

Microsoft®
System Center
Operations Manager 2007

**Руководство по пакету управления Metrex Cisco для
System Center Operations Manager 2007 R2.**

Metrex Engineering

Опубликовано: Ноябрь 2009г

Оглавление

Введение в руководство по пакету управления Metrex Cisco	4
Версия документа	4
Получение последнего пакета управления и документации к нему	4
Поддерживаемые конфигурации	4
Приступая к работе	6
Перед импортом пакета управления.....	6
Обнаружение сетевых устройств Cisco.....	6
Файлы данного пакета управления	7
Прочие требования	9
Установка пакета управления Metrex Cisco.....	9
Создание нового пакета управления для настроек.....	10
Дополнительная настройка	11
Включение отключенного по умолчанию монитора.....	11
Тонкая настройка правил обнаружения.....	12
Особенности внедрения пакета управления Metrex Cisco с учётом медленных каналов и удалённых офисов.....	13
Общие сведения о пакете управления Metrex Cisco.....	14
Объекты, которые обнаруживает пакет управления	14
Классы и отображение сводного показателя работоспособности	15
Ключевые сценарии мониторинга	16
Просмотр информации в консоли Operations Manager	18
Представления CPU.....	19
Представления IOS	19
Представления IP SLA Monitors	19
Представления Memory	19
Представления Network Interfaces	20
Представления Temperature	20
Устранение неполадок	21
Пакет управления Metrex Cisco не распознаёт некоторые сетевые устройства Cisco либо относит их к неверному типу.....	21
В сетевых устройствах Cisco обнаружены температурные датчики, но графики температур для этих устройств не появляются.....	21
Для некоторых сетевых устройств Cisco отображаются не все графики, обнаруживаются не все компоненты и так далее	22

Введение в руководство по пакету управления Metrex Cisco

Пакет управления Metrex Cisco позволяет вести как упреждающий, так и реагирующий мониторинг сетевых устройств Cisco, а именно:

- коммутаторов,
- маршрутизаторов,
- брандмауэров,
- беспроводных точек доступа.

При этом выполняется мониторинг как аппаратных компонентов сетевых устройств: оперативной памяти, процессоров, блоков питания, вентиляторов и других, так и логических компонентов: процессов, IPSLA-мониторов. Благодаря отслеживанию IPSLA-мониторов пакет управления Metrex Cisco позволяет следить за состоянием каналов между маршрутизаторами Cisco.

Мониторинг, выполняемый этим пакетом управления, включает отслеживание доступности и производительности, а также пороговые значения по умолчанию.

Версия документа

Данное руководство написано на основе версии 1.0.0.300 пакета управления Metrex Cisco.

Получение последнего пакета управления и документации к нему

Ограниченную по времени версию пакета управления Metrex Cisco можно запросить, заполнив форму на сайте <http://www.vpn.ru>.

Полную версию пакета управления Metrex Cisco можно приобрести на сайте <http://www.vpn.ru>.

Последняя версия данного документа доступна на сайте <http://www.vpn.ru>.

Поддерживаемые конфигурации

Пакет управления Metrex Cisco предназначен для работы в составе Operations Manager 2007 R2. Версии Operations Manager 2007 RTM и Operations Manager 2007 SP1 не поддерживаются.

Рекомендуется вести отслеживание не более чем 300 сетевых устройств для одного сервера, используемого в качестве агента по сбору информации с сетевых устройств. Это позволит избежать пиковых нагрузок на аппаратные ресурсы агентов, которые могут привести к сбоям в процессе сбора информации (пропускам на графиках и несвоевременной реакции мониторов на события).

Для того чтобы обеспечить наиболее полный мониторинг сетевых устройств, рекомендуется прошить в них IOS актуальной версии. Общие рекомендации следующие: коммутаторы – IOS не старше 2009 года, маршрутизаторы – IOS не старше 2007 года. Подробнее о проблемах, возникающих из-за слишком старой версии IOS, написано в главе [Устранение неполадок](#).

Пакет управления работает с любыми сетевыми устройствами Cisco, подпадающими под одну из категорий: коммутаторы, маршрутизаторы, брандмауэры и беспроводные точки доступа. Проблемы с распознаванием устройств и способы их решения описаны в главе [Устранение неполадок](#).

Приступая к работе

В этом разделе описаны действия, которые следует предпринять перед импортом пакета управления, действия после импорта пакета управления, а также сведения о настройках.

Перед импортом пакета управления

На сетевое устройство Cisco невозможно установить агент Operations Manager, поэтому мониторинг сетевых устройств Cisco осуществляется при помощи серверов, на которые можно установить агента Operations Manager, либо любую другую его роль – Gateway Server, Management Server, Root Management Server.

Данные серверы занимаются опросом сетевых устройств Cisco по протоколу SNMP, получением и обработкой Syslog информации, а также обработкой SNMP-трапов (обработка SNMP-трапов не реализована в данной версии пакета управления).

Пакет управления Metrex Cisco использует в качестве базовых стандартные сетевые устройства Operations Manager, поэтому, в случае, если сетевые устройства Cisco уже обнаружены как стандартные сетевые устройства, пакет управления Metrex Cisco немедленно приступит к их мониторингу. Однако это может привести к скачкообразному росту расхода аппаратных ресурсов серверов, используемых в качестве серверов мониторинга сетевых устройств.

Для того чтобы этого избежать, следует перед импортом пакета управления распределить сетевые устройства между серверами мониторинга, как это описано в главе [Обнаружение сетевых устройств Cisco](#).

Обнаружение сетевых устройств Cisco

Для того чтобы пакет управления Metrex Cisco приступил к отслеживанию сетевого устройства Cisco, следует стандартным образом обнаружить это сетевое устройство в консоли оператора Operations Manager. Для этого следует воспользоваться мастером **Discovery Wizard** панели **Administration**.

Предварительно следует настроить поддержку запросов по протоколу SNMP в сетевом устройстве Cisco. О том, как произвести такую настройку можно прочитать в следующей статье:

http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_cfg_snmp_sup_ps6441_TSD_Products_Configuration_Guide_Chapter.html

Каждое сетевое устройство, обнаруживаемое с помощью мастера **Discovery Wizard** приписывается к определённому серверу, с которого в дальнейшем и будет осуществляться мониторинг этого сетевого устройства. Сервер можно выбрать в графе **Management Server** шага **Discovery method** мастера **Discovery Wizard**.

Изначально, при обнаружении может быть выбран сервер исключительно с ролями Gateway Server, Management Server или Root Management Server. Однако, после успешного обнаружения, можно переназначить сетевое устройство Cisco на мониторинг с помощью сервера с любой ролью Operations Manager, в том числе и с ролью **агент**. Для этого нужно в узле **Network Devices** панели **Administration** выбрать нужное сетевое устройство, щёлкнуть **Change Proxy Agent** в панели **Actions** и выбрать сервер, к которому будет прикреплено сетевое устройство.

Таким образом, в качестве сервера мониторинга сетевых устройств Cisco может выступать, в том числе и рабочая станция с клиентской операционной системой Windows XP/Vista/7 при условии, что на ней установлен агент Operations Manager.

Как известно, для того, чтобы сервер с ролью **агент** мог участвовать в сборе информации с других компьютеров, нужно включить для него параметр **Agent proxy**. Однако для того, чтобы этот сервер смог отслеживать состояние сетевых устройств Cisco, данный параметр включать не обязательно.

Рекомендация вести мониторинг не более чем 300 устройств с одного сервера мониторинга, фигурирующая в главе [Поддерживаемые конфигурации](#), является очень приблизительной, так как многое зависит от аппаратной конфигурации сервера, от того, выполняет ли он какие-то дополнительные функции, а также от набора компонентов, которые отслеживаются у сетевых устройств. Наибольшими потребителями ресурсов сервера мониторинга являются сетевые устройства Cisco обладающие большим количеством IPSLA мониторов и интерфейсов (как физических, так и виртуальных). Такие устройства следует распределять поровну между серверами мониторинга сетевых устройств.

В общем случае, при соотношении отслеживаемых сетевых устройств Cisco к серверам мониторинга равным 100-300 к 1 стоит придерживаться тактики постепенного прикрепления сетевых устройств к серверам мониторинга с параллельным отслеживанием расхода аппаратных ресурсов серверов.

Файлы данного пакета управления

Пакет управления Metrex Cisco является сборным и состоит из нескольких пакетов управления.



Этот выпуск включает:



- Три пакета управления для маршрутизаторов Cisco
- Три пакета управления для коммутаторов Cisco
- Три пакета управления для брандмауэров Cisco
- Три пакета управления для беспроводных точек доступа Cisco
- Пакет управления Metrex Cisco Library, представляющий собой основной набор компонентов используемых вышеперечисленными пакетами управления
- Пакет управления Metrex Images Library, включающий в себя графические иконки для диаграмм, отчетов и т.д.
- Пакет управления Metrex Licensing, предназначенный для контроля соответствия количества лицензированных и фактически мониторящихся сетевых устройств Cisco.

Все файлы пакетов управления импортируются автоматически при инсталляции пакета управления Metrex Cisco на сервер с ролью Operations Manager RMS, как это описано в главе Инсталляция пакета управления. Однако если пакет управления Metrex Cisco был установлен с полным набором компонентов, а со временем необходимость в мониторинге одного или нескольких типов сетевых устройств Cisco отпала, то для экономии ресурсов неиспользуемые пакеты управления могут быть удалены вручную с помощью пункта **Management Packs** панели **Администрирование**.

В следующей таблице описаны файлы, включенные в пакет управления.

Имя файла	Краткое имя	Описание
Metrex.Cisco.AccessPoint.Discovery.mp	Metrex Cisco Access Point Discovery	Содержит логику обнаружения всех компонентов устройств типа беспроводные точки доступа Cisco.

Имя файла	Краткое имя	Описание
Metrex.Cisco.AccessPoint.Library.mp	Metrex Cisco Access Point Library	Содержит определения типов объектов компонент устройств типа беспроводные точки доступа Cisco.
Metrex.Cisco.AccessPoint.Monitoring.mp	Metrex Cisco Access Point Monitoring	Обеспечивает весь мониторинг устройств типа беспроводные точки доступа Cisco.  Примечание. Мониторинг беспроводных точек доступа Cisco не будет вестись, если не импортирован этот пакет управления.
Metrex.Cisco.Firewall.Discovery.mp	Metrex Cisco Firewall Discovery	Содержит логику обнаружения всех компонентов устройств типа брандмауэры Cisco.
Metrex.Cisco.Firewall.Library.mp	Metrex Cisco Firewall Library	Содержит определения типов объектов компонент устройств типа брандмауэры Cisco.
Metrex.Cisco.Firewall.Monitoring.mp	Metrex Cisco Firewall Monitoring	Обеспечивает весь мониторинг устройств типа брандмауэры Cisco.  Примечание. Мониторинг брандмауэров Cisco не будет вестись, если не импортирован этот пакет управления.
Metrex.Cisco.Images.Library.mp	Metrex Cisco Images Library	Содержит графические иконки для диаграмм, отчётов и т.д.
Metrex.Cisco.Library.mp	Metrex Cisco Library	Содержит основной набор компонентов используемых остальными пакетами управления
Metrex.Cisco.Router.Discovery.mp	Metrex Cisco Router Discovery	Содержит логику обнаружения всех компонентов устройств типа маршрутизаторы Cisco.
Metrex.Cisco.Router.Library.mp	Metrex Cisco Router Library	Содержит определения типов объектов компонент устройств типа маршрутизаторы Cisco.

Имя файла	Краткое имя	Описание
Metrex.Cisco.Router.Monitoring.mp	Metrex Cisco Router Monitoring	Обеспечивает весь мониторинг устройств типа маршрутизаторы Cisco.  Примечание. Мониторинг маршрутизаторов Cisco не будет вестись, если не импортирован этот пакет управления.
Metrex.Cisco.Switch.Discovery.mp	Metrex Cisco Switch Discovery	Содержит логику обнаружения всех компонентов устройств типа коммутаторы Cisco.
Metrex.Cisco.Switch.Library.mp	Metrex Cisco Switch Library	Содержит определения типов объектов компонент устройств типа коммутаторы Cisco.
Metrex.Cisco.Switch.Monitoring.mp	Metrex Cisco Switch Monitoring	Обеспечивает весь мониторинг устройств типа коммутаторы Cisco.  Примечание. Мониторинг коммутаторов Cisco не будет вестись, если не импортирован этот пакет управления.

Прочие требования

Для работы пакета управления Metrex Cisco необходимо установить на серверы, к которым прикреплены сетевые устройства Cisco, а также на сервер с ролью Operations Manager RMS следующий набор исправлений и компонентов:

- Стандартный компонент Windows **Simple Network Management Protocol**
- Стандартный компонент Windows **WMI SNMP Provider**
- Windows PowerShell (входит в состав Windows 2008/2008 R2; для Windows 2003 и XP можно скачать на странице <http://www.microsoft.com/windowsserver2003/technologies/management/powershell/download.mspx>)
- [Исправление 942589](#) (требуется только для Windows 2003 x64)

Их можно установить как до установки пакета управления, так и во время установки. Инсталлятор пакета управления Metrex Cisco подскажет, каких компонентов/исправлений не хватает. Следует учесть, что установка исправления 942589 повлечёт за собой обязательную перезагрузку сервера.

Установка пакета управления Metrex Cisco

Установку пакета управления Metrex Cisco можно условно разделить на два шага:

1. Установка на серверы мониторинга, участвующие в мониторинге сетевых устройств Cisco
2. Установка пакета управления на сервер Operations Manager с ролью RMS

Для более быстрого обнаружения сетевых устройств Cisco и их компонентов при внедрении пакета управления Metrex Cisco его установку следует проводить в следующем порядке: сначала шаг 1, затем – шаг 2. Соблюдение этой последовательности может дать выигрыш в скорости первоначального обнаружения сетевых устройств Cisco и их компонент до 4х часов.

Для установки пакета управления на сервер Operations Manager с ролью RMS следует запустить на нём файл setup_rms.exe, входящий в дистрибутив пакета управления Metrex Cisco и следовать подсказкам мастера установки.

Для установки пакета управления на сервер Operations Manager с ролями, отличными от RMS, следует запустить на нём файл setup_gtw.exe, входящий в дистрибутив пакета управления Metrex Cisco и следовать подсказкам мастера установки.

Устанавливать пакет управления следует только на серверы, непосредственно участвующие в сборе информации с сетевых устройств Cisco и на сервер Operations Manager с ролью RMS.

Создание нового пакета управления для настроек

Пакеты управления, входящие в состав сборного пакета управления Metrex Cisco, запечатаны, и оригинальные параметры файлов пакетов управления изменить нельзя. Однако можно создавать настройки, как, например, переопределения, а затем сохранять их в другие пакеты управления. По умолчанию Operations Manager сохраняет все настройки в пакете управления по умолчанию (**Default Management Pack**). В качестве лучшего решения следует создавать отдельные пакеты управления для каждого запечатанного пакета управления, настройки которого изменяются.

Создание нового пакета управления для хранения переопределений имеет следующие выгоды:

- Простота процесса экспорта настроек, созданных в качестве тестовых, в рабочую среду. Например, вместо экспортирования пакета управления по умолчанию, содержащего настройки нескольких пакетов управления, можно экспортировать только один пакет управления с настройками конкретного пакета управления.
- Это позволяет удалить изначальный пакет управления без необходимости удаления пакета управления по умолчанию. Пакет управления, который содержит настройки, является зависимым от оригинального пакета управления. Эта зависимость обуславливает необходимость удаления пакета управления с настройками перед удалением изначального пакета управления. Если все настройки сохранены в пакете управления по умолчанию, необходимо удалить пакет управления по умолчанию перед тем, как можно будет удалить изначальный пакет управления.
- Гораздо легче отслеживать и обновлять настройки для отдельных пакетов управления.

Дополнительные сведения о запечатанных и незапечатанных пакетах управления см. в разделе [Форматы пакетов управления](#). Дополнительные сведения о настройке пакетов управления и пакете управления по умолчанию см. в разделе [Общие сведения о пакетах управления](#).

Создание нового пакета управления для настроек

1. Откройте консоль управления и нажмите кнопку **Администрирование**.
2. Щелкните правой кнопкой **Пакеты управления**, а затем выберите команду **Создать новый пакет управления**.
3. Введите название (например, Metrex Cisco Routers Overrides), затем нажмите **Дальше**.
4. Нажмите кнопку **Создать**.

Дополнительная настройка

Включение отключенного по умолчанию монитора

По умолчанию в пакете управления Metrex Cisco включены все правила и все мониторы кроме одного.

Отключенный по умолчанию монитор нацелен на объекты типа "сетевой интерфейс" и используется для реакции на аварийное отключение интерфейса (когда административный статус – **up**, а фактический статус – **down**). В большинстве случаев данный монитор бесполезен, по следующим причинам:

- Согласно рекомендациям компании Microsoft интервалы опроса для мониторов не могут быть меньше 5 минут, поэтому монитор не способен отследить быстрые переходы между состояниями up/down.
- Сетевые администраторы редко выставляют административный статус "down" у неиспользуемых сетевых интерфейсов, поэтому, к примеру, все незанятые сетевые порты у коммутаторов могут быть отмечены монитором как сбойные.

Однако если вы по каким-то причинам решили воспользоваться данным монитором, то вы можете сделать это с помощью переопределения.

Чтобы использовать переопределение для включения монитора, отслеживающего статус интерфейса

1. В панели "Authoring" раскройте **Management Pack Objects** и нажмите **Monitors**.
2. На панели инструментов Operations Manager щелкните **Change Scope**, а затем установите фильтр для объектов в области сведений, чтобы оставить в списке только объекты со словом **Interface** в названии.
3. В списке **Target** отметьте объекты типа **Cisco Router Interface**, **Cisco Firewall Interface**, **Cisco Switch Interface**, **Cisco AccessPoint Interface**. Нажмите кнопку **OK**.
4. Выберите один из мониторов: **Cisco AccessPoint Interface Status Is Down**, **Cisco Router Interface Status Is Down**, **Cisco Switch Interface Status Is Down**, **Cisco Firewall Interface Status Is Down**.
5. На панели инструментов Operations Manager выберите пункты **Overrides**, **Override the object discovery**, а затем — **For all objects of class**, **For a group...** или **For a specific object of class**.
6. В диалоговом окне **Override control parameter** измените конфигурацию параметра **Enabled** с **False** на **True**.
7. В группе **Management pack** щелкните **New**, чтобы создать незапечатанную версию пакета управления, а затем нажмите кнопку **OK** или выберите предварительно созданный незапечатанный пакет управления для сохранения этого переопределения. Не рекомендуется сохранять переопределения в пакете управления по умолчанию.

Тонкая настройка правил обнаружения

Для экономии ресурсов серверов мониторинга, а также, во избежание бесполезного роста баз данных Operations Manager, два правила обнаружения объектов (для интерфейсов и для процессов) имеют ограничения – они обнаруживают не все объекты данного типа, а только самые важные.

Правило обнаружения процессов обнаруживает только самые ресурсоёмкие с точки зрения расхода процессорного времени процессы. В качестве мерил ресурсоёмкости принимается параметр процесса **processor time**. Всего обнаруживается не более 8 самых ресурсоёмких процессов для каждого сетевого устройства Cisco. Список обнаруженных процессов может меняться при каждом срабатывании правила обнаружения (по умолчанию – каждые 4 часа).

Правило обнаружения интерфейсов обнаруживает только интерфейсы с административным статусом **up**. Таким образом, если сетевой администратор явным образом указал в настройках сетевого устройства, что сетевой интерфейс выключен, то такой интерфейс не будет обнаружен.

Кроме того, правило обнаружения интерфейсов не обнаруживает интерфейсы, фактический статус которых – **down** в течение долгого срока (по умолчанию – более 7 дней). Этот функционал называется **Smart Discover** и может быть сконфигурирован с помощью переопределений. Его можно отключить совсем (параметр **Smart Discover Enabled** – true/false), также можно изменить срок, после которого постоянно выключенный сетевой интерфейс перестаёт обнаруживаться (параметр **Retention Time (Days)**).

Чтобы использовать переопределение для изменения параметра автоматического обнаружения

1. В панели **Authoring** раскройте **Management Pack Objects** и нажмите **Discoveries**.
2. На панели инструментов Operations Manager щелкните **Change Scope**, а затем установите фильтр для объектов в области сведений, чтобы оставить в списке только объекты со словом **Interface** в названии.
3. В списке **Target** отметьте объекты типа **Cisco Router Interface**, **Cisco Firewall Interface**, **Cisco Switch Interface**, **Cisco AccessPoint Interface**. Нажмите кнопку **OK**.
4. Выберите одно из правил: **Cisco Firewall Interface Discovery Rule**, **Cisco Router Interface Discovery Rule**, **Cisco Switch Interface Discovery Rule** или **Cisco AccessPoint Interface Discovery Rule**.
5. На панели инструментов Operations Manager выберите пункты **Overrides**, **Override the object discovery**, а затем — **For all objects of class**, **For a group...** или **For a specific object of class**.
6. В диалоговом окне **Override control parameter** произведите переконфигурацию нужного параметра.
7. В группе **Management pack** щелкните **New**, чтобы создать незапечатанную версию пакета управления, а затем нажмите кнопку **OK** или выберите предварительно созданный незапечатанный пакет управления для сохранения этого переопределения. Не рекомендуется сохранять переопределения в пакете управления по умолчанию.

Для правил и мониторов, отслеживающих утилизацию пропускной способности (bandwidth utilization) сетевых интерфейсов, в качестве отправной точки необходимо значение максимальной

пропускной способности каждого интерфейса. По умолчанию максимальная пропускная способность берётся правилом обнаружения из свойств интерфейса, настроенных в сетевом устройстве Cisco. Однако если необходимо изменить значение максимальной пропускной способности сетевого интерфейса, не прибегая к перенастройке сетевого устройства Cisco, то для этого можно воспользоваться переопределением параметра **Override Speed**. Значение **Override Speed** должно быть числом, в размерности бит в секунду. Переопределение данного параметра аналогично процедуре описанной выше, за исключением того, что на шаге 4 нужно выбрать одно из правил обнаружения **Cisco Router Interface Speed Discovery Rule**, **Cisco Switch Interface Speed Discovery Rule**, **Cisco Firewall Interface Speed Discovery Rule** или **Cisco AccessPoint Interface Speed Discovery Rule**.

Особенности внедрения пакета управления Metrex Cisco с учётом медленных каналов и удалённых офисов

Сбор информации с сетевых устройств Cisco осуществляется по ненадёжным udp протоколам SNMP, syslog и SNMP-trap. Поэтому, в случае, если часть сетевых пакетов не достигла адресата, возможна потеря важной информации, что может выражаться в пропусках на графиках и несвоевременной реакции мониторов на события или даже полной отсутствию таковой. В связи с этим, не рекомендуется схема, при которой сетевое устройство Cisco и сервер, осуществляющий мониторинг этого сетевого устройства, разделены ненадёжной сетью типа Internet. Лучшее решение – располагать по серверу мониторинга в каждом сайте, в котором имеются сетевые устройства Cisco.

Общие сведения о пакете управления Metrex Cisco

Этот раздел содержит сведения по следующим темам:

- Объекты, которые обнаруживает пакет управления
- Отображение сводного показателя работоспособности
- Ключевые сценарии мониторинга
- Просмотр информации в консоли Operations Manager

Объекты, которые обнаруживает пакет управления

Пакет управления Metrex Cisco предназначен для мониторинга компонентов сетевых устройств Cisco. Он обнаруживает типы объектов, приведенные в следующей таблице. Все объекты обнаруживаются автоматически. Однако не во всех моделях сетевых устройств Cisco все типы компонентов доступны для отслеживания.

Категория	Тип объекта	Описание
Физический компонент	CPU	Процессор
Физический компонент	Memory	Оперативная память
Логический компонент	IOS	IOS
Физический компонент	Temperature Sensor	Температурный датчик
Физический компонент	Power Supply Unit	Блок питания
Физический компонент	Network Interface	Сетевой интерфейс (физический или логический)
Физический компонент	Fan	Вентилятор
Логический компонент	Process	Процесс
Логический компонент	Echo IPSLA	IPSLA-монитор типа Echo, UDP-Echo, Path-Echo*
Логический компонент	Jitter IPSLA	IPSLA-монитор типа UDP-Jitter*

* доступны только в сетевых устройствах Cisco типа маршрутизатор

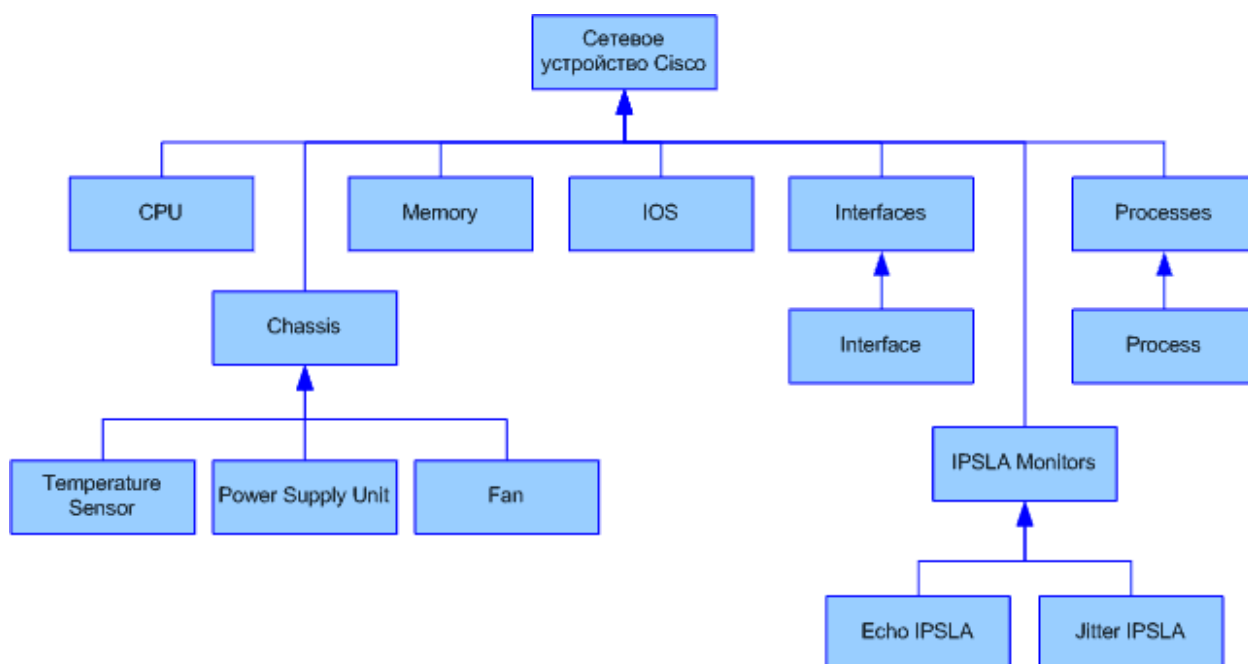


Примечание

IPSLA-мониторы, как правило, используются для мониторинга качества каналов между маршрутизаторами Cisco. Инструкцию по настройке IPSLA-мониторов можно прочитать в статье http://www.cisco.com/en/US/docs/ios/12_4/ip_sla/configuration/guide/hsla_c.html.

Классы и отображение сводного показателя работоспособности

Диаграмма сводного показателя работоспособности сетевого устройства Cisco, она же – диаграмма структуры классов:



Примечание

Для настройки сводного показателя работоспособности можно создать мониторы зависимостей (dependency monitors). Чтобы просмотреть диаграмму сводных показателей работоспособности для данной конфигурации, выберите объект и щелкните **Health Explorer** в области **Actions**.

По умолчанию мониторы зависимостей **IOS** → **Сетевое устройство Cisco** и **IPSLA Monitors** → **Сетевое устройство Cisco** отключены, но их можно включить с помощью переопределений.


Классы **Interfaces**, **Chassis** и **IPSLA Monitors** предназначены в основном для группировки объектов на представлениях типа “диаграмма”.


Ключевые сценарии мониторинга

В следующей таблице перечислены ключевые сценарии в данном пакете управления и описываются элементы сценариев мониторинга, которые обычно настраивают пользователи.

Примечание

Этот список не имеет целью полностью охватить функциональные возможности пакета управления.

Сценарий	Настраиваемые элементы
Мониторинг качества каналов (туннелей)	<p>В случае если есть необходимость отслеживать качество канала между офисами, и в каждом офисе имеется маршрутизатор Cisco, нужно настроить на маршрутизаторах IPSLA-мониторы.</p> <p> Примечание</p> <p>IPSLA-мониторы – это специализированные процессы, инициирующие тестирование канала передачи данных между локальным и удалённым маршрутизаторами. Удаленные маршрутизаторы в этом случае работают в режиме ответа. Для IPSLA-мониторов типа udp-jitter тестирование каналов осуществляется путем периодической отправки специального блока данных, состоящего из 10 UDP-пакетов (“замер”). Удаленный маршрутизатор анализирует количество потерянных пакетов, разницу во времени доставки пакетов и т.д. и отправляет пакеты назад. В общем случае по состоянию и проценту потерянных пакетов IPSLA-монитора можно судить о состоянии и проценте потерянных пакетов в канале во время выполнения замера. Процедура настройки IPSLA-мониторов подробно описана в следующей статье: http://www.cisco.com/en/US/docs/ios/12_4/ip_sla/configuration/guide/hsla_c.html.</p> <p>Пакет управления Metrex Cisco автоматически обнаруживает объекты типа “IPSLA-монитор” и отслеживает их состояние. Основные показатели IPSLA-мониторов отображаются на графиках, а, в зависимости от общего состояния IPSLA-монитора и от процента потерянных во время выполнения замера пакетов, генерируются предупреждения.</p> <p>Если предупреждения о полной недоступности канала или о больших потерях пакетов возникают слишком часто, либо наоборот не возникают, когда следовало бы, то нужно перенастроить с помощью переопределений параметры мониторов, отвечающих за отслеживание состояния IPSLA-мониторов.</p> <p>Для IPSLA типа UDP-jitter мониторы</p> <ul style="list-style-type: none">• Cisco Router IP SLA Monitor Jitter Lost Packets Critical• Cisco Router IP SLA Monitor Jitter Lost Packets Warning <p>отвечают за отслеживание потерь пакетов, а монитор Cisco Router IPSLA Monitor Jitter State is notConnected or timeout отвечает за отслеживание общего состояния канала (доступен/не доступен).</p> <p>Для IPSLA типа Echo технически невозможно отследить процент потерянных пакетов, а за отслеживание общего состояния канала отвечает монитор Cisco Router IPSLA Monitor Echo State is notConnected or timeout.</p> <p>О том, какие параметры у мониторов следует перенастроить, можно прочитать в базах знаний (knowledge base) этих мониторов.</p>

Сценарий	Настраиваемые элементы
	<p> Примечание</p> <p>Так как, для IPSLA-мониторов типа udr-jitter доступно наибольшее количество пригодных для анализа показателей, то лучшим решением является использование именно этого типа IPSLA.</p> <p>В пакете управления Metrex Cisco интервал опроса состояния IPSLA-мониторов автоматически принимается равным частоте выполнения IPSLA-монитора, настроенной в маршрутизаторе Cisco, но не меньше двух минут.</p>
<p>Мониторинг утилизации пропускной способности сетевых интерфейсов (физических и логических)</p>	<p>Сразу после автоматического обнаружения сетевых интерфейсов пакет управления Metrex Cisco предоставляет возможность, отслеживать, на сколько процентов от максимума загружены трафиком эти интерфейсы.</p> <p>Утилизация пропускной способности интерфейсов (процент загруженности от максимума) вычисляется по следующим формулам:</p> <ul style="list-style-type: none"> • входящий трафик/максимальная пропускная способность*100% • исходящий трафик/максимальную пропускную способность*100%. <p>Из формул ясно, что ключевую роль в определении текущей утилизации пропускной способности интерфейсов играет величина максимальной пропускной способности. По умолчанию эта величина автоматически определяется правилом обнаружения из свойств сетевых интерфейсов сетевых устройств Cisco. Однако, очень часто, заявленная производителем (для физических интерфейсов) или провайдером (для туннелей) величина максимальной пропускной способности не соответствует реальной. В пакете управления Metrex Cisco имеется возможность задать максимальную пропускную способность для каждого интерфейса в отдельности, для групп интерфейсов или всех интерфейсов сразу. Это возможно сделать с помощью переопределения параметра Override Speed правила обнаружения Cisco Device Interface Speed Discovery Rule, нацеленного на сетевые интерфейсы. Подробнее о переопределении правил обнаружения можно прочитать в главе Дополнительные настройки.</p> <p>Утилизация пропускной способности интерфейсов отображается в виде отдельных графиков для входящего и исходящего трафика на представлении Network Interfaces Bandwidth Usage пакета управления Metrex Cisco.</p> <p>Для генерации предупреждений о постоянной высокой утилизации пропускной способности интерфейсов в пакете Metrex Cisco предусмотрены следующие мониторы, нацеленные на сетевые интерфейсы:</p> <ul style="list-style-type: none"> • Cisco Device Interface Inbound Bandwidth Usage Too High • Cisco Device Interface Inbound Bandwidth Usage Critical • Cisco Device Interface Outbound Bandwidth Usage Too High • Cisco Device Interface Outbound Bandwidth Usage Critical <p>Эти мониторы раз в пять минут считывают текущую утилизацию пропускной способности сетевого интерфейса и меняют свой статус в случае, если среднее значение утилизации из 6 замеров больше порогового значения. По умолчанию пороговое значение для критических мониторов – 90%, для предупреждающих – 75%. Интервал срабатывания монитора, количество усредняемых замеров, а также пороги могут быть изменены с помощью переопределений.</p>

Просмотр информации в консоли Operations Manager

В течение четырёх часов после развертывания можно просмотреть сводное представление типов объектов в развертывании Metrex Cisco. Можно ускорить этот процесс, переопределив обнаружение некоторых объектов.

Представление может содержать длинный список объектов. Чтобы найти отдельный объект или группу объектов, можно использовать кнопки **Scope**, **Find** и **Search** на панели инструментов Operations Manager. Дополнительные сведения см. в разделе **How to Manage Monitoring Data Using Scope, Search, and Find** в справке Operations Manager 2007.

Следующие представления присутствуют непосредственно в группе узла **Metrex Cisco Monitoring** на панели "Monitoring" консоли управления.



Примечание

Список дан для всех сетевых устройств Cisco. Встречающийся в названиях представлений текст "Тип_ сетевого_устройства" следует читать как Routers для маршрутизаторов, Switches для коммутаторов, Firewalls для брандмауэров и Access Points для беспроводных точек доступа.

- "Тип_ сетевого_устройства" Active Alerts: отображает сводку всех незакрытых предупреждений.
- "Тип_ сетевого_устройства" All Alerts: отображает сводку всех предупреждений.
- "Тип_ сетевого_устройства": отображает представление состояний всех маршрутизаторов Cisco.
- "Тип_ сетевого_устройства" Performance: отображает все графики производительности маршрутизаторов Cisco и их компонентов.
- "Тип_ сетевого_устройства" Diagram: отображает сводную диаграмму всех обнаруженных маршрутизаторов Cisco.
- CPU: подробности описаны в таблице ниже.
- IOS: подробности описаны в таблице ниже.
- IP SLA Monitors: подробности описаны в таблице ниже.
- Memory: подробности описаны в таблице ниже.
- Network Interfaces: подробности описаны в таблице ниже.
- Temperature: подробности описаны в таблице ниже.

Представления CPU

Имя представления	Описание
CPU	Отображает список всех процессоров сетевых устройств Cisco и их текущее состояние
CPU Utilization	Отображает графики производительности процессоров сетевых устройств Cisco
Processes	Отображает список самых ресурсоёмких процессов сетевых устройств Cisco и их текущее состояние
Processes CPU Usage	Отображает графики утилизации процессора процессами сетевых устройств Cisco

Представления IOS

Имя представления	Описание
IOS	Отображает список всех IOS сетевых устройств Cisco и их текущее состояние

Представления IP SLA Monitors

Имя представления	Описание
Echo Monitors	Отображает список всех IPSLA-мониторов типа Echo, pathEcho и udpEcho сетевых устройств Cisco и их текущее состояние
Echo Monitors Performance	Отображает графики производительности всех IPSLA-мониторов типа Echo, pathEcho и udpEcho сетевых устройств Cisco
Jitter Monitors	Отображает список всех IPSLA-мониторов типа udp-jitter сетевых устройств Cisco и их текущее состояние
Jitter Monitors Performance	Отображает графики производительности всех IPSLA-мониторов типа udp-jitter сетевых устройств Cisco

Представления Memory

Имя представления	Описание
Memory	Отображает список всех типов оперативной памяти сетевых устройств Cisco и их текущее состояние

Имя представления	Описание
Memory Performance	Отображает графики производительности для всех типов оперативной памяти сетевых устройств Cisco

Представления Network Interfaces

Имя представления	Описание
Network Interfaces	Отображает список всех сетевых интерфейсов (физических и логических) сетевых устройств Cisco и их текущее состояние
Network Interfaces Bandwidth Usage	Отображает графики утилизации пропускной способности сетевых интерфейсов сетевых устройств Cisco
Network Interfaces Errors	Отображает графики ошибок различного типа, возникших на сетевых интерфейсах сетевых устройств Cisco
Network Interfaces Traffic	Отображает графики трафика, проходящего через сетевые интерфейсы сетевых устройств Cisco

Представления Temperature

Имя представления	Описание
Temperature	Отображает графики температуры с температурных датчиков всех сетевых устройств Cisco



Примечание

Следует принимать во внимание, что на представлениях будут отображаться только те компоненты, которые фактически доступны для отслеживания в конкретных моделях и типах сетевых устройств.

Устранение неполадок

При работе с пакетом управления Metrex Cisco у вас могут возникнуть следующие проблемы.

Пакет управления Metrex Cisco не распознаёт некоторые сетевые устройства Cisco либо относит их к неверному типу.

Проблема: Вы успешно обнаружили сетевое устройство Cisco с помощью мастера **Discovery Wizard**, оно имеет нормальный статус в представлении **Network Device State** папки **Network Device** панели **Monitoring**. Однако по прошествии 4х часов, сетевое устройство Cisco не появилось в представлениях пакета управления Metrex Cisco вообще, либо появилось, но было отнесено к неправильному типу (к примеру, маршрутизатор появился в папке Switches).

Объяснение: В пакете управления Metrex Cisco имеется механизм автоматического распознавания моделей и типов сетевых устройств Cisco, однако, для некоторых моделей устройств этот механизм может работать некорректно либо не работать вообще. Для таких моделей устройств в пакете управления Metrex Cisco предусмотрен механизм принудительного присвоения устройствам модели и типа, ориентируясь на Device Oid (уникальный SNMP-идентификатор модели устройства). Список таких моделей постоянно пополняется, но он всё ещё не полон.

Инструкции по решению: Сначала следует убедиться, что у вас установлена наиболее актуальная версия пакета управления Metrex Cisco. Посмотреть историю версий можно на сайте vrp.ru.

Если вы обновили пакет управления до актуальной версии, но по прошествии 4х часов устройства всё равно не обнаружены, то вам необходимо прислать в техподдержку компании Metrex Engineering на e-mail scom-team@metrex.ru следующие сведения:

1. Модель устройства
2. Тип устройства (коммутатор, маршрутизатор, брандмауэр или беспроводная точка доступа)
3. Oid устройства (**Device Oid** можно увидеть в представлении **Network Device State** папки **Network Device** панели **Monitoring**, он выглядит примерно так: 1.3.6.1.4.1.9.1.670)

В течение нескольких дней вы получите новую версию пакета управления, которая успешно распознает ваши устройства.

В сетевых устройствах Cisco обнаружены температурные датчики, но графики температур для этих устройств не появляются.

Проблема: В сетевом устройстве Cisco обнаружен температурный датчик, он виден на диаграмме устройства, но график температуры для этого датчика не появляется.

Объяснение: Некоторые модели сетевых устройств Cisco с IOS 2005го года и старше некорректно отдают информацию о температуре по протоколу SNMP. Они рапортуют, что температурный датчик в них есть, но при попытке получить значение температуры, отдают пустое значение вместо величины температуры. Для проверки можно посмотреть на состояние монитора **Cisco Device IOS Temperature Data Is Inconsistent**, нацеленного на IOS устройства. Если монитор имеет статус Warning, то имеет место быть вышеописанная проблема.

Инструкции по решению: Данная проблема решается перепрошивкой в устройство более новой версии IOS.

Для некоторых сетевых устройств Cisco отображаются не все графики, обнаруживаются не все компоненты и так далее.

Проблема: В некоторых сетевых устройствах Cisco не обнаруживаются компоненты, которые в них точно есть (к примеру, блоки питания). Для некоторых сетевых устройств Cisco отрисовываются не все графики (к примеру, нет части графиков об ошибках на интерфейсах – CRC, Runts и других).

Объяснение:

1. Разные модели сетевых устройств Cisco обладают различным набором компонентов, пригодных для мониторинга. Так, к примеру, температурные датчики есть далеко не во всех моделях.
2. Даже если компоненты имеются в сетевом устройстве Cisco, оно может не отдавать информацию об этих компонентах по SNMP. Различные модели сетевых устройств Cisco представляют разный объем информации, пригодный для отслеживания. В общем случае действуют следующие правила:
 - Устройства типа брандмауэр предоставляют информации меньше чем остальные типы
 - Чем выше модель устройства в иерархии моделей, тем больше информации для отслеживания оно предоставляет

Инструкции по решению: В критичных для отслеживания местах сети предпочтительно ставить старшие модели сетевых устройств Cisco, чтобы обеспечить максимальный уровень мониторинга.