FLUKE networks

Устранение сбоев в сетях - борьба на переднем крае

Практика использования универсального сетевого тестера LinkRunner™ компании Fluke Networks

Когда пользователь жалуется сетевому администратору, что у него не работает сеть, его пожелания предельно просты: “Пусть все заработает!”. В современном мире сделать так, чтобы “все заработало”, причем быстро и экономически эффективным путем, чрезвычайно важно для успешного ведения бизнеса. Для любой сети верна закономерность: если у сетевых специалистов есть нужный инструментарий, знания и правильная методология, то сбои устраняются быстро, экономя время и сетевым специалистам, и пользователям, которые могут сразу же вернуться к своей работе.

Сущность и методология устранения сбоев

Ключ к успешному устранению сбоев - детальные знания специалиста о том, как сеть должна работать в нормальных условиях. Это позволяет ему сразу же распознавать отклонения от штатной работы сети. Все остальные подходы подобны блужданию впотьмах.

К сожалению, многие сетевые продукты поставляются без подробных технических характеристик, без описания стратегии применения и других вспомогательных материалов, которые облегчили бы устранение сбоев. Профессиональный сетевой инженер должен глубоко изучить все доступные сетевые данные, детально разобраться в функциях всех компонентов сети и особенностях их совместной работы. Тогда он будет видеть полную картину происходящего и в том числе знать, какие сбои могут быть результатом злоупотреблений, неверных настроек или ошибок пользователей.

Чтобы научиться видеть картину в целом, обычно сетевым специалистам надо проходить курсы обучения. Затем их опыт растет по ходу работы. Настоящий системный администратор, мастер устранения сбоев, закаляется в реальных условиях - накапливает опыт методом проб и ошибок, делится им с коллегами по профессии, отрабатывает практические навыки, которым не учат в школе. Информация, приведенная далее в этой статье, поможет сократить время обучения и познакомит вас с несколькими проверенными способами обнаружения и устранения сетевых проблем.

Опытные сетевые инженеры быстро усваивают простую истину: несколько минут, потраченных на изучение и оценку симптоматики, могут сэкономить часы напряженной работы по устранению не той проблемы, что есть на самом деле. Всю информацию и выявленные симптомы надо оценивать в совокупности, комплексно, учитывая также, как они влияют на общую работоспособность сети. Только таким путем сетевой инженер в состоянии правильно понять суть происходящего.

Пять шагов для успешного устранения сбоев

Для успешного устранения любых проблем, связанных с сетью, важно применять правильную методологию:

1. Документируйте вашу сеть

Если у вас всегда есть под рукой актуальная сетевая документация (физические и логические схемы, базисные характеристики сети, результаты аудита или инвентаризации, настройки, таблицы адресов и привязок к хостам и т.п.), это существенно уменьшает время на устранение сбоя - время, которое, в противном случае, вы вынуждены тратить на работу в режиме обследования, чтобы всего лишь определить, в какой точке сети (общей схемы) подключен персональный компьютер, который, возможно, несет ответственность за возникновение проблемы.

2. Собирайте всю доступную информацию и анализируйте симптомы сбоя

Спросите себя, можете ли вы правильно истолковать обнаруженные симптомы? Может ли пользователь показать проблему “живьем” или вы можете воссоздать ее сами? Определите, изменялось ли что-либо в сети или в настройках самой рабочей станции непосредственно перед тем, как возникла проблема.

Прибор LinkRunner компании Fluke Networks - это карманный тестер для системных администраторов, незаменимый при устранении проблем и сбоев в сетях, особенно на начальных этапах диагностики.

Прибор LinkRunner можно подключать в любой конечной точке сети; он позволяет сетевым инженерам без труда находить неисправности в среде передачи и исключать проблемы с физическим уровнем до того, как проводить диагностику на более высоком уровне.

Прибор LinkRunner идеально подходит для быстрого тестирования подключения на рабочем месте пользователя, что позволяет сходу устранить значительную часть сетевых сбоев - или же правильно подготовиться к следующим этапам диагностики, если проблема окажется более сложной. Подключенный в той точке, где возникла проблема, прибор LinkRunner позволяет проверить ряд критически важных сетевых параметров, а также выдает информацию, на основе которой можно подготовиться к устранению сбоев, причины которых относятся к более высоким уровням модели взаимодействия OSI.

3. Локализуйте сбой

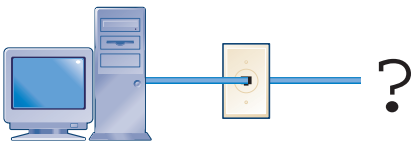
Прежде всего, необходимо сузить зону поиска. Проблема затрагивает целый участок сети или только одного из пользователей? Даже если сбой касается только одного пользователя, причина может быть и в сети, и в физической среде передачи, и в самой рабочей станции. Зачастую процессы сбора информации и локализации проблемы проходят параллельно.

4. Устраните сбой и убедитесь, что проблема исчерпана

Если вы локализовали сбой, то определить его конкретный тип и необходимые меры по устранению будет несложно. Если причина в аппаратном обеспечении, то, скорее всего, придется физически заменить неисправный компонент, например, подключить новый патч-шнур, сменить порт на хабе или коммутаторе на другой или заменить сетевую карту в компьютере. Этот этап работы считается полностью завершенным, как только пользователь, вернувшись к своему компьютеру, убеждается, что проблема исчезла.

5. Задокументируйте свои действия

Вернитесь к пункту 1. Если по каждому возникшему сбою есть запись (о том, как он появился и как был устранен - такую функцию предлагает большинство соответствующих учетных приложений), то из них постепенно сформируется ваша внутренняя база данных. В будущем вы всегда сможете обратиться к ней, если похожая проблема возникнет снова.



Действительно ли нужно так делать?

Хотя операционные системы и программное обеспечение становятся с каждым годом все надежнее, все равно первым ответом системного администратора на жалобу пользователя будет: “Попробуйте перегрузиться”. К сожалению, холодная перезагрузка устраняет так много разных проблем (часть из которых вообще необъяснима!), что этот шаг действительно необходим. Приятный побочный эффект состоит в том, что если перезагрузка устранила проблему, то системному администратору нет нужды вставать и идти на рабочее место пользователя.

Кроме совета перегрузиться, полезно также расспросить пользователя о том, какие симптомы он наблюдает - это можно сделать по телефону, и тогда тоже есть вероятность, что системному инженеру не придется вставать со стула.

Большинство пользователей в состоянии запустить командную строку и сообщить администратору, что они получили в ответ на команду IPCONFIG. Это позволит убедиться, правильный ли адрес подсети установлен в компьютере.

- Если персональный компьютер сконфигурирован по протоколу динамической конфигурации хоста (DHCP), но возвращает в ответ IP-адрес Windows по умолчанию (169.254.x.x), значит, у клиента нет связи с DHCP-сервером.
- Портативные компьютеры обычно используют адрес той сети, к которой они подключаются в настоящий момент (динамический адрес), но иногда настройка DHCP предыдущей сети остается и после того, как компьютер уже перемещен. Попросите пользователя набрать две следующие команды в командной строке:

  C:\>ipconfig /release

  C:\>ipconfig /renew

  Пусть пользователь попробует взять себе другой IP-адрес, который придет ему в ответ на вторую команду. Если команда IPCONFIG выдает в ответ сообщение о том, что DHCP-операцию выполнить невозможно, то, скорее всего, у пользователя установлен статический IP-адрес. Сверьте установленный IP-адрес с вашей документацией.
- Если пользователь подтверждает правильность IP-адреса, попробуйте отправить на него со своего рабочего места запрос ping. Если рабочая станция откликается, то тогда надо попросить пользователя выполнить какое-либо другое действие с сетью, например, зайти на какую-нибудь веб-страницу или отправить запрос ping на локальный маршрутизатор, чтобы убедиться в том, что основное соединение с сетью есть.

Если проделанные тесты проблемы не устраняют, то все-таки придется нанести визит на рабочее место пользователя.

Идентификация сбоя с рабочего места пользователя

Когда сетевой специалист приходит на рабочее место пользователя, очень важно серьезно отнестись к сбору информации о сбое. Расспросите пользователя обо всем, что он делал, когда с сетью возникла проблема. Иногда такой опрос провести нелегко, потому что зачастую пользователи даже не подозревают, как много самых обычных действий, выполненных на рабочей станции, влияет на параметры системы в целом. В худшем же случае пользователь отлично знает: то, что он натворил, делать было категорически нельзя. Тогда он ни за что не признается в этом. Как известно, все сомнения толкуются в пользу обвиняемого, поэтому сначала надо расспросить пользователя обо всех недавних изменениях, включая даже перестановку мебели или скачку новой программки-хранителя экрана.

Повторите лично все те тесты, которые по телефону вы просили провести пользователя. Успешно прошедший запрос ping к сетевому серверу или к устройству за пределами сети немедленно говорит о том, что у рабочей станции проблемы с соединением с сетью на уровне 3 (сетевом) или выше. Тогда тесты всех более низких уровней уже не нужны, так что инженер может не принимать их во внимание.

Если же установку соединения на уровне 3 подтвердить не удается, то вам придется начать с уровня 1.

Если проблема то появляется, то исчезает, или носит нерегулярный характер, то к целевому устройству необходимо отправлять непрерывный запрос ping с бесконечным потоком пакетов с запросами отклика. В ответ вы получите время отклика для каждого успешного запроса ping или время истечения для запросов, не получивших ответа.

C:\> ping -t x.x.x.x

Долгий отклик или пропущенные запросы можно затем проверить, отследив их до целевого устройства с помощью команд TRACERT или PATHPING. Трассировка

покажет, в какой точке пути по сети возникает задержка или пропадают пакеты, и в этой точке надо будет проверить все, начиная с уровня 1.

C:\> tracert x.x.x.x

или

C:\> pathping x.x.x.x

Всегда ли нужна полная диагностика?

Если проблему сразу идентифицировать не удается или по описанию пользователя картина получается неоднозначной, то может потребоваться полный анализ, долгий и сложный. Однако в большинстве случаев для определения проблемы будет вполне достаточно нескольких несложных операций, по тому же принципу, как те вопросы, которые мы рекомендовали задавать пользователю по телефону еще до того, как вы отправитесь на его рабочее место.

Если по описанию пользователя мы можем сделать заключение, что сеть ему действительно недоступна, возникает следующий вопрос: в чем причина - в сети или в персональном компьютере пользователя? Чтобы выяснить это, надо проверить, на месте ли аппаратный шнур, подключающий пользователя к сети, и в рабочем ли он состоянии? Такая проверка сразу устраняет большинство простых проблем и закладывает нужную основу для устранения более сложных. Чтобы сетевые сбои можно было устранять быстро и без финансовых потерь, необходимо, чтобы у каждого сетевого специалиста был под рукой инструмент, который позволяет быстро проверить базовые параметры сети – например, универсальный сетевой тестер LinkRunner Network Multimeter производства компании Fluke Networks.

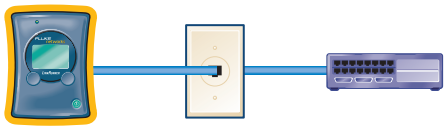
Первые тесты при проведении диагностики на рабочем месте:

1. Тест на наличие соединения
2. Проверка общей активности в сегменте сети
3. Использование DHCP для диагностических целей
4. Отправка запроса ping на локальные и удаленные адреса

Тестирование соединения

Многие сетевые специалисты свято верят в то, что если светодиод на сетевой карте мигает, то подключение к сети есть и оно активно. Хотя это действительно так для некоторых видов оборудования, но в большинстве сетевых устройств светодиоды управляются программным обеспечением хоста, поэтому они “включены” всегда, когда в системе обнаруживается сетевая активность высокого уровня. Некоторые сетевые карты мигают, чтобы показать наличие трафика; в этом случае можно с относительной уверенностью считать, что раз светодиод мигает, то сетевое подключение “живое”. Однако никакие светодиоды не покажут вам ни настройки дуплекса, ни скорость - для этого необходимо предпринимать другие действия.

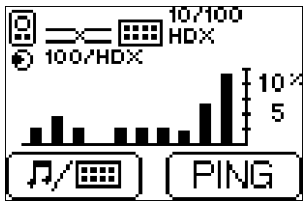
Определить наличие подключения можно с помощью процесса автосогласования, в ходе которого два участника обмениваются информацией о своей скорости и настройках дуплекса. В результате такого обмена участники сравнивают свои возможности, а затем устанавливают соединение друг с другом на максимальной скорости, приемлемой для обоих устройств, и с соответствующими настройками дуплекса. Если у одного из участников не вполне корректные настройки или драйвера работают ненадлежащим образом, то процесс может



Прибор LinkRunner проверяет подключение к сети, отправляя и принимая сигналы в сегменте кабельной системы.

дать сбой: приемлемые для обеих сторон настройки подобрать не удастся, поэтому связь будет неустойчивой, а может, даже будет полностью отсутствовать.

Как только вы подключили тестер LinkRunner к сегменту сети, он сразу же пытается установить связь с устройством на дальнем конце, каким бы оно ни было - хаб, коммутатор или сетевая карта персонального компьютера. Прибор LinkRunner в точности следует процедуре автосогласования, как она описана в стандарте IEEE 802.3, при этом его светодиодный индикатор контролируется аппаратно, а не программным обеспечением. После того, как автосогласование успешно завершится, светодиод прибора LinkRunner будет гореть ярким зеленым светом, а результирующие скорость и дуплекс будут показаны в верхнем левом углу экрана.



На экране тестера LinkRunner показаны параметры успешно установленного соединения: скорость, дуплекс и процент использования.

Все большее количество сетевых инфраструктур переходит на принцип работы “коммутация до рабочего места”: новые сети сразу же исповедуют этот подход, а старые модернизируются. Преимущества полностью коммутируемой архитектуры очевидны: сегментирование трафика, предотвращение распространения ошибок Ethernet по всей сети. К сожалению, коммутируемая среда маскирует некоторые проблемы низких уровней, которые напрямую влияют на характеристики отдельных сегментов сети, и инженерам остается только гадать, работает ли подключение нормально или нет.

Более подробная информация о процессе автосогласования в сетях Ethernet, о проблемах, которые могут возникать, если он дает сбой, и о том, как их определять и устранять, содержится в технической статье на нашем веб-сайте: **flukenetworks.com/autonegotiation**.

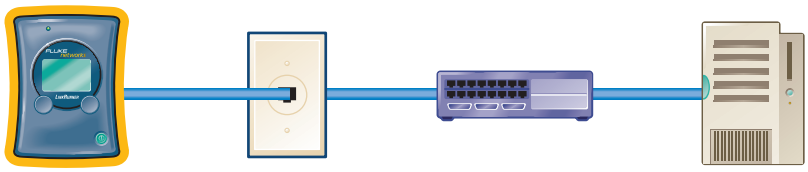
Проверка общей активности в сегменте сети

Если в кабеле присутствует сетевой трафик, прибор LinkRunner показывает на экране степень использования в виде гистограммы. Однако следует помнить, что если среда не является совместно используемой, если мы подключены к одиночному порту коммутатора, то единственным видимым трафиком могут быть широковещательные пакеты, которые по своей природе могут быть весьма неоднородны в сетях с небольшим трафиком.

Если вы тестируете совместно используемую среду Ethernet, где по-прежнему вместо коммутаторов используются хабы, то весьма вероятно, что сеть использует полудуплекс. Полудуплексный Ethernet ограничивает и количество станций, которые могут вести передачу одновременно, и размеры передаваемых пакетов. Если вести передачу одновременно пытается слишком много станций, то производительность Ethernet может значительно ухудшиться из-за коллизий. Если же вы тестируете сеть, в которой каждая станция подключена к отдельному порту коммутатора, риск чрезмерных коллизий уменьшается до пренебрежимо малого значения.

Хотя существование коллизий - нормальное явление для полудуплексных сетей Ethernet, тем не менее, существует очень неприятный эффект лавины: когда количество коллизий растет вместе с ростом трафика, сам трафик начинает увеличиваться за счет перепосылки пакетов. В результате производительность сети не просто снижается, а резко падает, при том, что количество отправленных пакетов, количество коллизий, а также пакетов, вынужденно отправленных повторно, растет как снежный ком. Как это всегда бывает, если производительность резко упала - ждите шквала жалоб от пользователей.

В большинстве сетей Ethernet обычный уровень трафика незначителен, и тогда проблему надо искать где-то в другом месте. Прибор LinkRunner может предоставить вам базовую статистику по уровням использования в сегменте, и это может стать ключом к пониманию проблем с низкой производительностью сети.



Успешное назначение DCHP-адреса подтверждает, что пользователь имеет работающее сетевое подключение и в состоянии получить правильный IP-адрес: это проверка с первого по третий сетевой уровень за один шаг.

Использование DHCP для диагностических целей

Если удалось установить соединение, а уровень использования похож на правду, то теперь следует нажать кнопку, оправляющую запрос ping. Прибор LinkRunner попытается получить от DHCP-сервера корректный IP-адрес. Поскольку нормальная работа DHCP основана на широковещательной технологии, то либо необходимо ставить по отдельному DHCP-серверу для каждой подсети (что дорого и сложно с точки зрения управления), либо использовать агенты-ретрансляторы DHCP, сортирующие и перенаправляющие запросы и отклики между клиентами и серверами, физически находящимися в разных подсетях. Такие вспомогательные приложения на маршрутизаторах, регулирующие широковещательные рассылки - самый распространенный способ работы для корпоративных сетей, где предпочитают держать DHCP-сервера только в центре сети, в штаб-квартире. Невозможность автоматически получить от DHCP-сервера корректную настройку для клиента или прибора LinkRunner указывает на возможные проблемы системой ретрансляции DHCP.

Хотя в большинстве современных сетей используется протокол DHCP, тем не менее, прибор LinkRunner позволяет установить IP-адрес и вручную, статически. Успешное получение DHCP-адреса свидетельствует о том, что кабель, порт хаба или коммутатора и вся сетевая инфраструктура до DHCP-сервера работают корректно. Одна простая процедура позволяет проверить прилегающие участки сетевой инфраструктуры вплоть до уровня 3.

Отправка запроса ping на локальные и удаленные адреса

Запрос ping - одно из самых популярных средств диагностики в истории компьютерных сетей. Эта функция включена во все распространенные операционные системы, которые предусматривают взаимодействие с Интернет, и когда нужно провести диагностику сбоя, чаще всего сетевые инженеры используют ее первой. Почему эта простая утилита так полезна?

По сути, отправка запроса ping сродни методам, используемым в гидролокации для изучения дна океана. Утилита ping посылает сигнал (как правило, пакет ICMP с запросом отклика), который “отражается” устройством назначения (точнее, оно генерирует сигнал-отклик), что позволяет отправителю удостовериться, что устройство назначения находится в нужном месте, а заодно определить, сколько времени занимает путь сигнала туда и обратно.

Получив в самом начале адрес от DHCP-сервера и настроившись на него, прибор LinkRunner немедленно начинает отправку тестовых запросов ping к DNS-серверу (проверяя службу доменных имен) и к маршрутизатору, установленному по умолчанию. Адреса обоих были получены в ходе конфигурирования протокола DHCP.

Запрос ping можно отправлять и в локальные системы, и транзитом в удаленные, через Интернет.

Прибору LinkRunner можно дополнительно задать до четырех IP-адресов, один из которых можно отвести для функции автоматической отправки запросов ping. Успешное получение отклика на запрос ping при проверке веб-приложений, при идентификации пользователя и т.п. показывает, что эти сетевые сервисы принципиально доступны с рабочей станции клиента.

Сам факт прохождения запроса ping свидетельствует о том, что в сети вплоть до уровня 3 существует связь между двумя устройствами. Период кругового обращения (время путешествия сигнала туда и обратно) следует сравнить с известными значениями, и это уже дает вам представление о работе сети, достаточное для того, чтобы решить, нужно ли применить более глубокий анализ. Тем не менее, запросы ICMP сами по себе относятся к трафику с низким приоритетом, поэтому они могут оказаться отброшенными, если один из маршрутизаторов в сетевом пути или устройство назначения заняты. Вот почему следует отправлять запросы ping сериями - это даст устройству назначения больше возможностей ответить.

Сервера за пределами корпоративной сети тоже можно использовать в качестве точек назначения запросов ping, это позволяет проверить связь по глобальной сети между рабочей станцией клиента и локальным или удаленным узлом. Если сервера в пределах ответственности брандмауэра отвечают на запрос ping, а за пределами - нет, то сетевому инженеру стоит проверить маршрутизаторы или другие пограничные сетевые устройства - проблема может заключаться в них. Если часть серверов отвечает, а другая часть - нет, следует проанализировать отдельные сегменты сети и выяснить, почему они недоступны. Если запросы ping успешно получают отклик как от внутренних, так и от внешних серверов, включая приложения и сервисы, но клиент ими воспользоваться не может, значит, проблема возникает на каком-то другом уровне - она не связана с физической передачей сигналов. Успешное прохождение запросов ping говорит о том, что определенные типы трафика достигают сервера назначения; значит, невозможность получить доступ к каким-либо сервисам связана с учетной записью или настройками сервера.

Что дальше?

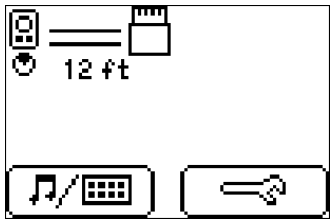
Если проблему не удалось сходу идентифицировать и устранить с помощью описанных тестов “первой помощи”, то дальнейшие события могут развиваться по двум возможным направлениям.

- Если тесты показывают, что отсутствует связь, нет подключения к Ethernet, надо внимательно проверить сетевой кабель.
- Если первые тесты прошли успешно, связь есть, в сегменте присутствует некоторый трафик, похожий на обычный, от DHCP-сервера удается получить адреса, и запросы ping к самым важным сетевым серверам проходят успешно, тогда проблема, скорее всего, возникает на более высоких сетевых уровнях. И разрешать их также следует на соответствующих сетевых уровнях: администратору надо будет проверять настройки учетной записи и конфигурацию рабочей станции.

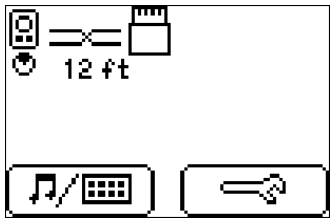
Тестирование кабеля

Первый кабель, который обязательно надо проверять - это патч-шнур, подключающий рабочую станцию или другое устройство к настенной розетке. Для такой проверки следует подключить один конец патч-шнура к сетевому гнезду прибора LinkRunner, а другой - ко второму гнезду, специально предназначенному для тестирования схемы разводки. Если с патч-шнуром все в порядке, его можно снова подключить к настенной или напольной розетке и использовать в следующих этапах тестирования.

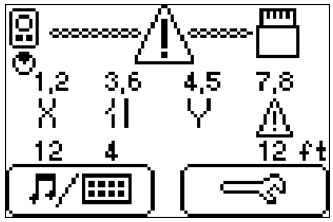
Затем необходимо проверить, не кроется ли проблема со средой передачи в других участках кабеля - от стенной розетки до порта ближайшего коммутатора. Если в телекоммуникационном помещении очень много разных сетевых подключений, то найти нужный кабель в массе других, лежащих в трассе, не так-то легко - на это может потребоваться масса времени. Но прибор LinkRunner оснащен двумя функциями, которые существенно облегчают эту задачу и сводят затраты времени к минимуму. Тестер LinkRunner может работать как тон-генератор, подавая



Так прибор LinkRunner показывает, что патч-шнур нормальный...



...что патч-шнур кроссоверный...



...и что патч-шнур очень плохой.

в кабель тональный сигнал, который можно обнаруживать специальным детектором. С помощью стандартного детектора кабели можно перебрать по порядку, пока тональный сигнал не укажет на нужный из них. Эта методика используется в тех случаях, когда точно не известно, подключен ли кабель к коммутатору, или в документации нет данных о том, какая настенная розетка к какому порту ведет.

После того, как удаленный конец сегмента обнаружен, к нему следует подключить адаптер для тестирования схемы разводки: LinkRunner Wiremap Adapter или один из аксессуаров к прибору - например, идентификатор LinkRunner Cable ID, заказываемый дополнительно. При таком подключении схема разводки и наличие контакта проверяются во всем горизонтальном сегменте.

Одновременно с тональным сигналом прибор Link Runner подает в кабель питание, чтобы светодиод над портом коммутатора мигал каждые три секунды. Эта функция очень облегчает поиск нужного порта. Когда порт установлен,

попробуйте переключить патч-шнур в другой (свободный) порт. Довольно часто порты, с которыми что-то не в порядке или которые уже совсем вышли из строя, все еще показывают светодиодами наличие подключения, и в таких случаях простая смена порта устраняет проблему.

Если же порт хаба или коммутатора в порядке, то проблему надо искать на рабочей станции. Сетевую карту на рабочей станции можно проверить, подключив к ней прибор LinkRunner напрямую. Так же, как и с портами хаба или коммутатора, тестер LinkRunner покажет наличие соединения, скорость и настройки дуплекса, предлагаемые сетевой картой. Если соединение есть, то следует перезагрузить компьютер или использовать утилиту командной строки для отправки запроса ping, чтобы сгенерировать трафик, который прибор LinkRunner сможет оценить. Если LinkRunner не показывает никакого трафика вообще (даже если персональный компьютер подтверждает, что ведет передачу), то необходимо проверить привязку драйверов и другие параметры конфигурации персонального компьютера. Если прибор LinkRunner сообщает о наличии и соединения, и трафика от персонального компьютера, то тогда следует детально проверять сетевые настройки персонального компьютера.

Диагностика на более высоких уровнях

Если рабочая станция устанавливает связь с сетью, то следующий этап проверки - убедиться, что адрес рабочей станции соответствует маске подсети, в которой она физически находится. Проверьте, чтобы рабочая станция оперировала правильным набором протоколов и чтобы они были правильно настроены. Наконец, сетевой инженер должен убедиться, что на компьютере установлены все необходимые программные компоненты и библиотеки. Обычно это проверяется путем удаления и последующей установки заново протокола или сетевой карты в конфигурации рабочей станции. Если все нужные компоненты на месте и правильно сконфигурированы, но при этом рабочая станция все еще не может корректно подключиться к сети и запустить соответствующие приложения, это говорит о том, что проблема имеет более высокий уровень и потребует проведения сетевого анализа другими техническими средствами.

Нужный инструмент для нужной задачи

Прибор LinkRunner, недорогой и простой в работе - это правильный инструмент для повседневного использования. Сетевые специалисты всегда носят его с собой, в руке или на поясе. Наличие нужного инструмента под рукой во многих случаях избавит вас от сложного, продолжительного и дорогого сетевого тестирования с помощью ноутбука.

Любой сетевой специалист вам скажет, что наивное предположение о том, что клиентская часть сети “точно работает нормально” только создает проблемы, вместо того, чтобы помогать решать их. В процесс неоправданно вовлекаются лишние участники, принимаются политические и организационные меры, порой дело доходит до того, что поддержкой сети и пользователей занимаются два отдела вместо одного. Хотя политически вроде все выглядит просто, техническая часть неоправданно усложняется - так, вместо жалобы на сбой с настольным компьютером (который несложно устранить) вы в итоге получаете претензии к работе сетевых устройств и общее недовольство сетевой инфраструктурой.

В таких случаях правильная идентификация проблемы (ее связь с сегментом сети или отсутствие этой связи) позволяет быстро найти и устранить ее причину без проведения дорогостоящей диагностики. Большую часть проблем в итоге можно разрешать на уровне обычных сетевых инженеров, не привлекая к работе ИТ-специалистов более высокой квалификации; при этом растет эффективность работы, в том числе и в финансовом отношении. Более сложные и дорогие устройства следует применять лишь в тех случаях, когда они действительно необходимы, в ходе же обычной эксплуатации для устранения простых проблем следует применять такие устройства как LinkRunner.

NETWORKSUPERVISION

Fluke Networks
P.O. Box 777, Everett, WA USA 98206-0777

Компания Fluke Networks представлена в более чем 50 странах по всему миру. Чтобы найти ближайшее к вам представительство, зайдите на веб-сайт **www.flukenetworks.com/contact**.

Напечатано в США. 12/2003 2566738 A-RUS-N Rev A