

Основные принципы поиска неисправностей

В этой части...

Глава 1. "Общее описание процесса поиска неисправностей"

Глава 2. "Инструментальные средства поиска неисправностей"



Общее описание процесса поиска неисправностей

За последние десять лет резко возросла потребность в сетевых ресурсах. В современном мире успешная работа любой компании во многом зависит от бесперебойного функционирования применяемой в ней сети, поэтому любое нарушение в работе сети считается недопустимым. В связи с этим задача поиска неисправностей в сети стала одним из самых важных направлений работы на многих предприятиях.

В последние годы не только возросла зависимость от успешного функционирования сети, но и усложнилась структура самой сетевой среды. В сетях все чаще применяются разные типы передающей среды, многочисленные протоколы, а иногда в процессе работы устанавливаются соединения с сетями неизвестного типа. Такая необходимость возникает при использовании транзитных сетей, принадлежащих провайдерам служб Internet (ISP — Internet Service Provider) или телекоммуникационным компаниям, которые предоставляют услуги по обеспечению взаимодействия отдельных сетей. Сложность сетей и важность обеспечения их надежной работы возрастают также в связи с тем, что сети передачи данных все чаще применяются для передачи аудио- и видеоинформации.

В связи с общим усложнением сетевой среды возрастает вероятность появления проблем нарушения связности и снижения производительности в объединенных сетях, но при этом первопричины таких проблем часто очень сложно обнаружить.

Признаки неисправностей, проблемы и решения

Нарушения функционирования объединенных сетей характеризуются определенными признаками. Такие признаки могут быть общими (например, нельзя получить доступ к конкретным серверам с клиентских компьютеров) или более определенными (например, отсутствие информации о маршрутах в таблице маршрутизации). Анализ каждого признака неисправности, проводимый с помощью специальных инструментальных средств и методов поиска неисправностей, может выявить одну или несколько причин или проблем. А каждую причину неисправности после ее распознавания можно устранить путем реализации решения, состоящего из ряда действий.

В настоящей книге описано, как определять признаки неисправностей, выявлять проблемы и реализовывать решения в любой сетевой среде. В процессе поиска неисправностей в конкретной среде следует всегда учитывать условия, в которых осуществляется поиск неисправностей, что позволяет правильно определять признаки и диагностировать причины нарушения в работе.

Общая модель решения проблемы поиска неисправностей

В процессе поиска неисправностей в сетевой среде должен применяться систематический подход. Если поиск неисправностей ведется бессистемно, то могут непродуктивно затрачиваться ценные временные и материальные ресурсы, а иногда при этом положение даже ухудшается. В процессе устранения нарушений в работе сети необходимо определить конкретные признаки неисправности, выявить все потенциальные проблемы, которыми могут быть вызваны эти признаки, а затем систематически устранять все возможные причины проблем (от наиболее вероятных до наименее вероятных) до тех пор, пока все признаки неисправности не исчезнут.

На рис. 1.1 показана блок-схема общей модели решения проблемы поиска неисправностей. Эта блок-схема не является жесткой схемой поиска неисправностей в объединенной сети, а может служить лишь основой, на которой формируется конкретный процесс устранения нарушений в работе, соответствующий конкретной сетевой среде.



Рис. 1.1. Общая модель решения проблемы поиска неисправностей

Ниже описаны конкретные этапы процесса поиска неисправностей, общая блок-схема которого приведена на рис. 1.1.

Шаг 1. При анализе нарушения работы в сети четко сформулируйте проблему. Проблема должна быть определена как набор наблюдаемых признаков неисправностей и возможных причин.

В процессе анализа проблемы необходимо определить общие признаки неисправности, а затем установить, какими причинами могли быть вызваны эти признаки. Например, предположим, что хост не отвечает на запросы к службам, поступающие от клиентов (признак неисправности). Возможными причинами этого может быть неправильная настройка конфигурации хоста, неисправные интерфейсные платы или отсутствие необходимых команд в конфигурации маршрутизатора.

Шаг 2. Соберите факты, которые позволят более точно установить возможные причины.

Необходимо провести опрос всех заинтересованных пользователей, сетевых администраторов, руководителей и других специалистов, а также собрать информацию из таких источников, как системы управления сетью, трассировки анализаторов протокола, ознакомиться с результатами выполнения команд диагностики маршрутизатора или прочитать документацию к применяемой версии программного обеспечения.

Шаг 3. Изучите возможные проблемы с учетом собранных фактов. Накопленная вами информация позволит исключить некоторые потенциальные проблемы из списка подозреваемых.

Например, полученные данные могут свидетельствовать о том, что аппаратное обеспечение работает нормально. Это позволит сосредоточиться на нарушениях в работе программного обеспечения. При любой возможности нужно стремиться сузить круг потенциальных проблем, чтобы можно было разработать эффективный план действий.

Шаг 4. Подготовьте план действий, охватывающий все оставшиеся потенциальные проблемы. Начните с наиболее вероятной неисправности и разработайте план, который предусматривает устранение только одной конкретной причины.

Если план действий направлен на устранение только одной причины, он позволит найти искомое решение конкретной проблемы. Пытаясь одновременно устранить сразу несколько причин, также можно решить проблему, но при этом сложно определить, какое именно действие привело к устранению признаков неисправности, поэтому при повторном возникновении такой же проблемы в будущем поиск решения придется начать с самого начала.

Шаг 5. Осуществите план действий, тщательно выполняя каждый этап и проверяя, удалось ли устранить признаки неисправности.

Шаг 6. После внесения каждого изменения обязательно проконтролируйте результаты. Как правило, для этого должен применяться тот же метод сбора данных, как и на шаге 2 (в частности, при этом снова привлекайте к такой работе заинтересованных специалистов и используйте диагностические инструментальные средства).

Шаг 7. Проанализируйте полученные результаты, чтобы определить, решена ли проблема. В случае положительного ответа процесс поиска неисправности заканчивается.

Шаг 8. Если проблема не решена, разработайте план действий по устранению следующей менее вероятной проблемы из списка. Возвратитесь к шагу 4, снова вносите по одному изменению и повторяйте процесс до тех пор, пока проблема не будет решена.

Примечание

Если исследованы все обычные причины и проведены все возможные действия (описанные в данной книге или определенные в конкретной сетевой среде), но неисправность не удалось устранить, следует обратиться к представителю службы технической поддержки корпорации Cisco.

Подготовка к возникновению сетевых отказов

Возобновление нормальной работы после сетевого отказа всегда проходит легче, если заранее проведена определенная подготовка. Для этого в любой сетевой среде должно соблюдаться определенное требование, которое можно считать наиболее важным: наличие своевременной и точной информации о сети, к которой может в любое время обратиться обслуживающий персонал сети. Только при наличии полной информации можно принять обоснованное решение о том, какие изменения должны быть сделаны в сети для возобновления ее работы, и только с помощью такой информации можно максимально быстро и легко провести поиск неисправностей.

В процессе поиска неисправностей в сети следует ожидать, что функционирование сети будет нарушено. Поэтому рекомендуется обязательно выделять определенный интервал времени на поиск возможных неисправностей, чтобы свести к минимуму нарушение нормальной производственной деятельности. Следует всегда документировать все внесенные изменения. Это позволяет легко вернуться к прежней конфигурации, если поиск неисправности не привел к выявлению проблемы в течение времени, отведенного на техническое обслуживание.

Чтобы определить степень готовности к устранению сетевого отказа, ответьте на следующие вопросы контрольного списка.

- Есть ли точные физические и логические схемы объединенной сети?

На предприятии или в подразделении необходимо иметь схемы, которые полностью отражают современное состояние объединенной сети. На физической схеме должно быть показано местонахождение всех устройств в сети и обозначены связи между ними, а на логической схеме должны быть указаны сетевые адреса, номера сетей, подсетей и т.д.

- Имеется ли список всех сетевых протоколов, реализованных в сети?

Для каждого из реализованных протоколов необходимо иметь список номеров сетей, подсетей, зон, областей, а также всю прочую информацию, касающуюся протоколов.

- Имеются ли данные о том, для каких протоколов предусмотрена маршрутизация трафика?

Для каждого из маршрутизируемых протоколов должна быть собрана точная и актуальная информация о конфигурации маршрутизатора.

- Известно ли, трафик каких протоколов передается с помощью мостов?

Если конфигурация каких-либо мостов предусматривает применение фильтров, то необходимо иметь копию этой информации о конфигурации.

- Известны ли все точки контакта с внешними сетями, включая все соединения с Internet?

Для каждого внешнего сетевого соединения необходимо иметь информацию о применяемом протоколе маршрутизации.

- Накоплены ли эталонные данные о работе сети в основных режимах?

На предприятии должны быть накоплены данные о характеристиках и производительности сети в нормальных условиях в разное время суток. Это позволяет определить, какие характеристики изменились в результате возникновения неисправности.

Если специалисты по сетям конкретного предприятия дадут положительный ответ на все эти вопросы, они смогут устранить любую неисправность быстрее и легче, чем при отсутствии соответствующей подготовки. И, наконец, после устранения любой неисправности следует обязательно документировать обнаруженные проблемы и принятые решения. Это позволяет создать базу данных проблем и решений, которой смогут воспользоваться все сотрудники предприятия при возникновении в дальнейшем подобных проблем. Такие мероприятия, безусловно, позволят сократить время на устранение неисправностей в сети и поэтому свести к минимуму их воздействие на деятельность предприятия.



Инструментальные средства поиска неисправностей

В настоящей главе представлена информация о разнообразных инструментальных средствах, которые позволяют упростить поиск неисправностей в объединенной сети. В частности, здесь приведена информация об использовании диагностических команд маршрутизатора, инструментальных средств управления сетью корпорации Cisco и инструментальных средств поиска неисправностей других поставщиков.

Применение диагностических команд маршрутизатора

В маршрутизаторах Cisco предусмотрено множество встроенных команд, позволяющих контролировать работу и выполнять поиск неисправностей в объединенной сети. В следующих разделах описаны основные области применения этих команд.

- Команды `show` позволяют контролировать работу оборудования и определять характеристики сети, а также выявлять проблемные области.
- Команды `debug` позволяют диагностировать проблемы, возникающие из-за неправильной настройки конфигурации протоколов и оборудования.
- Команды `ping` позволяют проверить возможность взаимодействия устройств в сети.
- Команды `trace` дают возможность определить маршрут, по которому проходят пакеты от одного устройства к другому на пути к месту назначения.

Применение команд `show`

Команды `show` представляют собой мощное инструментальное средство текущего контроля и поиска неисправностей. Команды `show` могут применяться для выполнения следующих функций:

- текущий контроль характеристик маршрутизатора в процессе инсталляции;
- текущий контроль нормального функционирования сети;

- выявление интерфейсов, узлов, компонентов передающей среды или приложений, которые являются причиной неисправности;
- определение наличия заторов в сети;
- определение состояния смежных серверов, клиентов или других смежных устройств.

Ниже перечислены некоторые наиболее широко применяемые команды show.

- `show version`. Показывает конфигурацию аппаратных средств системы, версию программного обеспечения, имена файлов конфигурации, а также загрузочные образы.
- `show running-config`. Отображает применяемую в настоящий момент конфигурацию маршрутизатора.
- `show startup-config`. Показывает конфигурацию маршрутизатора, которая хранится в энергонезависимом ОЗУ (оперативное запоминающее устройство).
- `show interfaces`. Выводит статистические данные по всем интерфейсам, которые входят в конфигурацию маршрутизатора или сервера доступа. Отображаемые данные зависят от типа сети, для использования в которой настроен конкретный интерфейс.
- `show controllers`. Показывает статистические данные о контроллерах интерфейсных плат.
- `show flash`. Отображает компоновку и содержимое флэш-памяти.
- `show buffers`. Выводит статистические данные о буферных пулах маршрутизатора.
- `show memory summary`. Выводит статистические данные о пулах оперативной памяти и итоговую информацию о действиях программы распределения системной памяти, а также предоставляет отчет об использовании каждого блока памяти.
- `show process cpu`. Показывает информацию об активных процессах в маршрутизаторе.
- `show stacks`. Выводит информацию об использовании стека процессами и процедурами прерывания, а также показывает причину последней перезагрузки системы.
- `show cdp neighbors`. Предоставляет определенную информацию о возможности доступа к непосредственно подключенным (соседним, или смежным) устройствам Cisco. Эта команда — исключительно полезное инструментальное средство, позволяющее определить состояние функционирования физического уровня и уровня передачи данных. CDP (Cisco Discovery Protocol — протокол обнаружения устройств компании Cisco) представляет собой собственный протокол уровня передачи данных.
- `show debugging`. Выводит информацию о том, какой режим отладки разрешен для данного маршрутизатора.

Для получения списка подкоманд любых команд всегда можно ввести вопросительный знак (?) в командной строке.

Как и команды `debug`, некоторые команды `show`, перечисленные выше, доступны только в привилегированном режиме выполнения `exec`-команд маршрутизатора (в режиме `enable`). Дополнительные сведения об этом режиме приведены ниже, в разделе “Применение команд `debug`”.

Кроме перечисленных, имеются также сотни других команд show. Дополнительные сведения об использовании и интерпретации вывода конкретных команд show приведены в справочниках по командам IOS (Internetwork Operating System — операционная система для объединенных сетей) корпорации Cisco.

Применение команд debug

Привилегированные ехес-команды debug позволяют получить значительный объем информации о том, какой трафик наблюдается (или не наблюдается) в определенном интерфейсе, перехватить сообщения об ошибках, вырабатываемых узлами сети, сформировать диагностические пакеты, относящиеся к конкретному протоколу, а также ознакомиться с другими данными, необходимыми для поиска неисправностей. Чтобы получить доступ к перечню привилегированных ехес-команд и ознакомиться с ним, введите следующий код:

```
Router> enable
Password: XXXXXX
Router# ?
```

Обратите внимание на то, как изменяется приглашение к вводу информации в маршрутизаторе. Приглашение со знаком фунта “#” (вместо обычного приглашения со знаком больше “>”) указывает, что теперь работа выполняется в режиме привилегированных ехес-команд (в режиме enable).

Предостережение

Соблюдайте осторожность при использовании команд debug. Многие команды debug требуют больших затрат процессорного времени и могут вызвать серьезные нарушения в работе сети (такие как снижение производительности или нарушение связи) при их применении в маршрутизаторе, который уже испытывает значительную нагрузку. По завершении использования любой команды debug обязательно отмените ее с помощью соответствующей команды по debug (или введите команду по debug all, чтобы отменить действие всех команд отладки).

Команды debug должны применяться только для поиска причин неисправностей, а не для контроля над нормальным функционированием сети. Команды debug требуют больших затрат процессорного времени, поэтому должны применяться исключительно при анализе трафика определенного типа или при устранении неисправностей, если они позволяют сузить круг поиска возможных причин неисправностей.

Формат вывода результатов зависит от конкретной команды debug. Некоторые команды вырабатывают по одной строке вывода для каждого пакета, а другие при обработке каждого пакета вырабатывают несколько строк вывода. Одни команды генерируют большой объем выходной информации, а другие выводят данные лишь время от времени. Одни команды выдают текст построчно, а другие формируют отчеты с данными, представленными в отдельных полях.

Чтобы свести к минимуму негативное влияние, связанное с использованием команд debug, соблюдайте следующие рекомендации.

Шаг 1. Используйте в маршрутизаторе глобальную команду конфигурации по logging console, которая отменяет весь вывод журнала на терминал консоли.

Шаг 2. Подключитесь по протоколу Telnet к порту маршрутизатора и введите ехес-команду enable, которая переводит маршрутизатор в режим привилегированных ехес-команд. После ввода пароля enable, обеспечивающего доступ, вы получите приглашение к вводу информации, которое состоит из имени маршрутизатора и знака фунта (#).

Шаг 3. Используйте команду terminal monitor для копирования вывода команды debug и сообщений системы об ошибках на дисплей своего текущего терминала.

Перенаправив вывод на дисплей своего текущего терминала, вы сможете дистанционно просматривать вывод команды debug, не подключаясь через порт консоли.

Если команды debug выполняются через порт консоли, то при передаче каждого символа активизируется прерывание процессора, поэтому и без того значительная нагрузка процессора, вызванная использованием команды debug, возрастает до предела.

Если вывод команды debug необходимо сохранить для справок, выведите его в файл. Процедура подготовки такого файла вывода debug описана в справочнике по командам отладки *Debug Command Reference*.

В настоящей книге упоминаются только конкретные команды debug, необходимые для устранения определенных нарушений в работе сети. Подробные сведения о назначении и результатах применения команд debug приведены в документе *Debug Command Reference*.

Во многих ситуациях более полезными и менее требовательными к ресурсам по сравнению с командами debug могут оказаться диагностические инструментальные средства, предоставляемые независимыми поставщиками. Дополнительная информация о них приведена ниже, в разделе “Инструментальные средства поиска неисправностей, предоставляемые независимыми поставщиками”.

Применение команд ping

Команда ping, которая может быть вызвана на выполнение в режиме непривилегированных и привилегированных ехес-команд, применяется для проверки доступности хоста и связи по сети. После регистрации на маршрутизаторе или сервере доступа автоматически устанавливается режим непривилегированных ехес-команд. Доступные на непривилегированном уровне ехес-команды являются подмножеством ехес-команд, применяемых на привилегированном уровне. Как правило, непривилегированные ехес-команды позволяют подключаться к удаленным устройствам, изменять на время установки терминала, выполнять простейшие проверки и выводить на экран информацию о системе. Команда ping позволяет выполнять простые проверки наличия связи в сетях AppleTalk, CLNS (Connectionless Network Service — сетевое обслуживание без установления соединения) по стандарту ISO, IP, Novell, Apollo, VINES, DECnet или XNS.

В сетях IP при выполнении команды ping происходит отправка запросных сообщений эхо-тестирования ICMP (Internet Control Messages Protocol — протокол управляющих сообщений Internet). ICMP — это протокол Internet, с помощью которого передаются сообщения об ошибках и предоставляется информация, касающаяся адресации IP-пакетов. При получении запросного сообщения эхо-тестирования ICMP станция передает отправителю этого сообщения ответное сообщение эхо-тестирования ICMP.

Расширенный командный режим команды ping позволяет указать поддерживаемые опции заголовка IP-пакета. При этом в маршрутизаторе может быть выполнен ряд проверок, предусматривающих более широкий набор функций. Для перехода в расширенный командный режим ping введите yes в ответ на приглашение extended commands команды ping.

Рекомендуем воспользоваться командой ping при нормальном функционировании сети, чтобы узнать, как работает эта команда в обычных условиях, и сравнить полученные при этом результаты с результатами, характерными для нарушений в работе.

Дополнительная информация об использовании обычных и расширенных команд ping приведена в справочнике по основным командам конфигурации операционной системы Cisco IOS *Configuration Fundamentals Command Reference*.

Применение команд trace

Непривилегированная ехес-команда trace позволяет определить, по каким маршрутам следуют пакеты определенного маршрутизатора на пути к месту назначения. Привилегированная ехес-команда trace дает возможность указать поддерживаемые опции заголовков IP-пакетов, в результате чего в маршрутизаторе может быть применен более широкий набор опций проверки.

В команде trace используются сообщения об ошибках, вырабатываемые маршрутизаторами при достижении дейтаграммой минимального значения срока жизни (TTL — Time-To-Live). Вначале рассылаются пакеты запросов (специальные дейтаграммы) со значением TTL, равным 1. В результате первый маршрутизатор отбрасывает запросы и возвращает сообщения об ошибках "time exceeded", которые указывают, что срок жизни пакета истек. На следующем этапе выполнения команды trace передается еще несколько запросов и для каждого из них отображается время кругового обращения. После отправки каждого третьего запроса значение TTL увеличивается на 1.

Отправка каждого исходящего пакета может привести к получению одного из двух сообщений об ошибках. Сообщение об ошибке "time exceeded" указывает, что промежуточный маршрутизатор получил и отбросил запрос, поскольку истек срок жизни пакета. Сообщение об ошибке "port unreachable" указывает, что узел назначения получил и отбросил пакет, поскольку не мог доставить его приложению. А если установка таймера истекла до того, как поступил ответ, команда trace выводит символ звездочки (*).

Выполнение команды trace заканчивается после получения ответа от хоста назначения, при превышении максимального значения TTL или при вводе пользователем управляющей последовательности, которая прерывает трассировку.

Как и при использовании команды ping, рекомендуем выполнить команду trace при нормальном функционировании сети, чтобы узнать, как работает эта команда в обычных условиях, и сравнить полученные при этом результаты с результатами, характерными для нарушений в работе.

Дополнительная информация об использовании простых и расширенных команд trace приведена в справочнике по основным командам конфигурации операционной системы Cisco IOS *Configuration Fundamentals Command Reference*.

Инструментальные средства управления сетью, предоставляемые корпорацией Cisco

Корпорация Cisco поставляет семейство программных продуктов управления сетью CiscoWorks 2000, в состав которого входят инструментальные средства проектирования, текущего контроля и поиска неисправностей, позволяющие упростить управление объединенной сетью.

При поиске неисправностей в объединенной сети могут применяться следующие инструментальные средства управления объединенной сетью.

- Программа CiscoView выполняет функции динамического текущего контроля и поиска неисправностей, в частности, позволяет получить графическую схему соединений устройств Cisco, статистические данные и исчерпывающую информацию о конфигурации.
- Монитор производительности объединенной сети (IPM — Internetwork Performance Monitor) позволяет сетевым инженерам заблаговременно определять отклонения характеристик сетевого отклика от нормы с использованием отчетов, полученных в настоящее время и в прошлом.
- Инструментальное средство дистанционного текущего контроля (RMON — Remote MONitoring) TrafficDirector дает возможность накапливать данные, контролировать действия, происходящие в сети, и диагностировать потенциальные проблемы.
- Приложение управления коммутатором VlanDirector представляет собой инструментальное средство управления, которое позволяет получить полное представление о состоянии виртуальных локальных сетей.

Программа CiscoView

Графические средства управления программы CiscoView позволяют получить в оперативном режиме сведения о состоянии, статистические данные и исчерпывающую информацию о конфигурации продуктов корпорации Cisco для объединенных сетей (коммутаторов, маршрутизаторов, концентраторов и серверов доступа). Программа CiscoView дает возможность упростить управление сетью, поскольку схематически отображает информацию о состоянии устройств Cisco, в частности, предоставляет схему портов устройства с цветовой кодировкой, позволяющую быстро получить сведения о состоянии портов и охватить одним взглядом всю необходимую информацию. Ниже описаны основные возможности программы.

- Просмотр на графическом экране из центрального пункта информации о продуктах Cisco; это средство позволяет сетевым администраторам получить полное представление о работе устройств Cisco без физической проверки каждого устройства на удаленных узлах.
- Непрерывно обновляемая схема с информацией о маршрутизаторах, концентраторах, коммутаторах или серверах доступа в сети, полнота которой не зависит от их физического расположения.
- Постоянное обновление данных текущего контроля в реальном времени и отслеживание основной информации и данных, характеризующих производительность

устройств, объем трафика и степень загрузки. Эти данные содержат такие ключевые характеристики, как процент использования, число переданных и полученных фреймов, относительное количество ошибок, а также целый ряд других показателей, касающихся каждого конкретного устройства.

- Возможность изменять такие опции конфигурации, как прерывания, IP-маршруты, параметры настройки виртуальных локальных сетей и мостов.

Монитор производительности объединенной сети

Приложение управления сетью IPM (Internetwork Performance Monitor — монитор производительности объединенной сети) обеспечивает текущий контроль над производительностью мультипротокольных сетей. Приложение IPM позволяет измерять время отклика и определять характеристики доступа сетей IP на каждом транзитном переходе (от одного маршрутизатора к другому). Это приложение позволяет также измерять время отклика на участках между маршрутизаторами и мэйнфреймом в сетях SNA (Systems Network Architecture — системная сетевая структура).

Приложение IPM применяется для выполнения следующих задач.

- Поиск неисправностей в сети путем проверки сетевой задержки на участках между устройствами.
- Передача прерываний SNMP (Simple Network Management Protocol — простой протокол управления сетью) и предупреждающих сообщений SNA при превышении порогового значения, установленного пользователем, при разрыве и восстановлении соединения или при возникновении тайм-аута.
- Анализ данных о потенциальных проблемах еще до их возникновения путем накопления статистических данных, которые могут использоваться для моделирования и прогнозирования характеристик будущих сетевых топологий.
- Текущий контроль времени отклика на участке между двумя окончательными точками.

Программный продукт IPM состоит из трех частей: серверного и клиентского приложения IPM, а также модуля генератора отчетов о времени отклика (RTR — Response Time Reporter), который входит в состав программного обеспечения Cisco IOS.

Приложение RMON TrafficDirector

Усовершенствованные фильтры пакетов приложения TrafficDirector дают возможность пользователям контролировать сетевой трафик на всех семи уровнях протоколов. С использованием встроенных агентов RMON операционной системы Cisco IOS и средств формирования автономных запросов SwitchProbe сетевые администраторы могут просматривать сетевой трафик в масштабах всего предприятия на канальном, сетевом, транспортном или прикладном уровнях. Итоговый отчет о многоуровневом трафике приложения TrafficDirector позволяет быстро получить общую оценку степени загрузки сети и определить относительный объем трафика различных протоколов. Затем сетевые администраторы могут перейти к подробному изучению конкретного сегмента, кольца, порта коммутатора или магистрального канала и применить инструментальные средства анализа и диагностики в реальном времени для просмотра информации о хостах и конкретных сеансах обмена данными, а также для перехвата пакетов.

Средства текущего контроля пороговых значений приложения TrafficDirector позволяют создать среду управления, которая обеспечивает заблаговременное устранение возможных неисправностей. Для этого прежде всего в агенте RMON устанавливаются пороговые значения важных переменных MIB (Management Information Base — информационная база управления). При превышении этих пороговых значений на соответствующую станцию управления передаются прерывания, позволяющие предупредить сетевого администратора о потенциальной проблеме.

Приложение управления коммутатором VlanDirector

Приложение управления коммутатором VlanDirector позволяет упростить распределение портов виртуальной локальной сети и обеспечивает управление виртуальными локальными сетями. Приложение VlanDirector выполняет следующие функции.

- Точное отображение физической сети, позволяющее разработать проект виртуальной локальной сети и выполнить проверку конфигурации.
- Сбор информации о конфигурации виртуальной локальной сети, которая относится к конкретному устройству или каналному интерфейсу.
- Формирование отчетов о несоответствиях при наличии противоречивой информации о конфигурации.
- Поиск неисправностей и выявление отдельных конфигураций устройств, которые не соответствуют характеристикам виртуальных локальных сетей на уровне всей системы.
- Своевременное обнаружение изменений в состоянии портов коммутаторов виртуальной локальной сети.
- Проверка подлинности пользователей и защита данных.

Инструментальные средства поиска неисправностей, предоставляемые независимыми поставщиками

Диагностические инструментальные средства независимых поставщиков часто могут оказаться более полезными по сравнению с командами, встроенными в маршрутизатор. Например, применение команды `debug`, требующей большого объема процессорного времени, в сетевой среде с исключительно интенсивным трафиком может привести к разрушительным последствиям. Но подключение сетевого анализатора к исследуемой сети практически не нарушает ее работу и позволяет с большей вероятностью получить необходимую информацию, не препятствуя нормальному функционированию маршрутизатора. Ниже перечислены некоторые типичные инструментальные средства поиска неисправностей, предоставляемые независимыми поставщиками, которые применяются для устранения нарушений в работе объединенных сетей.

- Для проверки физических характеристик кабельной сети применяются вольтметры, цифровые мультиметры и кабельные тестеры.

- Поиск обрывов в кабелях, рассогласований импедансов и других технических неисправностей кабельной сети осуществляется с использованием динамических рефлектометров и оптических динамических рефлектометров
- Для поиска неисправностей периферийных интерфейсов применяются коммутационные боксы, генераторы тестовых последовательностей и тестеры частоты ошибочных битов/частоты ошибочных блоков
- Сетевые мониторы позволяют получить полное представление о функционировании сети на протяжении определенного периода времени путем непрерывного отслеживания пакетов, проходящих по сети.
- Такие сетевые анализаторы, как перехватчики сетевых пакетов, автоматически декодируют информацию, передаваемую на всех семи уровнях эталонной модели OSI, и способствуют выявлению нарушений в работе в реальном масштабе времени, позволяя получить полное представление о функционировании сети и классифицируя проблемы по степени важности.

Вольтметры, цифровые мультиметры и кабельные тестеры

Вольтметры и цифровые мультиметры относятся к числу наиболее простых инструментальных средств, предназначенных для измерения физических характеристик кабельной сети. Эти устройства измеряют такие параметры, как напряжение переменного и постоянного тока, силу тока, сопротивление и емкость, а также позволяют определить наличие обрывов в кабеле. Они применяются для проверки физического состояния сети.

Кабельные тестеры (сканеры) также позволяют проверить физическое состояние сети. Для проверки экранированной витой пары (STP), неэкранированной витой пары (UTP), кабелей 10BaseT, одинарных и двойных коаксиальных кабелей применяются кабельные тестеры соответствующего типа. Как правило, кабельные тестеры обеспечивают выполнение следующих функций.

- Проверка состояния кабеля и предоставление отчета, в том числе с результатами измерения перекрестной наводки на ближнем конце, затухания и шума.
- Выполнение функций динамического рефлектометра, текущий контроль трафика и подготовка схемы кабельной системы.
- Предоставление информации уровня MAC (Media Access Control — управление доступом к передающей среде) о трафике в локальной сети, накопление статистических данных, которые необходимы для расчета таких показателей, как коэффициент использования сети и частота ошибочных пакетов, а также выполнение некоторых функций проверки работы протокола (например, такой проверки связи по протоколу TCP/IP, как эхо-тестирование).

Аналогичное испытательное оборудование предусмотрено и для волоконно-оптических кабелей. В связи с относительно высокой стоимостью и самого кабеля, и его монтажа, волоконно-оптический кабель должен проверяться перед монтажом (на кабельном барабане) и после монтажа. Для проверки стекловолкна на обрыв требуется источник видимого света или рефлектометр. Источники света, способные излучать свет с тремя основными значениями длины волны, 850, 1300 и 1550 нанометров (нм), применяются

в сочетании с измерителями мощности, позволяющими проводить измерения на той же длине волны, проверять затухание и потери на отражение в стекловолокне.

Динамические рефлектометры и оптические динамические рефлектометры

К числу наиболее сложных приборов, применяемых для проверки характеристик медного кабеля, относятся динамические рефлектометры. Эти устройства позволяют быстро находить обрывы и короткозамкнутые цепи, скрутки, петли, острые изгибы, рассогласования импедансов и другие дефекты монтажа кабелей.

Динамический рефлектометр действует по принципу приема сигнала, отраженного от противоположного конца кабеля. При наличии обрывов, короткозамкнутых цепей и других дефектов амплитуда отраженного сигнала изменяется по-разному, в зависимости от дефекта. Динамический рефлектометр измеряет время, по истечении которого поступает отраженный сигнал, и вычисляет расстояние до дефекта в кабеле. Динамические рефлектометры могут также применяться для измерения длины кабеля. Некоторые динамические рефлектометры позволяют вычислить скорость распространения сигнала путем измерения характеристик эталонного участка кабеля.

Для измерения характеристик волоконно-оптических кабелей применяются оптические динамические рефлектометры, которые позволяют точно измерить длину стекловолокна, найти обрывы в кабеле, определить затухание сигнала в стекловолокне, а также измерить величину потерь в стыке (месте сращивания волокна) или разъеме. Оптический динамический рефлектометр может применяться для подготовки протокола испытания смонтированной кабельной системы, в котором отмечены значения затухания и указаны потери в каждом стыке. Эти эталонные результаты измерений могут затем сравниваться с результатами текущей проверки кабельной системы для обнаружения неисправностей.

Коммутационные боксы, генераторы тестовых последовательностей и тестеры частоты ошибочных битов/частоты ошибочных блоков

Коммутационные боксы, генераторы тестовых последовательностей и тестеры частоты ошибочных битов/частоты ошибочных блоков представляют собой инструментальные средства проверки с цифровым интерфейсом, которые часто применяются для измерения цифровых сигналов в интерфейсах периферийного оборудования персональных компьютеров, принтеров, модемов, модулей обслуживания канала/модулей обработки данных (CSU/DSU) и других аппаратных средств. Эти устройства позволяют контролировать характеристики каналов передачи данных, анализировать и перехватывать передаваемые данные, а также диагностировать неисправности, которые часто возникают в системах передачи данных. С их помощью можно исследовать трафик, передаваемый от терминального оборудования (DTE — Data Terminal Equipment) через терминальное оборудование канала передачи данных (DCE — Data Circuit-terminating Equipment) для ускорения поиска неисправностей, выявления типичных последовательностей двоичных сигналов и проверки правильности монтажа кабельных соединений. Эти устройства не могут применяться для проверки сигналов в такой сетевой среде, как Ethernet, Token Ring или FDDI.

Сетевые мониторы

Сетевые мониторы непрерывно отслеживают пакеты, проходящие по сети, и позволяют получить точное представление о функционировании сетей в любой момент времени или сформировать хронологический отчет об активности сети за определенный период времени. Мониторы не декодируют содержимое фреймов. Они могут применяться для накопления эталонных данных. При этом в течение определенного времени фиксируются данные о характеристиках работы сети для формирования так называемого *эталонного профиля производительности*, т.е. данных о работе сети при нормальных условиях.

Сетевые мониторы собирают информацию о размерах и количестве пакетов, включая ошибочные. Они позволяют определить общие показатели использования соединения, выяснить количество хостов и их MAC-адреса, а также получить подробные сведения о сеансах обмена данными между хостами и другими устройствами. Эти данные могут использоваться для создания профилей трафика локальной сети, а также для обнаружения участков с чрезмерным объемом трафика, планирования расширения сети, обнаружения нарушителей правил защиты сети, накопления эталонных данных о производительности, а также для более эффективного распределения трафика.

Сетевые анализаторы

Сетевые анализаторы (называемые также *анализаторами протокола*) декодируют информацию о разных уровнях протокола в зарегистрированных фреймах и представляют накопленную информацию в виде удобных для чтения кратких отчетов или сводок, по которым можно определить, на каких уровнях осуществлялась обработка данных (физическом, канальном и т.д.) и какие функции выполняет каждый байт заголовка или информационного наполнения.

Большинство сетевых анализаторов в основном выполняет следующие функции:

- отбирают трафик, который соответствует определенным критериям; это позволяет, например, перехватывать все фреймы, входящие или исходящие из конкретного устройства;
- регистрируют время перехвата данных;
- представляют информацию об уровнях протокола в форме, удобной для чтения;
- генерируют фреймы и выводят их в сеть;
- предоставляют возможность воспользоваться “экспертной” системой, в которой применяется набор правил в сочетании с информацией о конфигурации и функционировании сети для диагностики и устранения нарушений в работе сети или для выработки рекомендаций по улучшению ее работы.





Устранение нарушений в работе аппаратных средств, средств загрузки и передающей среды

В этой части...

Глава 3. “Устранение нарушений в работе аппаратных средств и средств загрузки”

Глава 4. “Устранение нарушений в работе сети Ethernet”

Глава 5. “Устранение нарушений в работе сети FDDI”

Глава 6. “Устранение нарушений в работе сети Token Ring”



Устранение нарушений в работе аппаратных средств и средств загрузки

В настоящей главе описаны процедуры поиска неисправностей аппаратных средств и устранения нарушений загрузки. Здесь представлены конкретные процедуры, относящиеся к определенным продуктам Cisco, но изложенные рекомендации всегда следует применять в соответствии с документацией по установке и техническому обслуживанию аппаратных средств, обращаясь к ней для получения более подробной информации о версии для конкретной платформы, назначении тех или иных светодиодов, а также сведений о настройке конфигурации и поиске неисправностей.

Глава начинается со следующих разделов, в которых описаны возможные нарушения в работе аппаратных средств.

- **Запуск маршрутизаторов ряда Cisco 7500.** Описаны аппаратные средства и процедуры диагностики нарушений процесса загрузки маршрутизаторов ряда Cisco 7500.
- **Запуск маршрутизаторов ряда Cisco 7000.** Описаны аппаратные средства и процедуры диагностики нарушений процесса загрузки маршрутизаторов ряда Cisco 7000.
- **Запуск маршрутизаторов ряда Cisco 4000.** Описаны аппаратные средства и процедуры диагностики нарушений процесса загрузки маршрутизаторов ряда Cisco 4000.
- **Запуск маршрутизаторов ряда Cisco 2500.** Описаны аппаратные средства и процедуры диагностики нарушений процесса загрузки маршрутизаторов ряда Cisco 2500.
- **Запуск коммутаторов ряда Catalyst 5000.** Описаны аппаратные средства и процедуры диагностики нарушений процесса загрузки LAN-коммутаторов ряда Catalyst 5000.

- **Запуск коммутаторов ряда Catalyst 2900.** Описаны аппаратные средства и процедуры диагностики нарушений процесса загрузки LAN-коммутаторов ряда Catalyst 2900.
- **Проверка и аттестация сменного оборудования.** Описаны действия, которые рекомендуется осуществлять при замене аппаратных средств маршрутизатора.
- **Запуск коммутаторов ряда Catalyst 6000.** Описаны аппаратные средства и процедуры диагностики нарушений процесса загрузки LAN-коммутаторов ряда Catalyst 6000.
- **Запуск маршрутизаторов ряда Cisco 2600.** Описаны аппаратные средства и процедуры диагностики нарушений процесса загрузки маршрутизаторов ряда Cisco 2600.
- **Запуск маршрутизаторов ряда Cisco 3600.** Описаны аппаратные средства и процедуры диагностики нарушений процесса загрузки маршрутизаторов ряда Cisco 3600.
- **Запуск коммутаторов ряда Catalyst 4000.** Описаны аппаратные средства и процедуры диагностики нарушений процесса загрузки LAN-коммутаторов ряда Catalyst 4000.

В последних разделах описаны признаки неисправностей, проблемы и решения, касающиеся нарушений загрузки из флэш-памяти, загрузки по сети с помощью протокола TFTP, загрузки из ПЗУ, а также других нарушений начальной загрузки.

- Начальная загрузка: маршрутизатор не может загрузиться из флэш-памяти.
- Начальная загрузка: при загрузке из флэш-памяти возникает векторная ошибка.
- Начальная загрузка: маршрутизатор частично загружается из флэш-памяти и отображает приглашение процедуры начальной загрузки.
- Начальная загрузка: маршрутизатор не может загрузиться по сети от TFTP-сервера.
- Начальная загрузка: маршрутизатор не может загрузиться по сети от другого маршрутизатора.
- Начальная загрузка: тайм-ауты и пакеты с нарушением порядка следования препятствуют выполнению загрузки по сети.
- Начальная загрузка: недействительные маршруты препятствуют выполнению загрузки по сети.
- Начальная загрузка: клиентские запросы ARP завершаются по тайм-ауту во время загрузки по сети.
- Начальная загрузка: во время загрузки по сети возникает ошибка “неопределенный загрузочный модуль”.
- Начальная загрузка: маршрутизатор зависает после инициализации режима ROMmon.
- Начальная загрузка: маршрутизатор не выходит из режима ROMmon.
- Начальная загрузка: искаженный вывод при загрузке из ПЗУ.
- Начальная загрузка: возникновение локальных тайм-аутов при загрузке из ПЗУ.

- Начальная загрузка: не функционирующее терминальное соединение с ненастроенным сервером доступа.

Загрузка маршрутизатора

Для инициализации системы (начальной загрузки) маршрутизаторов Cisco предусмотрено четыре способа.

- **Начальная загрузка по сети.** Маршрутизаторы можно загружать с сервера с помощью протокола TFTP (Trivial File Transfer Protocol — простейший протокол передачи файлов), протокола MOP (Maintenance Operation Protocol — протокол обслуживания) корпорации DEC или протокола RCP (Remote Copy Protocol — протокол дистанционного копирования) по любому из поддерживаемых видов передающей среды, таким как Ethernet, Token Ring, FDDI (Fiber Distributed Data Interface — распределенный интерфейс передачи данных по волоконно-оптическим каналам), HSSI (High-Speed Serial Interface — высокоскоростной последовательный интерфейс) и по последовательным каналам.
- **Загрузка из флэш-памяти.** Маршрутизаторы могут загружаться из флэш-памяти — энергонезависимого носителя данных, который можно стирать и перепрограммировать с помощью электронных средств.
- **Загрузка из ПЗУ.** Начальная загрузка операционной системы маршрутизаторов может осуществляться с помощью встроенного постоянного запоминающего устройства (ПЗУ).
- **Загрузка с помощью платы флэш-памяти.** Для начальной загрузки маршрутизаторов может применяться съемная плата флэш-памяти.

В настоящем разделе приведены общие сведения о загрузке маршрутизаторов.

Рекомендации по загрузке через сеть

Во время сеансов начальной загрузки по сети маршрутизаторы действуют как обычные хосты. Их трафик маршрутизируется с помощью информации протокола ARP (Address Resolution Protocol — протокол преобразования адресов), SLARP (Serial Line Address Resolution Protocol — протокол преобразования адресов последовательного канала), перенаправлений протокола ICMP или с применением шлюза, заданного по умолчанию. Во время загрузки по сети маршрутизаторы игнорируют динамическую информацию маршрутизации, статические IP-маршруты и информацию о перенаправлении фреймов мостами. Поэтому успешная загрузка маршрутизатора в основном зависит от функционирования промежуточных маршрутизаторов, которые должны правильно обрабатывать запросы ARP и UDP (User Datagram Protocol — протокол пользовательских дейтаграмм). При использовании в качестве передающей среды последовательных каналов и интерфейса HSSI протокол ARP не применяется.

Перед выполнением начальной загрузки по сети с сервера необходимо выполнить эхо-тестирование сервера с помощью программного обеспечения, записанного в ПЗУ. Если эхо-тестирование сервера невозможно выполнить, обратитесь к процедурам, описанным ниже, в разделе “Начальная загрузка: маршрутизатор не может загрузиться по сети от TFTP-сервера”. Если и после этого невозможно выполнить эхо-тестирование сервера, то, вероятно, имеются ошибки в конфигурации сервера или неисправности аппа-

ратных средств. Изучите документацию по TFTP-серверу или обратитесь за помощью к представителю службы технической поддержки.

Надежные методы начальной загрузки

Метод начальной загрузки по сети является очень удобным, но его применение может стать невозможным при нарушениях в работе сети или сервера. После установки и настройки флэш-памяти маршрутизатора необходимо правильно определить последовательность начальной загрузки маршрутизатора, чтобы свести к минимуму влияние нарушений в работе сервера или сети. Рекомендуется следующий порядок загрузки.

1. Загрузка образа системы из флэш-памяти.
2. Загрузка образа системы по сети.
3. Начальная загрузка с применением образа системы, записанного в ПЗУ.

Ниже приведен пример того, как нужно выполнить настройку конфигурации маршрутизатора с учетом указанной последовательности начальной загрузки.

```
goriot# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
goriot(config)# boot system flash gsxx
goriot(config)# boot system gsxx 131.108.1.101
goriot(config)# boot system rom
goriot(config)# ^Z
goriot#
%SYS-5-CONFIG_I: Configured from console by console
goriot# copy running-config startup-config
[ok]
goriot#
```

Если применяется описанный метод, то маршрутизатор имеет три источника информации для начальной загрузки: он может загружаться из флэш-памяти, по сети, а также из ПЗУ. Предоставление альтернативных источников загрузочной информации позволяет уменьшить влияние любых нарушений в работе TFTP-сервера или сети.

Примечание

Чтобы обеспечить загрузку записанного в ПЗУ образа системы после неудачных попыток начальной загрузки по сети, необходимо выполнить настройку регистра конфигурации. Дополнительная информация приведена в руководстве по настройке конфигурации аппаратных средств для конкретной платформы.

Тайм-ауты и пакеты, поступающие с нарушением порядка следования

Во время начальной загрузки по сети клиенту может потребоваться повторно передавать запросы перед получением ответа на определенный ARP-запрос. При таких повторных передачах могут возникать тайм-ауты и появляться пакеты, поступающие с нарушением порядка следования.

Тайм-ауты (показанные точками на дисплее начальной загрузки по сети) и пакеты с нарушением порядка следования (показанные прописными буквами О) не всегда препятствуют успешной начальной загрузке по сети. Поэтому в процессе начальной загрузки по сети вполне допустимо появление тайм-аутов или пакетов с нарушением порядка следования, или тех и иных.

В следующих примерах показан вывод на консоль во время сеансов начальной загрузки по сети, которые оказались успешными, даже несмотря на появление тайм-аутов и пакетов с нарушением порядка следования (восклицательными знаками указаны успешно принятые пакеты):

```
Booting gs3-bfx from 131.108.1.123: !!!!!!!!!!!!!!!!!!!!!!!
```

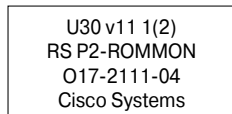
```
Booting gs3-bfx from 131.108.1.123: !O.O!!!!!!!!!!!!!!!!!!!!!!
```

Но если в ходе начальной загрузки по сети появляется слишком много тайм-аутов и пакетов с нарушением порядка следования, то могут возникнуть проблемы. Эти проблемы рассматриваются ниже в этой главе, в разделе “Начальная загрузка: тайм-ауты и пакеты с нарушением порядка следования препятствуют выполнению загрузки по сети”.

Информация для службы технической поддержки

Если вы не можете решить проблему начальной загрузки с использованием процедур, описанных в настоящей главе, подготовьте следующую информацию для представителя службы технической поддержки.

- Версии образов системы, записанных в ПЗУ. (Используйте `exec`-команду `show version`.)
- Надписи на программируемых ПЗУ. (Эта информация отпечатана на корпусе микросхемы и пример ее показан на рис. 3.1.)



```
U30 v11 1(2)
RS P2-ROMMON
O17-2111-04
Cisco Systems
```

Рис. 3.1. Пример надписи на ПЗУ начальной загрузки версии 11.1(2)

- Конфигурации энергонезависимых ОЗУ для клиентского маршрутизатора и смежных маршрутизаторов.
- Отладочный вывод, полученный со смежных маршрутизаторов с использованием следующих привилегированных `exec`-команд:
 - `debug ip packet`;
 - `debug arp`;
 - `debug ip udp`;
 - `debug tftp`.

Дополнительная информация о командах `debug` приведена в справочнике по отладочным командам *Debug Command Reference*.

Поиск неисправностей аппаратных средств

В настоящем разделе описаны процедуры устранения нарушений связи между устройствами, возникающих при начальной загрузке. Здесь описаны конкретные признаки нарушений начальной загрузки, проблемы, которые могут вызвать появление каждого признака неисправности, а также представлены решения этих проблем.

Запуск маршрутизаторов ряда Cisco 7500

При запуске маршрутизаторов ряда Cisco 7500 должно произойти следующее.

- Светодиод AC OK (или DC OK) должен немедленно загореться и продолжать гореть до тех пор, пока в систему подается питание.
- Должен работать внутренний вентилятор.
- Должны загореться светодиоды Normal процессора маршрутизации/коммутации (RSP — Route Switch Processor) и лицевой панели и продолжать гореть на протяжении всего времени функционирования системы; светодиод CPU Halt не должен гореть.
- Должен гореть светодиод Enabled на каждом интерфейсном процессоре (указывая на то, что процессор RSP выполнил инициализацию интерфейсного процессора).

После успешной инициализации системы маршрутизаторов ряда 7500 на экране консоли должна отобразиться системная заставка. Если она не отображается, убедитесь в том, что терминал консоли правильно подключен к порту RSP и настроен должным образом. Системная заставка должна выглядеть примерно так:

```
System Bootstrap, Version 4.6(5), SOFTWARE
Copyright (c) 1986-1995 by cisco Systems
RSP2 processor with 16384 Kbytes of memory
### [...] ###
F3: 2012356+47852+194864 at 0x1000
    Restricted Rights Legend
Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.
    cisco Systems, Inc.
    170 Tasman Drive
    San Jose, CA 95134
GS Software (RSP-K), Version 10.3(571) [fc3], RELEASE SOFTWARE
Copyright (c) 1986-1995 by cisco Systems, Inc.
[...]
Press RETURN to get started!
```

При обнаружении неисправности попытайтесь выяснить, в какой именно подсистеме она возникла. Маршрутизаторы ряда Cisco 7500 имеют следующие подсистемы.

- **Подсистема питания.** Включает блоки питания, внешний силовой кабель и объединительную плату.
- **Подсистема охлаждения.** В зависимости от системы, включает следующее.
 - **Cisco 7505.** Плоский вентиляторный модуль, запасной плоский вентиляторный модуль с шестью отдельными вентиляторами и пультом управления вентиляторами.
 - **Cisco 7507.** Внутренний вентилятор блока.
 - **Cisco 7513.** Модуль внутреннего вентилятора, включая внутренний вентилятор, пульт регулировки скорости внутреннего вентилятора, светодиоды лицевой панели и сам модуль.
- **Подсистема процессора.** В зависимости от системы, включает все интерфейсные процессоры, а также процессоры маршрутизации/коммутации RSP1 или RSP2.

В табл. 3.1 перечислены основные области, в которых могут возникать проблемы при запуске маршрутизаторов ряда Cisco 7500, и описаны решения этих проблем.

Таблица 3.1. Аппаратные средства: проблемы запуска маршрутизаторов ряда Cisco 7500 и их решения

Проблема	Решение
Подсистема питания	<p>Шаг 1. Проверьте, работает ли внутренний вентилятор и горят ли светодиоды на процессорных модулях. Если внутренний вентилятор работает и светодиоды горят, а светодиод источника питания Power Supply не горит, то, вероятно, неисправен светодиод Power Supply.</p> <p>Шаг 2. Убедитесь в том, что выключатель питания установлен правильно в положение “включено”.</p> <p>Шаг 3. Убедитесь в том, что источник питания, силовой кабель и блок питания функционируют нормально. Заменяйте эти компоненты заведомо исправными, чтобы определить, какой из компонентов неисправен.</p> <p>Шаг 4. Проверьте, установлен ли должным образом модуль внутреннего вентилятора. Убедитесь в том, что краевой соединитель блока управления внутреннего вентилятора полностью вставлен в гнездо объединительной платы.</p>
Подсистема охлаждения	<p>Шаг 1. Проверьте, работает ли внутренний вентилятор при запуске системы. Если внутренний вентилятор не работает, то, возможно, неисправен внутренний вентилятор или нарушена подача питания постоянным током с напряжением +24 В.</p> <ul style="list-style-type: none"> • Если горит светодиод Output Fail, то, вероятно, нарушена подача питания постоянным током с напряжением +24 В к внутреннему вентилятору или к плоскому вентиляторному модулю из-за неисправности блока питания или блока управления внутренним вентилятором. • Если внутренний вентилятор не работает и не горит светодиод Output Fail, проверьте, установлен ли должным образом модуль внутреннего вентилятора. Проверьте, полностью ли вставлен в гнездо объединительной платы краевой соединитель блока управления внутренним вентилятором. <p>Шаг 2. Если система и внутренний вентилятор запускаются, а затем останавлива-</p>

ются примерно через 2 минуты, то, возможно, один или несколько вентиляторов неисправны или работают в условиях, выходящих за пределы допустимых. На экране может появиться примерно такое сообщение об ошибке:

%ENVM-2-FAN: Fan has failed, shutdown in 2 minutes

Если произошел отказ внутреннего вентилятора или блока управления внутренним вентилятором, необходимо заменить модуль внутреннего вентилятора.

Шаг 3. Если при запуске появляется следующее сообщение, это означает, что система обнаружила в корпусе состояние перегрева или выходящие за пределы допустимых характеристики питания:

Queued messages:

%ENVM-1-SHUTDOWN: Environmental Monitor initiated shutdown

Окончание табл. 3.1

Проблема	Решение
	<p>Если причиной останова из-за нарушения условий эксплуатации явились характеристики питания, выходящие за пределы допустимых, то перед остановом системы загорается светодиод OutputFail.</p> <p>Приведенное выше сообщение об останове может также указывать на наличие неисправного компонента или датчика температуры. Прежде чем произойдет останов системы, воспользуйтесь командой show environment или show environment table, чтобы ознакомиться с температурными условиями внутри корпуса.</p>
	<p>Шаг 4. Убедитесь в том, что горячий отработанный воздух от другого оборудования не попадает в воздухоприемные отверстия и вокруг корпуса имеется достаточное свободное пространство, которое обеспечивает беспрепятственное протекание охлаждающего воздуха.</p>
Подсистема процессора	<p>Шаг 1. Проверьте светодиод RSP (Route Switch Processor — процессор маршрутизации/коммутации). Если светодиоды не горят, проверьте, функционируют ли должным образом источники питания и внутренний вентилятор.</p> <p>Шаг 2. Проверьте посадку в гнезде процессора RSP. Если процессор RSP не установлен должным образом, это приведет к зависанию системы.</p> <p>Шаг 3. Если горит светодиод CPU Halt процессора RSP, это означает, что система обнаружила отказ аппаратных средств процессора. Обратитесь к представителю службы технической поддержки для получения дальнейших указаний.</p> <p>Шаг 4. Выясните, горит ли светодиод Normal процессора RSP, который указывает, что системное программное обеспечение инициализировано успешно и что система работоспособна.</p> <p>Шаг 5. Проверьте светодиод Enabled на каждом интерфейсном процессоре. Этот светодиод должен гореть, когда происходит инициализация интерфейсного процессора процессором RSP.</p> <p>Шаг 6. Если не горит светодиод Enabled на отдельном интерфейсном процессоре, то, возможно, разъем интерфейсного процессора вынут из гнезда объединительной платы. Если интерфейсные процессоры не установлены долж-</p>

Запуск маршрутизаторов ряда Cisco 7000

При запуске маршрутизаторов ряда Cisco 7000 должно произойти следующее.

- Должен загореться светодиод DC OK и продолжать гореть до тех пор, пока в систему подается питание от сети.
- Вентиляторы должны работать.
- Должен загореться светодиод Normal процессора маршрутизации (RP — Route Processor); светодиод Normal должен продолжать гореть, указывая на то, что система функционирует нормально; светодиод Halt CPU не должен гореть.
- После завершения процессором RP инициализации интерфейсного процессора, процессора коммутации (SP — Switch Processor) или кремниевого процессора коммутации (SSP — Silicon Switch Processor) в ходе его подготовки к работе должен загореться светодиод Enabled процессора SP или SSP, и каждый интерфейсный процессор должен начать работать.

После успешной инициализации системы на экране консоли должна отобразиться системная заставка. Если она не отображается, убедитесь в том, что терминал консоли правильно подключен к порту RP и настроен должным образом. Системная заставка должна выглядеть примерно так:

```
System Bootstrap, Version 4.6(5), SOFTWARE  
Copyright (c) 1986-1995 by cisco Systems  
RP1 processor with 16384 Kbytes of memory  
### [...] ###  
F3: 2012356+47852+194864 at 0x1000
```

Restricted Rights Legend

Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) of the Commercial Computer Software - Restricted Rights clause at FAR sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS sec. 252.227-7013.

cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706

GS Software (GS7), Version 10.3(1) [fc3], RELEASE SOFTWARE
Copyright (c) 1986-1995 by cisco Systems, Inc.

RP1 (68040) processor with 16384K bytes of memory.
[...]

Press RETURN to get started!