Система управления сетью: Рекомендации и Описание технологических решений

ID документа: 15114

Обновлено : 11 июля 2007

 Загрузка PDF

 Печать

Обратная связь

Родственные продукты

- Service Assurance Agent (SAA)
- CiscoWorks Resource Manager Essentials
- Режим высокой доступности
- Упрощенный протокол управления сетью (SNMP)
- Remote Monitoring (RMON)

Содержание

Введение

Модель управления сетью, разработанная Международной организацией по стандартизации (ISO), определяет пять функциональных областей управления сетью. В этом документе описываются все области применения. Основная цель этого документа – дать практические рекомендации по каждой из функциональных областей с целью повышения общей эффективности используемых инструментов и техник управления. Здесь также приводятся указания по проектированию для будущей реализации средств и технологий управления сетью.

Управление сетью

Модель ISO управления сетью включает в себя следующие пять функциональных областей.

- Управление обработкой отказов – обнаружение и локализация возникших в сети неисправностей, оповещение о них и их исправление.
- Управление конфигурацией – аспекты конфигурации сетевых устройств, такие как управление файлами конфигурации, перечнем устройств и программным обеспечением.
- Управление производительностью – мониторинг и измерение различных аспектов производительности, благодаря которым общая производительность сохраняется на приемлемом уровне.
- Управление безопасностью – предоставление доступа к сетевым устройствам и корпоративным ресурсам уполномоченным сотрудникам.
- Управление учетом сетевых ресурсов, которое дает информацию относительно их загруженности.

Следующая диаграмма демонстрирует эталонную архитектуру, которая, по мнению специалистов Cisco Systems, должна быть минимальным решением для управления сетью передачи данных. Эта архитектура включает сервер Cisco CallManager для тех, кто планирует управлять голосовой связью через Интернет-протокол (VoIP): Диаграмма показывает, как можно интегрировать сервер CallManager в топологию NMS.

Архитектура управления сетью включает такие элементы:

- Платформа протокола простого управления сетью (SNMP) для управления отказами
- Платформа мониторинга производительности для управления и анализа производительности с учетом перспективы
- Сервер CiscoWorks2000 для управления конфигурацией, сбора сведений системного журнала и управления имеющимся оборудованием и ПО

Некоторые платформы SNMP непосредственно разделяют данные с сервером CiscoWorks2000, используя методы общей информационной модели (CIM, Common Information Model) и расширяемого языка разметки (XML, eXtensible Markup Language). CIM — это распространенная модель данных схемы, не зависящей от реализации, для описания

суммарной административной информации в окружении сети или предприятия. CIM включает в себя спецификацию и схему. Спецификация определяет подробные сведения для интеграции с другими моделями управления, такими как SNMP MIB (Management Information Base, база управляющей информации) или файлы управляющей информации для рабочей группы по управлению настольными системами (Desktop Management Task Force Management Information Files, DMTF MIFs), в то время как схема предлагает описания действующей модели.

XML – это язык разметки, используемый для представления структурированных данных в текстовом виде. Конкретной целью XML было сохранить описательные возможности SGML, но в то же время максимально их упростить. Концепция XML аналогична HTML, но в то время как HTML используется для передачи графической информации о документе, XML используется для представления структурированных данных в документе.

К пользователям улучшенных услуг Cisco также относятся серверы Cisco NATkit для дополнительного инициативного управления и устранения неисправностей. К данным, находящимся на сервере CiscoWorks2000, у сервера NATkit будет доступ либо посредством монтирования удаленного диска (rmount), либо через протокол передачи файлов (FTP).

В главе Основы управления сетью в Обзоре сетевых технологий дается более подробный обзор основ управления сетью.

Управление обработкой отказов

Целью управления обработкой отказов является обнаружение и регистрация возникающих в сети неисправностей, уведомление о них пользователей и (в пределах возможного) автоматическое их устранение для дальнейшей эффективной работы сети. Поскольку отказы могут привести к простою или нежелательному снижению производительности сети, управление обработкой отказов является, возможно, наиболее часто реализуемым элементом сетевого управления ISO.

Платформы сетевого управления

Платформа управления сетью, развернутая на предприятии, управляет инфраструктурой, которая состоит из элементов элементов сетевого оборудования от разных поставщиков. Платформа получает и обрабатывает события от сетевых элементов в сети. События сервера и других важных ресурсов могут также пересылаться на управляющую платформу. В стандартную управляющую платформу включены следующие общедоступные функции:

- Обнаружение сети
- Сопоставление топологии элементов сети
- Обработчик событий
- Средство сбора данных и составления схем по производительности
- Обозреватель данных управления

Платформы управления сетью можно рассматривать как основную консоль для сетевых операций по обнаружению сбоев в инфраструктуре. Возможность быстро обнаруживать ошибки в сети является критически важной. Персонал по работе с сетями может отображать рабочие состояния критических сетевых элементов, например, маршрутизаторов и коммутаторов, на основе графической схемы сети.

Платформы управления сетью, такие как HP OpenView, Computer Associates Unicenter и

SUN Solstice, могут обнаруживать сетевые устройства. Каждое сетевое устройство представлено графическим элементом в консоли платформы управления. Разные цвета графических элементов указывают на текущий статус сетевых устройств. Сетевые устройства можно настраивать для отправки уведомлений, называемых прерываниями SNMP, на платформы управления сетью. При получении уведомлений графический элемент, отражающий сетевое устройство, меняет цвет в зависимости от важности полученного уведомления. Уведомление, обычно называемое событием, записывается в файле журнала. Особенно важно, что большинство текущих файлов баз управляющей информации (MIB) загружаются на платформу SNMP для проверки, что различные сигналы тревоги от устройств Cisco интерпретируются корректно.

Cisco публикует файлы MIB для управления различными сетевыми устройствами. Файлы Cisco MIB находятся на веб-сайте cisco.com и содержат следующую информацию:

- Файлы MIB, публикуемые в формате SNMPv1
- Публикация файлов MIB выполняется в формате SNMPv2
- Поддерживаемые прерывания SNMP на устройствах Cisco
- OID текущих объектов MIB SNMP для Cisco

Ряд платформ сетевого управления способны управлять множеством географически удаленных узлов. Это осуществляется путем обмена управляющими данными между консолями управления на удаленных сайтах и управляющей станцией на главном сайте. Главное преимущество распределенной архитектуры состоит в том, что она уменьшает управляющий трафик, таким образом предоставляя более эффективное использование полосы пропускания. Применение распределенной архитектуры обеспечивает сотрудникам возможность локального управления сетями с узлов удаленных систем.

Последнее усовершенствование управляющих платформ – это возможность удаленного управления сетевыми элементами через веб-интерфейс. Это усовершенствование устраняет потребность в специальном клиентском программном обеспечении на отдельных пользовательских рабочих станциях для получения доступа к управляющей платформе.

В типичном предприятии представлены различные элементы сети. Однако для каждого устройства в зависимости от поставщика требуется своя система управления сетевыми элементами. Поэтому дублированные управляющие станции могут последовательно запрашивать у сетевых элементов одни и те же данные. Данные, собранные различными системами, хранятся в отдельных базах данных, что создает дополнительную административную нагрузку для пользователей. Данное ограничение подсказало производителям сетей и программного обеспечения принять стандарты, такие как CORBA и CIM, чтобы облегчить обмен управляющими данными между платформами управления и системами управления элементами. Благодаря утвержденным производителями стандартам в управлении разработкой систем пользователи могут рассчитывать на взаимную совместимость и экономию средств при развертывании и управлении инфраструктурой.

CORBA задает систему, которая предоставляет совместимость между объектами в неоднородном, распределенной среде и способом, который очевиден для программиста. Этот стандарт базируется на объектной модели группы по управлению объектами (Object Management Group, OMG).

Устранение неполадок инфраструктуры

Серверы, работающие по протоколу TFTP (Простейший протокол передачи данных), и

серверы системных журналов (syslog) являются ключевыми компонентами инфраструктуры для устранения неполадок в сетевых операциях. Сервер TFTP используется преимущественно для хранения файлов конфигурации и образов программного обеспечения для сетевых устройств. Маршрутизаторы и коммутаторы поддерживают отправку сообщений системного журнала на syslog-сервер. Сообщения помогают в устранении ошибок в случае неопознанной ошибки. Иногда сообщения системного журнала требуются специалистам технической поддержки компании Cisco для поиска основных причин неполадок.

Распределенная функция сбора данных системного журнала "Основы управления ресурсами CiscoWorks2000" позволяет развертывать несколько станций UNIX или NT для сбора и фильтрации сообщений на удаленных сайтах. Фильтры могут указать, какие сообщения системного журнала будут отправлены на главный сервер Essentials. Главным преимуществом реализации распределенного сбора является уменьшение количества сообщений, пересылаемых на главные серверы syslog.

Обнаружение сбоев и уведомление о них

Задача управления обработкой отказов – обнаружить, изолировать отказы, сообщить о них и устранить неполадки, обнаруженные в сети. Сетевые устройства могут оповещать управляющие станции, когда в системах возникает ошибка. Эффективная система управления обработкой отказов состоит из нескольких подсистем. Обнаружение сбоев выполняется, когда устройства отправляют сообщения с прерываниями SNMP, последовательный опрос SNMP, пороговые значения для удаленного мониторинга (RMON) и сообщения системного журнала. Управляющая система оповещает конечного пользователя о произошедшем сбое, благодаря чему могут быть предприняты корректирующие действия.

Прерывания должны быть последовательно включены на сетевых устройствах. Дополнительные прерывания поддерживаются новыми Cisco IOS software releases для маршрутизаторов и коммутаторов. Важно проверять и обновлять файл конфигурации, чтобы обеспечить правильное декодирование прерываний. Периодический обзор настроенных ловушек группой Cisco Assured Network Services (ANS) гарантирует эффективное обнаружение неисправностей в сети.

В следующей таблице приводятся прерывания CISCO-STACK-MIB, которые поддерживаются и могут использоваться для мониторинга неисправных состояний на коммутаторах Cisco Catalyst для локальных сетей (LAN).

Trap-сообщение	**Описание**
moduleUp	**Объект агента обнаружил, что объект moduleStatus в данной базе MIB перешел в состояние ok(2) из-за одного из своих модулей.**
moduleDown	*Объект агента обнаружил, что объект moduleStatus в данной базе MIB вышел из состояния ok(2) из-за одного из своих модулей.*
chassisAlarmO	*Объект агента обнаружил, что объект chassisTempAlarm, chassisMinorAlarm или*

n	*chassisMajorAlarm в этой базе MIB перешел в состояние on(2). Прерывание chassisMajorAlarm обозначает наличие одного из следующих состояний:* • Любой сбой напряжения • Одновременная неисправность вентилятора и повышение температуры • Стопроцентный отказ источников питания (оба из имеющихся двух, или один при имеющемся одном) • Сбой электрически стираемого программируемого постоянного запоминающего устройства (EEPROM) • Сбой энергонезависимой оперативной памяти (NVRAM) • Сбой связи MCP • Неизвестное состояние NMP ChassisMinorAlarm обозначает наличие одного из следующих условий: • Аварийный сигнал перегрева • Отказ вентилятора • Частичный отказ в системе питания (одна из двух) • Несовместимость двух блоков питания
chassisAlarmOff	*Объект агента обнаружил, что объект chassisTempAlarm, chassisMinorAlarm или chassisMajorAlarm в этой базе MIB перешел в состояние off(1).*

Прерывания системы мониторинга состояния среды (envmon) определены в прерывании CISCO-ENVMON-MIB. Ловушка envmon осуществляет передачу уведомлений монитора для окружения Cisco в случае превышения всех пороговых значений для среды. При использовании системы мониторинга можно включить конкретный тип прерывания среды либо принять все типы прерываний этой системы. Если не выбран ни один параметр, то включаются все типы среды. Возможны одно или несколько таких значений:

- напряжение. Уведомление ciscoEnvMonVoltageNotification отсылается в том случае, когда напряжение, измеренное в контрольной точке, выходит за пределы нормального диапазона (например, на угрожающей, критической стадии или стадии аварийного отключения).
- отключение ciscoEnvMonShutdownNotification передается, если система контроля состояния окружающей среды обнаруживает, что контрольная точка достигает критического состояния и собирается инициировать завершение.
- питание. Уведомление ciscoEnvMonRedundantSupplyNotification отсылается в том случае, если резервный блок питания (если имеется) вышел из строя.
- вентилятор. Уведомление ciscoEnvMonFanNotification отсылается при выходе из строя какого-либо из вентиляторов в блоке вентиляторов (если имеется).
- температура. Уведомление ciscoEnvMonTemperatureNotification отсылается в том случае, когда температура, измеренная в данной контрольной точке, выходит за

пределы нормального диапазона (например, на угрожающей, критической стадии или стадии аварийного отключения).

Неисправное обнаружение и мониторинг сетевых элементов может расшириться с уровня устройств до уровня протоколов и интерфейсов. Для сетевой среды, контроль отказов может включать виртуальную локальную сеть (VLAN), Технологию ATM, индикацию отказов на физических интерфейсах и т.д. Внедрение управления сбоями на уровне протокола возможно с помощью системы управления элементами, такой как CiscoWorks2000 Campus Manager. Приложение TrafficDirector (управление трафиком) для системы Campus Manager в первую очередь предназначено для управления коммутацией с использованием поддержки mini-RMON на коммутаторах Catalyst.

При возрастающем количестве сетевых элементов и сложности сетевых проблем можно подумать о системе управления событиями, способной связывать между собой различные сетевые события (файлы syslog, прерываний, журнала). Данная архитектура, которая служит основой для системы управления событиями, сравнима с системой Manager of Managers (MOM). Хорошо спроектированная система управления событиями позволяет специалистам центра управления сетью (NOC) заблаговременно и эффективно обнаруживать и диагностировать возникающие в сети неполадки. Назначение приоритета событиям и их блокировка позволяют специалистам по сетевым технологиям сосредоточиться на критических событиях сети, изучить несколько систем управления событиями, в том числе Cisco Info Center (Информационный центр Cisco), и провести анализ технической применимости для полного исследования возможностей таких систем. Дополнительные сведения см. в разделе Cisco Info Center (информационный центр).

Профилактический мониторинг и уведомление о сбоях

Сигнал и событие RMON являются двумя группами, определенными в спецификации RMON. Обычно управляющая станция производит опрос устройств сети, чтобы определить состояние или значение некоторых переменных. Например, управляющая станция опрашивает маршрутизаторы на поиск использования центрального процессора и создание события, когда значение достигает конфигурированной пороговой величины. Этот метод растрачивает полосу пропускания сети и также может пропустить фактическое пороговое значение, зависящее от интервала опроса.

С оповещением и событиями RMON устройство сети настраивается для собственного контроля верхних и нижних порогов. За предопределенный интервал времени сетевое устройство делает замер переменной и сравнивает ее значение с пороговыми уровнями. Прерывание SNMP можно отправить на управляющую станцию, если фактическое значение превышает или опускается ниже установленных пороговых уровней. Группы аварийных сигналов и событий RMON дают профилактический метод управления критическими сетевыми устройствами.

Компания Cisco Systems рекомендует использовать систему аварийных сигналов и событий RMON на критических сетевых устройствах. Контролируемые переменные могут включать коэффициент загруженности CPU, количество ошибок буфера, показатель потерь входящих и выходящих данных и другие целочисленные переменные. Начиная с версии системы Cisco IOS 11.1(1), все образы ПО для маршрутизаторов поддерживают группы аварийных сигналов и событий RMON.

Дополнительные сведения о внедрении системы аварийных сигналов и событий RMON см. в разделе Реализация системы аварийных сигналов и событий RMON.

Ограничения памяти RMON

Использование памяти RMON, связанное со статистикой, хронологией, аварийной сигнализацией, и событиями, одинаково для всех платформ коммутаторов. *Для хранения хронологических и статистических данных в агенте RMON (в данном случае он является коммутатором) используется особый участок памяти – так называемый сегмент.* Размер "ведра" задается на RMON probe (устройство SwitchProbe) или приложении RMON (служебная программа TrafficDirector), а затем отправляется на коммутатор для установки.

Требуется приблизительно 450 Кб кодового пространства для поддержки системы mini-RMON (например четыре группы MON: статистика, хронология операций, аварийные сигналы и события). Требование к динамической памяти для RMON колеблется, так зависит от конфигурации в процессе выполнения.

В следующей таблице определены данные времени прогона памяти удаленного мониторинга для каждой мини группы RMON.

Определение группы RMON	Используемый размер динамического ОЗУ	Примечания
Statistics	140 байт на коммутируемый порт Ethernet/Fast Ethernet	На каждый порт
History	3,6 Кб для 50 сегментов *	Каждая дополнительная ячейка использует 56 байт
Аварийные сигналы и события	2,6 Кб на аварийный сигнал и записи о соответствующих ему событиях	На аварийный сигнал и на порт

**Для хранения хронологических и статистических данных об операциях в агенте RMON (например коммутаторе) используется особый участок памяти – так называемый сегмент.*

Реализация аварийных сигналов и событий RMON

Используя систему RMON как часть решения по управлению обработкой отказов, пользователь может вести профилактический мониторинг сети до возникновения потенциальной проблемы. Например, если число полученных широковещательных пакетов увеличится значительно, это может привести к увеличению загруженности центрального процессора. Путем реализации сигнала тревоги и события RMON пользователь может установить предел для отслеживания числа полученных транслируемых пакетов и оповестить платформу SNMP средствами прерываний SNMP при достижении установленного предела. Сигналы тревоги и события RMON позволяют предотвратить избыточный опрос, обычно выполняемый платформой SNMP для выполнения той же задачи.

Существует два метода настройки системы аварийных сигналов и событий RMON:

- Интерфейс командной строки (CLI)
- Операция SNMP SET

В следующих примерах процедур показано, как установить порог для отслеживания количества широковещательных пакетов, получаемых на интерфейсе. В этих процедурах используется тот же счетчик, который показан в примере команды show interface в конце этого раздела.

Пример интерфейса командной строки

Чтобы реализовать сигнал тревоги и событие RMON с помощью интерфейса CLI, выполните следующие действия:

1. Найдите индекс интерфейса, связанного с портом Ethernet 0, путем прохода базы MIB под названием ifTable.
```
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. Получите OID, связанный с полем CLI, которое следует отследить. Например, OID для 'broadcasts' - 1.3.6.1.2.1.2.2.1.12. Идентификаторы (OID) Cisco для отдельных переменных MIB доступны на веб-сайте cisco.com.
3. Определите следующие параметры для установки пороговых уровней и событий.значения верхнего и нижнего пороговтип дискретизации (абсолютная или дельта)интервал выборкидействие при достижении порогового уровняВ данном примере устанавливается порог для отслеживания количества широковещательных пакетов, полученных на порте Ethernet 0. Прерывание будет генерироваться, если количество полученных широковещательных пакетов между 60-секундными замерами больше 500. Порог будет повторно активирован после того, как число широковещательных пакетов входа перестанет возрастать от образца к образцу.**Примечание:** Для получения подробных данных о параметрах команды проверьте документацию оперативного режима соединений Cisco (CCO) на наличие сигналов удаленного мониторинга RMON и команд event для вашей конкретной версии Cisco IOS.
4. Укажите прерывание (событие RMON), которое отсылается при достижении порогового уровня, используя следующие команды CLI (команды Cisco IOS выделены жирным шрифтом):**rmon event 1 trap gateway description "High Broadcast on Ethernet 0" owner ciscormon event 2 log description "normal broadcast received on ethernet 0" owner cisco**
5. Задайте пороги и соответствующие параметры (сигнал RMON) с помощью следующих команд CLI:**rmon alarm 1 ifEntry.12.1 60 delta rising-threshold 500 1falling-threshold 0 2 owner cisco**
6. С помощью SNMP опросите эти таблицы и убедитесь в том, что на устройстве были созданы записи в таблице eventTable.
```
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. Чтобы убедиться, что записи в таблице alarmTable были заданы, последовательно опросите следующие таблицы.`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)
```

Пример SNMP SET

Чтобы реализовать систему аварийных сигналов и событий RMON с помощью операции SNMP SET, выполните следующие действия:

1. Установите прерывание (событие RMON), отсылаемое при достижении порогового уровня, с помощью следующих операций SNMP SET:`# 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. Задайте пороговые значения и соответствующие параметры (аварийный сигнал RMON) с помощью следующих операций SNMP SET:`# 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. Последовательно опросите эти таблицы и убедитесь, что на данном устройстве были сделаны записи в таблице eventTable.`% 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. Чтобы убедиться, что записи в таблице alarmTable были заданы, последовательно проверьте эти таблицы.`% snmpwalk -v 1 172.16.97.132 private .1.3.6.1.2.1.16.3.1`

show interface

В этом примере приведены выходные данные команды show interface.

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
```

Управление конфигурацией

Целью управления конфигурацией является мониторинг сетей и данных конфигурации системы с тем, чтобы отслеживать и управлять негативными последствиями различных версий аппаратных и программных элементов на работу сети.

Стандарты конфигурации

При возрастающем количестве внедряемых сетевых устройств критически важным является определение местоположения сетевого устройства. Эти сведения о размещении должны предоставлять подробное содержательное описание для ресурсов, отвечающих за диспетчеризацию в случае возникновения проблем в сети. Для ускорения разрешения проблемы сети проверьте наличие контактной информации лица или отдела, ответственного за устройства. Контактная информация должна включать телефонный номер и имя человека или название отдела.

Соглашения об именовании сетевых устройств, начиная с имени устройства и заканчивая отдельным интерфейсом, должны быть спланированы и реализованы как часть стандарта конфигурации. Хорошо определенное соглашение об именовании дает специалистам возможность получать точную информацию при устранении неполадок в сети. Соглашение об именовании устройств может использовать географическое положение, название здания, этаж и т. д. Для соглашения по присвоению имен интерфейсам может использоваться сегмент, к которому подключен порт, имя концентратора подключения и так далее. На последовательных интерфейсах в него следует включить фактическую пропускную способность, число идентификаторов локальных каналов передачи данных (DLCI) (если Frame Relay), место назначения и идентификатор линии связи или сведения,

предоставленные оператором связи.

Управление файлом конфигурации

При добавлении новых команд конфигурации по существующим запросам сетевых устройств необходимо проверить команду на достоверность перед фактической реализацией. Неправильная настройка сетевого устройства может иметь катастрофические последствия для связности и производительности сети. Параметры команды конфигурации необходимо проверить во избежание проблем несоответствия или несовместимости. Рекомендуется регулярно проводить тщательный анализ конфигураций вместе с инженерами Cisco.

Полнофункциональный набор средств CiscoWorks2000 Essentials позволяет автоматически выполнять резервное копирование файлов конфигурации на маршрутизаторах и коммутаторах Cisco Catalyst. Функция обеспечения безопасности в Essentials может использоваться для аутентификации при изменении конфигурации. С помощью контрольного журнала изменений можно отслеживать имена пользователей и выполняемые ими изменения. Для изменения конфигурации на нескольких устройствах есть два параметра: **средство NetConfig с веб-интерфейсом в текущей версии CiscoWorks2000 Essentials или сценарий cwconfig.** При помощи CiscoWorks2000 Essentials можно загружать и выводить файлы конфигурации, используя предварительно заданные шаблоны или шаблоны пользователей.

Применяя средства управления конфигурацией в системе CiscoWorks2000 Essentials, можно выполнять следующие функции:

- Поместите файлы конфигурации из архива конфигураций "Essentials" в одно или несколько устройств
- Извлеките конфигурацию из устройства в архив Essentials
- Распаковка самой последней конфигурации из архива и ее запись в файл
- Импортируйте конфигурацию из файла и поместите ее в устройства
- Сравнение двух последних конфигураций в архиве Essentials
- Удаление конфигураций, имеющих дату ранее указанной или версию, более раннюю по сравнению с версией из архива
- Скопируйте конфигурацию запуска в рабочую конфигурацию

Инвентаризация

Функция обнаружения на большинстве платформ управления сетью предназначена для обеспечения динамического перечисления устройств, обнаруженных в сети. Необходимо использовать модули анализа Discovery Engine подобные тем, которые внедрены в платформы управления сетью.

База данных с перечнем устройств содержит подробные сведения о конфигурации сетевых устройств. В общих сведениях указываются модели аппаратного обеспечения, установленные модули, образы программного обеспечения, уровни микрокодов и т. п. Все эти порции информации являются ключевыми при выполнении таких задач, как эксплуатация программного и аппаратного обеспечения. Обновленный перечень сетевых устройств, составленный в ходе процесса обнаружения, можно использовать как основной список для сбора сведений с помощью протокола SNMP или путем написания сценариев. Список устройств можно импортировать из приложения CiscoWorks2000 Campus Manager в

базу данных перечня устройств системы CiscoWorks2000 Essentials, чтобы получить самый последний перечень коммутаторов Catalyst.

Управление программным обеспечением

Для успешного обновления образов системы Cisco IOS на сетевых устройствах необходимо выполнить тщательный анализ требований, например памяти, загрузочного ПЗУ, уровня микрокода и т. д. Эти требования обычно документируются и доступны на веб-сайте Cisco в форме заметок о выпуске и руководств по установке. Процесс обновления сетевого устройства под управлением Cisco IOS включает загрузку нужного образа с CCO, резервное копирование текущего образа, выполнение всех требований к оборудованию и, наконец, загрузку нового образа в устройство.

Для некоторых организаций окно обновления для выполнения эксплуатации устройства в некоторой степени ограничено. Крупная сетевая среда с ограниченными ресурсами может потребовать составления расписания и автоматизации обновлений программного обеспечения после окончания рабочего дня. Для проведения этой процедуры можно воспользоваться языком составления сценариев, таким как Expect, или приложением, специально разработанным для выполнения подобной задачи.

Изменения в программном обеспечении на сетевых устройствах, например в образах Cisco IOS и версиях микрокодов, необходимо отслеживать для поддержки на фазе анализа, когда требуется сопровождение другого ПО. Имея легкодоступный отчет по хронологии операций, специалист, производящий обновление, может сократить риск загрузки несовместимых образов или микропрограмм на сетевые устройства.

Управление производительностью

Соглашение об уровне обслуживания

Соглашение о сервисном обслуживании (SLA) – письменное соглашение между поставщиком услуг и пользователями об ожидаемом уровне исполнения сетевых услуг. В этом соглашении между поставщиком и его клиентами оговариваются метрики. Значения, установленные для метрики, должны быть реальными, содержательными и измеримыми для обеих сторон.

Для измерения уровня производительности можно собирать с сетевых устройств различные статистические данные интерфейсов. Эта статистика может быть включена в SLA в качестве метрики. Статистические показатели, как например количество отброшенных пакетов во входной и выходной очередях, количество отклоненных пакетов, бывают полезны для диагностики неисправностей, связанных с производительностью.

На уровне устройства метрики производительности могут включать использование CPU, распределение буферов (big buffer, medium buffer, misses, hit ratio) и распределение памяти. Производительность некоторых сетевых протоколов прямо связана с наличием буферов в сетевых устройствах. Сбор и анализ статистики производительности на уровне физических устройств играет ключевую роль в оптимизации производительности протоколов высокого уровня.

Сетевые устройства, например маршрутизаторы, поддерживают различные высокоуровневые протоколы, такие как DLSW (Data Link Switching Workgroup, рабочая

группа по коммутации каналов передачи), RSRB (Remote Source Route Bridging, удаленная априорная маршрутизация через мосты), AppleTalk и т. д. Можно отслеживать и собирать статистические данные о производительности технологий глобальных сетей (WAN), в том числе о ретрансляции кадров (Frame Relay), режиме асинхронной передачи (ATM), цифровой сети с комплексными услугами (ISDN) и др.

Мониторинг, измерение и отчеты о быстродействии

Статистику производительности на уровне интерфейса, устройства и протокола следует регулярно собирать с помощью SNMP. Механизм опроса в системе управления сетью может использоваться для сбора данных. Большинство систем управления сетью имеют функции сбора, хранения и представления данных опросов.

На рынке есть решения, которые отвечают запросам корпоративных сред по управлению производительностью. В этих системах имеются функции сбора, хранения и представления данных, полученных от сетевых устройств и серверов. Веб-интерфейс большинства продуктов делает данные о производительности доступными из любой точки предприятия. Вот некоторые из обычно используемых решений по управлению эффективностью:

- InfoVista VistaView
- SAS IT Service Vision
- Trinagy TREND

Оценка перечисленных выше продуктов позволит определить, отвечают ли они требованиям различных пользователей. Некоторые поставщики поддерживают интеграцию с платформами сетевого и системного управления. Например, InfoVista поддерживает агента BMC Patrol, который служит для получения основных статистических данных о производительности серверов приложений. Модель ценообразования и возможности базового предложения зависят от конкретного продукта. Некоторые решения предусматривают поддержку функций управления производительностью устройств Cisco, таких как NetFlow, RMON или агент обеспечения обслуживания/генератор отчетов по времени отклика (RTR/SAA CSAA/RTR) Cisco IOS. В результате согласования недавно была добавлена поддержка коммутаторов Cisco WAN, которые можно использовать для сбора и просмотра эксплуатационных данных.

Средство CSAA/RTR агент гарантированного обслуживания (SAA)/генератор отчётов времени отклика (RTR) в Cisco IOS можно использовать для измерения времени отклика между устройствами IP. Исходный маршрутизатор, конфигурированный с CSAA, может считать время ответа IP устройству назначения, который может быть маршрутизатором или IP устройством. Время отклика может быть измерено между источником и точкой назначения или для каждого перехода на всем протяжении пути. Ловушки SNMP можно настроить для оповещения консолей управления, если время отклика превышает заранее установленное пороговое значение.

Последнее усовершенствование Cisco IOS расширяют возможности CSAA для следующих измерений:

- Производительность службы протокола передачи гипертекста (HTTP)Поиск в системе имен домена (DNS)Связь по протоколу управления передачей (TCP)Время транзакции HTTP
- Межпакетная задержка (неустойчивая синхронизация) трафика службы передачи голоса по сетям (VoIP)

- Время отклика между конечными точками для определенного качества обслуживания (QoS)Байты TOS (тип обслуживания) IP-заголовка
- Потеря пакетов при использовании функции CSAA

Можно настроить функцию CSAA на маршрутизаторах, используя приложение IPM (Cisco Internetwork Performance Monitor, монитор производительности объединенной сети). CSAA/RTR встроен во многие, но не во все, наборы возможностей программного обеспечения Cisco IOS. На устройство, которое используется приложением IPM для сбора статистических данных о производительности, необходимо установить версию ПО Cisco IOS, которая поддерживает средства CSAA и RTR. Дополнительные сведения о версиях Cisco IOS, поддерживающих функции CSAA, RTR и IPM, см. на веб-сайте Вопросы и ответы по функции IPM.

Дополнительная информация о функции IPM включает в себя следующее:

- Обзор IPM
- Агент гарантированных служб Service Assurance Agent

Анализ и регулировка производительности

Значительное увеличение пользовательского трафика ставит более высокие требования к сетевым ресурсам. У менеджеров сети, как правило, есть ограниченное представление о типах трафика, работающих в сети. Профилирование трафика приложения и пользователя предоставляет подробный представление сетевого трафика. Возможность сбора профилей трафика предоставляют две технологии: датчики RMON и NetFlow.

RMON

Стандарты RMON разрабатываются для внедрения в распределенной архитектуре, где агенты (встроенные или в автономных датчиках) устанавливают связь с центральной станцией (управляющей консолью) через протокол SNMP. Стандарт RMON, описанный в RFC 1757, разделяет функции мониторинга на девять групп для топологий Ethernet; RFC 1513 содержит описание десятой группы параметров для маркерного кольца. Мониторинг канала Fast Ethernet обеспечивается в инфраструктуре стандарта RFC 1757, а мониторинг кольца FDDI (Интерфейс для передачи распределенных данных по волоконно-оптическим каналам) – в инфраструктуре стандартов RFC 1757 и RFC 1513.

Новая спецификация RFC 2021 RMON ставит стандарты удаленного контроля выше уровня управления доступом к среде (MAC) для уровней сети и приложения. С помощью данной установки администратор может анализировать работу и устранять неполадки сетевых приложений управления Интернет-трафиком, электронной почты, доступа к базам данных, сетевой файловой системы (NFS), NetWare, Notes и других. Теперь сигналы, статистика, история и группы узлов/диалогов RMON могут использоваться для упреждающего мониторинга и сохранения доступности сети на основе трафика уровня приложений – наиболее критического трафика в сети. Система RMON2 позволяет сетевым администраторам продолжать внедрение решений мониторинга на основе стандартов для поддержки ответственных серверных приложений.

В следующих таблицах перечисляются функции групп RMON.

Группа RMON	Функция

(RFC 1757)	
Statistics	Счетчики для пакетов, октетов, широковещательных рассылок, ошибок и предложений на сегменте или порте.
History	Периодически делает выборку и сохраняет статистику счетчиков групп для последующего извлечения.
Хосты	Поддерживает статистику по каждому хост-устройству в сегменте или на порту.
Подгруппа определенного количества главных хостов	Отчет поднабора, определенного пользователем, группы хостов, отобранного статистическим счетчиком. Благодаря тому, что возвращаются только результаты, объем управляющего трафика снижается до минимума.
Матрица трафика	Ведение статистики разговоров между хостами в сети.
Сигналы тревоги	Пороговый уровень, который может быть установлен для критических переменных RMON для профилактического управления.
События	Генерация прерываний SNMP и записей в журнале при превышении порогового значения для группы аварийных сигналов.
Захват пакета	Управление буферами для пакетов, захваченных группой фильтров с их последующей выгрузкой на управляющую консоль.
Token Ring	Станция вызова — подробная статистика на заказе Станции вызова отдельных станций — упорядоченном списке станций в настоящее время на кольцевой конфигурации Станции вызова — конфигурации и вставки/удаления на Маршрутизацию источника станции — статистика по маршрутизации источника, таких как счетчики переходов и другие

RMON2	Функция
Каталог протоколов	Протоколы, для которых агент осуществляет мониторинг и сбор статистических данных.
Распределение трафика по протоколам	Статистика по каждому протоколу.

Узел сетевого уровня	Статистика для каждого адреса уровня сети в сегменте, кольце или порту.
Матрица сетевого уровня	Статистика трафика для пар адресов сетевого уровня.
Хост уровня приложения	Статистика по протоколу уровня приложения для каждого сетевого адреса.
Матрица уровня приложений	Статистика трафика по протоколу прикладного уровня для пар адресов сетевого уровня.
Определяемая пользователем хронология операций	Расширение хронологии операций за пределы статистики канального уровня RMON1 и включение любой из систем статистических показателей RMON, RMON2, MIB-I или MIB-II.
Сопоставление адресов	Связывание адресов уровня MAC-сеть.
Группа конфигураций	Возможности и конфигурации агента.

NetFlow

Функция Cisco NetFlow позволяет собирать подробную статистику потоков трафика для планирования пропускной способности, выставления счетов и функций устранения неполадок. NetFlow можно настроить в отдельных интерфейсах для получения информации о трафике, проходящем через эти интерфейсы. Следующие типы информации являются частью подробной статистики трафика:

- IP-адреса источника и получателя
- Номера входного и выходного интерфейсов
- Порт источника и порты назначения для протоколов TCP/UDP
- Число байт и пакетов в потоке
- Номера автономных систем источника и получателя
- Тип услуг IP (ToS)

Данные NetFlow, собранное с сетевых устройств, экспортируются на машину сбора. Коллектор выполняет такие функции, как уменьшение объема данных (фильтрация и агрегирование), хранение иерархических данных и управление файловой системой. Приложения NetFlow Collector и NetFlow Analyzer Cisco предназначены для сбора и анализа данных маршрутизаторов и коммутаторов Cisco Catalyst. Также имеются бесплатные программные средства, например, cflowd , осуществляющие сбор записей протокола датаграмм пользователя (UDP) Cisco NetFlow .

Данные NetFlow транспортируются с использованием пакетов UDP в трех различных

форматах:

- Версия 1. Исходный формат, поддерживаемый в первых версиях системы NetFlow.
- Версия 5. В более позднем расширении добавлены данные и номера последовательностей потоков для автономной системы BGP (Протокол пограничного шлюза).
- Версия 7. В еще более позднем расширении добавлена поддержка коммутации NetFlow для коммутаторов Cisco Catalyst серии 5000, которые оборудованы платой расширения NFFC (NetFlow feature card).

Версии со 2 по 4 и версия 6 либо не были выпущены, либо не поддерживаются FlowCollector. Во всех трех версиях дейтаграмма состоит из заголовка и одной или более потоковых записей.

Дополнительные сведения см. в официальном документе: Руководство по решениям и службам NetFlow.

В следующей таблице очерчены поддерживаемые версии Cisco IOS для сбора данных NetFlow с маршрутизаторов и коммутаторов Catalyst.

Cisco IOS Software Release	Поддержка аппаратных платформ Cisco	Поддерживаемая экспортируемая версия(и) NetFlow
11.1 CA и 11.1 CC	Cisco 7200, 7500 и RSP7000	V1 и V5
11.2 и 11.2 P	Cisco 7200, 7500 и RSP7000	V1
11.2 P	Модуль Cisco маршрутизации и коммутации (RSM)	V1
11.3 и 11.3 T	Cisco 7200, 7500 и RSP7000	V1
12.0	Cisco 1720, 2600, 3600, 4500, 4700, AS5800, 7200, uBR7200, 7500, RSP7000 и RSM	V1 и V5
12.0 T	Cisco 1720, 2600, 3600, 4500, 4700, AS5800, 7200, uBR7200, 7500, RSP7000, RSM, MGX 8800 RPM и BPX 8600	V1 и V5
12.0(3)T и более поздних версий	Cisco 1600*, 1720, 2500**, 2600, 3600, 4500, 4700, AS5300*, AS5800, 7200, uBR7200, 7500, RSP7000, RSM, MGX8800	V1, V5 и V8

	RPM и BPX 8650	
12.0 (6) S	Cisco 12000	V1, V5 и V8
—	Cisco Catalyst 5000 с платой расширения NetFlow (NFFC)***	V7

* Поддержка экспорта NetFlow в версиях V1, V5 и V8 на платформах Cisco 1600 и 2500 предназначена для системы Cisco IOS версии 12.0(T). Поддержка NetFlow для этих платформ недоступна в основном выпуске системы Cisco IOS версии 12.0.

** Поддержка NetFlow версий V1, V5, и V8 на платформе AS5300 предназначена для системы Cisco IOS версии 12.06(T).

*** Экспорт данных MLS и NetFlow поддерживается в программном обеспечении Supervisor Engine Catalyst серии 5000 версии 4.1(1) или более поздней.

Управление системой безопасности

Цель управления безопасностью – контролировать доступ к сетевым ресурсам согласно местным нормативам так, чтобы сеть не могла быть повреждена (намеренно или непреднамеренно). Например, подсистема управления безопасностью может следить за входом пользователей на сетевые ресурсы, отказывая в доступе тем, кто ввел неправильные коды доступа. Управление безопасностью – это очень широкая тема, поэтому в этом разделе документа безопасность рассматривается только в связи с протоколом SNMP и доступом к основным устройствам.

Дополнительные сведения о расширенной безопасности см. в следующих источниках:

- Повышение безопасности на IP-сетях
- OpenSystems

Правильная реализация управления безопасностью начинается с надежных политик и процедур безопасности. Важно создать стандарт минимальной конфигурации под данную платформу для всех маршрутизаторов и коммутаторов, что соответствует лучшим промышленным методам обеспечения безопасности и производительности.

Существуют различные методы контроля доступа на маршрутизаторах Cisco и коммутаторах Catalyst. Некоторые из этих способов включают:

- Списки управления доступом (ACL)
- Идентификаторы и пароли пользователей, локальные для данного устройства
- Система управления доступом к контроллеру терминального доступа (TACACS)

TACACS – это протокол безопасности по стандарту RFC 1492 комитета по инженерным вопросам Интернета (IETF, Internet Engineering Task Force), который запускается между клиентскими устройствами в сети и на сервере TACACS. TACACS – это механизм аутентификации, используемый для удостоверения подлинности устройства, пытающегося получить удаленный доступ к привилегированной базе данных. Варианты TACACS включают TACACS+, архитектуру AAA, которая разделяет функции аутентификации, авторизации и учета.

TACACS+ используется для обеспечения более надежного управления доступом к устройствам Cisco в привилегированном и непривилегированном режимах. В целях отказоустойчивости можно настроить несколько серверов TACACS+. При включенном TACACS+ маршрутизатор и коммутатор запрашивают у пользователя имя и пароль. Аутентификация может быть настроена для управления доступом в систему или проверки индивидуальных команд.

Authentication

Аутентификация – процесс идентификации пользователей, включающий проверку имени пользователя и паролем, запроса и ответа и поддержку обмена сообщениями. Аутентификация является способом, которым идентифицируется пользователь перед получением доступа к маршрутизатору или коммутатору. Существует фундаментальная связь между аутентификацией и авторизацией. Чем больше привилегий аутентификации получает пользователь, тем строже аутентификация.

Authorization

Авторизация предоставляет управление удаленным доступом, включая однократную авторизацию и авторизацию для каждой службы, запрошенной пользователем. Диапазон уровня авторизации на маршрутизаторе Cisco варьируется от 0 до 15, при этом 0 – это самый низкий уровень, а 15 – самый высокий.

Учет

Учет предусматривает сбор и отправку сведений о безопасности, используемых для учета трафика, проверки и создания отчетов, например, о проверке подлинности прав доступа пользователей, времени начала и окончания сеанса, а также выполненных командах. Учет позволяет сетевым администраторам отслеживать службы, к которым получают доступ пользователи, а также объем потребляемых ими сетевых ресурсов.

В следующей таблице перечислены основные типовые команды для использования TACACS+, аутентификации, авторизации и отчетности на маршрутизаторе Cisco и коммутаторе Catalyst. Дополнительные сведения об этих командах см. в документе Команды аутентификации, авторизации и учета.

Команда Cisco IOS	**Цель**
Маршрутизатор	
aaa new-model	Включение аутентификации, авторизации и учета (AAA) как основного метода контроля доступа.
AAA accounting {system | network | connection | exec | command level} {start-stop | wait-start | stop-only} {tacacs+ |	Включите учет с помощью команд глобального конфигурирования.

radius}	
AAA authentication login default tacacs+	Установка маршрутизатора в режим, при котором подключения к любой линии терминала, настроенной под регистрационное имя по умолчанию, будут аутентифицироваться с помощью TACACS+ и выдавать отказ, если аутентификация не удается по какой-либо причине.
AAA authorization exec default tacacs+ none	Настройте маршрутизатор на проверку того, разрешено ли пользователю запускать оболочку EXEC, опрашивая сервер TACACS+.
tacacs-server host tacacs+ server ip address	Укажите сервер TACACS+, который будет использоваться для аутентификации с помощью команд глобальной конфигурации.
tacacs-server key shared-secret	Укажите общий секрет, известный только серверам TACACS+ и маршрутизатору Cisco, при помощи команды global configuration.
Коммутатор Catalyst	
set authentication login tacacs enable [all | console | http | telnet] [primary]	Включение аутентификации TACACS+ для нормального режима входа в систему. Для включения TACACS+ только для попыток подключения к консольному порту или Telnet используются ключевые слова Telnet или консоли.
set authorization exec enable {option} fallback option} [console | telnet | both]	Включите авторизацию для стандартного режима регистрации. Используйте ключевые слова Telnet или консоль для разрешения авторизации только для попыток подключения к консольному порту или для подключения Telnet.
Set tacacs-server key shared-secret	Задайте общий секрет, известный серверам и коммутатору TACACS+.
Set tacacs-server host tacacs+ server ip address	Укажите сервер TACACS+, который будет использоваться для аутентификации с помощью команд глобальной конфигурации.
Set accounting commands enable {config | all} {stop-only} tacacs+	Включите учет команд настройки.

Дополнительные сведения о конфигурации AAA для мониторинга и управления доступом к

интерфейсу командной строки на коммутаторах Catalyst для корпоративных локальных сетей см. в документе Контроль доступа к коммутатору с помощью аутентификации, авторизации и учета.

Безопасность SNMP

Протокол SNMP может быть использован для внесения изменений в конфигурации на маршрутизаторах и коммутаторах Catalyst аналогично выполнению команд из интерфейса командной строки. Следует настроить на сетевых устройствах надлежащие меры безопасности, чтобы предотвратить несанкционированный доступ и изменения через SNMP. При задании строк имен сообществ необходимо следовать стандартным правилам для паролей по длине, набору допустимых символов и трудности угадывания. Важно изменить общие и частные значения по умолчанию строк сообществ.

Все узлы управления SNMP должны иметь статический IP-адрес и им должны быть явно предоставлены права соединения по протоколу SNMP с сетевым устройством, как это предопределенно IP-адресом и списком управления доступом (ACL). Программное обеспечение Cisco IOS и Cisco Catalyst обладает функциями обеспечения безопасности, с помощью которых можно обеспечить выполнение изменений на сетевых устройствах только со стороны авторизованных администраторских станций.

Функции безопасности маршрутизатора

Уровень привилегий протокола SNMP

Эта функция ограничивает количество типов операций, которые рабочая станция может производить на маршрутизаторе. На маршрутизаторах есть два уровня привилегий: Только для чтения (Read-Only, RO) и чтение-запись (Read-Write, RW). Уровень RO позволяет управляющей станции только запрашивать маршрутные данные. Он не позволяет выполнять такие команды настройки, как перезагрузка маршрутизатора и отключение интерфейсов. Для выполнения таких операций можно использовать только уровень привилегий RW.

SNMP Access Control List (ACL)

Функцию ACL протокола SNMP можно использовать вместе с возможностью привилегий SNMP для ограничения запросов управляющей информации от маршрутизаторов на определенных управляющих станциях.

Средство просмотра протокола SNMP

Эта возможность ограничивает определенные сведения, которые могут быть получены от маршрутизаторов станциями управления. Данная функция может использоваться совместно с функциями уровня привилегий SNMP и ACL для принудительного ограничения доступа к данным с помощью консоли управления. Примеры конфигураций для средства просмотра SNMP см. в разделе Средство просмотра сервера SNMP.

Протокол SNMP версии 3

SNMP версии 3 (SNMPv3) предоставляет возможность безопасного обмена управляющей информацией между устройствами сети и станциями управления. Функции шифрования и аутентификации в SNMPv3 обеспечивают высокий уровень безопасности при доставке

пакетов на консоль управления. Протокол SNMPv3 поддерживается в системе Cisco IOS версии 12.0(3)T и позднее. Дополнительные сведения о протоколе SNMPv3 см. в документе SNMPv3.

Список управления доступом (ACL) на интерфейсах

ACL является одной из мер безопасности и позволяет предотвратить имитацию IP-адресов (спуфинг). ACL можно применять к входящим или исходящим интерфейсам маршрутизаторов.

Функция безопасности коммутатора Catalyst для локальных сетей

Список разрешений IP

Функция IP Permit List ограничивает входящий доступ Telnet и SNMP к коммутатору с несанкционированных исходных IP-адресов. Поддерживаются сообщения Syslog и ловушки SNMP, чтобы уведомлять систему управления о нарушениях или о несанкционированном доступе.

Для управления маршрутизаторами и коммутаторами Catalyst можно использовать сочетание функций безопасности системы Cisco IOS. Необходимо установить политику безопасности, которая ограничивает количество управляющих станций с возможностью доступа к коммутаторам и маршрутизаторам.

Дополнительные сведения о повышении уровня безопасности в IP-сетях см. в документе Повышение уровня безопасности в IP-сетях.

Управление учетом

Управление учетом сетевых ресурсов – это процесс, используемый для измерения параметров загруженности сети, благодаря которому возможно регулировать работу отдельных пользователей сети или их групп в целях ведения учета или возврата платежей. Так же как и в управлении производительностью, первым шагом в управлении учетными данными является измерение использования всех важных сетевых ресурсов. Использование сетевых ресурсов можно измерить с помощью функций Cisco NetFlow и Cisco IP Accounting. Анализ данных, собранных с помощью этих методов, позволяет понять текущую модель использования.

Система учета использования ресурсов и выставления счетов является неотъемлемой частью соглашения об уровне обслуживания (SLA). Она предоставляет как практичный способ определения обязательств по SLA, так и ясные последствия поведения вне рамок SLA.

Необходимые данные можно собирать, применяя датчики или технологии Cisco NetFlow. Cisco предоставляет приложения NetFlow Collector и NetFlow Analyzer для сбора и анализа данных маршрутизаторов и коммутаторов Catalyst. Для сбора данных NetFlow также используются условно-бесплатные приложения, такие как cflowd. Постоянное измерение использования ресурса может собирать сведения для выставления счетов, а также справедливости оценки информации и оптимальности ресурсов. Некоторые из обычно развертываемых решений управления учетом:

- Evident Software

Активация NetFlow и стратегия сбора данных

NetFlow (поток в сети) - это технология измерений на стороне ввода, позволяющая получать данные, необходимые для приложений планирования сети, контроля и учета. На интерфейсах маршрутизаторов с поддержкой агрегирования или граничных маршрутизаторов поставщиков услуг или интерфейсах маршрутизаторов доступа к WAN корпоративных клиентов должен быть установлен NetFlow.

Cisco Systems рекомендует проводить тщательно распланированное развертывание NetFlow со службами NetFlow, активированными на данных стратегически расположенных маршрутизаторах. NetFlow можно развертывать пошагово (интерфейс за интерфейсом) и стратегически (на правильно подобранных маршрутизаторах), а не на каждом маршрутизаторе сети. Специалисты компании Cisco будут выяснять вместе с заказчиками, на каких ключевых маршрутизаторах и ключевых интерфейсах следует запускать технологию NetFlow, с учетом закономерностей потоков трафика, топологии сети и архитектуры системы.

Основные вопросы развертывания включают в себя:

- *Службы NetFlow должны использоваться в качестве средства измерения на границах сети и увеличения эффективности списков доступа. Однако их не следует активировать на маршрутизаторах для магистрали или ядра сети в горячих точках или маршрутизаторах, работающих с очень высоким коэффициентом загрузки процессора.*
- Сведения о требованиях к сбору данных со стороны приложений. Приложения учета могут использовать только сведения о потоках начального и конечного маршрутизатора, в то время как приложения мониторинга могут потребовать более полное (в контексте данных) представление канала от одного конца до другого.
- Необходимо учитывать влияние топологии сети и политики маршрутизации на стратегию сбора потоков. Например, можно избежать скопления дублирующих потоков путем активации NetFlow на главных маршрутизаторов агрегации – исходных или конечных пунктов трафика - а не на магистральных или промежуточных маршрутизаторах, которые дают дублированное представление одной и той же информации потока.
- *Поставщики услуг, обеспечивающие транзитную передачу (с поддержкой трафика, который ни начинается, ни заканчивается в собственных сетях), могут использовать данные NetFlow Export для измерения степени использования проходящим трафиком сетевых ресурсов в целях учета и выставления счетов.*

Настройка учета для протокола IP

Поддержка IP-учета Cisco обеспечивает основные функции IP-учета. При включенном учете для протокола IP пользователи могут видеть количество байтов и пакетов, прошедших коммутацию на операционной системе Cisco IOS, с отображением по исходному и конечному IP-адресу. Измеряется объем лишь исходящего транзитного IP-трафика. Трафик, который создается программным обеспечением или поступает в него, не входит в статистику учета. Для сохранения точности итоговых показателей учета в программе поддерживается ведение двух учетных баз данных: активной и контрольной.

Система Cisco поддержки IP-учета предоставляет также информацию, которая определяет IP-трафик, вызывающий сбой списков доступа IP. Идентификация исходных IP-адресов, изменяющих списки доступа IP, сигнализирует о возможных попытках нарушения безопасности. Такие данные указывают также на то, что следует проверить конфигурации списков доступа. **Чтобы сделать эту функцию доступной для пользователей, включите IP-учет нарушений в списке доступа, используя команду ip accounting access-violations.** Пользователи затем могут выводить количество байтов и пакетов с одного источника, связанных с попыткой нарушения системы безопасности, в сравнении со списком доступа для пары источник-назначение. По умолчанию служба IP Accounting отображает число пакетов, прошедших через списки доступа и маршрутизированных.

Чтобы включить IP-учет, используйте одну из следующих команд для каждого интерфейса в режиме настройки интерфейса:

Команда	Цель
ip-учет	Включение основной системы IP-учета.
ip accounting access violations	Включение IP-учета с возможностью определения IP-трафика, который приводит к сбою списков IP-доступа.

Чтобы настроить другие функции IP-учета, используйте одну или несколько следующих команд в режиме глобальной конфигурации:

Команда	Цель
ip accounting-threshold threshold	Установка максимального количества создаваемых учетных записей.
ip accounting-list ip-address wildcard	Учетные данные фильтра для хостов.
ip accounting-transits count	Управление количеством транзитных записей, которые будут храниться в базе данных учета IP.

Дополнительные сведения

- Руководство по основам конфигурации
- Решения Cisco для корпоративного управления, том I, Cisco Press, ISBN 1587050064
- Cisco Systems – техническая поддержка и документация

Соответствующие дискуссии сообщества технической

поддержки Cisco

Сообщество технической поддержки Cisco является форумом, в котором можно задавать вопросы и получать ответы, обмениваться предложениями и сотрудничать со своими равноправными коллегами.

См. Условные обозначения технических советов Cisco для получения информации по условным обозначениям, которые используются в данном документе.

Обновлено : 11 июля 2007
ID документа: 15114