Netzwerkmanagementsystem: Whitepaper zu Best Practices

Inhalt

Einführung

Das Netzwerkmanagementmodell der Internationalen Organisation für Standardisierung (ISO) definiert fünf Funktionsbereiche des Netzwerkmanagements. Dieses Dokument behandelt alle Funktionsbereiche. Das Gesamtziel dieses Dokuments besteht darin, praktische Empfehlungen für die einzelnen Funktionsbereiche vorzulegen, um die allgemeine Wirksamkeit der derzeitigen Verwaltungstools und -praktiken zu erhöhen. Darüber hinaus werden Design-Richtlinien für die zukünftige Implementierung von Netzwerkmanagement-Tools und -Technologien bereitgestellt.

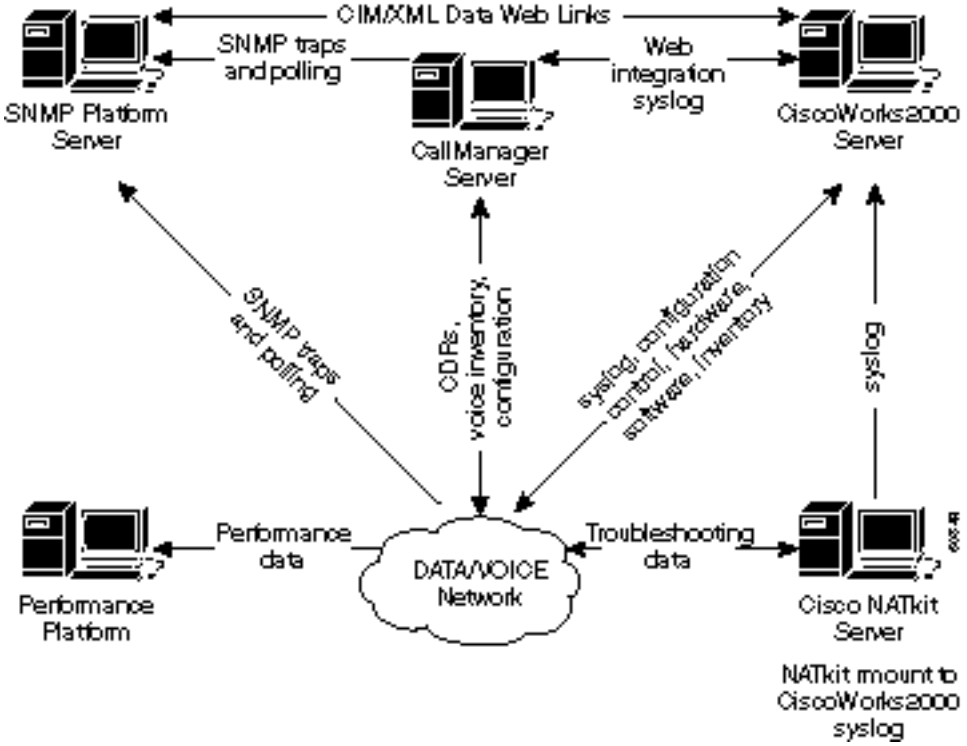
Netzwerkmanagement

Die fünf Funktionsbereiche des ISO-Netzwerkmanagementmodells sind nachfolgend aufgeführt.

- Fehlermanagement - Erkennen, Isolieren, Benachrichtigen und Beheben von im Netzwerk aufgetretenen Fehlern.

- Konfigurationsmanagement - Konfigurationsaspekte von Netzwerkgeräten wie Konfigurationsdateimanagement, Bestandsverwaltung und Softwaremanagement.
- Performance Management (Leistungsmanagement) - Überwachen und Messen verschiedener Leistungsaspekte, damit die Gesamtleistung auf einem akzeptablen Niveau gehalten werden kann.
- Sicherheitsmanagement - Zugriff auf Netzwerkgeräte und Unternehmensressourcen für autorisierte Personen
- Accounting-Management - Informationen zur Nutzung von Netzwerkressourcen.

Das folgende Diagramm zeigt eine Referenzarchitektur, die nach Ansicht von Cisco Systems die minimale Lösung für das Management eines Datennetzwerks sein sollte. Diese Architektur umfasst einen Cisco CallManager-Server für alle, die Voice over Internet Protocol (VoIP) verwalten möchten: Das Diagramm zeigt, wie Sie den CallManager-Server in die NMS-Topologie integrieren.



Die Netzwerkmanagement-Architektur umfasst folgende Komponenten:

- Simple Network Management Protocol (SNMP)-Plattform für das Fehlermanagement
- Leistungsüberwachungsplattform für langfristiges Performance-Management und Trendanalyse
- CiscoWorks2000 Server für Konfigurationsmanagement, Syslog-Sammlung sowie Hardware- und Software-Bestandsverwaltung

Einige SNMP-Plattformen können Daten mithilfe von CIM/XML-Methoden (Common Information Model/eXtensible Markup Language) direkt mit dem CiscoWorks200-Server gemeinsam nutzen. CIM ist ein gemeinsames Datenmodell eines implementierungsneutralen Schemas zur Beschreibung der allgemeinen Managementinformationen in einer Netzwerk-/Unternehmensumgebung. CIM besteht aus einer Spezifikation und einem Schema. Die Spezifikation definiert die Details für die Integration mit anderen Managementmodellen, wie SNMP MIBs oder Desktop Management Task Force Management Information Files (DMTF MIFs), während das Schema die eigentlichen Modellbeschreibungen bereitstellt.

XML ist eine Markupsprache, mit der strukturierte Daten in Textform dargestellt werden können.

Ein spezifisches Ziel von XML war es, den größten Teil der beschreibenden Kraft von SGML beizubehalten und gleichzeitig so viel Komplexität wie möglich zu beseitigen. XML ähnelt dem HTML-Konzept, während HTML jedoch verwendet wird, um grafische Informationen über ein Dokument zu übertragen, wird XML verwendet, um strukturierte Daten in einem Dokument darzustellen.

Die Kunden von Cisco für erweiterte Services würden darüber hinaus den Cisco NATkit-Server für zusätzliche proaktive Überwachung und Fehlerbehebung verwenden. Der NATkit-Server verfügt entweder über eine Remote-Laufwerksbereitstellung (Rmount) oder über FTP (File Transfer Protocol)-Zugriff auf die Daten auf dem CiscoWorks2000-Server.

Das Kapitel Netzwerkmanagement-Grundlagen im *Überblick über die Internetworking-Technologie* bietet einen detaillierteren Überblick über die Grundlagen des Netzwerkmanagements.

Fehlermanagement

Das Ziel des Fehlermanagements ist es, Netzwerkprobleme zu erkennen, zu protokollieren, Benutzer zu benachrichtigen und (soweit möglich) automatisch zu beheben, um einen effizienten Netzwerkbetrieb zu gewährleisten. Da Fehler Ausfallzeiten oder inakzeptable Netzwerkverschlechterung verursachen können, ist das Fehlermanagement die am weitesten verbreitete Anwendung der ISO-Netzwerkmanagementelemente.

Netzwerkmanagement-Plattformen

Eine im Unternehmen bereitgestellte Netzwerkverwaltungsplattform verwaltet eine Infrastruktur, die aus Netzwerkelementen verschiedener Anbieter besteht. Die Plattform empfängt und verarbeitet Ereignisse von Netzwerkelementen im Netzwerk. Ereignisse von Servern und anderen kritischen Ressourcen können ebenfalls an eine Verwaltungsplattform weitergeleitet werden. Die folgenden allgemein verfügbaren Funktionen sind in einer Standard-Managementplattform enthalten:

- Netzwerkerkennung
- Topologiezuordnung für Netzwerkelemente
- Ereignishandler
- Leistungsdatenerfasser und -grafiker
- Management-Datenbrowser

Netzwerkverwaltungsplattformen können bei der Erkennung von Infrastrukturfehlern als Hauptkonsole für den Netzwerkbetrieb angesehen werden. Die Fähigkeit, Probleme in jedem Netzwerk schnell zu erkennen, ist von entscheidender Bedeutung. Netzwerkbetriebspersonal kann sich auf eine grafische Netzwerkübersicht verlassen, um die Betriebszustände kritischer Netzwerkelemente wie Router und Switches anzuzeigen.

Netzwerkverwaltungsplattformen wie HP OpenView, Computer Associates Unicenter und SUN Solstice können eine Erkennung von Netzwerkgeräten durchführen. Jedes Netzwerkgerät wird durch ein grafisches Element auf der Konsole der Verwaltungsplattform dargestellt. Unterschiedliche Farben auf den grafischen Elementen stellen den aktuellen Betriebsstatus von Netzwerkgeräten dar. Netzwerkgeräte können so konfiguriert werden, dass sie Benachrichtigungen, so genannte SNMP-Traps, an Netzwerkverwaltungsplattformen senden. Beim Empfang der Benachrichtigungen ändert sich das grafische Element für das Netzwerkgerät je nach Schweregrad der empfangenen Benachrichtigung in eine andere Farbe. Die Benachrichtigung, die normalerweise als Ereignis bezeichnet wird, wird in einer Protokolldatei

gespeichert. Es ist besonders wichtig, dass die aktuellsten Cisco Management Information Base (MIB)-Dateien auf die SNMP-Plattform geladen werden, um sicherzustellen, dass die verschiedenen Warnungen von Cisco Geräten korrekt interpretiert werden.

Cisco veröffentlicht die MIB-Dateien zur Verwaltung verschiedener Netzwerkgeräte. Die Cisco MIB-Dateien befinden sich auf der Cisco.com-Website und enthalten folgende Informationen:

- MIB-Dateien im SNMPv1-Format veröffentlicht
- MIB-Dateien im SNMPv2-Format veröffentlicht
- Unterstützte SNMP-Traps auf Cisco Geräten
- OIDs für aktuelle SNMP MIB-Objekte von Cisco

Eine Reihe von Netzwerkverwaltungsplattformen ist in der Lage, mehrere geografisch verteilte Standorte zu verwalten. Dies wird durch den Austausch von Managementdaten zwischen Verwaltungskonsolen an Remote-Standorten mit einer Verwaltungsstation am Hauptstandort erreicht. Der Hauptvorteil einer verteilten Architektur besteht darin, dass sie den Verwaltungsdatenverkehr reduziert und somit eine effektivere Bandbreitennutzung ermöglicht. Eine verteilte Architektur ermöglicht es Mitarbeitern außerdem, ihre Netzwerke von Remote-Standorten aus mithilfe von Systemen zu verwalten.

Eine kürzlich erfolgte Erweiterung der Verwaltungsplattformen besteht in der Möglichkeit, Netzwerkelemente über eine Webschnittstelle remote zu verwalten. Durch diese Erweiterung entfällt der Bedarf an spezieller Client-Software auf einzelnen Benutzerkonsolen für den Zugriff auf eine Verwaltungsplattform.

Ein typisches Unternehmen besteht aus verschiedenen Netzwerkelementen. Jedes Gerät benötigt jedoch normalerweise anbieterspezifische Elementmanagementsysteme, um die Netzwerkelemente effektiv verwalten zu können. Aus diesem Grund werden bei doppelt vorhandenen Managementstationen möglicherweise Netzwerkelemente für dieselben Informationen abgespielt. Die von verschiedenen Systemen gesammelten Daten werden in separaten Datenbanken gespeichert, wodurch der Administrationsaufwand für Benutzer entsteht. Aufgrund dieser Einschränkung haben Netzwerk- und Softwareanbieter Standards wie Common Object Request Broker Architecture (CORBA) und Computer-Integrated Manufacturing (CIM) eingeführt, um den Austausch von Managementdaten zwischen Verwaltungsplattformen und Elementmanagementsystemen zu erleichtern. Wenn Anbieter Standards bei der Entwicklung von Managementsystemen einführen, können Benutzer bei der Bereitstellung und Verwaltung der Infrastruktur Interoperabilität und Kosteneinsparungen erwarten.

CORBA legt ein System fest, das die Interoperabilität zwischen Objekten in einer heterogenen, verteilten Umgebung und auf eine für den Programmierer transparente Weise ermöglicht. Sein Design basiert auf dem Objektmodell der Object Management Group (OMG).

Infrastruktur zur Fehlerbehebung

Trivial File Transfer Protocol (TFTP)- und System Log (Syslog)-Server sind wichtige Komponenten einer Infrastruktur zur Fehlerbehebung im Netzwerkbetrieb. Der TFTP-Server wird hauptsächlich zum Speichern von Konfigurationsdateien und Software-Images für Netzwerkgeräte verwendet. Router und Switches können Systemprotokollmeldungen an einen Syslog-Server senden. Die Meldungen erleichtern die Fehlerbehebung, wenn Probleme auftreten. Gelegentlich benötigen die Support-Mitarbeiter von Cisco Syslog-Meldungen, um eine Ursachenanalyse durchzuführen.

Die verteilte Syslog-Sammelfunktion CiscoWorks200 Resource Management Essentials (Essentials) ermöglicht die Bereitstellung mehrerer UNIX- oder NT-Sammelstellen an Remote-

Standorten, um die Erfassung und Filterung von Nachrichten durchzuführen. Die Filter können angeben, welche Syslog-Meldungen an den Essentials-Hauptserver weitergeleitet werden. Ein großer Vorteil bei der Implementierung einer verteilten Erfassung ist die Reduzierung der an die wichtigsten Syslog-Server weitergeleiteten Meldungen.

Fehlererkennung und -benachrichtigung

Das Fehlermanagement dient der Erkennung, Isolierung, Benachrichtigung und Behebung von Netzwerkfehlern. Netzwerkgeräte können Verwaltungsstationen benachrichtigen, wenn ein Fehler in den Systemen auftritt. Ein effektives Fehlermanagementsystem besteht aus mehreren Teilsystemen. Die Fehlererkennung wird durchgeführt, wenn die Geräte SNMP-Trap-Meldungen, SNMP Polling, RMON-Grenzwerte (Remote Monitoring) und Syslog-Meldungen senden. Ein Managementsystem benachrichtigt den Endbenutzer, wenn ein Fehler gemeldet wird und Korrekturmaßnahmen ergriffen werden können.

Traps sollten auf Netzwerkgeräten konsistent aktiviert werden. Zusätzliche Traps werden von neuen Cisco IOS-Softwareversionen für Router und Switches unterstützt. Es ist wichtig, die Konfigurationsdatei zu überprüfen und zu aktualisieren, um sicherzustellen, dass Traps korrekt dekodiert werden. Eine regelmäßige Überprüfung der konfigurierten Traps durch das Cisco Assured Network Services (ANS)-Team sorgt für eine effektive Fehlererkennung im Netzwerk.

In der folgenden Tabelle sind die CISCO-STACK-MIB-Traps aufgeführt, die von Cisco Catalyst Local Area Network (LAN)-Switches unterstützt werden und zum Überwachen von Fehlerzuständen verwendet werden können.

Trap	Beschreibung
ModulUp	Die Agent-Entität hat festgestellt, dass das **moduleStatus-**Objekt in dieser MIB in den **ok(2)**-Zustand für eines ihrer Module übergegangen ist.
ModulDown	Die Agent-Entität hat festgestellt, dass das *moduleStatus*-Objekt in dieser MIB den **ok(2)**-Status für eines ihrer Module verlassen hat.
ChassisAlarmOn	Die Agent-Einheit hat festgestellt, dass das *ChassisTempAlarm*, *ChassisMinorAlarm* oder *ChassisMajorAlarm*-Objekt in dieser MIB in den **on(2)**-Zustand übergegangen ist. Ein *ChassisMajorAlarm* gibt an, dass eine der folgenden Bedingungen zutrifft: • Beliebige Spannungsausfälle • Gleichzeitige Temperatur und Lüfterausfall • 100 % Ausfall des Netzteils (zwei von zwei oder einer von einem) • Elektrisch löschbarer EEPROM-Fehler (Programmable Read-Only Memory) • Nichtflüchtiger RAM-Ausfall (NVRAM) • MCP-Kommunikationsfehler • NMP-Status unbekannt Ein ChassisMinorAlarm gibt an, dass eine der folgenden Bedingungen vorhanden ist:

	• Temperaturalarm • Lüfterausfall • Teilweise Ausfall des Netzteils (einer von zwei) • Zwei Netzteile inkompatibler Art
ChassisAlarmAus	Die Agent-Einheit hat festgestellt, dass das *ChassisTempAlarm*, *ChassisMinorAlarm* oder *ChassisMajorAlarm*-Objekt in dieser MIB in den **Off(1)**-Zustand übergegangen ist.

Die Umgebungsüberwachungs-Traps (envmon) werden in CISCO-ENVMON-MIB-Traps definiert. Die Umweltfalle sendet Cisco Enterprise-spezifische Benachrichtigungen für Umgebungsüberwachungssysteme, wenn eine Umgebungsschwelle überschritten wird. Wenn envmon verwendet wird, kann ein bestimmter Umgebungs-Trap-Typ aktiviert oder alle Trap-Typen aus dem Umgebungsüberwachungssystem akzeptiert werden. Wenn keine Option angegeben ist, werden alle Umgebungstypen aktiviert. Dabei kann es sich um einen oder mehrere der folgenden Werte handeln:

- spannung - Eine ciscoEnvMonVoltageNotification wird gesendet, wenn die an einem bestimmten Prüfpunkt gemessene Spannung außerhalb des normalen Bereichs für den Prüfpunkt liegt (z. B. in der Warn-, Kritisch- oder Herunterschaltphase).
- shutdown - Eine ciscoEnvMonShutdownNotification wird gesendet, wenn der Umgebungsmonitor feststellt, dass ein Testpunkt einen kritischen Zustand erreicht und im Begriff ist, einen Herunterfahren zu starten.
- supply - Eine ciscoEnvMonRedundantSupplyNotification wird gesendet, wenn das redundante Netzteil (sofern vorhanden) ausfällt.
- fan - Eine ciscoEnvMonFanNotification wird gesendet, wenn einer der Lüfter im Lüfterarray (sofern vorhanden) ausfällt.
- temperature - Eine ciscoEnvMonTemperatureNotification wird gesendet, wenn die an einem bestimmten Prüfpunkt gemessene Temperatur außerhalb des normalen Bereichs für den Prüfpunkt liegt (z. B. in der Warn-, kritischen oder heruntergefahrenen Phase).

Die Fehlererkennung und Überwachung von Netzwerkelementen kann von der Geräteebene auf die Protokoll- und Schnittstellenebene erweitert werden. In einer Netzwerkumgebung kann die Fehlerüberwachung Virtual Local Area Network (VLAN), den asynchronen Übertragungsmodus (ATM), Fehleranzeigen an physischen Schnittstellen usw. umfassen. Die Fehlermanagement-Implementierung auf Protokollebene ist über ein Elementmanagementsystem wie den CiscoWorks2000 Campus Manager verfügbar. Der Schwerpunkt der TrafficDirector-Anwendung im Campus Manager liegt auf der Switch-Verwaltung. Dabei wird die Mini-RMON-Unterstützung für Catalyst Switches verwendet.

Angesichts der zunehmenden Anzahl von Netzwerkelementen und der Komplexität von Netzwerkproblemen kann ein Ereignismanagementsystem in Betracht gezogen werden, das verschiedene Netzwerkereignisse (Syslog, Trap, Protokolldateien) korrelieren kann. Diese Architektur hinter einem Event Management System ist vergleichbar mit einem Manager of Managers-System (MOM). Dank eines gut durchdachten Ereignismanagementsystems können die Mitarbeiter im Network Operations Center (NOC) Netzwerkprobleme proaktiv und effektiv erkennen und diagnostizieren. Durch die Priorisierung und Unterdrückung von Ereignissen können sich die Mitarbeiter im Netzwerkbetrieb auf kritische Netzwerkereignisse konzentrieren, verschiedene Ereignismanagementsysteme wie das Cisco Info Center untersuchen und eine Machbarkeitsanalyse durchführen, um die Funktionen solcher Systeme vollständig zu

untersuchen. Weitere Informationen erhalten Sie im Cisco Info Center.

Proaktive Fehlerüberwachung und -benachrichtigung

RMON-Alarm- und -Ereignis sind zwei Gruppen, die in der RMON-Spezifikation definiert sind. Normalerweise führt eine Managementstation Polling auf Netzwerkgeräten durch, um den Status oder Wert bestimmter Variablen zu bestimmen. Beispielsweise fragt eine Managementstation einen Router ab, um die CPU-Auslastung (Central Processing Unit) zu ermitteln und ein Ereignis zu generieren, wenn der Wert einen konfigurierten Grenzwert erreicht. Diese Methode verschwendet die Netzwerkbandbreite und kann den tatsächlichen Grenzwert je nach Abfrageintervall auch verpassen.

Bei RMON-Alarmen und -Ereignissen wird ein Netzwerkgerät so konfiguriert, dass es sich selbst auf steigende und fallende Schwellenwerte überwacht. In einem vordefinierten Zeitintervall nimmt das Netzwerkgerät ein Beispiel einer Variablen und vergleicht sie mit den Schwellenwerten. Ein SNMP-Trap kann an eine Managementstation gesendet werden, wenn der tatsächliche Wert die konfigurierten Schwellenwerte überschreitet oder unterschreitet. RMON-Alarm- und -Ereignisgruppen bieten eine proaktive Methode zum Verwalten kritischer Netzwerkgeräte.

Cisco Systems empfiehlt die Implementierung von RMON-Alarmen und -Ereignissen auf kritischen Netzwerkgeräten. Überwachte Variablen können die CPU-Auslastung, Pufferausfälle, Eingabe-/Ausgabeverwerfen oder beliebige Variablen von Integer-Typen umfassen. Ab Version 11.1(1) der Cisco IOS-Software unterstützen alle Router-Images RMON-Alarm- und Ereignisgruppen.

Ausführliche Informationen zur RMON-Alarm- und Ereignisimplementierung finden Sie im Abschnitt RMON Alarm and Event Implementation (RMON-Alarm- und Ereignisimplementierung).

RMON-Speichereinschränkungen

Die RMON-Speichernutzung ist auf allen Switch-Plattformen hinsichtlich Statistiken, Verlaufsdaten, Alarmen und Ereignissen konstant. RMON verwendet einen so genannten *Eimer*, um Verlaufshistorien und Statistiken auf dem RMON-Agent (in diesem Fall der Switch) zu speichern. Die Größe der Eimer wird auf der RMON-Sonde (SwitchProbe-Gerät) oder der RMON-Anwendung (TrafficDirector-Tool) definiert und dann zum Festlegen an den Switch gesendet.

Zur Unterstützung von Mini-RMON werden etwa 450 K Codespeicher benötigt (z. B. vier RMON-Gruppen: Statistiken, Verlauf, Alarme und Ereignisse). Die dynamische Speicheranforderung für RMON variiert, da sie von der Laufzeitkonfiguration abhängt.

In der folgenden Tabelle werden die Informationen zur RMON-Speichernutzung der Laufzeit für jede Mini-RMON-Gruppe definiert.

RMON-Gruppendefinition	Verwendeter DRAM-Speicher	Hinweise
Statistiken	140 Byte pro Switched Ethernet-/Fast Ethernet-Port	Pro Port
Geschichte	3,6 K für 50 Eimer *	Jede zusätzliche Gruppe benötigt 56

		Byte
Alarm und Veranstaltung	2,6 K pro Alarm und zugehörige Ereigniseinträge	pro Alarm pro Port

* RMON verwendet einen so genannten *Eimer*, um Verlaufsberichte und Statistiken auf dem RMON-Agent (z. B. einem Switch) zu speichern.

RMON-Alarm- und Ereignisimplementierung

Durch die Integration von RMON als Teil einer Fehlermanagementlösung kann der Benutzer das Netzwerk proaktiv überwachen, bevor ein potenzielles Problem auftritt. Wenn beispielsweise die Anzahl der empfangenen Broadcast-Pakete erheblich zunimmt, kann dies zu einer Erhöhung der CPU-Auslastung führen. Durch die Implementierung von RMON-Alarmen und -Ereignissen kann ein Benutzer einen Schwellenwert einrichten, um die Anzahl der empfangenen Broadcast-Pakete zu überwachen und die SNMP-Plattform über ein SNMP-Trap zu benachrichtigen, wenn der konfigurierte Grenzwert erreicht wird. Durch RMON-Alarme und -Ereignisse wird das übermäßige Polling, das normalerweise von der SNMP-Plattform ausgeführt wird, um dasselbe Ziel zu erreichen, eliminiert.

Es stehen zwei Methoden zum Konfigurieren von RMON-Alarmen und -Ereignissen zur Verfügung:

- Befehlszeilenschnittstelle (CLI)
- SNMP-SET

Die folgenden Beispielprozeduren zeigen, wie Sie einen Schwellenwert festlegen, um die Anzahl der über eine Schnittstelle empfangenen Broadcast-Pakete zu überwachen. In diesen Prozeduren wird derselbe Zähler verwendet, wie im Befehlsbeispiel **show interface** am Ende dieses Abschnitts gezeigt wird.

Beispiel für eine Befehlszeilenschnittstelle

So implementieren Sie RMON-Alarm und -Ereignis über die CLI-Schnittstelle:

1. Suchen Sie den Schnittstellenindex für Ethernet 0, indem Sie die ifTable-MIB durchlaufen.
```
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. Rufen Sie die OID ab, die dem zu überwachenden CLI-Feld zugeordnet ist. In diesem Beispiel lautet die OID für 'Broadcasts' 1.3.6.1.2.1.2.2.1.12. Die Cisco OIDs für bestimmte MIB-Variablen sind auf der Website cisco.com verfügbar.
3. Bestimmen Sie die folgenden Parameter zum Einrichten von Schwellenwerten und Ereignissen.SchwellenwerteStichprobenart (Absolue oder Delta)AbtastintervallAktion bei Erreichen des GrenzwertsFür dieses Beispiel wird ein Grenzwert eingerichtet, um die Anzahl der über Ethernet 0 empfangenen Broadcast-Pakete zu überwachen. Ein Trap wird generiert, wenn die Anzahl der empfangenen Broadcast-Pakete zwischen 60 Sekunden über 500 liegt. Der Grenzwert wird erneut aktiviert, wenn die Anzahl der eingehenden Übertragungen

zwischen den Stichproben nicht zunimmt.**Hinweis:** Ausführliche Informationen zu diesen Befehlsparametern finden Sie in der Cisco Connection Online (CCO)-Dokumentation zu RMON-Alarm- und Ereignisbefehlen für Ihre spezielle Cisco IOS-Version.

4. Geben Sie das gesendete Trap (RMON-Ereignis) an, wenn der Grenzwert mithilfe der folgenden CLI-Befehle erreicht wird (die Cisco IOS-Befehle werden fett angezeigt):**Rmon Ereignis 1 Trap Gateway Beschreibung "High Broadcast on Ethernet 0" Eigentümer CiscoRMON-Ereignis 2 Protokollbeschreibung "normaler Broadcast erhalten auf Ethernet 0" Eigentümer Cisco**
5. Geben Sie die Grenzwerte und relevanten Parameter (RMON-Alarm) mithilfe der folgenden CLI-Befehle an:**rmon alarm 1 ifEntry.12.1 60 delta ansteigender Grenzwert 500 1fallender Grenzwert 0 2 Eigentümer Cisco**
6. Verwenden Sie SNMP, um diese Tabellen abzufragen, um zu überprüfen, ob die eventTable-Einträge auf dem Gerät vorgenommen wurden.

```
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. Verwenden Sie SNMP, um diese Tabellen abzufragen, um zu überprüfen, ob die alarmTable-Einträge festgelegt wurden.

```
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)
```

Beispiel für SNMP-SET

Führen Sie die folgenden Schritte aus, um RMON-Alarme und -Ereignisse mit dem SNMP SET-Vorgang zu implementieren:

1. Geben Sie das gesendete Trap (RMON-Ereignis) an, wenn der Grenzwert mithilfe der folgenden SNMP SET-Vorgänge erreicht wird:
```
# 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. Geben Sie die Schwellenwerte und relevanten Parameter (RMON-Alarm) mithilfe der folgenden SNMP SET-Vorgänge an:
```
# 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. Rufen Sie diese Tabellen ab, um zu überprüfen, ob die eventTable-Einträge auf dem Gerät vorgenommen wurden.
```
% 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. Rufen Sie diese Tabellen ab, um zu überprüfen, ob die alarmTable-Einträge festgelegt wurden.

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

Anzeigeschnittstelle

Dieses Beispiel ist ein Ergebnis des Befehls **show interface**.

gateway> **Interface *Ethernet 0* anzeigen**

```
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
```

Konfigurationsverwaltung

Ziel des Konfigurationsmanagements ist es, Informationen zur Netzwerk- und Systemkonfiguration zu überwachen, sodass die Auswirkungen verschiedener Versionen von Hardware- und Softwareelementen auf den Netzwerkbetrieb nachverfolgt und verwaltet werden können.

Konfigurationsstandards

Da immer mehr Netzwerkgeräte bereitgestellt werden, ist es wichtig, den Standort eines Netzwerkgeräts genau identifizieren zu können. Diese Standortinformationen sollten eine detaillierte Beschreibung enthalten, die denjenigen aussagekräftig ist, die mit Dispatching-Ressourcen betraut sind, wenn ein Netzwerkproblem auftritt. Um eine schnelle Lösung bei einem Netzwerkproblem zu ermöglichen, stellen Sie sicher, dass Sie über die Kontaktdaten der für die Geräte zuständigen Person oder Abteilung verfügen. Die Kontaktinformationen müssen die Telefonnummer und den Namen der Person oder Abteilung enthalten.

Namenskonventionen für Netzwerkgeräte, angefangen beim Gerätenamen bis hin zur einzelnen Schnittstelle, sollten im Rahmen des Konfigurationsstandards geplant und implementiert werden. Eine klar definierte Namenskonvention bietet Mitarbeitern die Möglichkeit, bei der Behebung von Netzwerkproblemen präzise Informationen bereitzustellen. Die Namenskonvention für Geräte kann den geografischen Standort, den Namen des Gebäudes, den Boden usw. verwenden. Bei der Namenskonvention für die Schnittstelle kann es das Segment enthalten, mit dem ein Port verbunden ist, den Namen des verbindenden Hubs usw. Auf seriellen Schnittstellen sollten die tatsächliche Bandbreite, die DLCI-Nummer (Local Data Link Connection Identifier) (falls Frame Relay), das Ziel und die vom Carrier bereitgestellte Circuit-ID oder Information enthalten sein.

Konfigurationsdateiverwaltung

Wenn Sie neue Konfigurationsbefehle zu vorhandenen Netzwerkgeräteanforderungen hinzufügen, müssen Sie die Befehle auf Integrität überprüfen, bevor die tatsächliche Implementierung erfolgt. Ein falsch konfiguriertes Netzwerkgerät kann verheerende Auswirkungen auf die Netzwerkverbindung und -leistung haben. Konfigurationsparameter müssen überprüft werden, um Unstimmigkeiten oder Inkompatibilitätsprobleme zu vermeiden. Es empfiehlt sich, regelmäßige Überprüfungen der Konfigurationen mit Cisco Technikern zu planen.

Ein voll funktionsfähiger CiscoWorks200 Essentials ermöglicht die automatische Sicherung von Konfigurationsdateien auf Routern und Cisco Catalyst Switches. Die Sicherheitsfunktion von Essentials kann zur Authentifizierung von Konfigurationsänderungen verwendet werden. Ein Änderungsüberwachungsprotokoll ist verfügbar, um Änderungen und den Benutzernamen von Personen zu verfolgen, die Änderungen vornehmen. Für Konfigurationsänderungen auf mehreren Geräten stehen zwei Optionen zur Verfügung: das webbasierte NetConfig in der aktuellen Version von CiscoWorks200 Essentials oder das **cwconfig-**Skript. Konfigurationsdateien können mit CiscoWorks200 Essentials über vordefinierte oder benutzerdefinierte Vorlagen heruntergeladen und hochgeladen werden.

Diese Funktionen können mithilfe der Konfigurationsmanagement-Tools in CiscoWorks200 Essentials ausgeführt werden:

- Übertragen von Konfigurationsdateien vom Essentials-Konfigurationsarchiv auf ein Gerät oder mehrere Geräte
- Ziehen Sie die Konfiguration vom Gerät zum Essentials-Archiv.
- Extrahieren Sie die neueste Konfiguration aus dem Archiv, und schreiben Sie sie in eine Datei.

- Importieren der Konfiguration aus einer Datei und Übertragen der Konfiguration auf Geräte
- Vergleichen der letzten beiden Konfigurationen im Essentials-Archiv
- Löschen Sie Konfigurationen, die älter als ein bestimmtes Datum oder eine angegebene Version sind, aus dem Archiv.
- Kopieren der Startkonfiguration in die aktuelle Konfiguration

Bestandsverwaltung

Die Erkennungsfunktion der meisten Netzwerkmanagement-Plattformen soll eine dynamische Liste der im Netzwerk vorhandenen Geräte bereitstellen. Discovery Engines, wie sie in Netzwerkmanagement-Plattformen implementiert sind, sollten eingesetzt werden.

Eine Bestandsdatenbank bietet detaillierte Konfigurationsinformationen für Netzwerkgeräte. Zu den allgemeinen Informationen gehören Modelle für Hardware, installierte Module, Software-Images, Mikrocodeebenen usw. All diese Informationen sind für die Durchführung von Aufgaben wie Software- und Hardware-Wartung von entscheidender Bedeutung. Die aktuelle Liste der Netzwerkgeräte, die durch den Erkennungsprozess erfasst werden, kann als Masterliste verwendet werden, um mithilfe von SNMP oder Scripting Bestandsdaten zu erfassen. Eine Geräteliste kann aus CiscoWorks200 Campus Manager in die Inventardatenbank von CiscoWorks200 Essentials importiert werden, um eine aktuelle Aufstellung der Cisco Catalyst Switches zu erhalten.

Software-Management

Für ein erfolgreiches Upgrade von Cisco IOS-Images auf Netzwerkgeräten ist eine detaillierte Analyse der Anforderungen wie Arbeitsspeicher, Boot-ROM, Microcode-Ebene usw. erforderlich. Die Anforderungen sind in der Regel dokumentiert und auf der Cisco Website in Form von Versionshinweisen und Installationsanleitungen verfügbar. Das Upgrade eines Netzwerkgeräts, auf dem Cisco IOS ausgeführt wird, umfasst das Herunterladen eines korrekten Image von CCO, das Sichern des aktuellen Images, das Sichern aller Hardwareanforderungen und das Laden des neuen Images auf das Gerät.

Das Upgrade-Fenster für eine vollständige Gerätewartung ist für einige Unternehmen relativ begrenzt. In einer großen Netzwerkumgebung mit begrenzten Ressourcen kann es erforderlich sein, Software-Upgrades außerhalb der Geschäftszeiten zu planen und zu automatisieren. Die Prozedur kann entweder mit Skriptsprache wie Expect oder mit einer speziell für die Ausführung einer solchen Aufgabe geschriebenen Anwendung abgeschlossen werden.

Softwareänderungen an Netzwerkgeräten wie Cisco IOS-Images und Mikrocodeversionen sollten nachverfolgt werden, um in der Analysephase zu helfen, wenn eine weitere Softwarewartung erforderlich ist. Da ein Bericht zur Versionsgeschichte sofort verfügbar ist, kann die Person, die das Upgrade durchführt, das Risiko minimieren, inkompatible Bilder oder Mikrocode in Netzwerkgeräte zu laden.

Performance-Management

Service Level Agreement

Ein Service Level Agreement (SLA) ist eine schriftliche Vereinbarung zwischen einem Service Provider und seinen Kunden über das erwartete Leistungsniveau von Netzwerkservices. Das SLA

besteht aus Kennzahlen, die zwischen Anbieter und Kunden vereinbart wurden. Die für die Kennzahlen festgelegten Werte müssen realistisch, aussagekräftig und für beide Parteien messbar sein.

Zur Messung des Leistungsniveaus können von Netzwerkgeräten verschiedene Schnittstellenstatistiken erfasst werden. Diese Statistiken können als Kennzahlen in das SLA aufgenommen werden. Statistiken wie Verwerfen von Eingangswarteschlangen, Verwerfen von Ausgabewarteschlangen und ignorierte Pakete sind nützlich für die Diagnose leistungsbezogener Probleme.

Auf Geräteebene können Leistungsmetriken die CPU-Auslastung, die Pufferzuweisung (großer Puffer, mittlerer Puffer, Verluste, Trefferquote) und die Speicherzuweisung umfassen. Die Leistung bestimmter Netzwerkprotokolle steht in direktem Zusammenhang mit der Pufferverfügbarkeit in Netzwerkgeräten. Die Messung von Leistungsstatistiken auf Geräteebene ist für die Optimierung der Leistung von Protokollen auf höherer Ebene von entscheidender Bedeutung.

Netzwerkgeräte wie Router unterstützen verschiedene Protokolle höherer Schichten wie Data Link Switching Workgroup (DLSW), Remote Source Route Bridging (RSRB), AppleTalk usw. Leistungsstatistiken von WAN-Technologien (Wide Area Network) wie Frame Relay, ATM, Integrated Services Digital Network (ISDN) usw. können überwacht und erfasst werden.

Leistungsüberwachung, -messung und -berichte

Regelmäßig sollten mithilfe von SNMP verschiedene Leistungsmetriken auf Schnittstellen-, Geräte- und Protokollebene erfasst werden. Die Polling-Engine eines Netzwerkmanagementsystems kann für Datenerfassungszwecke verwendet werden. Die meisten Netzwerkmanagementsysteme sind in der Lage, abgefragte Daten zu erfassen, zu speichern und darzustellen.

Auf dem Markt gibt es verschiedene Lösungen, die auf die Anforderungen des Performance-Managements in Unternehmensumgebungen zugeschnitten sind. Diese Systeme sind in der Lage, Daten von Netzwerkgeräten und Servern zu sammeln, zu speichern und zu präsentieren. Die webbasierte Benutzeroberfläche für die meisten Produkte ermöglicht den Zugriff auf die Leistungsdaten von einem beliebigen Standort im Unternehmen aus. Zu den häufig eingesetzten Lösungen für das Leistungsmanagement gehören:

- InfoVista VistaView
- SAS-IT-Service-Vision
- Trinagy TREND

Eine Bewertung der oben genannten Produkte bestimmt, ob sie die Anforderungen verschiedener Anwender erfüllen. Einige Anbieter unterstützen die Integration mit Netzwerkmanagement- und Systemverwaltungsplattformen. InfoVista unterstützt beispielsweise den BMC Patrol Agent, um wichtige Leistungsstatistiken von Anwendungsservern bereitzustellen. Jedes Produkt hat ein anderes Preismodell und andere Funktionen mit dem Basisangebot. Einige Lösungen bieten Unterstützung für Leistungsmanagement-Funktionen für Geräte von Cisco wie NetFlow, RMON und Cisco IOS Service Assurance Agent/Response Time Reporter (RTR/SAA CSAA/RTR). Concord hat kürzlich die Unterstützung für Cisco WAN-Switches hinzugefügt, die zum Erfassen und Anzeigen von Leistungsdaten verwendet werden können.

Die Funktion CSAA/RTR Service Assurance Agent (SAA)/Response Time Reporter (RTR) in Cisco IOS kann zum Messen der Reaktionszeit zwischen IP-Geräten verwendet werden. Ein mit CSAA konfigurierter Quellrouter ist in der Lage, die Reaktionszeit auf ein Ziel-IP-Gerät zu messen,

das ein Router oder ein IP-Gerät sein kann. Die Reaktionszeit kann zwischen Quelle und Ziel oder für jeden Hop auf dem Pfad gemessen werden. SNMP-Traps können so konfiguriert werden, dass die Managementkonsolen benachrichtigt werden, wenn die Antwortzeit die vordefinierten Grenzwerte überschreitet.

Neueste Erweiterungen von Cisco IOS erweitern die Funktionen von CSAA, um Folgendes zu messen:

- Leistung des HyperText Transfer Protocol (HTTP)-ServiceDNS-NamensauflösungTCP-Verbindung (Transmission Control Protocol)HTTP-Transaktionszeit
- Interpaketverzögerungsvarianz (Jitter) des VoIP-Datenverkehrs
- Reaktionszeit zwischen Endpunkten für eine bestimmte Quality of Service (QoS)IP Type of Service (ToS)-Bits
- Paketverlust durch CSAA-generierte Pakete

Die Konfiguration der CSAA-Funktion auf Routern kann mithilfe der Cisco Internetwork Performance Monitor (IPM)-Anwendung erfolgen. CSAA/RTR ist in viele, aber nicht alle Funktionssätze der Cisco IOS-Software integriert. Eine Version der Cisco IOS-Softwareversion, die CSAA/RTR unterstützt, muss auf dem Gerät installiert sein, das IPM zum Erfassen von Leistungsstatistiken verwendet. Eine Zusammenfassung der Cisco IOS-Versionen, die CSAA/RTR/IPM unterstützen, finden Sie auf der Website für häufig gestellte Fragen (Frequently Asked Questions, IPM).

Weitere Informationen zu IPM:

- Überblick über IPM
- Service Assurance Agent

Leistungsanalyse und -optimierung

Der Benutzerdatenverkehr hat erheblich zugenommen und die Nachfrage nach Netzwerkressourcen gestiegen. Netzwerkmanager haben in der Regel nur einen begrenzten Überblick über die Arten von Datenverkehr, der im Netzwerk läuft. Die Profilerstellung für Benutzer- und Anwendungsdatenverkehr bietet eine detaillierte Ansicht des Datenverkehrs im Netzwerk. Zwei Technologien, RMON-Probes und NetFlow, ermöglichen die Erfassung von Datenverkehrsprofilen.

RMON

Die RMON-Standards wurden für die Bereitstellung in einer verteilten Architektur entwickelt, in der Agenten (entweder integriert oder in Standalone-Tests) über SNMP mit einer zentralen Station (der Verwaltungskonsole) kommunizieren. Der RFC 1757-RMON-Standard organisiert Überwachungsfunktionen in neun Gruppen, um Ethernet-Topologien zu unterstützen, und fügt eine zehnte Gruppe in RFC 1513 für eindeutige Token-Ring-Parameter hinzu. Die Fast Ethernet-Link-Überwachung erfolgt im Rahmen des RFC 1757-Standards, und die Ringüberwachung über Fibre-Distributed Data Interface (FDDI) erfolgt im Rahmen von RFC 1757 und RFC 1513.

Die neue RFC 2021 RMON-Spezifikation unterstützt Remote-Überwachungsstandards über die Media Access Control (MAC)-Ebene hinaus bis hin zu den Netzwerk- und Anwendungsebenen. Diese Konfiguration ermöglicht es Administratoren, netzwerkfähige Anwendungen wie Web-Datenverkehr, NetWare, Hinweise, E-Mail, Datenbankzugriff, Network File System (NFS) und andere zu analysieren und Fehler zu beheben. RMON-Alarme, Statistiken, Verlauf und Host-

/Gesprächsgruppen können nun proaktiv zur Überwachung und Aufrechterhaltung der Netzwerkverfügbarkeit basierend auf dem Datenverkehr auf Anwendungsebene verwendet werden - dem wichtigsten Datenverkehr im Netzwerk. RMON2 ermöglicht Netzwerkadministratoren die weitere Bereitstellung von standardbasierten Überwachungslösungen zur Unterstützung geschäftskritischer, serverbasierter Anwendungen.

In der folgenden Tabelle sind die Funktionen der RMON-Gruppen aufgeführt.

RMON Group (RFC 1757)	Funktion
Statistiken	Zähler für Pakete, Oktette, Broadcasts, Fehler und Angebote auf dem Segment oder Port.
Geschichte	Regelmäßige Stichproben und Speichern von Statistikgruppenzählern zum späteren Abrufen.
Hosts	Führt Statistiken zu jedem Host-Gerät im Segment oder Port auf.
Host Top N	Ein benutzerdefinierter Untersatzbericht der Hostgruppe, sortiert nach einem statistischen Zähler. Wenn nur die Ergebnisse zurückgegeben werden, wird der Verwaltungsdatenverkehr minimiert.
Datenverkehrsmatrix	Speichert Gesprächsstatistiken zwischen Hosts im Netzwerk.
Alarme	Ein Schwellenwert, der auf kritischen RMON-Variablen für proaktives Management festgelegt werden kann.
Veranstaltungen	Generiert SNMP-Traps und Protokolleinträge, wenn ein Schwellenwert für Alarmen-Gruppen überschritten wird.
Paketerfassung	Verwaltet Puffer für von der Filtergruppe erfasste Pakete zum Hochladen in die Managementkonsole.
Token-Ring	Ringstation - detaillierte Statistiken zur Reihenfolge der einzelnen Stationen der Ringstationen - eine geordnete Liste der Stationen, die sich derzeit in der Ringstation-Konfiguration befinden - Konfiguration und Einfüge/Entfernen pro Station Quell-Routing - Statistiken zum Quellrouting, z. B. Hop-Zähler und andere

RMON2	Funktion
Protokollverzeichnis	Protokolle, für die der Agent Statistiken überwacht und verwaltet.
Protokollverteilung	Statistiken für jedes Protokoll.

Netzwerk-Layer-Host	Statistiken für jede Netzwerkschichtadresse im Segment, Ring oder Port.
Netzwerk-Layer-Matrix	Datenverkehrsstatistiken für Paare von Netzwerkschichtadressen.
Anwendungs-Layer-Host	Statistiken nach Anwendungs-Layer-Protokoll für jede Netzwerkadresse.
Anwendungsschichtmatrix	Datenverkehrsstatistiken nach Anwendungs-Layer-Protokoll für Paare von Netzwerkschichtadressen.
Benutzerdefinierbarer Verlauf	Erweitert den Verlauf über die RMON1-Link-Layer-Statistiken hinaus und schließt alle RMON-, RMON2-, MIB-I- oder MIB-II-Statistiken ein.
Adressenzuordnung	MAC-zu-Netzwerk-Layer-Adressenbindungen.
Konfigurationsgruppe	Agenten-Funktionen und -Konfigurationen.

NetFlow

Die Cisco NetFlow-Funktion ermöglicht die Erfassung detaillierter Statistiken zu Datenverkehrsflüssen für Funktionen zur Kapazitätsplanung, Abrechnung und Fehlerbehebung. NetFlow kann auf einzelnen Schnittstellen konfiguriert werden, um Informationen zum Datenverkehr bereitzustellen, der durch diese Schnittstellen fließt. Die folgenden Informationsarten sind Teil der detaillierten Verkehrsstatistik:

- Quell- und Ziel-IP-Adressen
- Eingabe- und Ausgabe-Schnittstellennummern
- Quell- und Ziel-Ports für TCP/UDP
- Anzahl der Byte und Pakete im Fluss
- Eigenständige System-Nummern für Quelle und Ziel
- IP Type of Service (ToS)

Die auf Netzwerkgeräten erfassten NetFlow-Daten werden auf eine Collector-Maschine exportiert. Der Collector führt Funktionen wie die Reduzierung des Datenvolumens (Filterung und Aggregation), die hierarchische Datenspeicherung und das Dateisystemmanagement aus. Cisco stellt NetFlow Collector und NetFlow Analyzer-Anwendungen zum Erfassen und Analysieren von Daten von Routern und Cisco Catalyst Switches bereit. Es gibt auch Shareware-Tools wie cflow, die Datensätze des Cisco NetFlow User Datagram Protocol (UDP) erfassen können.

NetFlow-Daten werden mithilfe von UDP-Paketen in drei verschiedenen Formaten übertragen:

- Version 1 - Das ursprüngliche Format, das von den ersten NetFlow-Versionen unterstützt wird.
- Version 5 - Eine spätere Erweiterung, die die autonomen Systeminformationen und Flow Sequence Numbers (Border Gateway Protocol) (BGP) hinzugefügt hat.
- Version 7 - Eine weitere Erweiterung, die NetFlow-Switching-Unterstützung für Cisco Catalyst Switches der Serie 5000 mit einer NetFlow-Funktionskarte (NFFC) hinzugefügt hat.

Die Versionen 2 bis 4 und 6 wurden entweder nicht veröffentlicht oder werden von FlowCollector

nicht unterstützt. In allen drei Versionen besteht das Datagramm aus einem Header und einem oder mehreren Flow-Datensätzen.

Weitere Informationen finden Sie im Whitepaper NetFlow Services Solutions Guide.

In der folgenden Tabelle sind die unterstützten Cisco IOS-Versionen zum Erfassen von NetFlow-Daten von Routern und Catalyst Switches aufgeführt.

Cisco IOS Softwareversion	Unterstützte Cisco Hardwareplattformen	Von NetFlow exportierte Version(en)
11.1 CA und 11.1 CC	Cisco 7200, 7500 und RSP7000	V1 und V5
11.2 und 11.2 P	Cisco 7200, 7500 und RSP7000	V1
11,2 P	Cisco Route Switch Module (RSM)	V1
11,3 und 11,3 T	Cisco 7200, 7500 und RSP7000	V1
12.0	Cisco 1720, 2600, 3600, 4500, 4700, AS5800, 7200, uBR7200, 7500, RSP7000 und RSM	V1 und V5
12,0 Bio.	Cisco 1720, 2600, 3600, 4500, 4700, AS5800, 7200, uBR7200, 7500, RSP7000, RSM, MGX 8 000 U/min und BPX 8600	V1 und V5
12.0(3)T und spätere Version	Cisco 1600*, 1720, 2500*, 2600, 3600, 4500, 4700, AS5300*, AS5800, 7200, uBR720 0, 7500, RSP7000, RSM, MGX8800 U/min und BPX 8650	V1, V5 und V8
12,0(6)S	Cisco 12000	V1, V5 und V8
—	Cisco Catalyst 5000 mit NetFlow Feature Card (NFFC)***	V7

* Unterstützung für NetFlow Export V1, V5 und V8 auf den Cisco Plattformen 1600 und 2500 ist für Cisco IOS Software Release 12.0(T) vorgesehen. NetFlow-Unterstützung für diese Plattformen ist in der Cisco IOS 12.0-Hauptversion nicht verfügbar.

** Die Unterstützung für NetFlow V1, V5 und V8 auf der AS5300-Plattform ist für die Cisco IOS-Softwareversion 12.06(T) vorgesehen.

*** MLS- und NetFlow-Datenexport wird von der Supervisor Engine-Software der Catalyst 5000-Serie, Version 4.1(1) oder höher, unterstützt.

Sicherheitsmanagement

Ziel des Sicherheitsmanagements ist es, den Zugriff auf Netzwerkressourcen gemäß lokaler Richtlinien zu kontrollieren, sodass das Netzwerk nicht (absichtlich oder unabsichtlich) sabotiert werden kann. Ein Sicherheitsmanagement-Subsystem kann beispielsweise Benutzer überwachen, die sich bei einer Netzwerkressource anmelden, und den Zugriff auf Benutzer verweigern, die unangemessene Zugriffscodes eingeben. Das Sicherheitsmanagement ist ein sehr breites Thema. Daher wird in diesem Bereich des Dokuments nur die Sicherheit im Zusammenhang mit SNMP und der grundlegenden Gerätezugriffssicherheit behandelt.

Zu den detaillierten Informationen zu erweiterten Sicherheitsfunktionen gehören:

- Erhöhte Sicherheit in IP-Netzwerken
- OpenSystems

Eine gute Implementierung des Sicherheitsmanagements beginnt mit soliden Sicherheitsrichtlinien und -verfahren. Es ist wichtig, einen plattformspezifischen Mindestkonfigurationsstandard für alle Router und Switches zu erstellen, der branchenweit bewährte Sicherheits- und Leistungsstandards einhält.

Es gibt verschiedene Methoden zur Zugriffskontrolle auf Cisco Routern und Catalyst Switches. Zu diesen Methoden gehören:

- Zugriffskontrolllisten (ACL)
- Benutzer-IDs und lokale Kennwörter für das Gerät
- Terminal Access Controller Access Control System (TACACS)

TACACS ist ein standardmäßiges Sicherheitsprotokoll der Internet Engineering Task Force (RFC 1492), das zwischen Client-Geräten in einem Netzwerk und mit einem TACACS-Server ausgeführt wird. TACACS ist ein Authentifizierungsmechanismus, mit dem die Identität eines Geräts authentifiziert wird, das Remotezugriff auf eine privilegierte Datenbank benötigt. Zu den Varianten von TACACS gehören TACACS+, die AAA-Architektur, die Authentifizierungs-, Autorisierungs- und Accounting-Funktionen trennt.

TACACS+ wird von Cisco verwendet, um eine genauere Kontrolle darüber zu ermöglichen, wer im nicht privilegierten und privilegierten Modus auf das Cisco Gerät zugreifen kann. Für Fehlertoleranz können mehrere TACACS+-Server konfiguriert werden. Wenn TACACS+ aktiviert ist, fordert der Router und Switch den Benutzer zur Eingabe eines Benutzernamens und eines Kennworts auf. Die Authentifizierung kann für die Anmeldesteuerung oder die Authentifizierung einzelner Befehle konfiguriert werden.

Authentifizierung

Bei der Authentifizierung werden Benutzer identifiziert, z. B. Anmelde- und Kennwortdialog, Challenge- und Antwortfunktionen sowie Messaging-Unterstützung. Die Authentifizierung ist die Art und Weise, wie ein Benutzer identifiziert wird, bevor ihm der Zugriff auf den Router oder Switch gewährt wird. Zwischen Authentifizierung und Autorisierung besteht ein grundlegender Zusammenhang. Je mehr Autorisierungsberechtigungen ein Benutzer erhält, desto sicherer sollte die Authentifizierung sein.

Autorisierung

Die Autorisierung ermöglicht eine Remote-Zugriffskontrolle, einschließlich einmaliger Autorisierung und Autorisierung für jeden vom Benutzer angeforderten Service. Auf einem Cisco Router liegt die Autorisierungsebene für Benutzer zwischen 0 und 15, wobei 0 die niedrigste und 15 die höchste Ebene ist.

Buchhaltung

Die Abrechnung ermöglicht das Sammeln und Senden von Sicherheitsinformationen, die für die Abrechnung, Überprüfung und Berichterstellung verwendet werden, z. B. Benutzeridentitäten, Start- und Stoppzeiten sowie ausgeführte Befehle. Die Buchhaltung ermöglicht es Netzwerkmanagern, die Services, auf die Benutzer zugreifen, sowie die Menge der Netzwerkressourcen zu verfolgen, die sie benötigen.

In der folgenden Tabelle sind die grundlegenden Beispielbefehle für die Verwendung von TACACS+, Authentifizierung, Autorisierung und Abrechnung auf einem Cisco Router und einem Catalyst Switch aufgeführt. Ausführlichere Befehle finden Sie im Dokument Befehle für Authentifizierung, Autorisierung und Abrechnung.

Cisco IOS-Befehl	Zweck
Router	
aaa neues Modell	Aktivieren Sie Authentication, Authorization, Accounting (AAA) als primäre Zugriffskontrollmethode.
AAA Accounting {*System* | *Netzwerk* | *Verbindung* | *exec* | *Befehlsebene*} {*start-stop* | *Wartebeginn* | *stop-only*} {*tacacs+* | *Radius*}	Aktivieren Sie die Abrechnung mit den globalen Konfigurationsbefehlen.
Standardtakacs für die AAA-Authentifizierung+	Richten Sie den Router so ein, dass Verbindungen zu allen Terminalleitungen, die mit dem Anmeldungsstandard konfiguriert sind, mit TACACS+ authentifiziert werden und fehlschlagen, wenn die Authentifizierung aus irgendeinem Grund fehlschlägt.
AAA-Autorisierung exec Standard-Takacs+ keine	Richten Sie den Router ein, um zu überprüfen, ob der Benutzer eine EXEC-Shell ausführen darf, indem Sie den TACACS+-Server fragen.
tacacs-server host *tacacs+ server ip address*	Geben Sie den TACACS+-Server an, der für die Authentifizierung mit den globalen Konfigurationsbefehlen verwendet wird.

tacacs-server key ***shared-secret***	Geben Sie den gemeinsamen geheimen Schlüssel an, der von den TACACS+-Servern und dem Cisco-Router mit dem globalen Konfigurationsbefehl bekannt ist.
Catalyst-Switch	
Authentifizierungs-Anmeldetaktiken aktivieren [*alle* **/** ***Konsole*** **/** ***http*** **/** ***telnet***] [***primary***]	Aktivieren Sie die TACACS+-Authentifizierung für den normalen Anmeldemodus. Verwenden Sie die Konsolen- oder Telnet-Schlüsselwörter, um TACACS+ nur für Konsolenport- oder Telnet-Verbindungsversuche zu aktivieren.
set authorized exec enable {***option***} ***fallback option***} [***console*** **/** ***Telnet*** **/** ***beide***]	Aktivieren Sie die Autorisierung für den normalen Anmeldemodus. Verwenden Sie die Konsolen- oder Telnet-Schlüsselwörter, um die Autorisierung nur für Konsolenport- oder Telnet-Verbindungsversuche zu aktivieren.
Festlegen des ***gemeinsam genutzten geheimen*** **"tacacs-server-***Schlüssels***"**	Geben Sie den gemeinsamen geheimen Schlüssel an, der von den TACACS+-Servern und dem Switch bekannt ist.
Festlegen der ***IP-Adresse*** **des TACACS-Server-Hosts** ***+ des Servers***	Geben Sie den TACACS+-Server an, der für die Authentifizierung mit den globalen Konfigurationsbefehlen verwendet wird.
Festlegen von Accounting-Befehlen aktivieren {*config*** /** ***all***} {***stop-only***} ***takacs+***	Aktivieren der Abrechnung von Konfigurationsbefehlen

Weitere Informationen zur Konfiguration von AAA zur Überwachung und Steuerung des Zugriffs auf die Befehlszeilenschnittstelle der Catalyst Enterprise LAN-Switches finden Sie im Dokument Controller Access to the Switch Using Authentication, Authorization, and Accounting (Steuerung des Zugriffs auf den Switch über Authentifizierung, Autorisierung und Abrechnung).

SNMP-Sicherheit

Das SNMP-Protokoll kann verwendet werden, um Konfigurationsänderungen auf Routern und Catalyst-Switches vorzunehmen, die denen der CLI ähneln. Auf Netzwerkgeräten sollten angemessene Sicherheitsmaßnahmen konfiguriert werden, um nicht autorisierten Zugriff und Änderungen über SNMP zu verhindern. Community-Strings sollten die Standard-Passwortrichtlinien für Länge, Zeichen und Ratenschwierigkeiten befolgen. Es ist wichtig, die Community-Strings von ihren öffentlichen und privaten Standardeinstellungen zu ändern.

Alle SNMP-Management-Host(s) sollten über eine statische IP-Adresse verfügen und explizit SNMP-Kommunikationsrechte für das Netzwerkgerät erhalten, indem die vordefinierte IP-Adresse und Zugriffskontrollliste (ACL) verwendet wird. Die Cisco IOS- und Cisco Catalyst-Software bietet Sicherheitsfunktionen, die sicherstellen, dass nur autorisierte Management-Stationen Änderungen an Netzwerkgeräten vornehmen dürfen.

Router-Sicherheitsfunktionen

SNMP-Berechtigungsebene

Diese Funktion schränkt die Arten von Vorgängen ein, die eine Managementstation auf einem Router ausführen kann. Auf Routern gibt es zwei Arten von Berechtigungen: Schreibgeschützt (Read-Only, RO) und Schreibzugriff (Read-Write, RW). Auf der RO-Ebene kann eine Managementstation nur die Routerdaten abfragen. Konfigurationsbefehle wie der Neustart eines Routers und das Herunterfahren von Schnittstellen sind nicht zulässig. Nur die RW-Berechtigungsebene kann für solche Vorgänge verwendet werden.

SNMP-Zugriffskontrollliste (ACL)

Die SNMP-ACL-Funktion kann in Verbindung mit der SNMP-Berechtigungsfunktion verwendet werden, um zu verhindern, dass bestimmte Verwaltungsstationen Managementinformationen von Routern anfordern.

SNMP-Ansicht

Diese Funktion schränkt bestimmte Informationen ein, die von Routern von Managementkonsolen abgerufen werden können. Sie kann mit der SNMP-Berechtigungsebene und den ACL-Funktionen verwendet werden, um den eingeschränkten Zugriff auf Daten über Managementkonsolen zu erzwingen. Konfigurationsbeispiele für die SNMP-Ansicht finden Sie in der SNMP-Server-Ansicht.

SNMP-Version 3

SNMP Version 3 (SNMPv3) ermöglicht den sicheren Austausch von Managementdaten zwischen Netzwerkgeräten und Managementstationen. Die Verschlüsselungs- und Authentifizierungsfunktionen in SNMPv3 gewährleisten eine hohe Sicherheit beim Transport von Paketen zu einer Managementkonsole. SNMPv3 wird von der Cisco IOS-Softwareversion 12.0(3)T und höher unterstützt. Eine technische Übersicht über SNMPv3 finden Sie in der SNMPv3-Dokumentation.

Zugriffskontrollliste (ACL) auf Schnittstellen

Die ACL-Funktion bietet Sicherheitsmaßnahmen, um Angriffe wie IP-Spoofing zu verhindern. Die ACL kann auf ein- und ausgehende Schnittstellen der Router angewendet werden.

Catalyst LAN Switch-Sicherheitsfunktion

IP-Berechtigungsliste

Die Funktion "IP Permit List" (IP-Berechtigungsliste) schränkt den eingehenden Telnet- und SNMP-Zugriff auf den Switch von nicht autorisierten Quell-IP-Adressen ein. Syslog-Meldungen und SNMP-Traps werden unterstützt, um ein Managementsystem zu benachrichtigen, wenn eine Verletzung oder ein nicht autorisierter Zugriff auftritt.

Eine Kombination der Cisco IOS-Sicherheitsfunktionen kann zur Verwaltung von Routern und Catalyst-Switches verwendet werden. Es muss eine Sicherheitsrichtlinie festgelegt werden, die die Anzahl der Verwaltungsstationen, die auf die Switches und Router zugreifen können, begrenzt.

Weitere Informationen zur Erhöhung der Sicherheit in IP-Netzwerken finden Sie unter Erhöhte Sicherheit in IP-Netzwerken.

Accounting-Management

Das Accounting-Management ist der Prozess zur Messung von Netzwerknutzungsparametern, sodass einzelne oder Gruppenbenutzer im Netzwerk für die Zwecke der Abrechnung oder der Abrechnung entsprechend reguliert werden können. Ähnlich wie beim Performance-Management besteht der erste Schritt hin zu einem angemessenen Accounting-Management darin, die Auslastung aller wichtigen Netzwerkressourcen zu messen. Die Auslastung von Netzwerkressourcen kann mithilfe der Cisco NetFlow- und Cisco IP Accounting-Funktionen gemessen werden. Die Analyse der mithilfe dieser Methoden gesammelten Daten bietet Einblicke in aktuelle Nutzungsmuster.

Ein nutzungsbasiertes Abrechnungs- und Abrechnungssystem ist ein wesentlicher Bestandteil jeder Service Level Agreement (SLA). Sie bietet sowohl eine praktische Methode zur Definition von Verpflichtungen im Rahmen eines SLA als auch klare Konsequenzen für Verhalten außerhalb der SLA-Bedingungen.

Die Daten können über Sonden oder Cisco NetFlow gesammelt werden. Cisco stellt NetFlow Collector und NetFlow Analyzer-Anwendungen zum Erfassen und Analysieren von Daten von Routern und Catalyst Switches bereit. Shareware-Anwendungen wie cflow werden auch zum Erfassen von NetFlow-Daten verwendet. Eine laufende Messung der Ressourcennutzung kann zu Abrechnungsinformationen führen und die kontinuierliche, faire und optimale Nutzung von Ressourcen einschätzen. Zu den gängigen Lösungen für das Accounting-Management gehören:

- Evident-Software

NetFlow-Aktivierungs- und Datenerfassungsstrategie

NetFlow (Network Flow) ist eine Technologie zur Messung von Eingangsschnittstellen, mit der die für Netzwerkplanungs-, Überwachungs- und Abrechnungsanwendungen erforderlichen Daten erfasst werden können. NetFlow sollte an Edge-/Aggregation-Router-Schnittstellen für Service Provider oder WAN Access Router-Schnittstellen für Enterprise-Kunden bereitgestellt werden.

Cisco Systems empfiehlt eine sorgfältig geplante NetFlow-Bereitstellung mit aktivierten NetFlow-Services auf diesen strategisch positionierten Routern. NetFlow kann schrittweise (Schnittstelle für Schnittstelle) und strategisch (auf gut ausgewählten Routern) bereitgestellt werden, anstatt NetFlow auf jedem Router im Netzwerk bereitzustellen. Die Mitarbeiter von Cisco arbeiten mit Kunden zusammen, um zu ermitteln, auf welchen wichtigen Routern und Schnittstellen NetFlow basierend auf den Datenverkehrsfluss-Mustern, der Netzwerktopologie und der Architektur des Kunden aktiviert werden soll.

Wichtige Überlegungen bei der Bereitstellung:

- NetFlow-Services sollten als Edge-Messungs- und Zugriffslistenleistungs-Beschleunigungstool verwendet werden und nicht auf *Hot*-Core/Backbone-Routern oder -

Routern aktiviert werden, die mit sehr hohen CPU-Nutzungsraten ausgeführt werden.
- Analyse der anwendungsgesteuerten Datenerhebungsanforderungen Buchhaltungsanwendungen erfordern unter Umständen nur die Flow-Informationen des Ursprungs- und Terminierungsrouters, während Überwachungsanwendungen eine umfassendere (datenintensive) End-to-End-Ansicht erfordern.
- Analyse der Auswirkungen von Netzwerktopologie und Routing-Richtlinien auf die Flow Collection-Strategie Vermeiden Sie beispielsweise das Sammeln doppelter Datenflüsse, indem Sie NetFlow auf zentralen Aggregationsroutern aktivieren, von denen der Datenverkehr ausgeht oder endet, und nicht auf Backbone-Routern oder zwischengeschalteten Routern, die doppelte Ansichten derselben Flow-Informationen bereitstellen.
- Service Provider im Geschäft der *Transit Carrier* (die Datenverkehr, der nicht aus ihrem Netzwerk stammt oder dort endet, befördern) können NetFlow Export-Daten zur Messung der Nutzung von Netzwerkressourcen für die Abrechnung und Abrechnung verwenden.

Konfigurieren der IP-Buchhaltung

Die Cisco IP Accounting-Unterstützung bietet grundlegende IP Accounting-Funktionen. Durch die Aktivierung der IP-Abrechnung können Benutzer die Anzahl der über die Cisco IOS-Software geswitchten Byte und Pakete auf der Basis der Quell- und Ziel-IP-Adresse sehen. Nur der IP-Datenverkehr der Transit wird gemessen und nur auf Basis des ausgehenden Datenverkehrs. Der von der Software generierte oder in der Software terminierende Datenverkehr ist nicht in der Buchführungsstatistik enthalten. Um eine genaue Bilanzierung zu gewährleisten, unterhält die Software zwei Buchhaltungsdatenbanken: eine aktive und eine überprüfte Datenbank.

Die Cisco IP Accounting-Unterstützung stellt außerdem Informationen zur Identifizierung von IP-Datenverkehr bereit, der in IP-Zugriffslisten fehlschlägt. Die Identifizierung von IP-Quelladressen, die gegen IP-Zugriffslisten verstoßen, signalisiert mögliche Versuche, die Sicherheit zu verletzen. Die Daten weisen auch darauf hin, dass die Konfigurationen der IP-Zugriffslisten überprüft werden sollten. Um diese Funktion Benutzern zur Verfügung zu stellen, aktivieren Sie die IP-Abrechnung für Verstöße gegen die Zugriffslisten mithilfe des Befehls **ip accounting access-verletzungen**. Benutzer können dann die Anzahl der Byte und Pakete aus einer einzigen Quelle anzeigen, die versucht haben, die Sicherheit gegen die Zugriffsliste für das Quell-Zielpaar zu verletzen. Standardmäßig zeigt IP Accounting die Anzahl der Pakete an, die Zugriffslisten bestanden und geroutet wurden.

Um die IP-Abrechnung zu aktivieren, verwenden Sie für jede Schnittstelle im Schnittstellenkonfigurationsmodus einen der folgenden Befehle:

Command	Zweck
ip accounting	Aktivieren Sie die grundlegende IP-Abrechnung.
Verstöße gegen die IP Accounting-Zugriffsrechte	Aktivieren Sie IP Accounting mit der Möglichkeit, IP-Datenverkehr zu identifizieren, der in IP-Zugriffslisten fehlschlägt.

Um andere IP-Accounting-Funktionen zu konfigurieren, verwenden Sie einen oder mehrere der folgenden Befehle im globalen Konfigurationsmodus:

Command	Zweck

ip accounting-Grenzwert (*Grenzwert* für Abrechnung)	Legen Sie die maximale Anzahl der zu erstellenden Buchhaltungseinträge fest.
ip accounting-list *ip-address wildcard*	Filtern von Accounting-Informationen für Hosts.
ip accounting-transits *count*	Steuern Sie die Anzahl der Transitdatensätze, die in der IP-Buchhaltungsdatenbank gespeichert werden.

Informationen zu den in diesem Dokument verwendeten Konventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).