CiscoWorks LAN Management Solution

Обзор решения

Содержание

Рисунки

1. Обзор решения Cisco LAN Management Solution

1.1. Введение

Телекоммуникационная сеть формирует инфраструктуру для работы приложений, которые позволяют повысить эффективность работы предприятия, поэтому эффективное управление сетью является одной из наиболее важных задач ИТ-подразделений. Развитие предприятия приводит к расширению ИТ-инфраструктуры, что сказывается на количестве установленных сетевых устройств и сложности применяемых технологий, поднимая следующие вопросы:

- Как сократить время и снизить себестоимость внедрения новых устройств?
- Как повысить надежность сети и ускорить возврат инвестиций?

Решение CiscoWorks LAN Management Solution (LMS) — это семейство программных продуктов для упрощения настройки, мониторинга и диагностики сетей, построенных на базе продукции Cisco. LMS является интегрированной системой, которая предоставляет данные о сетевых устройствах для других информационных систем, автоматизирует рутинные задачи по управлению сетью, обеспечивает сбор и предоставление данных о загрузке устройств и предоставляет функции для локализации сетевых проблем и их диагностики. Все компоненты системы используют общий модуль хранения информации об устройствах, что значительно упрощает настройку решения и его интеграцию с существующими информационными системами компании.

Детальная информация о CiscoWorks LMS доступна на сайте http://www.cisco.com/go/lms.

1.2. Приложения LMS

Решение CiscoWoks LMS состоит из нескольких приложений. Пользователь может установить все приложения или только некоторые из них в соответствии со своими задачами. Все приложения поставляются в одном пакете и функционируют в соответствии с единой лицензией (за исключением приложения Health and Utilization Monitor, для использования которого требуется приобретение отдельной лицензии).

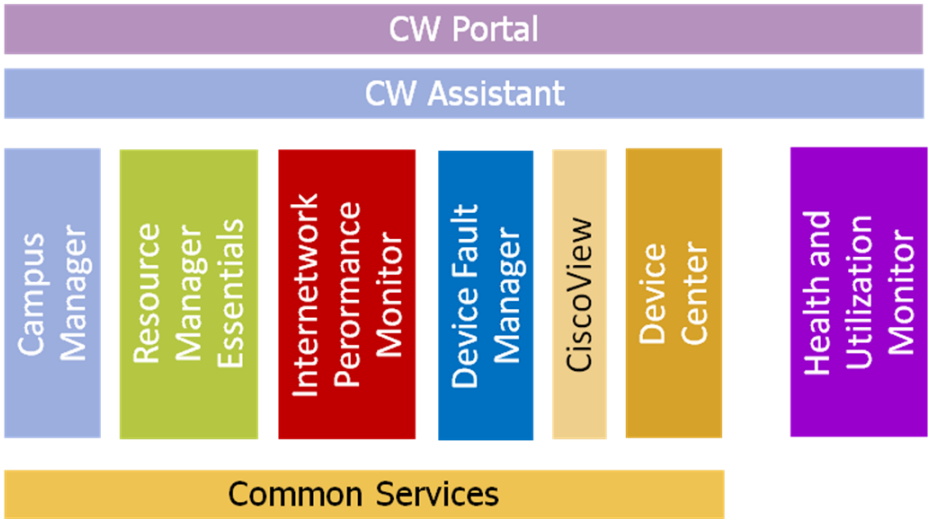


Рисунок 1. Приложения, входящие в состав LMS

Полный перечень приложений CiscoWorks LMS представлен на рисунке 1. Рассмотрим

их функциональное назначение:

- **Common Services**

  Приложение Common Services предоставляет функционал, используемый всеми приложениями LMS, и включает модули CiscoView, Integration Utility, LMS Portal и CiscoWorks Assistant (CWA).

  - Портал LMS Portal дает возможность пользователям изменять структуру предоставляемой информации по своему усмотрению, а также выводить часто используемые данные на одной странице для ускорения навигации и поиска . При работе с порталом пользователям не требуется просматривать несколько страниц для поиска нужных данных, поскольку пользователи могут самостоятельно создать нужную страницу, используя готовые программные компоненты, и вывести на нее информацию, которая поступает из разных приложений.
  - Модуль Integration Utility — это модуль, который обеспечивает интеграцию решения с системами сторонних производителей.
  - CiscoWorks Assistant значительно облегчает процесс настройки решения в случае, когда необходимо добавить какой-то модуль или перенести одно из приложений на другой сервер для повышения быстродействия решения в целом.

- **Campus Manager (CM)**

  Приложение Campus Manager предоставляет функции отображения топологии сети, управления VLAN, обнаружения ошибок в настройке устройств, а также возможности трассировки трафика заданного сервиса в рамках корпоративной ИТ-инфраструктуры.

- **Resource Manager Essentials (RME)**

  Приложение RME управляет инвентарной информацией о каждом устройстве, обеспечивает функции резервного копирования и восстановления конфигурации и программного обеспечения устройства, а также ведет учет всех изменений состояния оборудования и анализирует сообщения, которые поступают от устройств по протоколу Syslog.

- **Internetwork Performance Monitor (IPM)**

  Приложение Internetwork Performance Monitor измеряет производительность сети, базируясь на результатах выполнения синтетических тестов с помощью функции программного обеспечения Cisco IOS®, известной как Cisco IOS IP SLA (Service Level Agreement). Используемые синтетические тесты из IPM дают возможность администратору сети измерить производительность сети между двумя произвольно выбранными сетевыми устройствами. Гибкость настройки функции IP SLA делает модуль IPM чрезвычайно эффективным средством для измерения производительности сети.

- **Device Fault Manager (DFM)**

  Приложение Device Fault Manager обеспечивает мониторинг устройств в режиме реального времени с возможностью оповещения оператора по электронной почте. Все события сохраняются в базе данных и могут быть просмотрены пользователем по мере необходимости.

- **CiscoView**

Приложение CiscoView отображает устройства Cisco в графическом виде и позволяет пользователям легко изменять параметры оборудования и получать статистическую информацию о работе оборудования .

- **Health and Utilization Monitor (HUM)**

  Приложение Health and Utilization Monitor позволяет выполнять сбор статистики по производительности устройств. HUM использует протокол SNMP для сбора данных и может обеспечить мониторинг любых параметров устройств Cisco. В частности, HUM выполняет мониторинг загрузки центрального процессора, памяти, интерфейсов и сетевых соединений.

.

2. Обзор портала и модуля Common Services

В этом разделе описываются функции портала и модулей Setup Center и Common Services.

Портал LMS — это информационная панель сервера, позволяющая пользователю работать с большинством приложений, включая Common Services, Resource Management Essentials, Campus Manager и Device Fault Manager.

Common Services является ядром сервера LMS и требует правильной настройки. От правильности настройки данного модуля зависит корректность работы всех приложений решения.

2.1. Портал LMS

Портал LMS представляет собой информационную панель и обеспечивает быстрый доступ к данным и функциям управления сетью, позволяя значительно повысить удобство использования системы. Например, с помощью это портала можно легко получить доступ к информации о статусе сервера LMS, сетевых устройств и топологии сети.

Основные функциональные возможности портала:

- Настройка представления. Пользователь может персонализировать свою домашнюю страницу в CiscoWorks, используя функции перемещения, добавления, удаления и редактирования информационных компонентов.
- Доступ к данным по одному нажатию кнопки мышки. Уменьшение количества операций для доступа к часто используемой информации из различных приложений CiscoWorks LMS.
- Поддержка инсталляции решения на несколько серверов. Отображение на одном портале информации, которая поступает из приложений, установленных на разных серверах.
- Простой графический интерфейс. Не требует установки дополнительных модулей для доступа к приложениям.

Компоненты портала LMS
Первое, что видит пользователь, когда начинает работать с LMS, — это портал. Интерфейс портала LMS состоит из нескольких компонентов:

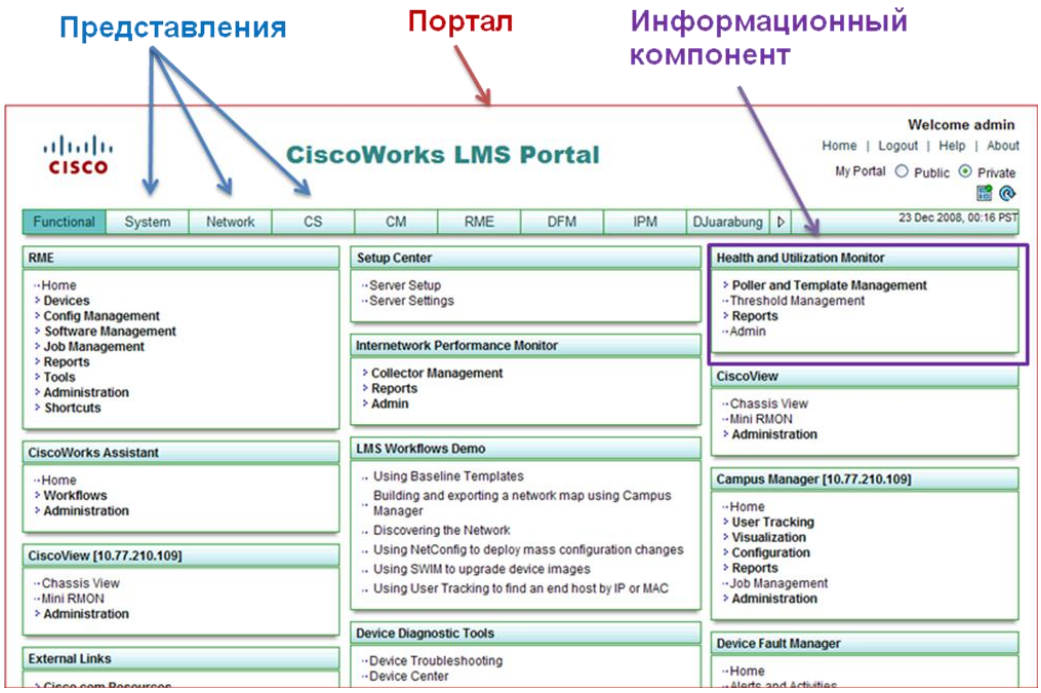


Рисунок 2. Компоненты портала

- **Портал**. Портал представляет собой оболочку, которая содержит несколько различных представлений. Можно настроить портал для работы с одним сервером или группой серверов, на которых установлены приложения LMS.
- **Представления**. Представления — это отдельные страницы, доступные с помощью меню, которые содержат набор различных информационных компонент. LMS поставляется с набором предварительно настроенных представлений, которые называются Function, System, Network, DFM, CM, RME, и IPM. Вы можете добавлять или изменять все представления, кроме представления Function. Новое представление может быть общедоступным (доступным для всех пользователей) или личным (доступным только для пользователя, создавшего это представление).
- **Информационные компоненты**. Информационные компоненты представляют собой блоки данных, в которых отображаются результаты работы, параметры приложения или отчеты. Можно добавлять и удалять информационные компоненты любого представления (за исключением представление Function). Список доступных информационных компонентов зависит от количества установленных приложений LMS.

2.2. Приложение Common Services

Приложение Common Services — это центральная часть решения CiscoWorks LMS, которая предоставляет общий функционал для всех приложений. Common Services обслуживает базу данных устройств, в которой хранится вся информацию об устройствах, находящихся под управлением LMS. Эта база данных называется Device Credential Repository (DCR).

Device Credential Repository (DCR)
База данных DCR является частью приложения Common Services, которая хранит

информацию об устройствах, их атрибутах и параметрах доступа, используемые различными приложениями LMS. Данные об устройствах, которые вносятся в DCR, автоматически становятся доступными для всех приложений решения. Например, если для определенного устройства изменились параметры доступа, их необходимо изменить только в DCR — все приложения будут использовать обновленную информацию при последующих обращениях к данному устройству.

Для администрирования DCR используется специальный интерфейс, называемый Device and Credential Admin (DCA).

3. Управление устройствами: приложения CiscoView и RME

3.1. Сценарии использования

С ростом сети предприятия управление постоянно увеличивающимся количеством устройств становится все труднее. Задачи, кажущиеся на первый взгляд простыми, могут вызвать большие проблемы в сети, состоящей из сотен или тысяч устройств. С помощью приложений LMS, которые рассматриваются в этом разделе, можно легко дать ответы на следующие вопросы:

1. Каким образом собрать инвентарную информацию по устройствам, используемым в сети организации? Как можно создать отчет с детализацией по составу оборудования и серийными номерами сетевых устройств и их модулей?
2. Как внести изменения в конфигурацию группы устройств без использования CLI и выполнения задачи вручную? Как сохранить историю изменений конфигурации?
3. Как минимизировать время на обновление программного обеспечения на сетевых устройствах? Как это сделать автоматически?
4. Как обеспечить мониторинг сообщений Syslog и получить оповещение в случае, если в сети что-то произошло?
5. Как обеспечить своевременное получение данных об уязвимостях PSIRT и окончании поддержки программного обеспечения Cisco IOS? Что для этого необходимо сделать?

Все эти и множество других задач решаются с помощью 3-х приложений CiscoWorks LMS:

- Resource Management Essentials (RME),
- CiscoView,
- Device Center.

3.2. Управление устройствами в RME

3.2.1. Обзор RME

Приложение RME можно назвать центральным компонентом решения CiscoWorks LMS. Это приложение используется для управления конфигурациями и включает множество функций, которые значительно упрощают выполнение таких задач, как обновление программного обеспечения IOS или изменение конфигурации группы устройств. RME также предоставляет несколько функций для управления инцидентами, например, сбор и обработка сообщений Syslog.

Основные модули RME:

- **Inventory Manager.** Обеспечивает сбор и хранение актуальной инвентарной информации по оборудованию и программному обеспечению. Все собранные данные могут быть получены в виде отчетов. RME поставляется с рядом готовых отчетов и позволяет создавать новые отчеты в соответствии с требованиями пользователей.
- **Configuration Manager.** Обслуживает архив файлов конфигураций и всех

изменений конфигурации по каждому устройству, которое находится под управлением CiscoWorks LMS. Использование Configuration Manager упрощает внесение изменений в конфигурацию устройств. Для изменения, сравнения и распространения конфигурации на устройства может использоваться модуль ConfigEditor. ConfigEditor позволяет распространить новую конфигурацию как на одно устройство, так и на группу устройств. Для удобства использования RME предоставляет возможность создания шаблонов конфигураций и выполнения действий после внесения изменений в конфигурацию устройств.

- **Software Manager.** Упрощает и сокращает время анализа версий установленного программного обеспечения и развертывания новых версий ПО Cisco IOS.
- **Syslog Analysis.** Обеспечивает сбор и анализ сообщений Syslog, что позволяет своевременно обнаруживать неполадки в работе сетевых устройств. По факту получения сообщения RME может выполнить заранее определенное действие.
- **Change Audit Services.** Обеспечивает непрерывный мониторинг изменений конфигурации оборудования и предоставляет отчетность по программному обеспечению, комплектности оборудования и изменения конфигурации.
- **Audit Trails.** Обеспечивает непрерывный контроль и регистрацию всех действий пользователей при работе с RME.

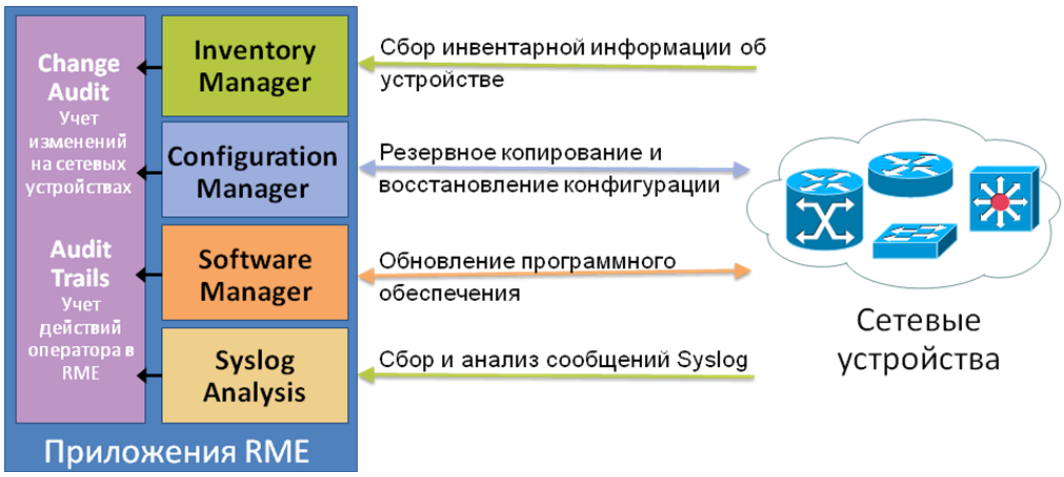


Рисунок 3. Приложения RME

3.2.2. Управление инвентарной информацией

Модуль Inventory Manager обеспечивает сбор и хранение инвентарной информации, которая включает данные о составе оборудования и версии программного обеспечения. На основании эти данных в дальнейшем системный администратор обслуживает оборудование, производит его настройку и диагностику. Собранная инвентарная информация также используется другими приложениями LMS. Собранные данные могут использоваться системным администратором при проведении инвентаризации оборудования или во время подготовки к модернизации устройств и программного обеспечения.

Например, для обновления программного обеспечения устройства необходимо точно знать объем доступной оперативной памяти и конфигурацию оборудования. Все эти данные собираются с помощью RME и могут быть получены в любой момент времени.

Сбор инвентарных данных

В процессе установки RME на сервере создаются 2 задачи для сбора и проверки изменений конфигурации оборудования. Каждая из этих задач выполняется по своему расписанию.

Задача сбора данных обеспечивает сбор инвентарной информации со всех устройств и сохранение собранной информации в локальной базе данных. Вторая задача (проверка изменений) обеспечивает периодическую проверку определенного значения переменной SNMP MIB, содержащей метку времени последнего обновления конфигурации, и определяет, были ли изменения в конфигурации устройства после последней проверки. В случае если метка времени была изменена по сравнению со значением, сохраненным в базе данных, RME получает инвентарные данные и сохраняет их в базе данных.

По умолчанию задача сбора данных выполняется один раз в неделю и получает инвентарные данные независимо от изменения конфигурации оборудования. Задача проверки изменения конфигурации выполняется один раз в день. Такой подход позволяет минимизировать нагрузку на сеть при сборе инвентарных данных.

Генератор отчетов
Приложение RME начинает сбор инвентарных данных сразу после добавления устройства в DCR. Собранные данные могут быть представлены пользователю в виде отчетов. В комплект поставки системы входит ряд предварительно настроенных отчетов для разных приложений LMS.

Таблица 1. Отчеты RME

Группа отчетов	Описание
Audit Trail	Аудит действий пользователей в CiscoWorks
BugToolkit	Отчеты по ошибкам в программном обеспечении Cisco IOS, установленном на сетевом оборудовании
Change Audit	Аудит изменений конфигурации установленного оборудования
Contract Connection	Отчеты по наличию поддержки на установленное на сети оборудование
Device Credential	Отчеты по параметрам доступа к оборудованию
Inventory	Отчеты по инвентарным данным по установленному оборудованию
Syslog	Отчеты по сообщениям Syslog, полученным с оборудования

В каждую группу отчетов входит один или несколько отчетов. Например, в группе **Inventory** пользователю доступны отчеты, представленные в таблице 2.

Таблица 2. Отчеты Inventory

Отчет	Описание
24-Hour Inventory Change Report	Отчет по изменениям конфигурации оборудования за последние 24 часа.
Chassis Slot Details	Отчет по загруженности шасси для выбранного набора устройств. Отображает наличие свободных/занятых слотов и месторасположение устройств.
Chassis Slot Summary	Отчет по устройствам со свободными слотами
Detailed Device Report	Детальный отчет по текущей конфигурации устройства. Включает информацию по программному обеспечению, шасси, модулям, портам, модулям памяти, процессорам и т.д.
Hardware Report	Отчет по составу оборудования для выбранного набора устройств. Включает информацию о процессорах, шасси, объеме памяти, категории устройства.
Software Report	Отчет по программному обеспечению, установленному на оборудовании.

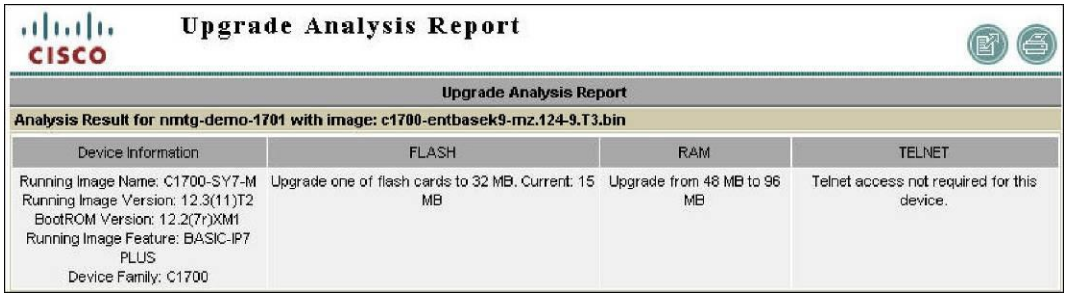
PSIRT Summary Report	Отчет по ошибкам в ПО IOS, установленном на сетевом оборудовании, которые являются критическими с точки зрения безопасности.
EoSale/EoL Report	Отчет по оборудованию и программному обеспечению, которое больше не продается и не поддерживается компанией Cisco Systems
Hardware Summary Graph	Графический отчет, отображающий распределение разных типов устройств, установленных на сети.
Software Version Graph	Графический отчет, отображающий распределение версий программного обеспечения, используемого на сети.

Все перечисленные отчеты строятся на основании предварительно подготовленных шаблонов и набора переменных. Например, отчет Inventory/Software Report формирует список версий программного обеспечения, сгруппированного по предварительно определенным группам устройств. Существующие отчеты могут быть модифицированы. Для получения нового отчета, который должен отражать требования пользователя, можно воспользоваться функцией **Custom Reports Template**.

3.2.3. Управление программным обеспечением

Модуль управления версиями программного обеспечения (Software Manager) взаимодействует с сайтом Cisco.com и значительно упрощает поиск нужного образа Cisco IOS. Новое программное обеспечение может быть развернуто за несколько простых шагов:

- **Шаг 1 — анализ программного обеспечения.** RME помогает пользователю проанализировать конфигурацию устройства и сделать вывод о достаточности ресурсов для работы новой версии ПО. RME дает рекомендации по каждому выбранному устройству, предоставляя перечень доступного программного обеспечения для каждого устройства. После выбора необходимой версии RME выдает рекомендации по действиям, которые необходимо произвести до установки нового программного обеспечения.


Upgrade Analysis Report

Upgrade Analysis Report

Analysis Result for nmtg-demo-1701 with image: c1700-entbasek9-mz.124-9.T3.bin

Device Information	FLASH	RAM	TELNET
Running Image Name: C1700-SY7-M Running Image Version: 12.3(11)T2 BootROM Version: 12.2(7r)XM1 Running Image Feature: BASIC-IP7 PLUS Device Family: C1700	Upgrade one of flash cards to 32 MB. Current: 15 MB	Upgrade from 48 MB to 96 MB	Telnet access not required for this device.

Рисунок 4. Отчет по результатам анализа программного обеспечения в RME

- **Шаг 2 — добавление образа программного обеспечения в библиотеку.** RME предлагает пользователю перечень доступных версий программного обеспечения на сайте Cisco.com, которые могут быть загружены на локальный сервер и в дальнейшем установлены несколько раз. Эта функция значительно экономит время, необходимое на поиск нужного образа ПО.

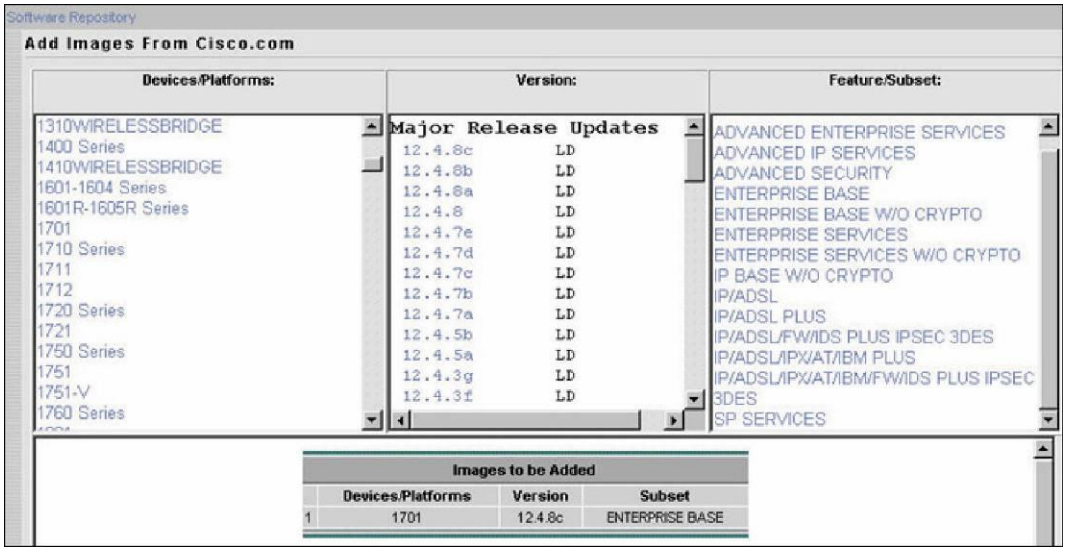


Рисунок 5. Добавление в библиотеку образа программного обеспечения

- **Шаг 3 — Создание задачи для установки программного обеспечения**. Пользователь создает задачу установки программного обеспечения и указывает время и группу устройств, на которой нужно обновить IOS. Установка ПО может выполняться с использованием различных методов:
  - **Простой.** При использовании данного метода установки можно выбрать группу устройств и выполнить установку программного обеспечения на них. Система проверит текущую версию ПО оборудования и предложит для установки подходящую версию Cisco IOS.
  - **По устройствам.** При использовании данного метода пользователь сам выбирает необходимую версию ПО и указывает его расположение на диске для устройства или группы устройств. Перед установкой система производит проверку возможности установки выбранного образа программного обеспечения.
  - **По версии программного обеспечения.** При использовании данного метода у пользователя есть возможность выбрать необходимую версию программного обеспечения и выполнить ее установку на всех устройствах в сети, для которых применимо выбранное ПО.
  - **Использование удаленного устройства.** При использовании данного метода можно выбрать необходимую версию программного обеспечения, временно сохранить ее на сетевом устройстве и в дальнейшем производить установку образа IOS с данного устройства. Эта функция особенно удобна в случаях, когда сервер Resource Manager Essentials и сетевые устройства находятся в разных сегментах сети, соединенных каналами связи с невысокой пропускной способностью.

Сбор текущих установленных версий программного обеспечения
После запуска системы рекомендуется импортировать все версии программного обеспечения, установленные в данный момент на оборудовании. Система импортирует копии образов установленного программного обеспечения и сохраняет их в библиотеке. Импортированные резервные копии могут понадобиться в случае выхода из строя или замены оборудования, когда необходимо быстро восстановить работоспособность сети. В процессе эксплуатации системы пользователь может получить отчет об устройствах,

для которых нет резервной копии ПО.

Методы загрузки программного обеспечения на оборудование
Для загрузки программного обеспечения RME может использовать несколько протоколов. Порядок использования протоколов настраивается в конфигурации системы. Во время загрузки ПО система использует первый протокол в списке. Если происходит ошибка, RME пробует использовать следующий протокол, и так до тех пор, пока операция не будет проведена успешно или не будут перебраны все заданные протоколы. Для загрузки ПО поддерживаются протоколы RCP, TFTP, SCP и HTTP.

3.2.4. Управление конфигурациями

Модуль управления конфигурациями (Configuration Manager) реализует 3 функции:

- **Архивирование (Archive Management)**

  Функция архивирования обслуживает архив конфигураций оборудования, которое находится под управлением RME, и обеспечивает решение следующих задач.

  ◦ Получение, архивирование и восстановление конфигурации устройства.

  ◦ Получение файла конфигурации на основании сообщения Syslog для синхронизации информации, хранящейся в базе данных, с новой конфигурацией устройства.

  ◦ Возможность формирования отчетов по данным в архиве.

  ◦ Возможность сравнения версий конфигураций и проверки на соответствие принятым стандартам и правилам..

- **Редактор конфигурации (Config Editor)**

  Редактор конфигурации используется для изменения конфигурации устройства, сохраненной в архиве, и загрузки новой конфигурации на устройство. Функция редактирования конфигурации дает пользователю возможность вносить изменения в любую сохраненную версию конфигурации, просматривать изменения и загружать изменения на устройство.

  После открытия в редакторе файл конфигурации блокируется от изменений другими пользователями. Попытка открытия данного файла другим пользователем будет сопровождаться сообщением о том, что файл уже редактируется и будет открыт в режиме «только для чтения». Файл будет находиться в заблокированном состоянии до момента загрузки на устройство или закрытия пользователем, который начал вносить изменения первым.

- **Функция Netconfig**

  Функция NetConfig предоставляет возможность изменения конфигурации одного устройства или группы устройств с помощью шаблонов. Использование шаблонов позволяет значительно сократить время внесения изменений на сетевых устройствах в случае глобальных изменений в сети. Шаблон может состоять из одной или нескольких команд IOS и выполняться на группе устройств параллельно. Например, для повышения уровня безопасности системный администратор может регулярно с помощью одного и того же шаблона изменять пароль (community) для доступа к устройству по протоколу SNMP. Копия обновленного файла конфигурации будет сохранена в архиве RME. NetConfig поставляется с набором подготовленных шаблонов, которые могут использоваться сразу после установки системы. Шаблоны содержат команды отката на

предыдущую версию конфигурации, что может быть полезно в случае возникновения ошибки.

Для работы с конфигурациями используется несколько протоколов. В систему заложен алгоритм использования протоколов в определенном порядке. Порядок может быть изменен администратором LMS для каждого приложения в отдельности.

Доступные протоколы:

- Telnet
- TFTP (Trivial File Transport Protocol)
- RCP (Remote copy protocol)
- SSH (Secure Shell)
- SCP (Secure Copy Protocol)
- HTTPS (Hyper Text Transfer Protocol Secured)

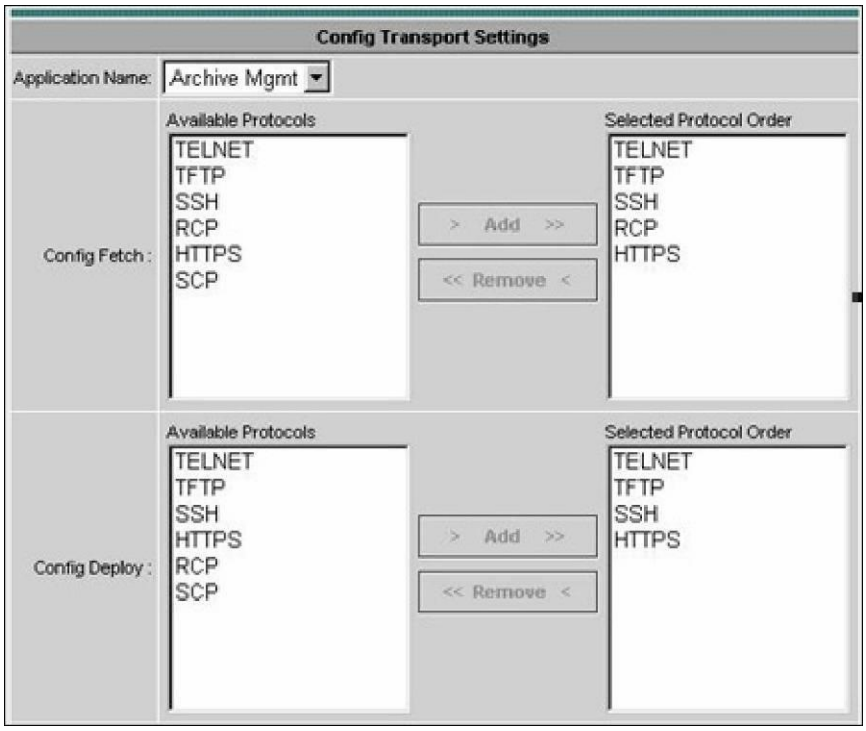


Рисунок 6. Настройка используемых протоколов в RME

По умолчанию в LMS хранятся все версии файлов конфигураций, но для экономии дискового пространства можно установить максимальное время хранения конфигурации. Файлы конфигураций могут удаляться по нескольким критериям:

- По сроку хранения. Система может удалять файлы, хранящиеся определенное время.
- По максимальному количеству хранимых версий.

3.3. Управление устройствами с помощью CiscoView

Приложение CiscoView обеспечивает отображение графического представления устройства и его параметров в режиме реального времени. С помощью графического интерфейса пользователь может производить настройку устройства и в режиме

реального времени просматривать статистику по интерфейсам, использованию ресурсов и производительности устройства.

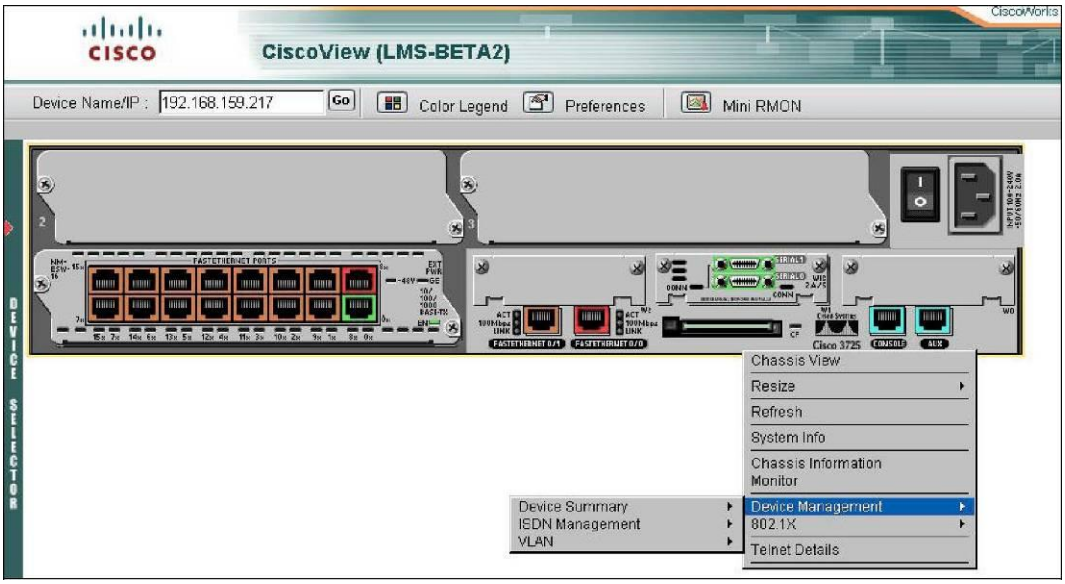


Рисунок 7. Окно приложения CiscoView

Функции, поддерживаемые приложением CiscoView:

- Отображение графического представления устройства и статуса всех компонентов, включая интерфейсы, модули, блоки питания и состояние световых индикаторов.
- Настройка параметров устройства, модулей и интерфейсов.
- Мониторинг состояния интерфейсов, использования ресурсов и производительности устройства.
- Настройка параметров пользователей.
- Выполнение специфических операций для каждого устройства. Например, изменение мощности портов PoE.
- Управление группой коммутаторов в стеке.

3.3.1. Использование Mini-RMON

CiscoView Mini-RMON — это модуль, которое позволяет включить сбор данных RMON с последующим сбором и отображением статистики по портам Ethernet в режиме реального времени. Пользователь может производить мониторинг интересующих его параметров, устанавливая граничные значения для собираемых данных. Если значение параметра выходит за пределы граничных значений, пользователь получит извещение об этом событии.

Детальная информация по Mini-RMON доступна по ссылке

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000_d/cs303/cv_ug/ug_app.htm.

3.3.2. Модуль Device Center

Модуль Device Center позволяет пользователям просматривать всю основную информацию об устройстве, а также выполнять диагностику оборудования. На панели “Summary” отображается информация об IP-адресе устройства, его типе, общие сводные данные по изменениям конфигурации оборудования за последние 24 часа и информация о неполадках, связанных с данным устройством.

Модуль Device Center также предоставляет ряд функций, которые позволяют проводить диагностику устройства, формировать отчеты или выполнять действия по администрированию устройства, например, изменять параметры доступа к устройству.

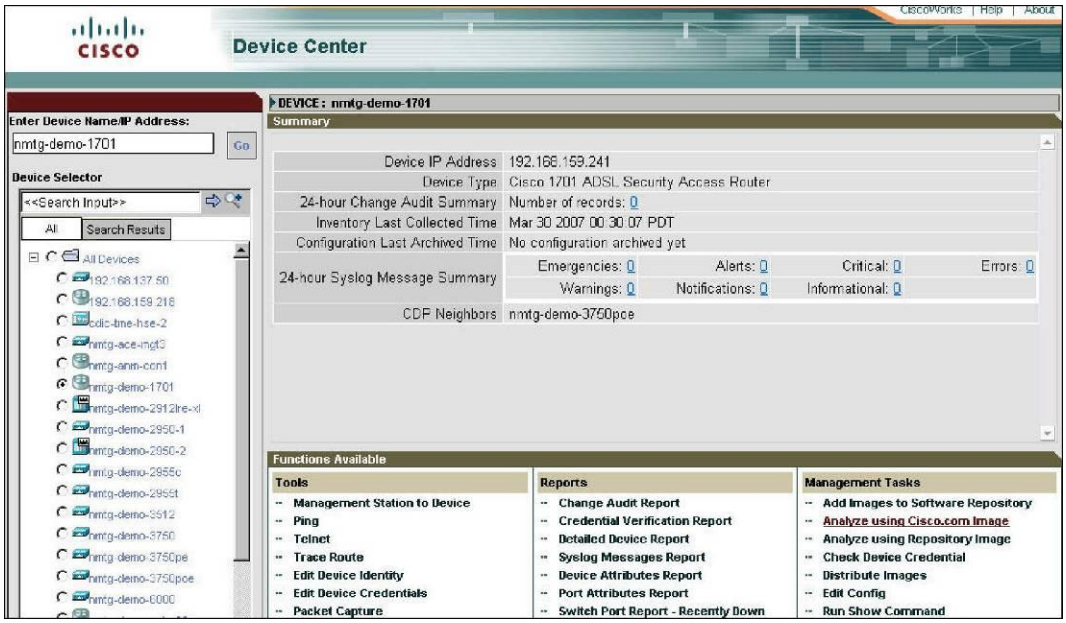


Рисунок 8. Окно модуля CiscoWorks Device Center

4. Управление сетью: приложение Campus Manager

4.1. Сценарии использования

Приложение LMS Campus Manager выполняет функции управления сетью и помогает администратору сети дать ответы на следующие вопросы:

- Как автоматически отображать топологию сети и просматривать ежедневные изменения топологии?
- Как диагностировать проблемы на канальном уровне, возникающие в работе VLAN или Spanning Tree, без последовательной проверки каждого коммутатора с помощью CLI вручную?
- Каким образом проанализировать путь прохождения данных между устройствами без проверки физического подключения кабелей?
- Как найти точки подключения пользователей и компьютеры, которые перемещаются в пределах сети?
- Как найти порт, к которому подключен IP-телефон?

4.2. Модули приложения Campus Manager

Приложение Campus Manager состоит из 2-х модулей, которые представлены на рисунке 9.

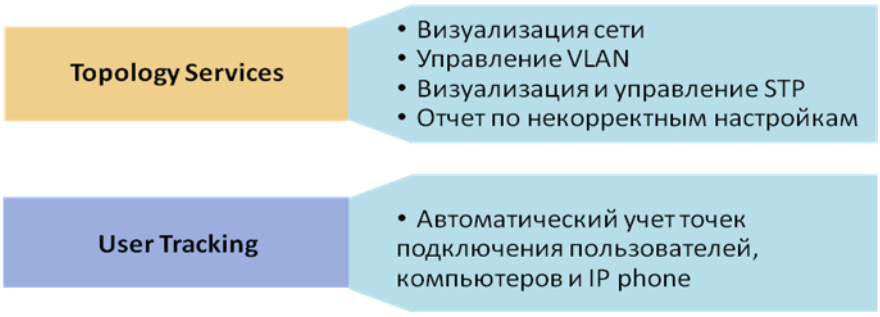


Рисунок 9. Модули Campus Manager

Модуль работы с топологией
Модуль работы с топологией (Topology Services) позволяет администратору значительно сократить время на поиск устройств и их точек подключения в сети. Данный модуль автоматически отображает топологию сети в графическом виде и позволяет администратору настраивать домены VTP и виртуальными сетями VLAN, с помощью графического интерфейса. Пользователь всегда может создать новую сеть VLAN или изменить существующую без ручного ввода команд на оборудовании. Для проверки корректности настроек оборудования можно получить отчет (Discrepancy Report), в котором будет приведена информация о несоответствиях в конфигурации устройств, что позволяет сократить время на поиск причины неполадок в работе сети.

Модуль отслеживания пользователей
В больших сетях администраторам сети нередко приходится сталкиваться с проблемой поиска точки подключения пользователей. Модуль отслеживания пользователей (User Tracking) автоматически идентифицирует все устройства, подключенные к сети, включая принтеры, серверы и рабочие станции пользователей. Данный модуль также собирает

подробную информацию о каждом устройстве, включая MAC-адрес, IP-адрес, доменное имя, интерфейс подключения и номер VLAN. Кроме того, модуль User Tracking может быть настроен на сбор сведения об учетных записях пользователей, которыми они пользуются на рабочих станциях, что позволяет быстро определить точку подключения пользователя к сети. Данная информация может собираться с компьютеров, работающих под управлением UNIX, с контроллера домена Windows или Novell Directory Services.

Campus Manager поддерживает динамический режим отслеживания пользователей. Данный режим работы детально описан ниже.

4.2.1. Определение топологии и управление сетью

В процессе поиска устройств в сети и определения топологии Campus Manager использует протокол SNMP для получения данных из таблиц Cisco Discovery Protocol (CDP), что позволяет определить и построить топологию сети. После получения первичной информации об устройствах, подключенных к сети, Campus Manager собирает дополнительную информацию о каждом устройстве, включая имена интерфейсов, данные протокола STP, информацию о доменах VTP, конфигурацию VLAN и таблицы CAM.

В версии LMS 3.0 возможности по определению топологии сети были значительно усовершенствованы. Приложение Common Services дополняет возможности Campus Manager, используя для определения топологии данные BGP, OSPF, ARP, HSRP и других протоколов, а также позволяет произвести поиск устройств по указанному диапазону IP-адресов с помощью команды ping.

Все собранные данные сохраняются в базе данных и автоматически обновляются с заданной периодичностью. Все сохраненные данные могут быть легко получены пользователем системы с помощью различных отчетов, доступных в Campus Manager.

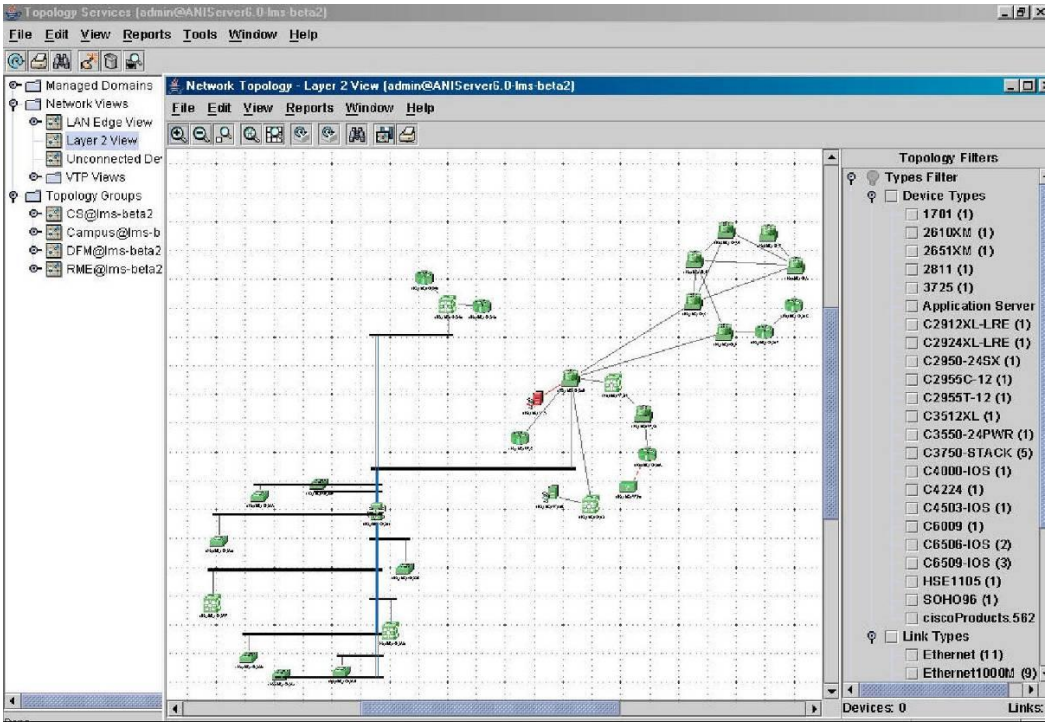


Рисунок 10. Окно модуля Topology Services

Приложение Campus Manager поставляется с набором предопределенных представлений, которые позволяют вывести на экран информацию об устройствах определенных типов или об определенных сегментах сети.

Таблица 3. Представления в приложении Campus Manager

Представление	Описание	Доступные данные и функции
LAN Edge View	Отображает топологию подключения устройств на сетевом уровне (Layer 3). Устройства, которые не предоставляют функций работы на сетевом уровне, доступны в представлении Switch Cloud View.	Параметры устройств Параметры портов Параметры соединений IP-адреса Настройка маршрутизации Inter-VLAN Удаление соединений
Switch Cloud View	Отображает устройства, работающие на канальном уровне (Layer 2) между двумя устройствами сетевого уровня (Layer 3)	Параметры устройств Параметры портов Параметры сервисов Параметры соединений Параметры транковых соединений IP-адреса Отчет по VLAN Отчет TDR Настройка маршрутизации Inter-VLAN Настройка EtherChannel Создание транковых соединений
Layer 2 View	Отображает топологию сети на канальном уровне.	Параметры устройств Параметры портов Параметры сервисов Параметры соединений Параметры транковых соединений IP-адреса Отчет по VLAN Отчет TDR Настройка маршрутизации Inter-VLAN Настройка EtherChannel Создание транковых соединений
Unconnected Devices View	Отображает устройства, по которым не удалось собрать данные по их связям с другими устройствами, или устройства, которые не поддерживаются модулем Topology Services.	Параметры устройств Параметры портов Параметры соединений IP-адреса Отчет по VLAN Настройка маршрутизации Inter-VLAN
VTP Views	Отображает устройства, которые входят в VTP-домен.	Параметры устройств Параметры портов Параметры сервисов Параметры соединений Параметры транковых соединений Отчет по VLAN Отчет TDR Настройка маршрутизации Inter-VLAN Настройка EtherChannel Создание транковых соединений

Настройка карты

Пользователь может добавить географическую карту в качестве фона для отображения топологии сети и разместить устройства в соответствии с их географическим положением. Для больших сетей есть возможность объединять оборудование в

топологические группы (Topology Groups) и организовывать иерархические карты. Например, можно создать одну группу устройств для головного офиса и несколько групп для филиалов.

Отчетность

Ряд отчетов может быть получен непосредственно из окна Network Topology. Перечень доступных отчетов зависит от открытой карты (представления). Например, для представления “Layer 2 View” пользователь увидит список отчетов, представленный на рисунке 11.

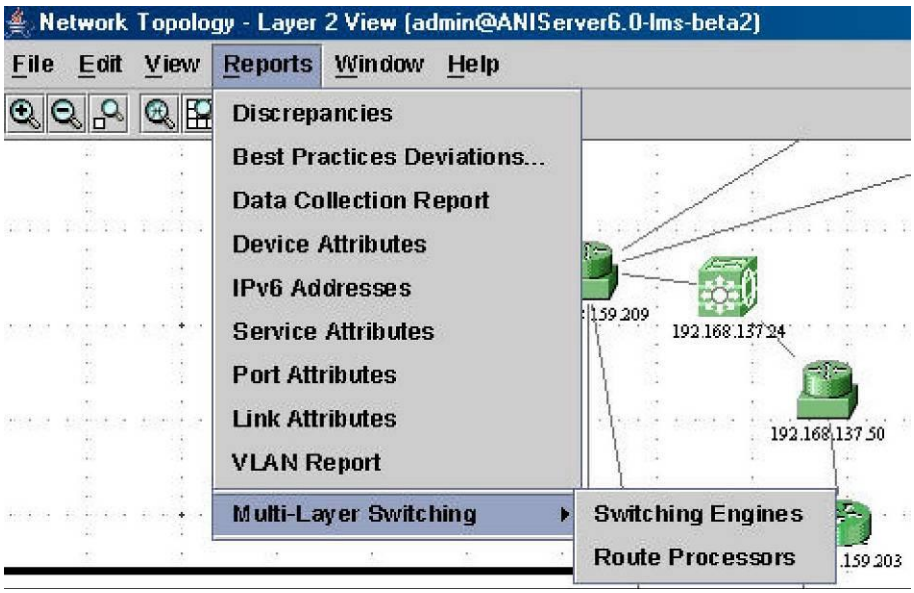


Рисунок 11. Отчеты Campus Manager для представления «Layer 2»

Настройка сетевых устройств

Модуль работы с топологией предоставляет возможность управления сетевыми настройками устройств с помощью графического интерфейса. Все команды, которые могут быть выполнены на устройстве, сгруппированы в меню Tools, как указано на Рисунке 12.

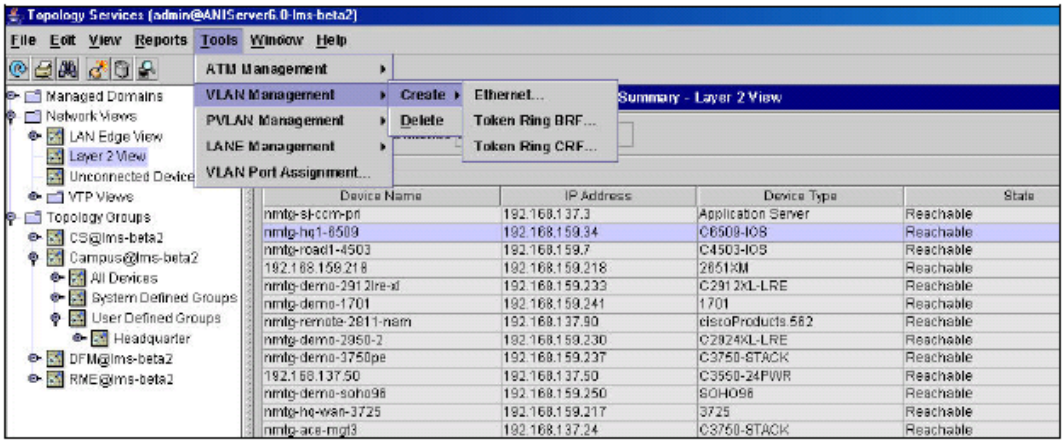


Рисунок 12. Управление VLAN

Перечень доступных команд и их описание представлены в таблице «Перечень команд

для настройки устройств». Некоторые команды (например, изменение параметров интерфейса) доступны только пользователям с правами сетевого или системного администратора.

Таблица 4. Перечень команд для настройки устройств

Команда	Описание
VLAN Management -> Create	Создание VLAN для сетей Ethernet, Token Ring BRF или Token Ring CRF.
VLAN Management -> Delete	Удаление VLAN.
PVLAN Management -> Create	Создание Private VLAN.
PVLAN Management -> Delete	Удаление Private VLAN.
LANE Management -> Add/Modify LANE Services	Добавление или модификация сервисов LANE для Ethernet VLAN, Token Ring CRF или ATM-VLAN.
LANE Management -> Configure Config Server	Настройка основного и резервного серверов LE Config.
VLAN Port Assignment	Изменение номера VLAN на порту в пределах домена VTP.
ATM Management -> Display VCs	Отображение списка виртуальных соединений на устройстве или между устройствами.
ATM Management -> Create SPVC/SPVP	Создание SPVC или SPVP.
ATM Management -> OAM Ping	Выполнение OAM ping для проверки доступности соединения
ATM Management -> Interface Configuration	Изменение параметров интерфейса ATM.
ATM Management -> RMON Data Collection	Отключение сбора данных RMON.
ATM Management -> Template Manager	Создание или изменение шаблонов трафика

4.2.2. Отслеживание пользователей

Периодическое отслеживание пользователей
Модуль отслеживания пользователей позволяет найти точку подключения рабочей станции к сети и предоставляет данные, которые могут понадобиться для диагностики и анализа проблем с доступностью. Приложение идентифицирует все устройства, подключенные к оборудованию Cisco, включая принтеры, серверы, рабочие станции и IP-телефоны с помощью периодического опроса сети.

Данные о подключенных устройствах могут быть получены несколькими методами:

- Разовый опрос всех устройств и наполнение базы данных (Major Acquisition)
- Отслеживание изменений в сети (например, подключение устройства к порту коммутатора) и периодическое обновление базы данных (Minor Acquisition)

Отслеживание изменений происходит автоматически с предопределенным интервалом времени, составляющим по умолчанию 60 минут. Интервал может быть изменен администратором системы.

После наполнения базы данных пользователь может получить отчет, представленный на рисунке 13, в котором указывается имя пользователя и порт устройства, к которому он подключен.

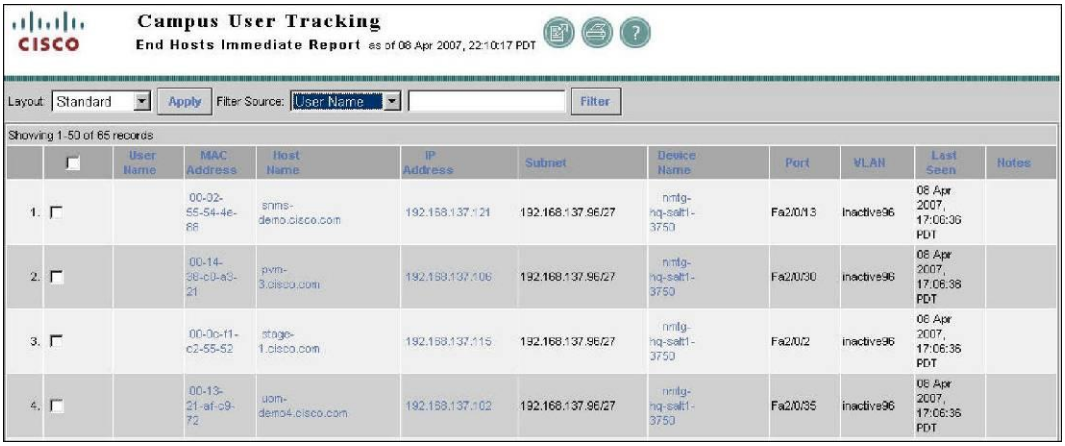


Рисунок 13. Отчет «Отслеживание пользователей в Campus Manager»

Чтобы поле «имя пользователя» не оставалось пустым, необходимо установить модуль UTLite. Данный модуль позволяет получать информацию с контроллера домена Windows NT, из Windows Active Directory и с серверов Novell. Таким образом, администратор может получить информацию не только о том, где подключена рабочая станция, но и том, кто сейчас на ней работает.

Для удобства работы с системой администратор может установить на свою рабочую станцию дополнительный модуль, User Tracking Utility. Данный модуль встраивается в панель задач Windows и позволяет выполнять быстрый поиск рабочих станций и пользователей в сети без обращения к интерфейсу CiscoWorks.

Динамическое отслеживание пользователей
Приложение Campus Manager может получать SNMP-сообщения «trap» о регистрации на оборудовании новых MAC-адресов, что позволяет отслеживать перемещения пользователей в режиме реального времени. SNMP-сообщение «trap» отсылается сразу же после подключения устройства, например, рабочей станции, к коммутатору. В этом сообщении содержится значение MAC-адреса подключенного устройства. При отключении устройства Campus Manager получает подобное SNMP-сообщение «trap» и заносит в базу данных информацию об отключении.

Основные различия между механизмами периодического и динамического отслеживания пользователей:

- В режиме периодического отслеживания данные собираются с определенным интервалом времени.
- В режиме динамического отслеживания данные собираются в режиме реального времени по факту подключения или отключения устройства.

5. Управление отказами: приложение Device Fault Manager

5.1. Сценарии использования

Приложение Device Fault Manager (DFM) используется в ежедневной работе администратора сети и помогает дать ответы на вопросы:

- Как обнаружить причину неполадки в сети для устранения проблемы?
- Как обеспечить не только мониторинг работоспособности, но и превентивный контроль потенциальных проблем?
- Как обнаружить проблему до того, как снижение сервиса повлияет на пользователей?
- Как минимизировать время простоя?

Приложение CiscoWorks Device Fault Manager обеспечивает мониторинг оборудования. В DFM заложена информация о том, какие параметры оборудования необходимо контролировать для проверки работоспособности устройств, что позволяет сетевому администратору определить точную причину неполадки.

5.2. Архитектура DFM

Приложение DFM использует протокол SNMP для постоянного опроса оборудования и принимает SNMP-сообщения «trap» для оперативного обнаружения отказов. DFM с помощью внутренней логики анализирует сообщения и определяет место отказа и его критичность. На основании полученных данных DFM может оповестить заинтересованных пользователей. Все полученные данные сохраняются во внутренней базе данных и хранятся 31 день для последующей обработки.

Архитектура приложения DFM и процесс взаимодействия его модулей представлены на рисунке 14.

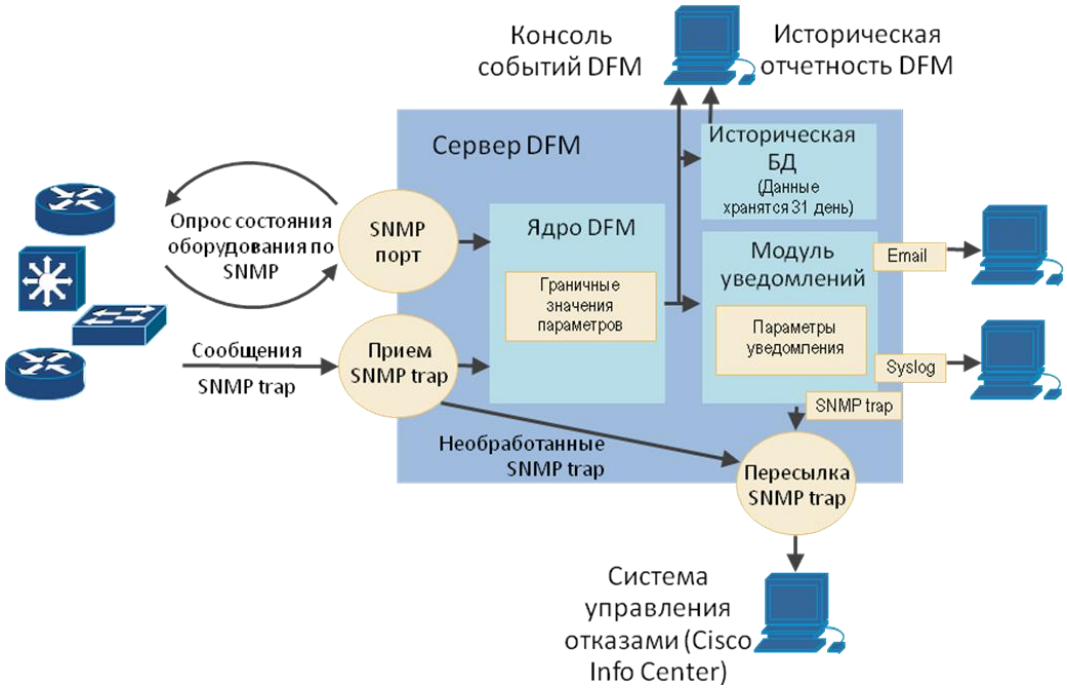


Рисунок 14. Архитектура DFM

В DFM также заложена информация о переменных SNMP MIB, которые необходимо проверять на каждом устройстве для контроля состояния устройства и его компонентов. Для некоторых параметров в системе предустановленны граничные значения, при превышении которых пользователь получит соответствующее уведомление. Администратор системы может изменить настройки по умолчанию или добавить новые граничные значения в зависимости от требований к мониторингу.

Приложение DFM может использоваться сразу после его установки — предустановленная конфигурация позволяет контролировать устройства сразу после их регистрации в системе мониторинга.

5.3. Консоль событий в DFM

Основным рабочим окном приложения CiscoWorks DFM является консоль событий. В данном окне отображаются как сообщения, полученные от оборудования (SNMP-сообщения «Trap"), так и события, созданные DFM во время периодического опроса оборудования.

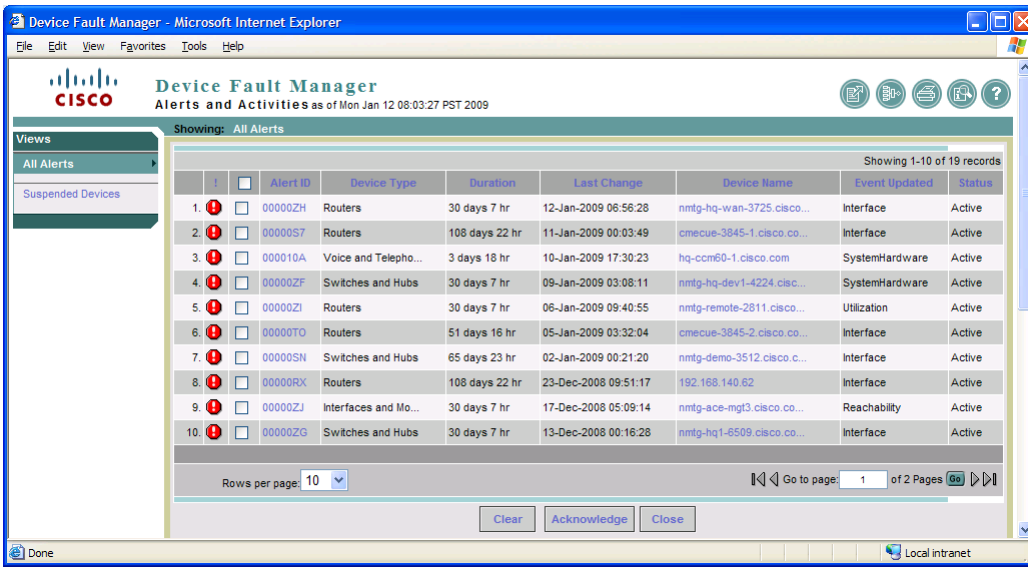


Рисунок 15. Консоль событий в DFM

Пользователь может просмотреть детали по каждому событию путем перехода по ссылке, представленной в поле Alert ID.

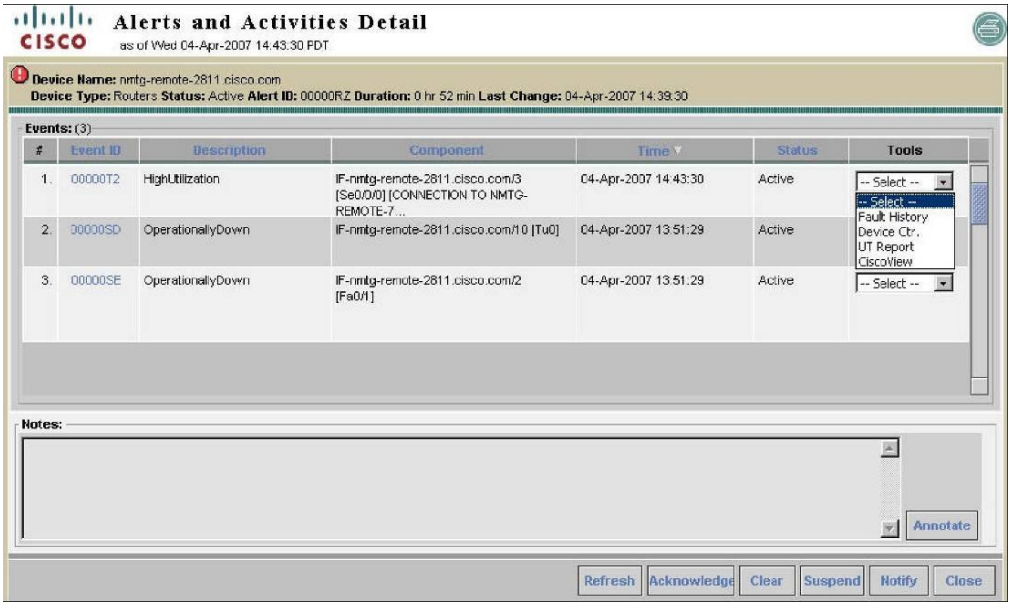


Рисунок 16. Детализация по событию

В одном событии может быть сгруппировано несколько аварийных сообщений. Для каждого сообщения пользователь может выполнить несколько действий:

- **Acknowledge.** Изменить статус сообщение на подтвержденное.
- **Clear.** Удалить событие и все сообщения по этому событию.
- **Suspend.** Приостановить прием SNMP-сообщений «trap» и периодический опрос по данному устройству или модулю устройства.
- **Notify.** Отослать уведомление по электронной почте.
- **Fault History.** Сформировать отчет по событиям по устройству или его модулям за последние 24 часа.
- **Device Ctr.** Открыть окно приложения CiscoWorks Device Center для выполнения действий по диагностике оборудования или построению отчетов.
- **UT Report.** Сформировать отчет «User Tracking End Host», который позволяет просмотреть перечень подключенных к оборудованию пользователей и серверов.
- **CiscoView.** Открыть окно приложения CiscoView с графическим изображением устройства.

5.4. Уведомление пользователей

Мониторинг сети с помощью консоли событий требует постоянного внимания пользователя. Приложение DFM позволяет настроить механизм уведомления пользователей, чтобы освободить сетевого администратора от постоянного наблюдения за экраном компьютера. Уведомления могут быть отправлены в виде сообщения электронной почты, а также в виде SNMP-сообщений «trap» и сообщений Syslog. Вне зависимости от выбранного метода в каждом уведомлении будет содержаться краткая информация о событии, произошедшему в сети. Для просмотра более подробной информации о проблеме получатель уведомления может открыть окно приложения DFM.

Для получения информации о проблемах пользователю необходимо подписаться на определенную группу уведомлений (Notification Group). Группа уведомлений — это

перечень событий для определенной группы устройств. Данный механизм позволяет пользователю получать только интересующие его аварийные сообщения.

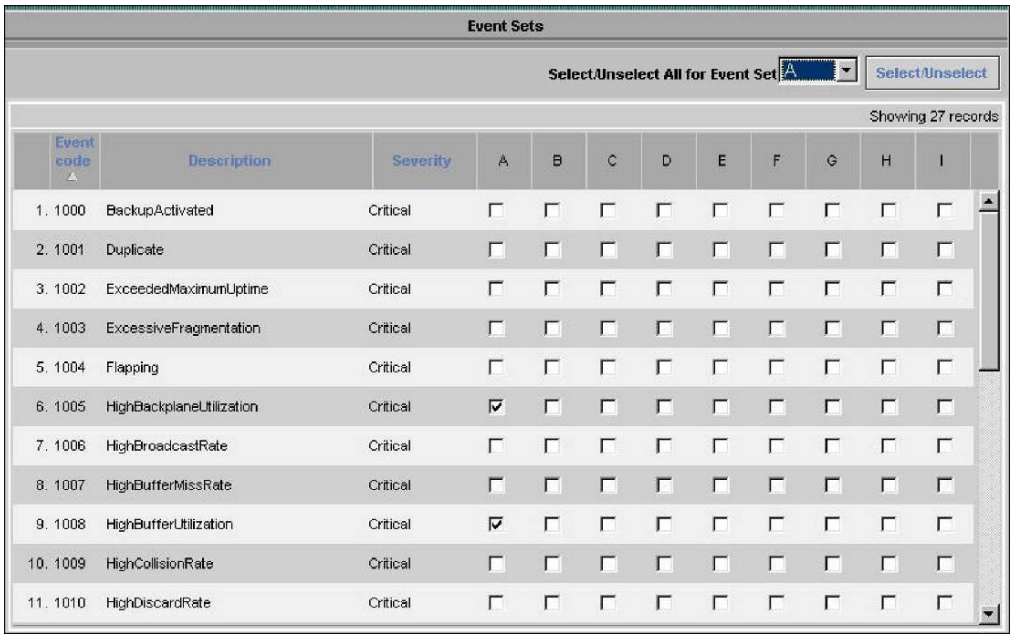


Рисунок 17. Настройка группы уведомлений в DFM

5.5. Опрос параметров устройства и установка граничных значений

Получения аварийных сообщений по факту прерывания связи или выхода из строя какого-то модуля устройства недостаточно для обеспечения полноценного мониторинга сети. Большинство сетевых неполадок можно предсказать за некоторое время до их появления путем мониторинга за состоянием параметров устройств. DFM позволяет установить периодичность опроса параметров, а также граничные значения, о превышении которых DFM сообщит с помощью соответствующей записи в консоли событий.

Приложение DFM поставляется с предустановленной конфигурацией по граничным значениям, которые могут быть изменены и дополнены пользователем самостоятельно.

Группы устройств
Все устройства объединяются в системные группы сразу после загрузки устройств из DCR в DFM. Для каждой группы существуют предустановленные значения частоты опроса параметров и граничные значения. В решении CiscoWorks LMS предусмотрены 3 типа системных групп:

- группы портов доступа,
- группы интерфейсов,
- группы транковых портов.

Пользователь может создать свою группу устройств, определить перечень параметров для контроля, а также указать частоту опроса и граничные значения. DFM позволяет создать до 28 пользовательских групп.

6. Управление производительностью: приложения Internetwork Performance Monitor и Health and Utilization Monitor

6.1. Сценарии использования

Современная ИТ-инфраструктура каждой компании оказывает непосредственное влияние на ее работоспособность. Компании не могут себе позволить использовать ненадежные или неконтролируемые сети. Сегодня операторы связи и ИТ-подразделения вводят практику предоставления соглашений об уровне обслуживания (SLA – Service Level Agreement) для обеспечения надежности и предсказуемости работы сети. На первый план выходят задачи измерения времени ответа сетевых устройств и приложений, определение коэффициента доступности оборудования, анализ показателей качества работы сетевой инфраструктуры и формирование оперативной и исторической отчетности для принятия решения по внедрению каких-либо изменений в сети.

Используя технологию Cisco IOS IP SLA, приложение CiscoWorks Internetwork Performance Monitor (IPM) обеспечивает сквозной мониторинг параметров производительности сети. IPM проводит измерения параметров производительности между двумя выбранными точками в сети и позволяет оценить качество работы сети с точки зрения пользователя. С помощью IPM можно измерить и отобразить статистику по пяти ключевым показателям: задержка передачи пакетов (latency), доступность (availability), вариации задержки (jitter), потери пакетов (packet loss) и ошибки передачи данных.

Детальная информация по Cisco IOS IP SLA доступна на сайте Cisco: http://www.cisco.com/go/ipsla.

Приложение CiscoWorks Health and Utilization Monitor (HUM) использует протокол SNMP для получения параметров производительности каждого устройства и его модулей. С помощью HUM можно измерить загрузку центрального процессора устройства, объем используемой памяти, нагрузку на интерфейсах и сетевых соединениях и любые другие параметры, доступные через SNMP MIB.

CiscoWorks HUM обеспечивает контроль каждого устройства в отдельности, в том время, как IPM позволяет контролировать параметры работы сети в целом.

6.2. Мониторинг производительности сети с помощью IPM

6.2.1. Обзор приложения IPM

Приложение Internetwork Performance Monitor (IPM) позволяет измерять производительность сети. Для этого IPM взаимодействует с функцией Cisco IOS IP SLA, выполняя ее настройку и сбор результатов работы на устройствах Cisco.

IPM используется для решения следующих задач.

- Диагностика проблем в сети.
- Настройка маршрутизаторов для отсылки SNMP-сообщений «trap» по факту превышения предустановленных граничных значений параметров

производительности.

- Формирование табличной и графической отчетности по параметрам производительности.
- Измерение сетевых задержек, показателй доступности и вариации задержки между двумя узлами сети.
- Мониторинг потери пакетов и ошибок между двумя узлами сети.
- Определение пути передачи трафика между двумя узлами сети и контроль производительности сети на каждом участке пути.
- Мониторинг доступности серверов.
- Контроль выполнения соглашений об уровне обслуживания (SLA).
- Мониторинг сети в реальном режиме времени.

6.2.2. Мониторинг выполнения SLA в IPM

Технология Cisco IP SLA разработана для проведения измерений показателей производительности между любыми выбранными точками сети. Без применения данной технологии системы мониторинга могут измерять параметры производительности только между сервером системы мониторинга и каким-либо узлом в сети, что не всегда дает возможность оценить степень влияния параметров сети на работоспособность приложений, например, когда пользователь работает с центром обработки данных из удаленного офиса.

В типовом варианте применения IP SLA в выбранном месте сети, например, возле центра обработки данных, устанавливается недорогой маршрутизатор Cisco, который будет тестировать доступность и параметры работы протоколов с различными узлами сети. В качестве удаленных узлов могут выступать любые IP-устройства или оборудование Cisco.

Результаты работы каждого теста IP SLA сохраняются в оперативной памяти устройства Cisco и могут быть получены через интерфейс CLI или с использованием протокола SNMP (который используется приложением IPM).

Для измерения параметров производительности сети с помощью IPM пользователь должен определить один или несколько коллекторов IP SLA, которые будут работать на устройствах, и собирать статистику. Каждый коллектор состоит из 4 следующих компонентов:

- **Source Router.** Маршрутизатор-инициатор, на котором IPM производит измерения. Для настройки IP SLA на данном устройстве IPM использует протокол SNMP. Маршрутизатор должен работать под управлением программного обеспечения Cisco IOS с функцией IP SLA.
- **Target Router.** Устройство-получатель запросов IP SLA. Данное устройство может быть как маршрутизатором, так и любым устройством, поддерживающим стек протоколов TCP/IP. Для некоторых типов измерений устройство-получатель должно быть только маршрутизатором или коммутатором Cisco с программным обеспечением Cisco IOS.
- **Test Operation.** Тест, эмулирующий работу определенного протокола, параметры работы которого необходимо измерить. Например, для измерения задержки (latency) для сессии VoIP используется тест Enhanced UDP, который пересылает

серию пакетов UDP длиной 60 байт с установленным параметром IP-заголовка «Тип обслуживания» (Type of Service, TOS) и заданным номером порта на удаленном устройстве.

- **Collection Schedule.** Коллектор может выполнить тест один раз в определенный момент времени или может быть настроен на периодическое тестирование сети с определенным интервалом времени. Гибкость в настройке времени запуска коллектора позволяет использовать механизмы IP SLA как для постоянного мониторинга сервисов, так и для разовой диагностики сети.

Пользователь должен определить устройства-источники и получатели и настроить коллекторы IP SLA с помощью интерфейса приложения IPM. После этого устройства Cisco смогут выполнять тесты с заданной периодичностью, а приложение IPM сможет собирать и отображать оперативную статистику и историческую отчетность.

Последовательность работы пользователя с приложением IPM изображена на Рисунке 18.

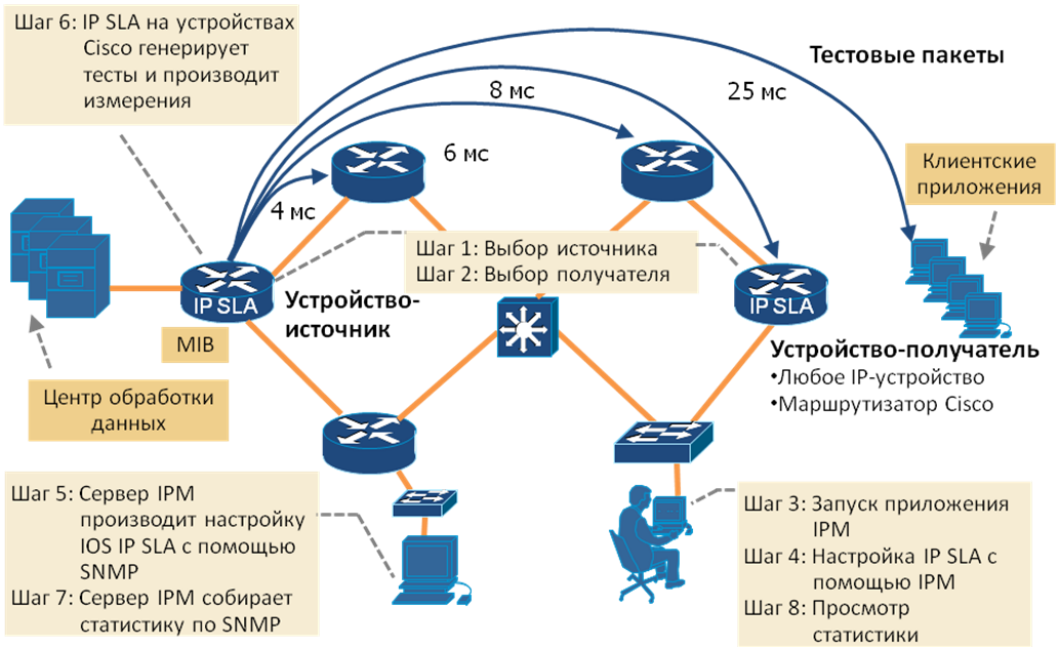


Рисунок 18. Последовательность работы с IPM

6.2.3. Типы тестов IP SLA

IPM позволяет выполнять следующие тесты:

- Контроль доступности
  - Ping Echo
  - Ping Path Echo
  - UDP Echo
- Контроль вариации задержки
  - ICMP Jitter
  - Enhanced UDP Jitter
- Контроль работы VoIP

- VoIP Post Dial Delay
- VoIP Gatekeeper Registration Delay
- RTP

- Контроль работы сервисов
  - DNS
  - DHCP
  - HTTP
  - FTP
  - DLSw
  - TCP Connect
- Контроль работы Metro Ethernet
  - Ethernet Ping
  - Ethernet Jitter
  - Ethernet Ping Auto IP SLA
  - Ethernet Jitter Auto IP SLA

Более подробную информацию о перечисленных тестах можно получить на сайте Cisco: http://www.cisco.com/en/US/products/ps6602/products_white_paper09186a00802d5efe.shtml.

Пользователи также могут создавать свои тесты для контроля работоспособности специфических сервисов.

6.2.4. Отчетность IPM

Статистика, собранная по результатам работы коллекторов IP SLA, сохраняется в базе данных IPM и может быть просмотрена в виде табличных или графических отчетов, а также экспортирована в другие системы для дальнейшей обработки.

IPM поставляется с предустановленным перечнем отчетов:

- отчеты по доступности (Availability),
- отчеты по задержкам (Latency , Round-Trip Time),
- отчеты по вариации задержки (UDP Jitter, ICMP Jitter),
- отчеты по работе протокола HTTP,
- отчеты Path Echo,
- отчеты по работе протокола RTP,
- отчеты по вариации задержки на уровне Ethernet (Ethernet Jitter).

Примеры графического и табличного отчетов приведены на рисунке 19 и рисунке 20.

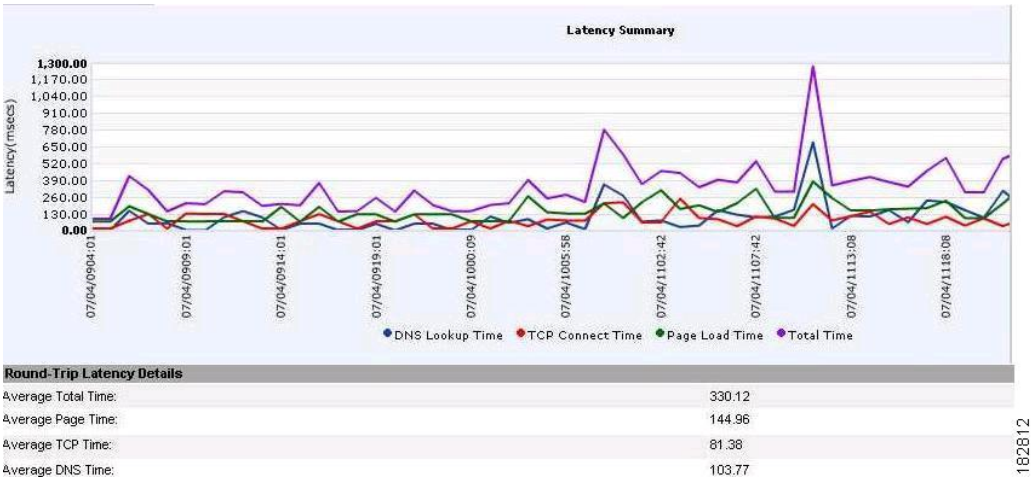


Рисунок 19. Графический отчет по сетевой задержке в приложении IPM – работа протокола HTTP

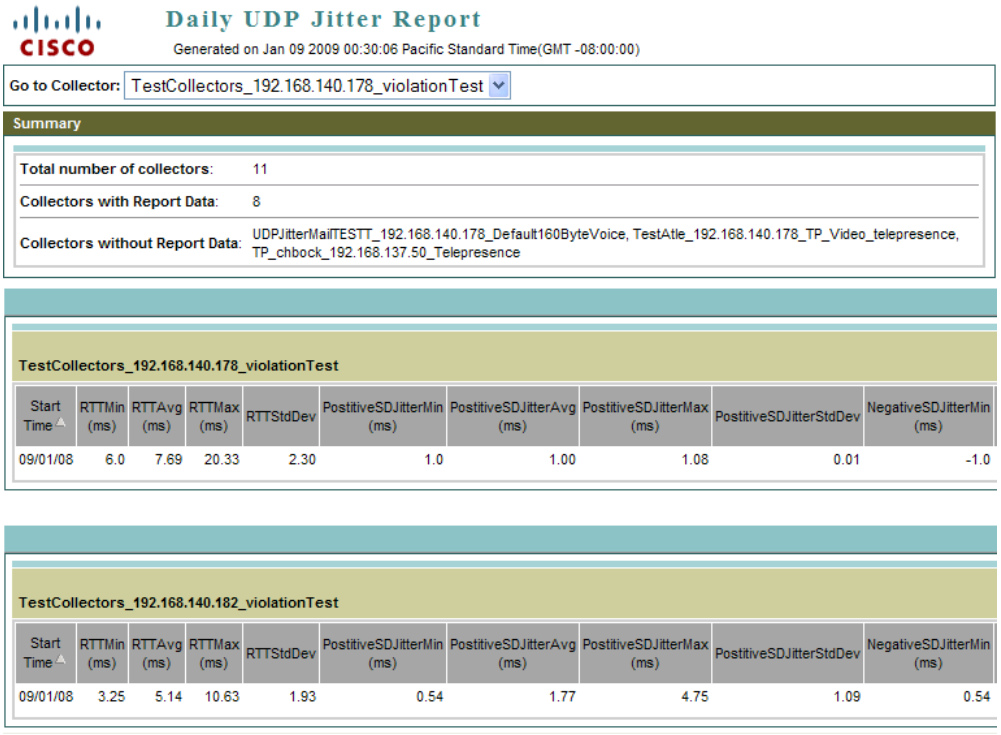


Рисунок 20. Табличный отчет по вариации задержки в приложении IPM

Табличные отчеты могут быть сформированы для разных интервалов времени: дневные, недельные и за 1 месяц. Графические отчеты формируются с шагом в 1 минуту, 1 день, 1 неделю и 1 месяц. Графические отчеты также могут выводиться в режиме мониторинга с интервалом получения статистики, равным 60 секунд, и отображением данных в режиме реального времени.

6.3. Мониторинг производительности устройств с помощью HUM

Health and Utilization Monitor (HUM) — одно из приложений решения CiscoWorks LMS, которое позволяет производить сбор статистики по производительности устройств. HUM

использует протокол SNMP для сбора данных и может обеспечить мониторинг любых параметров устройств Cisco. В частности, HUM производит мониторинг загрузки центрального процессора, памяти, интерфейсов и сетевых соединений.

Основные возможности приложения HUM:

- мониторинг загрузки процессоров, памяти, интерфейсов/портов,
- предоставление исторической отчетности,
- набор отчетов по умолчанию, входящий в комплект поставки,
- установка пороговых значений для измеряемых параметров и уведомление пользователей.

HUM не требует длительной настройки и способен работать с сетью сразу после установки приложения. В конфигурации системы указан перечень параметров для мониторинга (идентификаторы SNMP OID, значения которых будет собирать система). Пользователь может изменить или добавить свой набор параметров для мониторинга.

Приложение поставляется в комплекте с CiscoWorks LAN Management Solution (LMS), начиная с версии 3.1, и устанавливается как одно из приложений LMS. Вместе с тем, данное приложение требует отдельной лицензии.

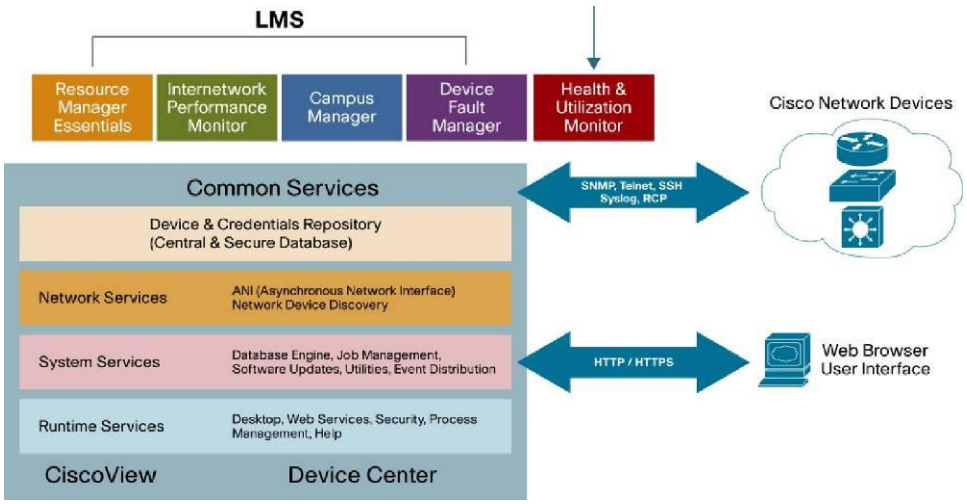


Рисунок 21. Позиционирование CiscoWorks HUM в архитектуре CiscoWorks LMS

Все собранные данные сохраняются в базе данных приложения и могут быть получены в графическом интерфейсе в виде отчетов для отображения оперативной и исторической информации (Рисунок 22).

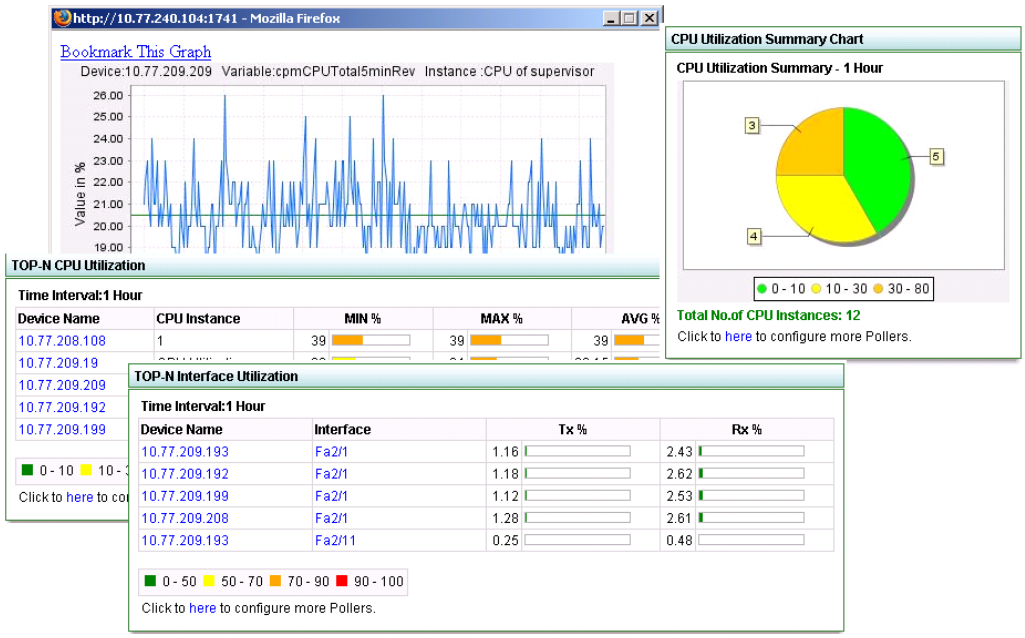


Рисунок 22. Примеры отчетов о производительности устройств в HUM

7. Управление безопасностью: использование Cisco Access Control Server

Сервер контроля доступа Cisco® Secure Access Control Server (ACS) – это комплексное решение для контроля доступа на основании идентификационных данных пользователя к интеллектуальным информационным сетям Cisco. Он предназначен для интеграции и управления пользователями и администраторами корпоративной сети, а также ресурсами сетевой инфраструктуры.

Сервер LMS обладает рядом встроенных механизмов для аутентификации пользователей и назначения ряда предопределенных прав доступа (ролей) для выполнения определенных задач. Cisco Secure ACS позволяет значительно расширить возможности решения LMS по обеспечению безопасности при работе с сетью. Возможности такой интеграции описаны дальше в данном разделе.

7.1. Обзор ACS

ACS – это приложение, обеспечивающее работу с сетью по протоколам Remote Access Dial-In User Service (RADIUS) и Terminal Access Controller Access Control System (TACACS+). ACS используется в качестве централизованного решения для контроля доступа пользователей к сетевым ресурсам и обеспечивает аутентификацию, авторизацию и учет доступа к сетевым устройствам (функции AAA), например, к серверам доступа (NAS), межсетевым экранам, коммутаторам и маршрутизаторам, а также к приложениям, таким как CiscoWorks LMS. Устройство или информационная система, где необходимо выполнить аутентификацию и авторизацию пользователя называется клиентом AAA.

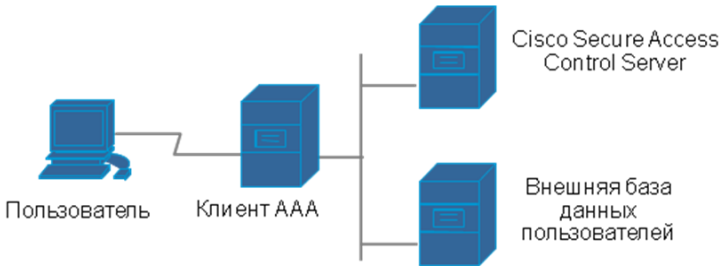


Рисунок 23. Компоненты AAA

Система CiscoWorks может быть интегрирована с сервером ACS для решения следующих задач:

- обеспечение централизованного управления пользователями для группы серверов CiscoWorks.
- Обеспечение авторизации на уровне устройств. Данный тип авторизации позволяет ограничить права пользователей при выполнении ряда задач, таких как изменения конфигурации или программного обеспечения на каждом устройстве.
- Предоставление возможности редактирования ролей пользователей. Роли в этом случае создаются в соответствии с задачами, которые пользователь может выполнять на устройствах. ACS позволяет модифицировать существующие системные роли в CiscoWorks и добавлять новые.

- Используя ACS, для каждой группы пользователей можно назначить определенную роль и связать ее с группой устройств отдельно для каждого приложения CiscoWorks. Так можно реализовать любую схему контроля доступа.

Сервер CiscoWorks будет работать как клиент AAA, наподобие сетевого устройства. В момент обращения пользователя к серверу и введения логина/пароля, CiscoWorks пошлет запрос на авторизацию на сервер ACS.

7.2. Сценарий использования ACS

Ниже приведен пример работы серверов LMS и ACS, интегрированных между собой.

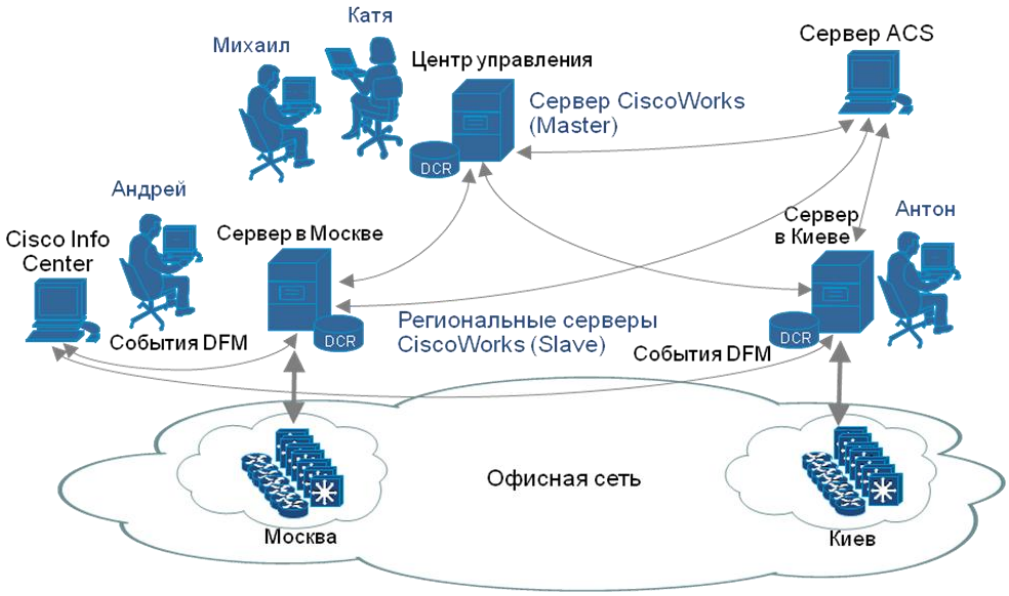


Рисунок 24. Взаимодействие LMS и ACS

В данном примере:

- Андрей работает системным администратором в Москве. Он может управлять устройствами только в сети московского офиса.
- Антон — системный администратор в Киеве. Он может управлять устройствами только в сети киевского офиса.
- Михаил и Катя работают в корпоративном центре управления. Они отвечают за работоспособность всех серверов систем управления и в случае необходимости могут управлять всеми устройствами в сети.

Для достижения такого распределения обязанностей необходимо выполнить следующие шаги.

- Определить роли согласно выполняемым задачам, назначить их пользователям и сгруппировать пользователей в группы.
- Создать несколько групп устройств: в данном примере необходимо создать группу «Киев» и группу «Москва».
- Связать группы пользователей и группы устройств.

Так можно настроить любую схему доступа к сетевым устройствам и повысить уровень безопасности сети.

8. Приложение: Перечень сокращений

Сокращение	Значение
AAA	Authentication, Authorization and Accounting
ACS	Access Control Server, программное обеспечение, реализующее функции AAA и разработанное компанией Cisco Systems, Inc.
CDP	Cisco Discovery Protocol. Протокол, разработанный компанией Cisco для определения соседних устройств.
DCR	DCR (Device and Credential Repository) - база данных информации об устройствах, из атрибутах и параметров доступа, необходимых для доступа из приложений CiscoWorks LMS.. База данных DCR используется как единый источник данных об устройствах для всех приложений CiscoWorks.
IOS	Internetwork Operating System. Программное обеспечение, используемое на оборудовании компании Cisco Systems.
LMS	LAN Management Solution
NMS	Network Management System
RCP	Remote Copy Protocol
IP SLA	Cisco IOS® IP Service Level Agreement (SLA), функция измерения параметров качества сети в программном обеспечении Cisco IOS Software. Данная функция позволяет исключить дополнительные затраты со стороны заказчика на установку оборудования для измерения качества работы сети.
SCP	Secure Copy Protocol
STP	Spanning Tree Protocol
Single Sign-On	Технология, которая позволяет работать с несколькими приложениями с одноразовой авторизации пользователя. Технология применяется в решении CiscoWorks и позволяет переключаться между приложениями на разных серверах без дополнительной авторизации на каждом сервере.
SNMP	Simple Network Management Protocol
SSH	Secure Shell Protocol
SSL	Secure Socket Layer. Протокол шифрования данных
STP	Spanning Tree Protocol. Протокол, который позволяет предотвратить создание петель в коммутируемых сетях
TACACS+	Terminal Access Controller Access Control System Plus. Протокол для авторизации пользователей на оборудовании.
VLAN	Virtual Local Area Network
VTP	VLAN Trunking Protocol

Cisco
Россия, 115054, Москва,
бизнес-центр
«Риверсайд Тауерс»
Космодамианская наб.,
52, стр. 1, этаж 4
Тел.: +7 (495) 961 14 10
Факс: +7 (495) 961 14 60
www.cisco.ru
www.cisco.com

Cisco
Россия, 191186,
Санкт-Петербург,
бизнес-центр «Регус»
Невский проспект, 25,
этаж 2, офис 30
Тел.: +7 (812) 346 77 17
Факс: +7 (812) 346 78 00
www.cisco.ru
www.cisco.com

Cisco
Казахстан, 480099,
Алматы,
бизнес-центр «Самал 2»
Ул. О. Жолдасбекова, 97,
блок А2, этаж 14
Тел.: + 7 (727) 244 21 01
Факс: + 7 (727) 244 21 02
www.cisco.ru
www.cisco.com

Cisco
Украина, 03038, Киев,
бизнес-центр
«Горизонт Парк»
(Horizon Park)
Ул. Николая Гринченко, 4В
Тел.: + 7 (38044) 391 36 00
Факс: + 7 (38044) 391 36 00
www.cisco.ua
www.cisco.com

Cisco
Азербайджан,
AZ 1065, Баку,
бизнес-центр «Карат»
Ул. М. Мухтарова, 201,
этаж 2
Тел.: + 7 (99412) 437 48 20
Факс: + 7 (99412) 437 48 21
www.cisco.ru
www.cisco.com

Cisco
Узбекистан, 100000,
Ташкент, бизнес-центр
«ИНКОНЕЛЬ»
Ул. Пушкина, 75, офис 605,
этаж 6
Тел.: + 7 (99871) 140 44 60
Факс: + 7 (99871) 133 44 64
www.cisco.ru
www.cisco.com

Cisco has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong • SAR • Hungary • India • Indonesia • Ireland • Israel •Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe