网络管理系统：最佳实践白皮书

Contents

Introduction

国际标准化组织(ISO)网络管理型号定义了网络管理五个功能区域。本文包括所有功能区域。本文的整体目的将提供实用的推荐标准在每个功能区域增加当前管理工具和实践的整体效果。它为网络管理管理工具和技术的将来实施也提供设计指南。

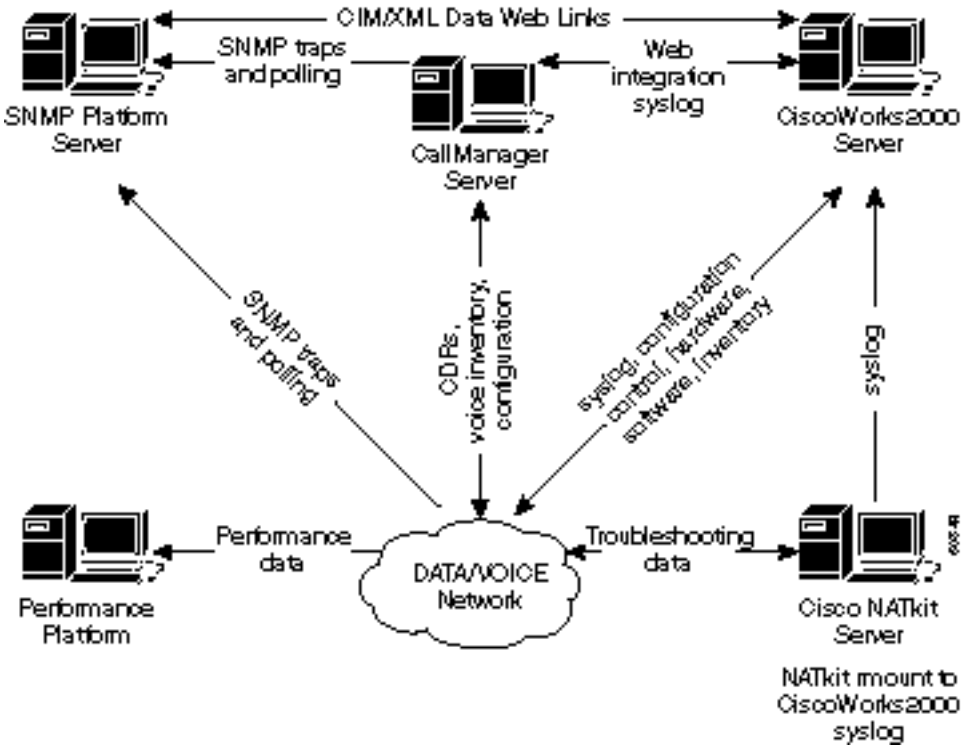
网络管理

ISO网络管理型号的五功能区域下面是列出的。

- 故障管理—发现，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、库存管理系统和软件管理。
- 性能管理—监控程序和测量多种性能方面，以便整体性能可以被维护在可接受的水平。
- 安全管理—提供对网络设备的访问和公司资源给被核准的单个。
- 记帐管理—网络资源使用信息。

以下图表显示参考体系结构Cisco系统相信应该是管理的数据网最小解决方案。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配置管理的服务器、系统日志收集和硬件和软件库存管理系统管理

使用公用信息模块/可扩展的标记语言(CIM/XML)方法，一些SNMP平台能与CiscoWorks2000服务器直接地共享数据。CIM是一个与实施无关的方案的一个普通的数据模型描述的整体管理信息在网络/企业环境。CIM包括规格和模式。而模式提供实际式样说明，规格定义了集成的详细资料与其他管理模型例如SNMP MIB或桌面管理工作组管理信息文件(DMTF MIFs)。

XML是表示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大多数SGML的说明性功率，取消一样许多复杂性尽可能。XML类似于在概念HTML，但是，而HTML用于表达关于文件的图形信息， XML用于表示在文件的结构化数据。

思科的高级服务用户也包括思科的另外积极监控和排除故障的NATkit服务器。NATkit服务器二者之一将有对驻留在CiscoWorks2000服务器的数据的一次远程磁盘登上(rmount)或文件传输协议(FTP)访问。

*互联网络技术概述的*网络管理基础章节提供关于网络管理基础的详细概要。

故障管理

故障管理目标是发现，记录，通知用户，并且(在可能的程度上)请自动地解决网络问题继续网络有效运行。由于故障能导致停工期或不能接受的网络性能降低，或许故障管理是广泛实现ISO网络管理元素。

网络管理平台

在企业中配置的网络管理平台管理包括多厂商网络元素的基础设施。平台从在网络的网络单元接受和处理事件。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

网络管理平台可以查看作为网络操作的主要控制台在发现在基础设施的故障。能力发现问题迅速在所有网络是重要。网络工作者能依靠一个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可进行在网络设备的发现上。每个网络设备由在管理平台控制台的一个图形要素表示。在图形要素的不同的颜色表示当前网络设备的运行状态。可以配置网络设备发送通知，称为SNMP陷阱，到网络管理平台。当接收通知后，表示网络设备的图形要素变成一个不同的颜色根据已接到的通知的严重性。通知，通常称为事件，在日志文件安置。重要的是特别最当前的Cisco管理信息库(MIB)文件在SNMP平台被装载保证从Cisco设备的多种戒备正确地被解释。

Cisco发布管理的多种网络设备MIB文件。Cisco MIB文件寻找cisco.com网站，并且包括以下信息：

- 以SNMPv1格式发布的MIB文件
- 以SNMPv2格式发布的MIB文件
- 在Cisco设备的支持的SNMP陷阱
- Cisco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。这通过交换在管理控制台之间的管理数据完成在远程站点与在主要站点的一个管理站。一个分布式体系结构的主要优点是减少管理数据流，因而，提供有效的带宽使用。一个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有系统的。

使用Web接口，对管理平台的一种最近的增强功能是能力对远程管理网络单元。此增进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络单元。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络单元。所以，复制管理站可能轮询网络单元对于同样信息。不同的系统收集的数据在独立的数据库存储，创建用户的管理开销。此限制提示网络和软件供应商采用标准例如Common Object Request Broker Architecture (CORBA)和集成计算机制造(CIM)实现管理数据交换在管理平台和网元管理系统之间的。当供应商采用在管理系统开发的标准，用户能期待互通性和成本节省在配置和管理基础设施。

CORBA指定提供对象之间的互通性在对程序员是透明的一个异种的系统，分布式环境里，并且有些。其设计根据对象管理组织(OMG)对象模型。

排除基础设施故障

简单文件传输协议(TFTP)和系统日志(Syslog)服务器是排除在网络操作的基础设施的关键的组件故障。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传送系统日志信息到系统日志服务器。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)被分配的系统日志收集功能允许几UNIX或NT收集站的配置在远程站点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。实现分布式收集的主要优点是消息的减少转发到主要系统日志服务器。

故障检测和通知

故障管理的目的将发现，隔离，通知，并且更正在网络遇到的故障。当故障在系统时，发生网络设备能够警告管理站。一个明显的故障管理系统包括几个子系统。当设备传送SNMP陷阱消息、SNMP轮询、远程监控(RMON)阈值和系统消息时，故障检测是实现的。管理系统警告终端用户，当故障报告时，并且纠正措施可以采取。

在网络设备应该一致启用陷井。另外的陷井用路由器和交换机新的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。一个配置陷阱的定期检查与Cisco保证的网络服务(ANS)小组的将保证在网络的明显的故障检测。

下面的表列出支持的CISCO-STACK-MIB陷井，并且可以使用监控故障状况， Cisco Catalyst区域网(LAN)交换机。

陷井	说明
moduleUp	代理实体发现在此MIB的模块状态对象有已转换的对其模块之一的**ok(2)**状态。
moduleDown	代理实体发现在此MIB的模块状态对象有已转换的在其模块之一的**ok(2)**状态外面。
chassisAlarmOn	代理实体发现*chassisTempAlarm*、*chassisMinorAlarm*或者*chassisMajorAlarm对象*在此MIB有已转换的对**on(2)**状态。 *chassisMajorAlarm*表明任一个下列的条件存在： • 任何电压故障 • 同时温度和风扇故障 • 百分之一百电源故障(两出于两或者一出于一个) • Electrically Erasable Programmable Read-Only Memory (EEPROM)故障 • 非易失性RAM (NVRAM)故障 • MCP通信故障 • NMP状态未知 chassisMinorAlarm表明任一个下列的条件存在： • 温度预警 • 风扇故障 • 部分电源故障(一出于两) • 不兼容类型两个电源
chassisAlarmOff	代理实体发现*chassisTempAlarm*、*chassisMinorAlarm*或者*chassisMajorAlarm对象*在此MIB有已转换的对**off(1)**状态。

环境监控器(envmon)陷井在CISCO-ENVMON-MIB陷井被定义。当一个环境门限值被超出时，envmon陷井发送Cisco企业特有环境监控器通知。当使用时envmon，一种特定环境的陷阱类型可以是启用的，或者从环境监控系统的所有陷阱类型可以被接受。如果选项没有指定，所有环境的类

型是启用的。它可以是一个或很多以下值：

- 电压—发送ciscoEnvMonVoltageNotification，如果电压被测量在一个特定测试点是测试点的正常范围的外部(例如在警告，重要或者关闭阶段)。
- 关闭—发送ciscoEnvMonShutdownNotification，如果环境监控器发现测试点到达一个严重状态并且将起动关闭。
- 用品—发送ciscoEnvMonRedundantSupplyNotification，如果冗余电源(哪里现存)出故障。
- 风扇—发送ciscoEnvMonFanNotification，如果任何一个在风扇阵列的风扇(哪里现存)发生故障。
- 温度—发送ciscoEnvMonTemperatureNotification，如果温度被测量在一个被测量的测试点是测试点的正常范围的外部(例如在警告，重要或者关闭阶段)。

故障检测和网络监控元素可以从设备级别被扩展到协议和界面水平。对于网络环境，故障监控能包括虚拟局域网，异步传输模式(ATM)，在物理接口的故障指示，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校园管理器。在校园管理器的流量控制器应用着重利用微型RMON技术支持的交换机管理在Catalyst交换机。

对于增长数能够关联不同的网络事件的网络单元和网络问题复杂性，事件管理系统(Syslog、陷井，日志文件)可能考虑。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在网络运营中心(NOC)的人员是积极和有效的在发现和诊断网络问题。事件优先级划分和抑制允许网络操作人员着重重要网络事件，调查几个事件管理系统包括思科信息中心和进行可行性分析充分地测试功能的这样系统。要得到更多信息，请去思科信息中心。

前摄性默认监控和通知

RMON告警和事件是在RMON规格定义的两个组。通常，管理站执行在网络设备的轮询确定某些变量的状况或值。例如，当值命中达到配置的门限值时，管理站轮询路由器发现中央处理器(CPU)利用率和生成事件。此方法浪费网络带宽，并且能根据轮询间隔也错过实际阈值。

使用RMON告警和事件，配置网络设备为上升的和下降阈值监控自己。在一个预定义的时间间隔，网络设备采取变量的示例并且对阈值比较它。如果实际值在配置的门限值之下，超出或下跌SNMP陷阱可以被发送到管理站。RMON告警和事件组提供管理重要网络设备一个主动手段。

Cisco系统推荐实现RMON告警和事件在重要网络设备。被监控的变量能包括CPU利用率、缓冲故障、输入-输出丢包，或者所有整数类型的变量。开始从Cisco IOS软件版本11.1(1)，所有路由器镜像支持RMON告警和事件组。

关于RMON警报和事件实现的详细信息，请参见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使用什么称为存储历史记录和统计数据的*桶*在这种情况下是交换机)的RMON代理程序(。桶大小在RMON探测(SwitchProbe设备)或RMON应用程序(流量控制器工具)被定义，然后被发送到将设置的交换机。

大约450 K代码空间是需要的支持微型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。

下面的表定义了每个微型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
统计数据	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
警报和事件	2.6每警报和其对应的事件项的K	每个警报每个端口

*RMON使用什么称为存储历史记录和统计数据的*桶*在RMON代理程序(例如交换机)。

RMON警报和事件实现

通过合并作为故障管理解决方案一部分的RMON，用户能主动地监控网络，在一个潜在问题发生前。例如，如果收到的广播包的数量极大增加，它能导致在CPU利用率的一个增量。通过实现RMON告警和事件，用户能设置阈值监控收到的广播包的数量和通过SNMP陷阱警告SNMP平台，如果配置的门限值达到。RMON告警和事件消除实现的同一个目标SNMP平台通常执行的额外的轮询。

两个方法从哪些是可得到配置RMON告警和事件：

- 命令行界面(CLI)
- SNMP SET

以下示例程序显示如何设置阈值监控在接口收到的广播包的数量。同一个计数器用于这些程序象在show interface命令示例显示在此部分结束时。

命令行界面示例

使用CLI接口，要实现RMON告警和事件，请执行以下步骤：

1. 查找接口索引产生关联与以太网0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. 获得与CLI字段产生关联的OID将被监控。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Cisco 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。上升的和下降阈值采样类型(绝对或Delta)采样间隔动作，当阈值达到为此示例的目的，阈值设置监控在以太网收到的广播包的数量0。如果收到的广播包的数量比500极大在60秒钟示例之间，陷井将形成。当输入广播的数量不增加在拿取的示例之间阈值将恢复活动。**Note:** 对于详细关于这些命令参数，请检查Cisco在线连接(CCO)文档您特定的Cisco IOS版本的RMON告警和事件命令。
4. 指定被发送的陷井(RMON事件)，当阈值达到使用以下CLI命令时(Cisco IOS命令在粗体显示)：**在以太网0"所有人Cisco的rmon event1陷阱网关描述“高广播rmon event2日志说明“正常广播在以太网0"所有人Cisco接受了**
5. 指定阈值和相关参数(RMON告警)使用以下CLI命令，：**RMON告警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轮询这些表验证设置告警表条目。

```
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

为了实现RMON告警和事件与SNMP设置的操作，请完成这些步骤：

1. 指定被发送的陷井(RMON事件)使用以下SNMP设置的操作时，当阈值达到：

```
# 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告警)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. 轮询这些表验证设置告警表条目。

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

show interface

此示例是结果的**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

配置管理目标是对监控网络和系统配置信息，以便对硬件与软件元素的多种版本的网络操作的作用可以被跟踪和管理。

配置标准

使用配置的增长数网络设备，能准确地识别网络设备的位置是重要的。当网络问题发生时，此位置信息应该提供有意义一个的详细规格说明给被分派任务的那些以调度资源。要加快解决方法，如果网络问题发生，请确定有人或部门的可用的联络信息负责对设备。联络信息应该包括电话号码和人或部门的名字。

应该计划和实现作为配置标准一部分，网络设备命名惯例，从设备名开始到单个接口。当排除网络问题故障时，一个明确定义的命名惯例提供人员以能力提供准确信息。设备命名惯例能使用地理位置，建立名字，楼层，等等。对于接口命名惯例，它能包括端口被连接的分段，连接集线器的名字，等等。在serial interfaces，它应该包括实际带宽、本地数据链路连接标识符(DLCI)编号(如果帧中继)，目的地和载波或者信息提供的电路ID。

配置文件管理

当您添加新的配置on命令现有的网络设备需要时，您必须验证完整性的命令，在实际实施发生前。

一个不正确地配置的网络设备在网络连通性和性能能有一个灾难性影响。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Cisco Catalyst交换机的配置文件。精华安全功能可以用于进行在配置更改的认证。更改审计日志是可用跟踪更改和发出更改的单个用户名。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**脚本的当前版本的基于Web的网络配置。配置文件可以下载和被加载使用CiscoWorks2000使用预定义的或用户定义的模板的精华。

这些功能可以用在CiscoWorks2000精华的配置管理工具完成：

- 推进从精华配置存档的配置文件到设备或多个设备
- 拉从设备的配置到Essentials文档
- 从档案提取新配置并且写它到文件
- 从文件导入配置并且推进配置到设备
- 在Essentials文档比较前两种配置
- 比一个指定的日期或版本删除配置旧从档案
- 复制启动配置到运行的配置

Inventory Management

多数网络管理平台的发现功能打算提供在网络找到的设备动态列表。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。普通的信息包括硬件型号，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。使用SNMP或写脚本，最新网络列表发现进程收集的设备可以用于作为一个主列表收集库存信息。设备清单可能从CiscoWorks2000校园管理器被导入到CiscoWorks2000精华库存数据库获得Cisco Catalyst交换机最新产品清单。

软件管理

成功的升级在网络设备的Cisco IOS镜像要求对需求的一个详细分析例如内存，引导程序ROM，微码级，等等。需求在思科的网站通常描述和可以找到以版本注释和安装指南的形式。升级运行Cisco IOS的网络设备的进程包括下载一个正确的镜像从CCO，备份当前镜像，保证所有硬件需求满足，然后装载新的镜像到设备。

完成设备维护的Upgrade窗口为一些组织是相当有限的。在与有限资源的一个大型网络环境里，在工作时间之后安排和自动化软件升级也许是必要的。程序可以完成使用脚本语言例如预计或特别地书面的应用程序执行这样任务。

当需要时，应该跟踪对软件的变化在网络设备上例如Cisco IOS镜像和微码版本协助解决分析阶段另一软件维护。使用可用的修改历史记录报告，执行升级的人能使装载减到最小不兼容镜像或微码风险到网络设备。

性能管理

服务级别协议

A服务级别协议是在服务提供商和他们的用户之间的一个书面协议在网络服务上的期望性能级别。

SLA包括权值同意在供应商和其用户之间。为权值设置的值一定是可实现，有意义和可测量的为两个当事人。

各种接口统计数据可以从网络设备收集测量性能级别。这些统计数据可以包括作为权值在SLA。统计数据例如输入队列丢弃、输出队列丢弃和忽略的信息包为诊断与表现有关的问题是有用的。

在设备级别，性能度量能包括CPU利用率、缓冲分配(大缓冲区、中等缓冲区、错过，命中率)和存储器分配。某些网络协议性能直接地与在网络设备的缓冲可用性有关。测量设备级性能统计数据是重要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例如数据链路交换工作组(DLSW)，远端源路由桥接(RSRB)， AppleTalk，等等。广域网(广域网)技术性能统计数据包括帧中继、ATM，综合业务数字网络(ISDN)和其他可以被监控和收集。

性能监控，测量和报告

应该经常收集使用SNMP，在接口、设备和协议级的不同的性能度量。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。

多种解决方案是可用在市场针对性能管理需要对企业环境。这些系统能够收集，存储和提交数据从网络设备和服务器。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。某些通常配置的性能管理解决方案包括：

- InfoVista VistaView
- SAS IT服务视觉
- Trinagy TREND

上述产品的评估确定他们是否符合不同的用户的要求。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数据。每个产品有一个不同的定价模型和功能与基本提供。性能管理功能的技术支持思科的设备的例如Netflow、RMON和Cisco IOS服务保证代理程序/响应时间报告程序(RTR/SAA CSAA/RTR)是可用的在一些解决方案。一致最近添加了能使用收集和查看性能数据的思科的广域网交换机的技术支持。

在Cisco IOS的CSAA/RTR Service Assurance Agent (SAA) /Response时间报告器(RTR)功能可以为测量IP设备之间的响应时间使用。源路由器配置有被配置的CSAA能够测量响应时间对可以是路由器或IP设备的目的地IP设备。响应时间可以被测量在来源和目的地之间或者为沿路径的每次跳跃。如果响应时间超出预定义的门限值，可以配置SNMP陷阱警告管理控制台。

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
- Interpacket延迟差异(抖动) VoIP数据流
- 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
- 信息包丢失使用CSAA生成了信息包

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软件的所有的功能集被嵌入。支持CSAA/RTR Cisco IOS软件版本的版本必须在IPM使用收集性能统计数据的设备上安装。关于支持CSAA/RTR/IPM Cisco IOS版本的汇总，请参见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了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张有限的视图在网络。用户和应用程序数据流描出提供数据流的一个详细视图在网络的。两技术、RMON探测和Netflow，提供能力收集数据流配置文件。

RMON

RMON标准设计在代理程序的一个分布式体系结构里配置(或者嵌入或在独立探测)与一个中央位置(管理控制台)连通通过SNMP。RFC 1757 RMON标准组织监控功能为九个组支持以太网拓扑，并且添加在RFC 1513的第十个组令牌的Ring-unique参数的。快速以太网链路监控提供在RFC 1757标准框架里，并且光纤分布式数据接口FDDI环监控提供在RFC 1757和RFC 1513框架里。

涌现的RFC 2021 RMON规格驱动在媒体访问控制(MAC)层之外的远程监控标准到网络和应用层。此设置分析和调试网络应用的enable (event)管理员例如Web数据流、NetWare、附注、电子邮件、数据库访问，网络文件系统和其他。可能当前使用RMON告警、统计数据、历史记录和主机/会话组主动地监控并且维护根据应用层数据流的网络可用性在网络的多数重要数据流。RMON2 enable (event)继续他们的部署基于标准的监控解决方案的网络管理员支持目标关键，基于服务器的应用。

下面的表列出RMON组的功能。

RMON组(RFC 1757)	功能
统计数据	信息包、八位位组、广播、错误和提供的计数器在分段或端口。
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	维护对每个主机设备的统计数据在分段或端口。
主机前N个	主机的用户定义子集报告组队，排序由统计计数器。通过返回仅结果，管理数据流减到最小。
数据流表	维护在主机之间的会话统计数据在网络。
警	在主动管理的重要RMON变量可以设置的阈值。

报	
事件	当警报组阈值被超出时，生成SNMP陷阱和日志条目。
信息包获取	管理加载的过滤器组获取的信息包的缓冲区到管理控制台。
令牌环	环位置—对单个的详细统计驻防环位置顺序—一个排好序的站列表当前在环环位置配置—配置和插入/删除每位置源路由统计数据在源路由，例如跳次计数和其他

RMON2	功能
协议目录	代理程序监控并且维护统计数据的协议。
协议分配	每个协议的统计数据。
网络层主机	每个网络层地址的统计数据在分段、环或者端口。
网络层一览表	对的数据流统计网络层地址。
应用层主机	由应用层协议的统计数据每个网络地址的。
应用层一览表	由应用层协议的数据流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统计数据。
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特点允许通信流详细统计为容量设计、计费和故障排除功能收集。Netflow在单个接口可以被配置，提供信息在穿过那些接口的数据流。信息的以下类型是详细的数据流统计的一部分：

- 来源和目的地IP地址
- 输入和输出接口编号
- TCP/UDP源端口和目的地端口
- 字节和信息包的数量在流
- 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数据对收集器机器被导出。收集器执行功能例如减少数据量(过滤和聚合)，分层的数据存储和文件系统管理。Cisco提供NetFlow收集器和Netflow分析程序应用收集和分析的数据从路由器和Cisco Catalyst交换机。也有共享件工具例如能收集Cisco NetFlow用户数据报协议(UDP)记录的cflowd。

使用UDP信息包以三种不同的格式， NetFlow数据被传输：

- 版本1 —支持初始NetFlow版本原始格式。

- 版本5 —添加边境网关协议(BGP)自控系统信息和流序号的一种最新增进。
- 版本7 —添加Cisco Catalyst 5000 series switches的Netflow交换技术支持的一种最新增进用a装备了Netflow功能卡。

版本2到4和版本6未发布也FlowCollector不支持。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，请参见NetFlow服务解决方案指南白皮书。

下面的表概述收集的NetFlow数据支持的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和以后	Cisco 1600*， 1720，2500**， 2600，3600， 4500， 4700，AS5300*， AS5800，7200， uBR7200，7500， RSP7000、RSM、MGX8800 RPM和BPX 8650	V1、V5和V-8
12.0(6)S	Cisco 12000	V1、V5和V-8
	与Netflow功能卡***的Cisco Catalyst 5000	V7

* NetFlow导出V1、V5和V-8的技术支持在Cisco 1600及2500平台瞄准Cisco IOS软件版本12.0(T)。这些平台的Netflow技术支持不是可用的在Cisco IOS 12.0主线版本。

** Netflow V1、V5和V-8的技术支持在AS5300平台瞄准Cisco IOS软件版本12.06(T)。

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

安全管理

安全管理的目标是控制对网络资源的访问根据本地指南，以便网络不可能被破坏(有意或无意)。安全管理子系统，例如，能监控注册对网络资源的用户，拒绝对输入不相应的接入代码的那些人的访问。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程序开始。创建跟随安全和性能的行业最佳实践的所有路由器和交换机一个特定平台的最小配置标准是重要的。

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是运行在客户端设备之间在网络和TACACS服务器的互联网工程任务组(RFC 1492)标准安全协议。TACACS是使用验证一设备寻找的远程访问的身份对一个权限控制的数据库的认证机制。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用于TACACS+允许对谁的一个更细微的控制在无特权和特权模式下能访问Cisco设备。多个TACACS+服务器可以为容错被配置。有TACACS+功能，路由器和交换机提示用户名和密码的用户。认证能为登录控制被配置或验证单个命令。

认证

认证是识别用户的进程，包括登录和密码对话、挑战和回应和消息支持。认证是用户在允许对路由器或交换机的访问之前被识别的方式。有认证和授权之间的一个基本关系。越多授权权限用户接受，越严格认证应该。

授权

授权为由用户请求的每项服务提供远程访问控制，包括一次性用户认证和授权。在Cisco路由器上，用户的授权级别范围是0到15与0最低级和15最高。

认为

记帐允许发单，审核和报告，例如用户身份、开始安全信息使用的收集和发送和停止时间和被执行的命令。跟踪用户访问的服务以及他们浪费的相当数量的认为的enable (event)网络管理器网络资源。

下面的表列出基本示例命令为使用TACACS+、认证、授权和记帐在Cisco路由器和Catalyst交换机。请参见更加详细的命令的认证、授权和记帐命令文件。

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+|半径}*	启用帐户用全局配置命令。
Aaa authentication login default tacacs+	设置路由器，以便与所有终端线路的连接配置有登录默认值将验证与TACACS+和出故障，如果认证因故发生故障。
AAA认证exec默认TACACS+无	设置路由器检查用户是否通过要求TACACS+服务器允许运行EXEC shell。
tacacs-server host *TACACS+服务器IP地址*	指定将使用认证用全局配置命令的TACACS+服务器。
tacacs-server key*共享密钥*	指定由TACACS+服务器和Cisco路由器知道用全局配置命令的共有的秘密。
Catalyst交换机	
set authentication login tacacs enable [*全部|控制台|http|telnet] [primary]*	正常登录方式的Enable (event) TACACS+认证。仅请使用控制台或Telnet关键字对enable (event) TACACS+控制台端口或Telnet连接测试。
set authorization exec enable {option}*回退选项* [*控制台|telnet|两个]*	正常登录方式的Enable (event)授权。仅请使用控制台或Telnet关键字对enable (event)授权控制台端口或Telnet连接测试。

设置 tacacs-server key*分享秘密*	指定由TACACS+服务器和交换机知道的共有的秘密。
设置 tacacs-server host *TACACS+服务器IP地址*	指定将使用认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、授权和记帐文件，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，请参见控制访问到交换机。

SNMP安全

SNMP协议在路由器和Catalyst交换机可以用于做配置更改类似于发出的那些从CLI。在网络设备应该配置适当的安全措施防止未被授权的访问和通过SNMP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。从他们的公共和专用默认值更改社区字符串是重要的。

应该有静态IP地址和IP地址和访问控制表(ACL)由那明确地授予所有SNMP管理主机SNMP通信用网络设备预定义的。Cisco IOS和Cisco Catalyst软件保证的提供安全功能仅授权管理站允许执行在网络设备的更改。

路由器安全功能

SNMP权限级别

此功能限制管理站在路由器能有操作的种类。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将执行的接口。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权限功能一道用于限制从请求管理信息的特定管理站从路由器。

SNMP视图

此功能限制可以从路由器被检索由管理站的特定信息。它可以与SNMP权限级别和ACL功能一起使用强制执行受限制的数据访问由管理控制台。对于SNMP视图配置示例，请去snmp-server view。

SNMP 版本 3

SNMP版本3 (SNMPv3)提供安全管理数据交换在网络设备和管理站之间的。加密和认证功能在SNMPv3保证高安全性在传输信息包对管理控制台。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适用。

Catalyst LAN交换机安全特性

IP Permit列表

IP Permit列表功能从未授权的源IP地址限制Inbound Telnet和SNMP访问对交换机。当侵害或未被授权的访问发生时，支持系统消息和SNMP陷阱通知管理系统。

Cisco IOS安全功能的组合可以用于管理路由器和Catalyst交换机。限制管理站的数量能够访问交换机和路由器的安全策略需要设立。

关于如何强化在IP网络的安全的更多信息，请去增强IP网络安全。

记帐管理

记帐管理是用于的进程测量网络利用率参数，以便网络的各自或组用户可以适当地调控为认为或拖欠款项。类似于性能管理，第一步往适当的记帐管理将测量首要的网络资源的利用率。使用Cisco NetFlow和Cisco IP记帐功能，网络资源利用率可以被测量。通过这些方法收集的对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一个重要部分的其中任一服务级别协议。它提供定义负债在SLA下和清楚的后果一个实用方式为工作情况SLA的外部术语。

数据可以通过探测或Cisco NetFlow收集。Cisco提供NetFlow收集器和Netflow分析程序应用收集和分析的数据从路由器和Catalyst交换机。共享件应用程序例如cflowd也用于收集NetFlow数据。资源使用的一持续的测量能产生计费信息，以及信息估计持续的公平和最佳的资源。一些通常配置的记帐管理解决方案包括：

- 明显的软件

Netflow启动和数据收集策略

Netflow (网络流)是允许获取对于网络计划、监控和记帐应用是必需的数据的输入端测量技术。在服务提供商或广域网访问路由器接口的边缘/聚合路由器接口应该配置Netflow企业用户的。

Cisco系统推荐与在这些启动的NetFlow服务的一个仔细计划内的NetFlow部署战略上被找出的路由器。Netflow可以递增(由接口的接口)和战略上配置(在精选路由器)，而不是配置在每个路由器的Netflow在网络。Cisco人员在应该根据用户的数据流模式、网络拓扑和体系结构激活哪关键路由器和键接口Netflow将工作与用户确定。

关键配置注意事项包括：

- 在运作以非常高CPU利用费率的*热核心*/骨干网路由器或者路由器应该利用NetFlow服务作为边

缘测量和访问列表性能加速工具，并且不应该激活。
- 了解应用驱动的数据收集需求。记帐应用可能只要求产生和终结路由器流信息，而监控应用程序可能要求一张更加全面的(数据密集的)端到端视图。
- 了解网络拓扑和路由策略的影响对流收集策略。例如，请避免集中复制流由激活Netflow在数据流起源或终止的关键聚合路由器和不在提供同样流信息的重复视图的骨干网路由器或中间路由器。
- 在*传输运营商*事务(起源和终止在他们的网络)的传输流量的服务提供商可能为测量网络资源过渡数据流使用应用NetFlow输出数据记帐和计费目的。

配置IP记帐

Cisco IP记帐支持提供基本的IP记帐功能。通过启用IP记帐，用户能看到通过根据源和目的地IP地址基本类型的Cisco IOS软件被转换字节和信息包的数量。仅转接IP数据流仅被测量和根据一个outbound基本类型。软件或终止生成的数据流在软件没有在计费统计数据里包括。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。安排此功能可用用户，访问列表侵害enable (event) IP记帐使用**ip accounting access-violations命令**。用户能然后显示字节和信息包的数量自尝试对破坏安全性访问列表源目的地对的一个单个资源。默认情况下，IP记帐显示通过了访问列表信息包的数量和路由。

对enable (event) IP记帐，请使用以下命令之一每个接口在Interface Configuration模式：

命令	目的
IP记帐	Enable (event)基本的IP记帐。
ip accounting access violations	Enable (event) IP记帐以能力识别发生故障IP访问列表的IP数据流。

要配置其他IP记帐功能，请使用一个或很多以下in命令全局配置模式：

命令	目的
ip accounting-threshold threshold	设置将被创建的记帐条目的最大数量。
ip accounting-list ip-address wildcard	主机的过滤器记帐信息。
ip accounting-transits count	控制的传输记录的数量在IP记帐数据库将被存储。

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