# 網路管理系統：最佳實踐白皮書

## 目錄



## 簡介

國際標準化組織(ISO)網路管理模式定義了網路管理的五個功能領域。本文檔涵蓋所有功能領域。本檔案的總體目的是就各個職能領域提供實際的建議，以提高當前管理工具和實踐的總體有效性。它還為將來實施網路管理工具和技術提供了設計手冊。

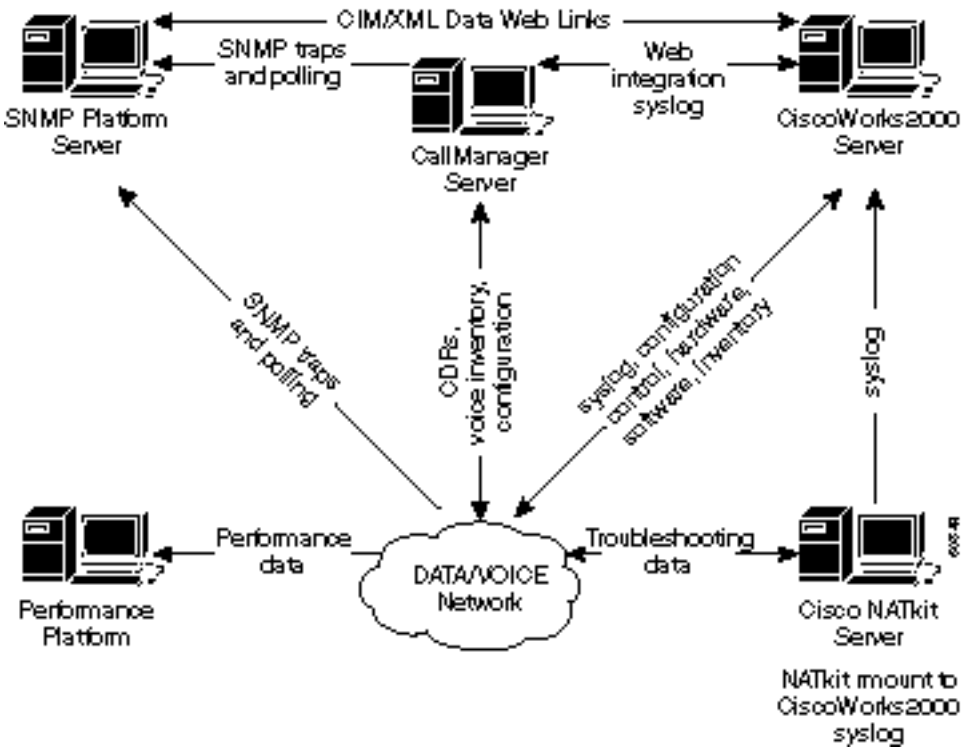
## 網路管理

ISO網路管理模式的五個功能領域如下所示。

- 故障管理 — 檢測、隔離、通知並更正網路中遇到的故障。
- 配置管理 — 網路裝置的配置方面，如配置檔案管理、庫存管理和軟體管理。
- 績效管理 — 監視和衡量績效的各個方面，以便將整體績效保持在可接受的水準。
- 安全管理 — 為獲得授權的人員提供對網路裝置和公司資源的訪問。
- 記帳管理 — 網路資源的使用情況資訊。

下圖顯示了思科系統公司認為應作為管理資料網路的最小解決方案的參考架構。此架構包括適用於

計畫管理網際網路協定語音(VoIP)的使用者的Cisco CallManager伺服器：該圖顯示了如何將CallManager伺服器整合到NMS拓撲中。




網路管理架構包括：

- 用於故障管理的簡單網路管理協定(SNMP)平台
- 用於長期效能管理和趨勢分析的效能監控平台
- CiscoWorks2000伺服器，用於配置管理、系統日誌收集以及硬體和軟體清單管理

某些SNMP平台可以使用公共資訊模型/可擴展標籤語言(CIM/XML)方法直接與CiscoWorks2000伺服器共用資料。CIM是一個通用資料模型，是一個實現無關的模式，用於描述網路/企業環境中的整體管理資訊。CIM由規範和架構組成。規範定義了與其他管理模型(如SNMP MIB或案頭管理任務組管理資訊檔案(DMTF MIF))整合的詳細資訊，而架構提供了實際的模型描述。

XML是一種標籤語言，用於以文本形式表示結構化資料。XML的一個特定目標是保持SGML的大部分描述能力，同時儘可能地降低複雜性。XML與HTML在概念上相似，但是HTML用於傳遞文檔的圖形資訊，XML用於表示文檔中的結構化資料。

思科的高級服務客戶還將包括思科的NATkit伺服器，用於其他主動監控和故障排除。NATkit伺服器將具有對CiscoWorks2000伺服器上駐留資料的遠端磁碟裝載（裝載）或檔案傳輸協定(FTP)訪問許可權。

*Internetworking Technology Overview*的Network Management Basics一章提供了有關網路管理基礎的更詳細的概述。

## 故障管理

故障管理的目標是檢測、記錄、通知使用者並（儘可能）自動修復網路問題，以保持網路有效運行。由於故障會導致停機或無法接受的網路降級，因此故障管理可能是ISO網路管理元素中實施最廣泛的。

### 網路管理平台

企業中部署的網路管理平台管理由多供應商網路元素組成的基礎設施。平台從網路中的網路元件接收和處理事件。來自伺服器和其他關鍵資源的事件也可以轉發到管理平台。標準管理平台中包括以下常用功能：

- 網路發現
- 網路元素的拓撲對映
- 事件處理程式
- 效能資料收集器和圖形繪製器
- 管理資料瀏覽器

網路管理平台可以視為檢測基礎設施故障的網路操作的主控制檯。能夠快速檢測任何網路中的問題至關重要。網路操作人員可以依靠圖形網路圖來顯示關鍵網路元素（如路由器和交換機）的操作狀態。

網路管理平台（如HP OpenView、Computer Associates Unicenter和SUN Solstice）可以執行網路裝置的發現。每個網路裝置都由管理平台控制檯上的圖形元素表示。圖形元素上的不同顏色表示網路裝置的當前運行狀態。可以將網路裝置配置為向網路管理平台傳送通知（稱為SNMP陷阱）。當接收到通知時，表示網路裝置的圖形元素根據接收到的通知的嚴重性而改變為不同的顏色。通知（通常稱為事件）將置於日誌檔案中。尤其重要的是，最新的思科管理資訊庫(MIB)檔案應載入到SNMP平台上，以確保正確解釋來自思科裝置的各種警報。

Cisco發佈MIB檔案來管理各種網路裝置。Cisco MIB files位於cisco.com網站，包括以下資訊：

- 以SNMPv1格式發佈的MIB檔案
- 以SNMPv2格式發佈的MIB檔案
- 思科裝置上支援的SNMP陷阱
- Cisco當前SNMP MIB對象的OID

許多網路管理平台能夠管理多個地理上分散的站點。這是通過在遠端站點的管理控制檯與主站點管理站之間交換管理資料來實現的。分散式架構的主要優勢在於它減少了管理流量，從而提供了更有效的頻寬使用。分散式架構還允許人員從具有系統的遠端站點本地管理他們的網路。

管理平台最近的一項增強功能是使用Web介面遠端管理網路元素。這種增強功能消除了各個使用者工作站上需要特殊的客戶端軟體來訪問管理平台的需要。

典型的企業由不同的網路元素組成。但是，每台裝置通常都需要特定於供應商的元素管理系統，以便有效地管理網路元素。因此，重複管理站可能正在輪詢網元以獲取相同的資訊。不同系統收集的資料儲存在不同的資料庫中，給使用者造成了管理開銷。這一限制促使網路和軟體供應商採用公共對象請求代理架構(CORBA)和電腦整合製造(CIM)等標準，以促進管理平台和元素管理系統之間的管理資料交換。隨著供應商採用管理系統開發標準，使用者期望在部署和管理基礎設施時實現互操作性和成本節約。

CORBA指定了一個系統，該系統在異構、分散式環境中以對於程式設計師透明的方式提供對象之間的互操作性。其設計基於對象管理組(OMG)對象模型。

## 基礎設施故障排除

簡單式檔案傳輸通訊協定(TFTP)和系統日誌(syslog)伺服器是網路運作中疑難排解基礎架構的重要元件。TFTP伺服器主要用於儲存網路裝置的配置檔案和軟體映像。路由器和交換機能夠將系統日誌消息傳送到系統日誌伺服器。當遇到問題時，這些消息有助於故障排除功能。有時，思科支援人員需要系統日誌消息來執行根本原因分析。

CiscoWorks2000 Resource Management Essentials(Essentials)分散式系統日誌收集功能允許在遠

端站點部署多個UNIX或NT收集站，以執行消息收集和過濾。過濾器可以指定將哪些系統日誌消息轉發到主Essentials伺服器。實施分散式收集的一個主要優點是減少了轉發到主系統日誌伺服器的消息。

## 故障檢測和通知

故障管理的目的是檢測、隔離、通知和糾正網路中遇到的故障。當系統發生故障時，網路裝置能夠向管理站發出警報。一個有效的故障管理系統由幾個子系統組成。當裝置傳送SNMP陷阱消息、SNMP輪詢、遠端監控(RMON)閾值和系統日誌消息時，即可完成故障檢測。當報告故障並且可以採取糾正措施時，管理系統向終端使用者發出警報。

在網路裝置上應一致啟用陷阱。適用於路由器和交換器的新Cisco IOS軟體版本支援其他設陷。檢查並更新配置檔案以確保正確解碼陷阱非常重要。思科保證網路服務(ANS)團隊定期檢查已配置的陷阱，以確保網路中的有效故障檢測。

下表列出了Cisco Catalyst區域網(LAN)交換機支援並可用於監控故障情況的CISCO-STACK-MIB陷阱。

| 陷阱 | 說明 |
|---|---|
| moduleUp | 代理實體檢測到此MIB中的**moduleStatus**對象已轉換為其其中一個模組的**ok**(2)狀態。 |
| moduleDown | 代理實體檢測到此MIB中的*moduleStatus*對象已從其其中一個模組的**ok(2)**狀態轉換出去。 |
| chassisAlarmOn | 代理實體檢測到此MIB中的*chassisTempAlarm*、*chassisMinorAlarm*或*chassisMajorAlarm*對象已轉換為*on(2)*狀態。<br>*chassisMajorAlarm*表示存在以下條件之一：<br>• 任何電壓故障<br>• 同時發生溫度和風扇故障<br>• 100%的電源故障（兩個或兩個中的一個故障，或其中一個電源出現故障）<br>• 電可擦可程式設計只讀儲存器(EEPROM)故障<br>• 非揮發性RAM(NVRAM)故障<br>• MCP通訊故障<br>• NMP狀態未知<br>chassisMinorAlarm表示存在以下條件之一：<br>• 溫度報警器<br>• 風扇故障<br>• 部分電源故障（兩個中一個）<br>• 兩個型別不相容的電源 |
| chassisAlarmOff | 代理實體檢測到此MIB中的*chassisTempAlarm*、*chassisMinorAlarm*或*chassisMajorAlarm*對象已轉換為**off(1)**狀態。 |

環境監控(envmon)陷阱在CISCO-ENVMON-MIB陷阱中定義。envmon陷阱在超過環境閾值時傳送思科企業特定的環境監控器通知。使用envmon時，可以啟用特定的環境陷阱型別，或者可以接受環境監控系統中的所有陷阱型別。如果未指定任何選項，則會啟用所有環境型別。可以是以下一個或多個值：

- voltage — 如果在給定測試點測量的電壓超出測試點的正常範圍（例如處於警告、嚴重或關閉階段），則傳送ciscoEnvMonVoltageNotification。
- shutdown — 如果環境監控器檢測到測試點達到臨界狀態並即將啟動關閉，則傳送ciscoEnvMonShutdownNotification。
- 電源 — 如果冗餘電源（存在時）出現故障，將傳送ciscoEnvMonRedundantSupplyNotification。
- 風扇 — 如果風扇陣列中的任何風扇（存在時）出現故障，將傳送ciscoEnvMonFanNotification。
- 溫度(Temperature) — 如果給定測試點測量的溫度超出測試點的正常範圍（例如處於警告、嚴重或關閉階段），則會傳送ciscoEnvMonTemperatureNotification。

網路元素的故障檢測和監控可以從裝置級別擴展到協定和介面級別。對於網路環境，故障監控可以包括虛擬區域網(VLAN)、非同步傳輸模式(ATM)、物理介面上的故障指示等。協定級故障管理實施可使用CiscoWorks2000 Campus Manager等元素管理系統來實施。Campus Manager中的TrafficDirector應用側重於在Catalyst交換機上利用迷你RMON支援進行交換機管理。

隨著網路元素數量的增加和網路問題的複雜性，可以考慮能夠關聯不同網路事件（系統日誌、陷阱、日誌檔案）的事件管理系統。事件管理系統背後的這種架構類似於經理經理(MOM)系統。設計合理的事件管理系統可使網路運營中心(NOC)的人員主動有效地檢測和診斷網路問題。事件優先順序和抑制允許網路操作人員專注於關鍵網路事件，調查包括思科資訊中心在內的多個事件管理系統，並進行可行性分析以充分探討此類系統的功能。如需詳細資訊，請前往思科資訊中心。

## 主動故障監控和通知

RMON警報和事件是在RMON規範中定義的兩個組。通常，管理站會對網路裝置執行輪詢，以確定某些變數的狀態或值。例如，管理站輪詢路由器以找出中央處理器(CPU)利用率，並在值達到配置的閾值時生成事件。此方法浪費了網路頻寬，並且根據輪詢間隔還可能會錯過實際閾值。

通過RMON警報和事件，網路裝置被配置為監控其自身是否有上升和下降閾值。在預定義的時間間隔內，網路裝置將取一個變數的樣本，並將其與閾值進行比較。如果實際值超過或低於配置的閾值，可以將SNMP陷阱傳送到管理站。RMON警報和事件組提供了一種主動管理關鍵網路裝置的方法。

Cisco Systems建議在關鍵網路裝置上實施RMON警報和事件。受監視的變數可能包括CPU利用率、緩衝區故障、輸入/輸出丟棄或任何整數型別的變數。從Cisco IOS軟體版本11.1(1)開始，所有路由器映像都支援RMON警報和事件組。

有關RMON警報和事件實施的詳細資訊，請參閱RMON警報和事件實施部分。

## RMON記憶體限制

在所有與統計資訊、歷史記錄、警報和事件有關的交換機平台上，RMON記憶體使用率是固定的。RMON使用所謂的*桶*來儲存RMON代理（本例中為交換機）的歷史記錄和統計資訊。 在RMON探測（SwitchProbe裝置）或RMON應用（TrafficDirector工具）上定義桶大小，然後傳送到要設定的交換機。

需要大約450 K的代碼空間來支援迷你RMON(例如，四個RMON組：統計資訊、歷史記錄、警報和事件)。 RMON的動態記憶體要求會有所不同，因為它取決於運行時配置。

下表定義了每個迷你RMON組的運行時RMON記憶體使用資訊。

| RMON組定義 | 已使用的DRAM空間 | 備註 |
|---|---|---|
| 統計 | 每個交換乙太網/快速乙太網埠140位元組 | 每個埠 |
| 歷史記錄 | 50桶3千6百* | 每個附加儲存桶使用56位元組 |
| 警報和事件 | 每個警報2.6 K及其相應的事件條目 | 每個埠每個警報 |

*RMON使用所謂的*桶*來儲存RMON代理（如交換機）上的歷史記錄和統計資訊。

## RMON警報和事件實施

通過將RMON作為故障管理解決方案的一部分，使用者可以在潛在問題發生之前主動監控網路。例如，如果接收的廣播資料包數量顯著增加，則可能導致CPU利用率增加。通過實施RMON警報和事件，使用者可以設定閾值來監控接收的廣播資料包數量，並在達到配置的閾值時通過SNMP陷阱向SNMP平台發出警報。RMON警報和事件消除了SNMP平台通常為實現同一目標而執行的過度輪詢。

有兩種方法可用於配置RMON警報和事件：

- 命令列介面(CLI)
- SNMP集

以下示例過程顯示如何設定閾值以監視介面上接收的廣播資料包的數量。這些步驟中使用了相同的計數器，如本節結尾的show interface命令示例所示。

### 命令列介面示例

要使用CLI介面實施RMON警報和事件，請執行以下步驟：

1. 通過瀏覽ifTable MIB查詢與乙太網0關聯的介面索引。
   ```
   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. 獲取與要監視的CLI欄位關聯的OID。在本示例中，「廣播」的OID是1.3.6.1.2.1.2.2.1.12。特定MIB變數的Cisco OID可從cisco.com網站獲得。
3. 確定下列用於設定閾值和事件的引數。起點和落點取樣型別（絕對或增量）取樣間隔達到閾值時的操作在本示例中，設定了一個閾值來監視乙太網0上接收的廣播資料包的數量。如果在60秒的取樣之間接收的廣播資料包的數量大於500，則會生成陷阱。如果兩次採集的樣本之間的輸入廣播數量沒有增加，閾值將重新啟用。**附註：** 有關這些命令引數的詳細資訊，請檢視Cisco Connection Online(CCO)文檔，瞭解針對您的特定Cisco IOS版本的RMON警報和事件命令。
4. 使用以下CLI命令指定達到閾值時傳送的陷阱（RMON事件）（Cisco IOS命令以粗體顯示）：**rmon event 1 trap gateway description "High Broadcast on Ethernet 0" owner ciscormon事件2日誌描述「在ethernet 0上接收的正常廣播」所有者cisco**
5. 使用以下CLI命令指定閾值和相關引數（RMON警報）：**rmon alarm 1 ifEntry.12.1 60 delta rising-threshold 500 1falling-threshold 0 2所有者cisco**
6. 使用SNMP輪詢這些表，以驗證eventTable條目是否在裝置上建立。
   ```
   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輪詢這些表以驗證是否已設定alarmTable條目。

```
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集合範例

為了使用SNMP SET操作實施RMON警報和事件，請完成以下步驟：

1. 使用以下SNMP SET操作指定達到閾值時傳送的陷阱（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操作指定閾值和相關引數（RMON警報）：

```
# 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. 輪詢這些表以驗證是否在裝置上建立了eventTable條目。

```
% 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. 輪詢這些表以驗證是否已設定alarmTable條目。

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

### 顯示介面

此範例是**show interface**命令的結果。

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
```

## 組態管理

配置管理的目的是監控網路和系統配置資訊，以便跟蹤和管理不同版本的硬體和軟體元素對網路操作的影響。

### 組態標準

隨著部署的網路裝置數量不斷增加，準確識別網路裝置的位置至關重要。此位置資訊應提供詳細的描述，這對於那些在網路出現問題時分派資源的任務具有一定意義。要在出現網路問題時加快解決速度，請確保擁有裝置負責人或部門的聯絡資訊。聯絡資訊應包括電話號碼以及個人或部門的姓名。

網路裝置的命名約定（從裝置名稱到單個介面）應作為配置標準的一部分進行規劃和實施。明確定義的命名約定使工作人員能夠在排除網路故障時提供準確的資訊。裝置的命名約定可以使用地理位置、建築名稱、樓層等。對於介面命名約定，它可以包括埠所連線的網段、連線集線器的名稱等。在串列介面上，它應該包括實際頻寬、本地資料鏈路連線識別符號(DLCI)編號（如果為幀中繼）、目的地以及運營商提供的電路ID或資訊。

### 組態檔管理

在現有網路裝置需要上新增新的配置命令時，必須在實際實施之前驗證這些命令的完整性。配置錯誤的網路裝置可能會對網路連線和效能產生災難性的影響。必須檢查配置命令引數以避免不匹配或不相容問題。建議定期與思科工程師一起對配置進行徹底檢查。

功能全面的CiscoWorks2000 Essentials允許自動備份路由器和Cisco Catalyst交換機上的配置檔案。Essentials的安全功能可用於對配置更改執行身份驗證。變更稽核日誌可用於跟蹤變更以及發佈變更的個人的使用者名稱。對於多個裝置上的配置更改，有兩種可用選項：當前版本的CiscoWorks2000 Essentials或**cwconfig**指令碼中的基於Web的NetConfig。使用預定義或使用者定義的模板，可使用CiscoWorks2000 Essentials下載和上傳配置檔案。

這些功能可以使用CiscoWorks2000 Essentials中的配置管理工具來完成：

- 將配置檔案從Essentials配置存檔推送到一台或多台裝置
- 將配置從裝置提取到Essentials存檔
- 從存檔中提取最新配置並將其寫入檔案
- 從檔案匯入配置並將配置推送到裝置
- 比較Essentials存檔中的最後兩種配置
- 從存檔中刪除早於指定日期或版本的配置
- 將啟動配置複製到運行配置

### 存貨管理

大多數網路管理平台的發現功能旨在提供網路中發現的裝置的動態清單。應使用發現引擎，如網路管理平台中實施的發現引擎。

清單資料庫提供有關網路裝置的詳細配置資訊。常見資訊包括硬體型號、已安裝模組、軟體映像、微碼級別等。所有這些資訊對於完成軟體和硬體維護等任務都至關重要。發現過程收集的網路裝置的最新清單可用作主清單，以使用SNMP或指令碼收集清單資訊。裝置清單可以從CiscoWorks2000 Campus Manager匯入到CiscoWorks2000 Essentials的清單資料庫中，以獲取Cisco Catalyst交換機的最新清單。

### 軟體管理

要成功升級網路裝置上的Cisco IOS映像，需要對記憶體、引導ROM、微碼級別等要求進行詳細分析。這些要求通常以版本說明和安裝指南的形式在思科網站上記錄和提供。升級運行Cisco IOS的網路裝置的過程包括：從CCO下載正確的映像、備份當前映像、確保滿足所有硬體要求，然後將新映像載入到裝置中。

某些組織完成裝置維護的升級視窗相當有限。在資源有限的大型網路環境中，可能有必要在工作時間結束後安排和自動執行軟體升級。可以使用指令碼語言（如Expect）或專門為執行此類任務而編寫的應用程式來完成該過程。

當需要另外的軟體維護時，應跟蹤Cisco IOS映像和微碼版本等網路裝置中軟體的更改，以幫助分析階段。有了修改歷史報告，執行升級的人員可以將載入不相容映像或微代碼到網路裝置的風險降至最低。

## 效能管理

### 服務級別協定

服務級別協定(SLA)是服務提供商與其客戶之間就網路服務的預期效能級別達成的書面協定。SLA由提供商與其客戶之間商定的指標組成。為指標設定的值必須為雙方現實、有意義且可衡量。

可以從網路裝置收集各種介面統計資訊來測量效能級別。這些統計資訊可以作為SLA中的指標包括在內。輸入佇列捨棄、輸出佇列捨棄和忽略封包等統計資料對於診斷效能相關問題很有用。

在裝置級別，效能度量可以包括CPU利用率、緩衝區分配（大緩衝區、中等緩衝區、未命中、命中率）和記憶體分配。某些網路協定的效能與網路裝置中緩衝區的可用性直接相關。測量裝置級效能統計資訊對於最佳化高級協定效能至關重要。

路由器等網路裝置支援各種高層協定，如資料鏈路交換工作組(DLSW)、遠端源路由橋接(RSRB)、AppleTalk等。廣域網(WAN)技術(包括訊框中繼、ATM、整合服務數位網路(ISDN)和其他技術)的效能統計資料均可監控和收集。

## 效能監控、測量和報告

應使用SNMP定期收集介面、裝置和協定等級的不同效能指標。網路管理系統中的輪詢引擎可用於資料收集目的。大多數網路管理系統能夠收集、儲存和呈現輪詢資料。

市場上有多種解決方案可滿足企業環境的效能管理需求。這些系統能夠從網路裝置和伺服器收集、儲存和呈現資料。大多數產品上基於Web的介面使效能資料可以從企業中的任何位置訪問。一些常用的效能管理解決方案包括：

- InfoVista VistaView
- SAS IT服務願景
- 特朗尼趨勢

對以上產品的評估將確定它們是否滿足不同使用者的需求。某些供應商支援與網路管理和系統管理平台的整合。例如，InfoVista支援BMC Patrol Agent，提供來自應用程式伺服器的關鍵效能統計資訊。每種產品都有不同的定價模型和功能。某些解決方案支援思科裝置的效能管理功能，例如NetFlow、RMON和Cisco IOS服務保證代理/響應時間報告器(RTR/SAA CSAA/RTR)。Concord最近增加了對Cisco WAN交換機的支援，可用於收集和檢視效能資料。

Cisco IOS中的CSAA/RTR服務保證代理(SAA)/響應時間報告器(RTR)功能可用於測量IP裝置之間的響應時間。配置了CSAA的源路由器能夠測量對目標IP裝置（可以是路由器或IP裝置）的響應時間。可在源與目的地之間測量響應時間，也可以測量路徑沿途每一跳的響應時間。可以將SNMP陷阱配置為在響應時間超過預定義閾值時向管理控制檯發出警報。

Cisco IOS的最新增強功能擴展了CSAA的功能，以衡量以下方面：

- 超文字傳輸通訊協定(HTTP)服務效能域名系統(DNS)查詢傳輸控制通訊協定(TCP)連線HTTP事務時間
- IP語音(VoIP)流量的資料包間延遲差異（抖動）
- 特定服務品質(QoS)的端點之間的響應時間IP服務型別(ToS)位元
- 使用CSAA生成的資料包丟失資料包

使用Cisco Internetwork Performance Monitor(IPM)應用程式可在路由器上配置CSAA功能。CSAA/RTR嵌入在Cisco IOS軟體的許多（但並非全部）功能集中。必須在IPM用於收集效能統計資訊的裝置上安裝支援CSAA/RTR的Cisco IOS軟體版本。有關支援CSAA/RTR/IPM的Cisco IOS版本的摘要，請參閱IPM常見問題網站。

有關IPM的其他資訊包括：

- IPM概述
- 服務保證代理

## 效能分析和調整

使用者流量顯著增加，對網路資源提出了更高的要求。網路管理員通常只能有限地檢視網路中運行的流量型別。使用者和應用流量分析提供網路中流量的詳細檢視。RMON探測功能和NetFlow技術提供了收集流量量變曲線的能力。

### RMON

RMON標準旨在部署於分散式架構中，在該架構中，代理（嵌入式或獨立探測器）通過SNMP與中央站（管理控制檯）通訊。RFC 1757 RMON標準將監控功能組織成九個組來支援乙太網拓撲，並在RFC 1513中增加第10個組用於令牌環唯一引數。快速乙太網路連結監控在RFC 1757標準框架中提供，而光纖分散式資料介面(FDDI)環監控在RFC 1757和RFC 1513框架中提供。

新興的RFC 2021 RMON規範將遠端監控標準從介質訪問控制(MAC)層擴展到網路和應用層。此設定使管理員能夠分析和排除網路應用程式(如Web流量、NetWare、Notes、電子郵件、資料庫訪問、網路檔案系統(NFS)等)的故障。現在，可以根據應用層流量（網路中最重要的流量）使用RMON警報、統計資訊、歷史記錄和主機/會話組來主動監控和維護網路可用性。RMON2使網路管理員能夠繼續部署基於標準的監控解決方案，以支援關鍵任務、基於伺服器的應用。

下表列出了RMON組的功能。

| RMON組(RFC 1757) | 功能 |
|---|---|
| 統計 | 區段或連線埠上的封包、八位元組、廣播、錯誤和提供的計數器。 |
| 歷史記錄 | 定期取樣並儲存統計組計數器供以後檢索。 |
| 主機 | 維護網段或埠上每個主機裝置的統計資訊。 |
| 主機前N | Hosts組的使用者定義的子集報告，按統計計數器排序。通過僅返回結果，可最小化管理流量。 |
| 流量矩陣 | 維護網路中主機之間的會話統計資訊。 |
| 警報 | 可以對關鍵RMON變數設定閾值，以進行主動管理。 |
| 活動 | 在超出警報組閾值時生成SNMP陷阱和日誌條目。 |
| 封包擷取 | 管理過濾器組捕獲的資料包的緩衝區，以便上傳到管理控制檯。 |
| 權杖環 | 環站點 — 有關各個站點的詳細統計資訊環站點順序 — 環站點配置中當前站點的有序清單 — 每個站點的配置和插入/刪除源路由 — 有關源路由的統計資訊，如跳數等 |

| RMON2 | 功能 |
|---|---|
| 協定目錄 | 代理監控和維護其統計資訊的協定。 |

| | |
|---|---|
| 通訊協定分佈 | 每個協定的統計資訊。 |
| 網路層主機 | 網段、環或埠上每個網路層地址的統計資訊。 |
| 網路層矩陣 | 網路層地址對的流量統計資訊。 |
| 應用層主機 | 每個網路地址按應用層協定統計。 |
| 應用層矩陣 | 按網路層地址對的應用層協定統計流量。 |
| 使用者可定義的歷史記錄 | 將歷史記錄擴展到RMON1鏈路層統計資訊之外，以包括任何RMON、RMON2、MIB-I或MIB-II統計資訊。 |
| 位址對應 | MAC到網路層地址繫結。 |
| 配置組 | 代理功能和配置。 |

### Netflow

Cisco NetFlow功能允許收集流量詳細統計資訊，以用於容量規劃、計費和故障排除功能。可以在單個介面上配置NetFlow，提供有關通過這些介面的流量資訊。以下資訊型別是詳細流量統計資訊的一部分：

- 源和目標IP地址
- 輸入和輸出介面編號
- TCP/UDP來源連線埠和目的地連線埠
- 流中的位元組數和資料包數
- 源和目標自治系統編號
- IP服務型別(ToS)

在網路裝置上收集的NetFlow資料將匯出到收集器電腦。收集器執行各種功能，如減少資料量（過濾和聚合）、分層資料儲存和檔案系統管理。Cisco提供NetFlow Collector和NetFlow Analyzer應用以收集和分析來自路由器和Cisco Catalyst交換機的資料。還有其他一些共用軟體工具（如cflowd），可以收集Cisco NetFlow使用者資料包協定(UDP)記錄。

NetFlow資料使用三種不同格式的UDP資料包傳輸：

- 版本1 — 初始NetFlow版本支援的原始格式。
- 第5版 — 新增邊界閘道通訊協定(BGP)自治系統資訊和流量序號的後續增強功能。
- 第7版 — 新增對配備NetFlow功能卡(NFFC)的Cisco Catalyst 5000系列交換器的NetFlow交換支援的更新功能。

版本2至4和版本6未發佈或FlowCollector不支援。在所有三個版本中，資料包都由一個報頭和一個或多個流記錄組成。

有關詳細資訊，請參閱NetFlow服務解決方案指南白皮書。

下表概述了用於從路由器和Catalyst交換機收集NetFlow資料的受支援的Cisco IOS版本。

| **Cisco IOS軟體** | **支援的思科硬體平台** | **支援的NetFlow匯出** |
|---|---|---|

| 版本 | | 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 便士 | 思科路由交換模組(RSM) | V1 |
| 11.3 和 11.3 公噸 | 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 公噸 | 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、RSP700、RSM、MGX8800 RPM和BPX 86 50 | V1、V5和V8 |
| 12.0(6)S | Cisco 12000 | V1、V5和V8 |
| — | 採用NetFlow功能卡(NFFC)的Cisco Catalyst 5000*** | V7 |

*在Cisco 1600和2500平台上支援NetFlow匯出V1、V5和V8，目標用於Cisco IOS軟體版本12.0(T)。 Cisco IOS 12.0 mainline版本不支援這些平台的NetFlow。

**平台對NetFlow V1、V5和V8的支援針對Cisco IOS軟體版本12.06(T)。

Catalyst ***系列管理引擎軟體版本4.1(1)或更高版本支援MLS和NetFlow資料匯出。

## 安全管理

安全管理的目標是根據本地准則控制對網路資源的訪問，以便網路不被破壞（有意或無意地）。例如，安全管理子系統可以監控登入到網路資源的使用者，拒絕訪問輸入不當訪問代碼的使用者。安全管理是一個非常廣泛的問題；因此，本檔案的此區域僅涵蓋與SNMP和基本裝置存取安全性相關的安全性。

有關高級安全的詳細資訊包括：

- 提高IP網路的安全性
- 開放系統

良好的安全管理實施始於實施健全的安全策略和程式。必須為所有遵循行業最佳安全和效能實踐的路由器和交換機建立特定於平台的最低配置標準。

有多種方法可以控制Cisco路由器和Catalyst交換機上的訪問。這些方法包括：

- 存取控制清單(ACL)
- 裝置的本地使用者ID和密碼
- 終端存取控制器存取控制系統(TACACS)

TACACS是網際網路工程任務組(RFC 1492)標準安全通訊協定，在網路上的使用者端裝置之間執行，且針對TACACS伺服器執行。TACACS是一種身份驗證機制，用於驗證尋求遠端訪問特權資料庫的裝置的身份。TACACS的變體包括TACACS+，這是將驗證、授權和記帳功能分隔開的AAA架構。

TACACS+由思科使用，可更有效控制哪些人可在非特權及特權模式下存取思科裝置。可以配置多個TACACS+伺服器以實現容錯功能。啟用TACACS+後，路由器和交換器會提示使用者輸入使用者名稱和密碼。可以配置身份驗證以進行登入控制或驗證單個命令。

## 驗證

身份驗證是識別使用者的過程，包括登入和密碼對話方塊、質詢和響應以及消息傳送支援。身份驗證是在允許使用者訪問路由器或交換機之前識別使用者的方法。身份驗證和授權之間存在基本關係。使用者獲得的授權許可權越多，身份驗證應該越強。

## Authorization

Authorization提供遠端訪問控制，包括使用者請求的每個服務的一次性授權和授權。在思科路由器上，使用者的授權級別範圍為0到15,0表示最低級別，15表示最高級別。

## 會計

記帳允許收集和傳送用於計費、審計和報告的安全資訊，例如使用者身份、開始和停止時間以及執行的命令。記帳使網路管理員能夠跟蹤使用者正在訪問的服務及其消耗的網路資源數量。

下表列出在Cisco路由器和Catalyst交換機上使用TACACS+、身份驗證、授權和記帳的基本示例命令。如需更深入的命令，請參閱驗證、授權和記帳命令檔案。

| Cisco IOS指令 | 目的 |
|---|---|
| **路由器** | |
| aaa new-model | 啟用身份驗證、授權、記帳(AAA)作為訪問控制的主要方法。 |
| AAA記帳 {*system*<br>*/網路*<br>*/連線* / | 使用全域性配置命令啟用記帳。 |

| | |
|---|---|
| *exec |命令級別} {start-stop | wait-start |僅停止} {tacacs+ | radius}* | |
| AAA驗證登入預設tacacs+ | 設定路由器，以便與使用登入預設設定配置的任何終端線路的連線將通過TACACS+進行身份驗證，並且如果身份驗證由於任何原因失敗，則連線將失敗。 |
| AAA授權exec預設tacacs+無 | 將路由器設定為通過詢問TACACS+伺服器來檢查是否允許使用者運行EXEC外殼。 |
| tacacs-server host *tacacs+伺服器ip地址* | 使用全域性配置命令指定將用於身份驗證的TACACS+伺服器。 |
| tacacs-server key *shared-secret* | 使用全域性配置命令指定TACACS+伺服器和思科路由器已知的共用金鑰。 |
| Catalyst交換器 | |
| set authentication login tacacs enable [*all |控制檯 | http | telnet*] [*primary*] | 為正常登入模式啟用TACACS+身份驗證。使用console或Telnet關鍵字僅對控制檯埠或Telnet連線嘗試啟用TACACS+。 |
| set authorization exec enable {*option*} *fallback* | 為正常登入模式啟用授權。使用console或Telnet關鍵字僅對控制檯埠或Telnet連線嘗試啟用授權。 |

| | |
|---|---|
| *option*} [控制台 / telnet /兩者] | |
| Set tacacs-server key *shared-secret* | 指定TACACS+伺服器和交換機已知的共用金鑰。 |
| 設定 tacacs-server host *tacacs+伺服器ip地址* | 使用全域性配置命令指定將用於身份驗證的TACACS+伺服器。 |
| Set accounting commands enable {*config* /*all*} {*stop-only*} *tacacs+* | 啟用配置命令記帳。 |

有關如何配置AAA以監控和控制對Catalyst企業LAN交換機上命令列介面的訪問的詳細資訊，請參閱使用身份驗證、授權和記帳控制對交換機的訪問文檔。

## SNMP安全性

SNMP通訊協定可用於對路由器和Catalyst交換器進行類似於CLI中發佈的組態變更。應在網路裝置上配置適當的安全措施，以防止通過SNMP進行未經授權的訪問和更改。社群字串應該依照標準的密碼准則來決定長度、字型和猜測的難度。將社群字串變更為其公共和私人預設值非常重要。

所有SNMP管理主機應具有靜態IP地址，並由IP地址和訪問控制清單(ACL)預定義的網路裝置明確授予SNMP通訊許可權。 Cisco IOS和Cisco Catalyst軟體提供安全功能，確保只允許授權的管理站在網路裝置上執行更改。

### 路由器安全功能

### SNMP許可權級別

此功能限制了管理站可以在路由器上執行的操作型別。路由器的許可權級別有兩種：唯讀(RO)和讀取/寫入(RW)。 RO級別僅允許管理站查詢路由器資料。它不允許執行配置命令，如重新啟動路由器和關閉介面。只有RW許可權級別可用於執行此類操作。

### SNMP存取控制清單(ACL)

SNMP ACL功能可與SNMP許可權功能結合使用，以限制特定管理站向路由器請求管理資訊。

### SNMP檢視

此功能限制了管理站可以從路由器檢索的特定資訊。它可以與SNMP許可權級別和ACL功能配合使用，以強制管理控制檯對資料進行受限訪問。有關SNMP檢視的配置示例，請轉至snmp-server view。

### SNMP版本3

SNMP第3版(SNMPv3)提供網路裝置和管理站之間管理資料的安全交換。SNMPv3中的加密和身份驗證功能可確保將資料包傳輸到管理控制檯時具有高安全性。Cisco IOS軟體版本12.0(3)T和更新版本支援SNMPv3。有關SNMPv3的技術概述，請轉到SNMPv3文檔。

### 介面上的存取控制清單(ACL)

ACL功能提供安全措施，以防止IP欺騙等攻擊。ACL可應用於路由器的傳入或傳出介面。

### Catalyst LAN交換器安全功能

### IP允許清單

IP Permit List功能限制來自未經授權的源IP地址的入站Telnet和SNMP對交換機的訪問。支援系統日誌消息和SNMP陷阱在出現違規或未授權訪問時通知管理系統。

Cisco IOS安全功能的組合可用於管理路由器和Catalyst交換機。需要建立安全策略，以限制能夠訪問交換機和路由器的管理站的數量。

有關如何提高IP網路安全性的詳細資訊，請轉至提高IP網路安全性。

# 會計管理

記帳管理是用來測量網路利用率引數的過程，以便可以出於記帳或按儲存容量使用計費的目的對網路上的個人或組使用者進行適當調整。與效能管理類似，適當的記帳管理的第一步也是衡量所有重要網路資源的利用率。可使用Cisco NetFlow和Cisco IP Accounting功能測量網路資源利用率。通過對通過這些方法收集的資料進行分析，可以深入瞭解當前的使用模式。

基於使用的記賬和計費系統是任何服務級別協定(SLA)的重要組成部分。 它既提供了定義SLA下義務的實用方法，也為SLA條款之外的行為提供了明確的後果。

資料可通過探測器或Cisco NetFlow收集。Cisco提供NetFlow Collector和NetFlow Analyzer應用以收集和分析來自路由器和Catalyst交換機的資料。共用軟體應用程式（如cflod）也用於收集NetFlow資料。對資源使用的持續測量可以產生計費資訊，以及評估持續公平和最佳資源的資訊。一些常用的會計管理解決方案包括：

- 明顯軟體

## NetFlow啟用和資料收集策略

NetFlow（網路流）是一種輸入側測量技術，可用於捕獲網路規劃、監控和計費應用程式所需的資料。應將NetFlow部署到服務提供商的邊緣/匯聚路由器介面或企業客戶的WAN接入路由器介面上。

Cisco Systems建議對這些具有戰略位置的路由器啟用NetFlow服務，進行精心計畫的NetFlow部署。NetFlow可以增量部署（逐個介面），也可以戰略性地部署（在精心選擇的路由器上），而不是在網路上的每台路由器上部署NetFlow。思科人員將與客戶合作，根據客戶的流量模式、網路拓撲和架構確定應在哪些關鍵路由器和關鍵介面上啟用NetFlow。

主要部署考慮事項包括：

- NetFlow服務應用作邊緣計量和訪問清單效能加速工具，且不應在運行在CPU利用率極高的*熱核/骨幹路由器或路由器上啟用。*
- 瞭解應用程式驅動的資料收集要求。記帳應用程式可能只需要傳送和終止路由器流資訊，而監控應用程式可能需要更全面（資料密集型）的端到端檢視。
- 瞭解網路拓撲和路由策略對流量收集策略的影響。例如，通過在流量發起或終止的關鍵聚合路由器上啟用NetFlow，而不是在骨幹路由器或中間路由器上啟用NetFlow（這些路由器會提供相同流量資訊的重複檢視），避免收集重複流。
- *中轉運營商業務*(承載在其網路中既不產生也不終止的流量)中的服務提供商可使用NetFlow Export資料來測量網路資源的中轉流量使用情況，以用於計費和計費。

## 配置IP記帳

Cisco IP記帳支援提供基本IP記帳功能。通過啟用IP記帳，使用者可以檢視通過Cisco IOS軟體在源IP地址和目標IP地址基礎上交換的位元組數和資料包數。僅對傳輸IP流量進行測量，並且僅對出站流量進行測量。由軟體生成或終止於軟體的流量不包括在記帳統計資訊中。為了維護準確的會計合計，軟體維護兩個會計資料庫：一個活動且有檢查點的資料庫。

Cisco IP accounting support還提供用於識別IP訪問清單失敗的IP流量的資訊。識別違反IP存取清單的IP來源位址，表示可能有人企圖破壞安全性。資料還指示應驗證IP訪問清單配置。要使此功能對使用者可用，請使用**ip accounting access-violations**命令啟用訪問清單違規的IP記帳。然後，使用者可以顯示嘗試違反源目標對訪問清單安全的單個源的位元組數和資料包數。預設情況下，IP記帳顯示已通過訪問清單且被路由的資料包數量。

要啟用IP記帳，請在介面配置模式下為每個介面使用以下命令之一：

| 指令 | 目的 |
|---|---|
| **ip記帳** | 啟用基本IP記帳。 |
| **ip記帳訪問違規** | 啟用IP記帳，能夠識別出未通過IP訪問清單的IP流量。 |

要配置其他IP記帳功能，請在全域性配置模式下使用以下一個或多個命令：

| 指令 | 目的 |
|---|---|
| ip accounting-threshold *threshold* | 設定要建立的會計分錄的最大數量。 |
| ip accounting-list *ip-address wildcard* | 過濾主機的記帳資訊。 |
| ip accounting-transits *count* | 控制將儲存在IP記帳資料庫中的傳輸記錄數。 |

請參閱思科技術提示慣例以瞭解有關本文中所用慣例的資訊。