	Enable (event) IP记帐以发生故障IP访问列表的能力识别IP数据流。

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	设置将创建的最大的记帐项目数。
ip accounting-list ip-address wildcard	主机的过滤器记帐信息。
ip accounting-transits count	控制将保存在IP记帐数据库的传输记录数量。

相关信息

- **配置基本原理配置指南**
- **Cisco企业管理解决方案，音量我由Cisco出版社， ISBN 1587050064**
- **技术支持和文档 - Cisco Systems**

本文档是否是有用？有 没有

感谢您的反馈。

打开支持案例（需要思科服务合同。）

相关的思科支持社区讨论

思科支持社区是提出和解答问题、分享建议以及与同行协作的论坛。

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

已更新：七月11， 2007
文档ID15114