Искусство диагностики локальных сетей

Если программы периодически работают медленно, компьютеры "зависают" или отключаются от сервера, и программисты при этом говорят, что во всем виновата сеть, а администратор сети, - что во всем виноваты программы, то эта статья адресована именно вам.

Данная статья начинает серию публикаций, посвященных вопросам диагностики и тестирования локальных сетей. Изложенный в этой и последующих статьях материал не что иное, как обобщение многолетнего практического опыта компании "ПроЛАН" по выявлению "скрытых дефектов" и "узких мест" локальных сетей.

Прежде чем приступить к описанию методики выявления "скрытых дефектов", мы хотели бы определиться с терминами: что, собственно, понимается под локальной сетью, диагностикой локальной сети и какую сеть следует считать "хорошей".

Очень часто под диагностикой локальной сети подразумевают тестирование только ее кабельной системы. Это не совсем верно. Кабельная система является одной из важнейших составляющих локальной сети, но далеко не единственной и не самой сложной с точки зрения диагностики. Помимо состояния кабельной системы на качество работы сети значительное влияние оказывает состояние активного оборудования (сетевых плат, концентраторов, коммутаторов), качество оборудования сервера и настройки сетевой операционной системы. Кроме того, функционирование сети существенно зависит от алгоритмов работы эксплуатируемого в ней прикладного программного обеспечения.

Под термином "локальная сеть" мы будем понимать весь комплекс указанных выше аппаратных и программных средств; а под термином "диагностика локальной сети" - процесс определения причин неудовлетворительной работы прикладного ПО в сети. Именно качество работы прикладного ПО в сети оказывается определяющим, с точки зрения пользователей. Все прочие критерии, такие как число ошибок передачи данных, степень загруженности сетевых ресурсов, производительность оборудования и т. п., являются вторичными. "Хорошая сеть" - это такая сеть, пользователи которой не замечают, как она работает.

Основных причин неудовлетворительной работы прикладного ПО в сети может быть несколько: повреждения кабельной системы, дефекты активного оборудования, перегруженность сетевых ресурсов (канала связи и сервера), ошибки самого прикладного ПО. Часто одни дефекты сети маскируют другие. Таким образом, чтобы достоверно определить, в чем причина неудовлетворительной работы прикладного ПО, локальную сеть требуется подвергнуть комплексной диагностике. Комплексная диагностика предполагает выполнение следующих работ (этапов).

- Выявление дефектов физического уровня сети: кабельной системы, системы электропитания активного оборудования; наличия шума от внешних источников.
- Измерение текущей загруженности канала связи сети и определение влияния величины загрузки канала связи на время реакции прикладного ПО.
- Измерение числа коллизий в сети и выяснение причин их возникновения.
- Измерение числа ошибок передачи данных на уровне канала связи и выяснение причин их возникновения.
- Выявление дефектов архитектуры сети.
- Измерение текущей загруженности сервера и определение влияния степени его загрузки на время реакции прикладного ПО.
- Выявление дефектов прикладного ПО, следствием которых является неэффективное использование пропускной способности сервера и сети.

В рамках данной статьи мы рассмотрим первые четыре этапа комплексной диагностики локальной сети, а именно: диагностику канального уровня сети.

Мы не будем подробно описывать методику тестирования кабельной системы сети. Несмотря на важность этой проблемы, ее решение тривиально и однозначно: полноценно кабельная система может быть протестирована только специальным прибором - кабельным сканером. Другого способа не существует. Нет смысла заниматься трудоемкой процедурой выявления дефектов сети, если их можно локализовать одним нажатием клавиши AUTOTEST на кабельном сканере. При этом прибор выполнит полный комплекс тестов на соответствие кабельной системы сети выбранному стандарту.

Хотелось бы обратить ваше внимание на два момента, тем более что о них часто забывают при тестировании кабельной системы сети с помощью сканера.

Режим AUTOTEST не позволяет проверить уровень шума создаваемого внешним источником в кабеле. Это может быть шум от люминесцентной лампы, силовой электропроводки, сотового телефона, мощного копировального аппарата и др. Для определения уровня шума кабельные сканеры имеют, как правило, специальную функцию. Поскольку кабельная система сети полностью проверяется только на этапе ее инсталляции, а шум в кабеле может возникать непредсказуемо, нет полной гарантии того, что шум проявится именно в период полномасштабной проверки сети на этапе ее инсталляции.

При проверке сети кабельным сканером вместо активного оборудования к кабелю подключаются с одного конца - сканер, с другого - инжектор. После проверки кабеля сканер и инжектор отключаются, и подключается активное оборудование: сетевые платы, концентраторы, коммутаторы. При этом нет полной гарантии того, что контакт между активным оборудованием и кабелем будет столь же хорош, как между оборудованием сканера и кабелем. Мы неоднократно встречались со случаями, когда незначительный дефект вилки RJ-45 не проявлялся при тестировании кабельной системы сканером, но обнаруживался при диагностике сети анализатором протоколов.

В рамках предлагаемой методики мы не будем рассматривать ставшую хрестоматийной методику упреждающей диагностики сети (см. врезку "Методика упреждающей диагностики сети"). Не подвергая сомнению важность упреждающей диагностики, заметим только, что на практике она используется редко. Чаще всего (хоть это и неправильно) сеть анализируется только в периоды ее неудовлетворительной работы. В таких случаях локализовать и исправить имеющиеся дефекты сети требуется быстро. Предлагаемую нами методику следует рассматривать как частный случай методики упреждающей диагностики сети.

ОРГАНИЗАЦИЯ ПРОЦЕССА ДИАГНОСТИКИ СЕТИ

Любая методика тестирования сети существенно зависит от имеющихся в распоряжении системного администратора средств. По нашему мнению, в большинстве случаев необходимым и достаточным средством для обнаружения дефектов сети (кроме кабельного сканера) является анализатор сетевых протоколов. Он должен подключаться к тому домену сети (collision domain), где наблюдаются сбои, в максимальной близости к наиболее подозрительным станциям или серверу (см. Правило # 3.3).

Если сеть имеет архитектуру с компактной магистралью (collapsed backbone) и в качестве магистрали используется коммутатор, то анализатор необходимо подключать к тем портам коммутатора, через которые проходит анализируемый трафик. Некоторые программы имеют специальные агенты или зонды (probes), устанавливаемые на компьютерах, подключенных к удаленным портам коммутатора. Обычно агенты (не путать с агентами SNMP) представляют собой сервис или задачу, работающую в фоновом режиме на компьютере пользователя. Как правило, агенты потребляют мало вычислительных ресурсов и не мешают работе пользователей, на компьютерах которых они установлены. Анализаторы и агенты могут быть подключены к коммутатору двумя способами.

При первом способе (см. Рисунок 1а) анализатор подключается к специальному порту (порту мониторинга или зеркальному порту) коммутатора, если таковой имеется, и на него по очереди направляется трафик со всех интересующих портов коммутатора.

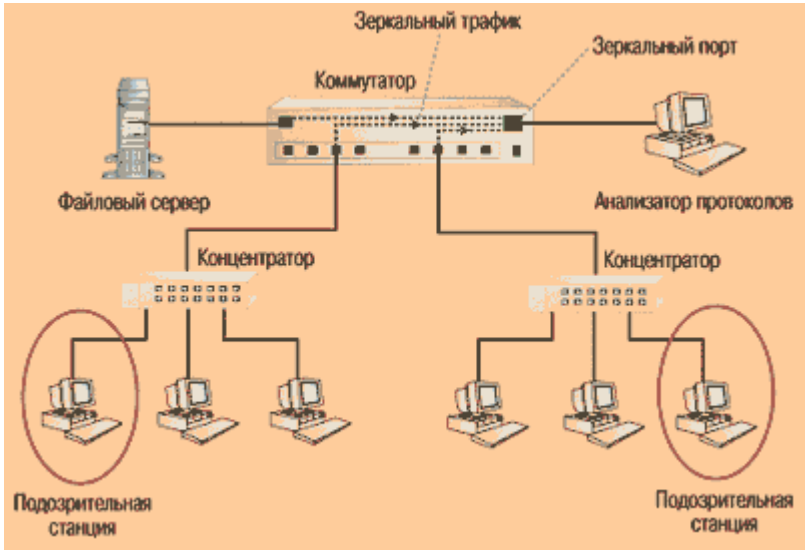

Рисунок 1а.
Зеркальный трафик со всех портов коммутатора по очереди направляется на порт коммутатора, к которому подключен анализатор протоколов.

Если в коммутаторе специальный порт отсутствует, то анализатор (или агент) следует подключать к портам интересующих доменов сети в максимальной близости к наиболее подозрительным станциям или серверу (см. Рисунок 1б). Иногда это может потребовать использования дополнительного концентратора. Согласно Правилу # 3.3, данный способ предпочтительнее первого. Исключение составляет случай, когда один из портов коммутатора работает в полнодуплексном режиме. Если это так, то порт предварительно необходимо перевести в полудуплексный режим.

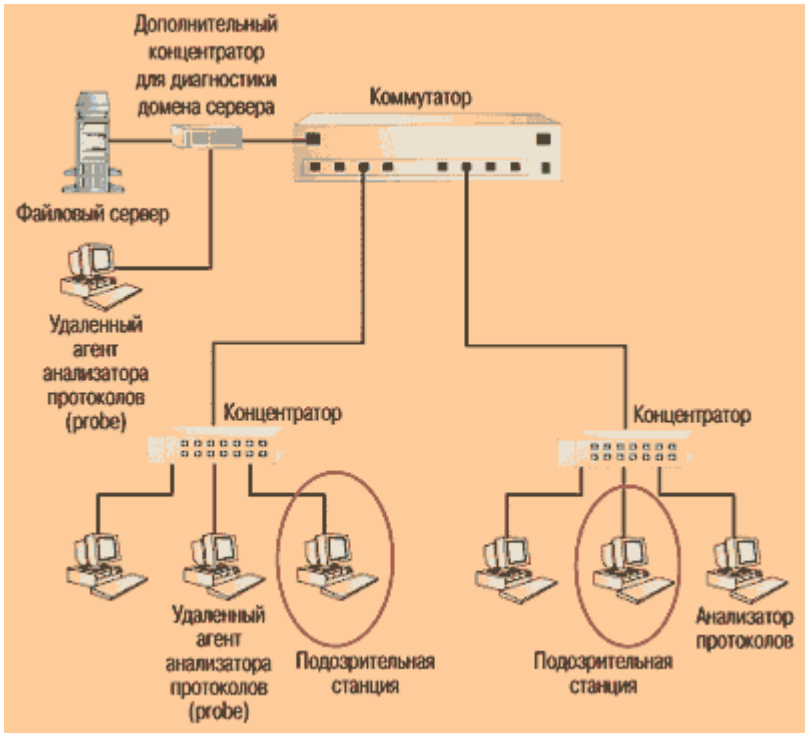

Рисунок 1б.
Анализатор протоколов и удаленные агенты контролируют основные домены сети. Для диагностики домена сервера используется дополнительный концентратор.

Первый ЭТАП

Измерение утилизации сети и установление корреляции между замедлением работы сети и перегрузкой канала связи.

Утилизация канала связи сети - это процент времени, в течение которого канал связи передает сигналы, или иначе - доля пропускной способности канала связи, занимаемой кадрами, коллизиями и помехами. Параметр "Утилизация канала связи" характеризует величину загруженности сети.

Канал связи сети является общим сетевым ресурсом, поэтому его загруженность влияет на время реакции прикладного программного обеспечения. Первоочередная задача состоит в определении наличия взаимозависимости между плохой работой прикладного программного обеспечения и утилизацией канала связи сети.

Предположим, что анализатор протоколов установлен в том домене сети (collision domain), где прикладное ПО работает медленно. Средняя утилизация канала связи составляет 19%, пиковая доходит до 82%. Можно ли на основании этих данных сделать достоверный вывод о том, что причиной медленной работы программ в сети является перегруженность канала связи? Вряд ли.

Часто можно слышать о стандарте де-факто, в соответствии с которым для удовлетворительной работы сети Ethernet утилизация канала связи "в тренде" (усредненное значение за 15 минут) не должна превышать 20%, а "в пике" (усредненное значение за 1 минуту) - 35-40%. Приведенные значения объясняются тем, что в сети Ethernet при утилизации канала связи, превышающей 40%, существенно возрастает число коллизий и, соответственно, время реакции прикладного ПО. Несмотря на то что такие рассуждения в общем случае верны, безусловное следование подобным рекомендациям может привести к неправильному выводу о причинах медленной работы программ в сети. Они не учитывают особенности конкретной сети, а именно: тип прикладного ПО, протяженность домена сети, число одновременно работающих станций.

Чтобы определить, какова же максимально допустимая утилизация канала связи в вашем конкретном случае, мы рекомендуем следовать приведенным ниже правилам.

Правило # 1.1. Если в сети Ethernet в любой момент времени обмен данными происходит не более чем между двумя компьютерами, то любая сколь угодно высокая утилизация сети является допустимой.

Сеть Ethernet устроена таким образом, что если два компьютера одновременно конкурируют друг с другом за захват канала связи, то через некоторое время они синхронизируются друг с другом и начинают выходить в канал связи строго по очереди. В таком случае коллизий между ними практически не возникает.

Если рабочая станция и сервер обладают высокой производительностью, и между ними идет обмен большими порциями данных, то утилизация в канале связи может достигать 80-90% (особенно в пакетном режиме - burst mode). Это абсолютно не замедляет работу сети, а, наоборот, свидетельствует об эффективном использовании ее ресурсов прикладным ПО.

Таким образом, если в вашей сети утилизация канала связи высока, постарайтесь определить, сколько компьютеров одновременно ведут обмен данными. Это можно сделать, например, собрав и декодировав пакеты в интересующем канале в период его высокой утилизации.

Правило # 1.2. Высокая утилизация канала связи сети только в том случае замедляет работу конкретного прикладного ПО, когда именно канал связи является "узким местом" для работы данного конкретного ПО.

Кроме канала связи узкие места в системе могут возникнуть из-за недостаточной производительности или неправильных параметров настройки сервера, низкой производительности рабочих станций, неэффективных алгоритмов работы самого прикладного ПО.

В какой мере канал связи ответственен за недостаточную производительность системы, можно выяснить следующим образом. Выбрав наиболее массовую операцию данного прикладного ПО (например, для банковского ПО такой операцией может быть ввод платежного поручения), вам следует определить, как утилизация канала связи влияет на время выполнения такой операции.

Проще всего это сделать, воспользовавшись функцией генерации трафика, имеющейся в ряде анализаторов протоколов (например, в Observer). С помощью этой функции интенсивность генерируемой нагрузки следует наращивать постепенно, и на ее фоне производить измерения времени выполнения операции. Фоновую нагрузку целесообразно увеличивать от 0 до 50-60% с шагом не более 10%.

Если время выполнения операции в широком интервале фоновых нагрузок не будет существенно изменяться, то узким местом системы является не канал связи. Если же время выполнения операции будет существенно меняться в зависимости от величины фоновой нагрузки (например, при 10% и 20% утилизации канала связи время выполнения операции будет значительно

различаться), то именно канал связи, скорее всего, ответственен за низкую производительность системы, и величина его загруженности критична для времени реакции прикладного ПО. Зная желаемое время реакции ПО, вы легко сможете определить, какой утилизации канала связи соответствует желаемое время реакции прикладного ПО.

В данном эксперименте фоновую нагрузку не следует задавать более 60-70%. Даже если канал связи не является узким местом, при таких нагрузках время выполнения операций может возрасти вследствие уменьшения эффективной пропускной способности сети.

Правило # 1.3. Максимально допустимая утилизация канала связи зависит от протяженности сети.

При увеличении протяженности домена сети допустимая утилизация уменьшается. Чем больше протяженность домена сети, тем позже будут обнаруживаться коллизии. Если протяженность домена сети мала, то коллизии будут выявлены станциями еще в начале кадра, в момент передачи преамбулы. Если протяженность сети велика, то коллизии будут обнаружены позже - в момент передачи самого кадра. В результате накладные расходы на передачу пакета (IP или IPX) возрастают. Чем позже выявлена коллизия, тем больше величина накладных расходов и большее время тратится на передачу пакета. В результате время реакции прикладного ПО, хотя и незначительно, но увеличивается.

Выводы. Если в результате проведения диагностики сети вы определили, что причина медленной работы прикладного ПО - в перегруженности канала связи, то архитектуру сети необходимо изменить. Число станций в перегруженных доменах сети следует уменьшить, а станции, создающие наибольшую нагрузку на сеть, подключить к выделенным портам коммутатора.

На рынке имеется множество разнообразных анализаторов протоколов - от чисто программных до программно-аппаратных. Несмотря на функциональную идентичность большинства анализаторов протоколов, каждый из них обладает теми или иными достоинствами и недостатками. В этой связи мы хотели бы обратить внимание на две важные функции, без которых эффективную диагностику сети провести будет затруднительно.

Во-первых, анализатор протоколов должен иметь встроенную функцию генерации трафика (см. Правило # 3.4). Во-вторых, анализатор протоколов должен уметь "прореживать" принимаемые кадры, т. е. принимать не все кадры подряд, а, например, каждый пятый или каждый десятый с обязательной последующей аппроксимацией полученных результатов. Если эта функция отсутствует, то при сильной загруженности сети, какой бы производительностью ни обладал компьютер, на котором установлен анализатор, последний будет "зависать" и/или терять кадры. Это особенно важно при диагностике быстрых сетей типа Fast Ethernet и FDDI.

Предлагаемую методику мы будем иллюстрировать на примере использования чисто программного анализатора протоколов Observer компании Network Instruments, работающего в среде Windows 95 и Windows NT. С нашей точки зрения, этот продукт обладает всеми необходимыми функциями для эффективного проведения диагностики сетей.

Итак, предположим, что прикладное программное обеспечение в вашей сети Ethernet стало работать медленно, и вам необходимо оперативно локализовать и ликвидировать дефект.

Второй ЭТАП

Измерение числа коллизий в сети.

Если две станции домена сети одновременно ведут передачу данных, то в домене возникает коллизия. Коллизии бывают трех типов: местные, удаленные, поздние.

Местная коллизия (local collision) - это коллизия, фиксируемая в домене, где подключено измерительное устройство, в пределах передачи преамбулы или первых 64 байт кадра, когда источник передачи находится в домене. Алгоритмы обнаружения местной коллизии для сети на основе витой пары (10BaseT) и коаксиального кабеля (10Base2) отличны друг от друга.

В сети 10Base2 передающая кадр станция определяет, что произошла локальная коллизия по изменению уровня напряжения в канале связи (по его удвоению). Обнаружив коллизию, передающая станция посылает в канал связи серию сигналов о заторе (jam), чтобы все остальные станции домена узнали, что произошла коллизия. Результатом этой серии сигналов оказывается появление в сети коротких, неправильно оформленных кадров длиной менее 64 байт с неверной контрольной последовательностью CRC. Такие кадры называются фрагментами (collision fragment или runt).

В сети 10BaseT станция определяет, что произошла локальная коллизия, если во время передачи кадра она обнаруживает активность на приемной паре (Rx).

Удаленная коллизия (remote collision) - это коллизия, которая возникает в другом физическом сегменте сети (т. е. за повторителем). Станция узнает, что произошла удаленная коллизия, если она получает неправильно оформленный короткий кадр с неверной контрольной последовательностью CRC, и при этом уровень напряжения в канале связи остается в

установленных пределах (для сетей 10Base2). Для сетей 10BaseT/100BaseT показателем является отсутствие одновременной активности на приемной и передающей парах (Tx и Rx).

Поздняя коллизия (late collision) - это местная коллизия, которая фиксируется уже после того, как станция передала в канал связи первые 64 байт кадра. В сетях 10BaseT поздние коллизии часто фиксируются измерительными устройствами как ошибки CRC.

Если выявление локальных и удаленных коллизий, как правило, еще не свидетельствует о наличии в сети дефектов, то обнаружение поздних коллизий - это явное подтверждение наличия дефекта в домене. Чаще всего это связано с чрезмерной длиной линий связи или некачественным сетевым оборудованием.

Помимо высокого уровня утилизации канала связи коллизии в сети Ethernet могут быть вызваны дефектами кабельной системы и активного оборудования, а также наличием шумов.

Даже если канал связи не является узким местом системы, коллизии несущественно, но замедляют работу прикладного ПО. Причем основное замедление вызывается не столько самим фактом необходимости повторной передачи кадра, сколько тем, что каждый компьютер сети после возникновения коллизии должен выполнять алгоритм отката (backoff algorithm): до следующей попытки выхода в канал связи ему придется ждать случайный промежуток времени, пропорциональный числу предыдущих неудачных попыток.

В этой связи важно выяснить, какова причина коллизий - высокая утилизация сети или "скрытые" дефекты сети. Чтобы это определить, мы рекомендуем придерживаться следующих правил.

Правило # 2.1. Не все измерительные приборы правильно определяют общее число коллизий в сети.

Практически все чисто программные анализаторы протоколов фиксируют наличие коллизии только в том случае, если они обнаруживают в сети фрагмент, т. е. результат коллизии. При этом наиболее распространенный тип коллизий - происходящие в момент передачи преамбулы кадра (т. е. до начального ограничителя кадра (SFD)) - программные измерительные средства не обнаруживают, так уж устроен набор микросхем сетевых плат Ethernet. Наиболее точно коллизии обнаруживают аппаратные измерительные приборы, например LANMeter компании Fluke.

Правило # 2.2. Высокая утилизация канала связи не всегда сопровождается высоким уровнем коллизий.

Уровень коллизий будет низким, если в сети одновременно работает не более двух станций (см. Правило # 1.1) или если небольшое число станций одновременно ведут обмен длинными кадрами (что особенно характерно для пакетного режима). В этом случае до начала передачи кадра станции "видят" несущую в канале связи, и коллизии редки.

Правило # 2.3. Признаком наличия дефекта в сети служит такая ситуация, когда невысокая утилизация канала (менее 30%) сопровождается высоким уровнем коллизий (более 5%).

Если кабельная система предварительно была протестирована сканером, то наиболее вероятной причиной повышенного уровня коллизий является шум в линии связи, вызванный внешним источником, или дефектная сетевая плата, неправильно реализующая алгоритм доступа к среде передачи (CSMA/CD).

Компания Network Instruments в анализаторе протоколов Observer оригинально решила задачу выявления коллизий, вызванных дефектами сети. Встроенный в программу тест провоцирует возникновение коллизий: он посылает в канал связи серию пакетов с интенсивностью 100 пакетов в секунду и анализирует число возникших коллизий. При этом совмещенный график. отображает зависимость числа коллизий в сети от утилизации канала связи.

Долю коллизий в общем числе кадров имеет смысл анализировать в момент активности подозрительных (медленно работающих) станций и только в случае, когда утилизация канала связи превышает 30%. Если из трех кадров один столкнулся с коллизией, то это еще не означает, что в сети есть дефект.

В анализаторе протоколов Observer график, показанный на Рисунке 3, меняет цвет в зависимости от числа коллизий и наблюдаемой при этом утилизации канала связи.

Правило # 2.4. При диагностике сети 10BaseT все коллизии должны фиксироваться как удаленные, если анализатор протоколов не создает трафика.

Если вы пассивно (без генерации трафика) наблюдаете за сетью 10BaseT и физический сегмент в месте подключения анализатора (измерительного прибора) исправен, то все коллизии должны фиксироваться как удаленные.

Если тем не менее вы видите именно локальные коллизии, то это может означать одно из трех: физический сегмент сети, куда подключен измерительный прибор, неисправен; порт концентратора или коммутатора, куда подключен измерительный прибор, имеет дефект, или измерительный прибор не умеет различать локальные и удаленные коллизии.

Правило # 2.5. Коллизии в сети могут быть следствием перегруженности входных буферов коммутатора.

Следует помнить, что коммутаторы при перегруженности входных буферов эмулируют коллизии, дабы "притормозить" рабочие станции сети. Этот механизм называется "управление потоком" (flow control).

Правило # 2.6. Причиной большого числа коллизий (и ошибок) в сети может быть неправильная организация заземления компьютеров, включенных в локальную сеть.

Если компьютеры, включенные в сеть, не имеют общей точки заземления (зануления), то между корпусами компьютеров может возникать разность потенциалов. В персональных компьютерах "защитная" земля объединена с "информационной" землей. Поскольку компьютеры объединены каналом связи локальной сети, разность потенциалов между ними приводит к возникновению тока по каналу связи. Этот ток вызывает искажение информации и является причиной коллизий и ошибок в сети. Такой эффект получил название ground loop или inter ground noise.

Аналогичный эффект возникает в случае, когда сегмент коаксиального кабеля заземлен более чем в одной точке. Это часто случается, если Т-соединитель сетевой платы соприкасается с корпусом компьютера.

Обращаем ваше внимание на то, что установка источника бесперебойного питания не снимает описанных трудностей. Наиболее подробно данные проблемы и способы их решения рассматриваются в материалах компании APC (American Power Conversion) в "Руководстве по защите электропитания" (Power Protection Handbook).

При обнаружении большого числа коллизий и ошибок в сетях 10Base2 первое, что надо сделать, - проверить разность потенциалов между оплеткой коаксиального кабеля и корпусами компьютеров. Если ее величина для любого компьютера в сети составляет более одного вольта по переменному току, то в сети не все в порядке с топологией линий заземления компьютеров.

ТРЕТИЙ ЭТАП

Измерение числа ошибок на канальном уровне сети.

В сетях Ethernet наиболее распространенными являются следующие типы ошибок.

Короткий кадр - кадр длиной менее 64 байт (после 8-байтной преамбулы) с правильной контрольной последовательностью. Наиболее вероятная причина появления коротких кадров - неисправная сетевая плата или неправильно сконфигурированный или испорченный сетевой драйвер.

Последнее время мы наблюдаем большое число ошибок этого типа на относительно медленных компьютерах (486/SX), работающих под Windows 95 с сетевыми платами NE2000. Причина нам неизвестна.

Длинный кадр (long frame) - кадр длиннее 1518 байт. Длинный кадр может иметь правильную или неправильную контрольную последовательность. В последнем случае такие кадры обычно называют jabber. Фиксация длинных кадров с правильной контрольной последовательностью указывает чаще всего на некорректность работы сетевого драйвера; фиксация ошибок типа jabber - на неисправность активного оборудования или наличие внешних помех.

Ошибки контрольной последовательности (CRC error) - правильно оформленный кадр допустимой длины (от 64 до 1518 байт), но с неверной контрольной последовательностью (ошибка в поле CRC).

Ошибка выравнивания (alignment error) - кадр, содержащий число бит, не кратное числу байт.

Блики (ghosts) - последовательность сигналов, отличных по формату от кадров Ethernet, не содержащая разделителя (SFD) и длиной более 72 байт. Впервые данный термин был введен компанией Fluke с целью дифференциации различий между удаленными коллизиями и шумами в канале связи.

Блики являются наиболее коварной ошибкой, так как они не распознаются программными анализаторами протоколов по той же причине, что и коллизии на этапе передачи преамбулы. Выявить блики можно специальными приборами или с помощью метода стрессового тестирования сети (мы планируем рассказать об этом методе в последующих публикациях).

Рискуя навлечь на себя праведный гнев дистрибьюторов программ сетевого управления на основе SNMP, мы осмелимся, тем не менее, утверждать, что степень влияния ошибок канального уровня сети на время реакции прикладного ПО сильно преувеличена.

В соответствии с общепринятым стандартом де-факто число ошибок канального уровня не должно превышать 1% от общего числа переданных по сети кадров. Как показывает опыт, эта величина перекрывается только при наличии явных дефектов кабельной системы сети. При этом многие

серьезные дефекты активного оборудования, вызывающие многочисленные сбои в работе сети, не проявляются на канальном уровне сети (см. Правило # 3.8).

Правило # 3.1. Прежде чем анализировать ошибки в сети, выясните, какие типы ошибок могут быть определены сетевой платой и драйвером платы на компьютере, где работает ваш программный анализатор протоколов.

Работа любого анализатора протоколов основана на том, что сетевая плата и драйвер переводятся в режим приема всех кадров сети (promiscuous mode). В этом режиме сетевая плата принимает все проходящие по сети кадры, а не только широковещательные и адресованные непосредственно к ней, как в обычном режиме. Анализатор протоколов всю информацию о событиях в сети получает именно от драйвера сетевой платы, работающей в режиме приема всех кадров.

Не все сетевые платы и сетевые драйверы предоставляют анализатору протоколов идентичную и полную информацию об ошибках в сети. Сетевые платы 3Com вообще никакой информации об ошибках не выдают. Если вы установите анализатор протоколов на такую плату, то значения на всех счетчиках ошибок будут нулевыми.

EtherExpress Pro компании Intel сообщают только об ошибках CRC и выравнивания. Сетевые платы компании SMC предоставляют информацию только о коротких кадрах. NE2000 выдают почти полную информацию, выявляя ошибки CRC, короткие кадры, ошибки выравнивания, коллизии.

Сетевые карты D-Link (например, DFE-500TX) и Kingstone (например, KNE 100TX) сообщают полную, а при наличии специального драйвера - даже расширенную, информацию об ошибках и коллизиях в сети.

Ряд разработчиков анализаторов протоколов предлагают свои драйверы для наиболее популярных сетевых плат.

Правило # 3.2. Обращайте внимание на "привязку" ошибок к конкретным MAC-адресам станций.

При анализе локальной сети вы, наверное, обращали внимание, что ошибки обычно "привязаны" к определенным MAC-адресам станций. Однако коллизии, произошедшие в адресной части кадра, блики, нераспознанные ситуации типа короткого кадра с нулевой длиной данных не могут быть "привязаны" к конкретным MAC-адресам.

Если в сети наблюдается много ошибок, которые не связаны с конкретными MAC-адресами, то их источником, скорее всего, является не активное оборудование. Вероятнее всего, такие ошибки - результат коллизий, дефектов кабельной системы сети или сильных внешних шумов. Они могут быть также вызваны низким качеством или перебоями питающего активное оборудование напряжения.

Если большинство ошибок привязаны к конкретным MAC-адресам станций, то постарайтесь выявить закономерность между местонахождением станций, передающих ошибочные кадры, расположением измерительного прибора (см. Правила # 3.3, # 3.4) и топологией сети.

Правило # 3.3. В пределах одного домена сети (collision domain) тип и число ошибок, фиксируемых анализатором протоколов, зависят от места подключения измерительного прибора.

Другими словами, в пределах сегмента коаксиального кабеля, концентратора или стека концентраторов картина статистики по каналу может зависеть от места подключения измерительного прибора.

Многим администраторам сетей данное утверждение может показаться абсурдным, так как оно противоречит принципам семиуровневой модели OSI. Впервые столкнувшись с этим явлением, мы также не поверили результату и решили, что измерительный прибор неисправен. Мы проверяли данный феномен с разными измерительными приборами, от чисто программных до программно-аппаратных. Результат был тот же.

Одна и та же помеха может вызвать фиксацию ошибки CRC, блика, удаленной коллизии или вообще не обнаруживаться в зависимости от взаимного расположения источника помех и измерительного прибора. Одна и та же коллизия может фиксироваться как удаленная или поздняя в зависимости от взаимного расположения конфликтующих станций и измерительного прибора. Кадр, содержащий ошибку CRC на одном концентраторе стека, может быть не зафиксирован на другом концентраторе того же самого стека.

Следствием приведенного эвристического правила является тот факт, что программы сетевого мониторинга на основе протокола SNMP не всегда адекватно отражают статистику ошибок в сети. Причина этого в том, что встроенный в активное оборудование агент SNMP всегда следит за состоянием сети только из одной точки. Так, если сеть представляет собой несколько стеков "неинтеллектуальных" концентраторов, подключенных к "интеллектуальному" коммутатору, то SNMP-агент коммутатора может иногда не видеть части ошибок в стеке концентраторов.

Подтверждение приведенного правила можно найти на серверах Web компаний Fluke (www.fluke.com) и Net3 Group (www.net3group.com).

Рекомендациям по разрешению описанного феномена посвящены Правила ## 3.4 и 3.5. Правило # 3.4. Для выявления ошибок на канальном уровне сети измерения необходимо проводить на фоне генерации анализатором протоколов собственного трафика.

Генерация трафика позволяет обострить имеющиеся проблемы и создает условия для их проявления. Трафик должен иметь невысокую интенсивность (не более 100 кадров/с) и способствовать образованию коллизий в сети, т. е. содержать короткие (<100 байт) кадры.

При выборе анализатора протоколов или другого диагностического средства внимание следует обратить прежде всего на то, чтобы выбранный инструмент имел встроенную функцию генерации трафика задаваемой интенсивности. Эта функция имеется, в частности, в анализаторах Observer компании Network Instruments и NetXray компании Cinco (ныне Network Associates).

Правило # 3.5. Если наблюдаемая статистика зависит от места подключения измерительного прибора, то источник ошибок, скорее всего, находится на физическом уровне данного домена сети (причина - дефекты кабельной системы или шум внешнего источника). В противном случае источник ошибок расположен на канальном уровне (или выше) или в другом, смежном, домене сети.

Правило # 3.6. Если доля ошибок CRC в общем числе ошибок велика, то следует определить длину кадров, содержащих данный тип ошибок.

Как мы уже отмечали, ошибки CRC могут возникать в результате коллизий, дефектов кабельной системы, внешнего источника шума, неисправных трансиверов. Еще одной возможной причиной появления ошибок CRC могут быть дефектные порты концентратора или коммутатора, которые добавляют в конец кадра несколько "пустых" байтов.

При большой доле ошибок CRC в общем числе ошибок целесообразно выяснить причину их появления. Для этого ошибочные кадры из серии надо сравнить с аналогичными хорошими кадрами из той же серии. Если ошибочные кадры будут существенно короче хороших, то это, скорее всего, результаты коллизий. Если ошибочные кадры будут практически такой же длины, то причиной искажения, вероятнее всего, является внешняя помеха. Если же испорченные кадры длиннее хороших, то причина кроется, вероятнее всего, в дефектном порту концентратора или коммутатора, которые добавляют в конец кадра "пустые" байты.

Сравнить длину ошибочных и правильных кадров проще всего посредством сбора в буфер анализатора серии кадров с ошибкой CRC.

Правило # 3.7. Таблица 1 систематизирует причины ошибок и коллизий для этапов 2 и 3.

Таблица 1 - Типы ошибок и коллизий, фиксируемые ИЗМЕРИТЕЛЬНЫМ СРЕДСТВОМ

Причина ошибок	Локальные коллизии	Удаленные коллизии	Поздние коллизии	Короткий кадр	Длинный кадр	Jabber	Ошибка CRC
Дефектная сетевая плата	>5% при U<30%	>5% при U<30%	Есть	Есть	Есть	Есть	Есть
Дефектный драйвер платы				Есть	Есть	Есть	Есть
Дефектный концентратор, повторитель, трансивер	>5% при U<30%	>5% при U<30%	Есть			Есть	Есть
Неправильное подключение активного оборудования	>5% при U<30%	>5% при U<30%	Есть			Есть	
Слишком длинный кабель			Есть				Есть
Более 4							

повторителей или объединенных в каскад концентраторов							
Неправильное заземление компьютеров или коаксиального кабеля	>5% при U<30%	>5% при U<30%	Есть			Есть	Есть
Дефекты кабельной системы и пассивного оборудования	>5% при U<30%	>5% при U<30%	Есть			Есть	Есть
Источник шума рядом с кабельной системой	>5% при U<30%	>5% при U<30%	Есть			Есть	Есть
Примечание. U - утилизация канала связи							

Если вы впервые диагностируете свою сеть и в ней наблюдаются проблемы, то не следует ожидать, что в вашей сети дефектен только один компонент.

Наиболее надежным способом локализации дефектов является поочередное отключение подозрительных станций, концентраторов и кабельных трасс, тщательная проверка топологии линий заземления компьютеров (особенно для сетей 10Base2).

Если сбои в сети происходят в непредсказуемые моменты времени, не связанные с активностью пользователей, проверьте уровень шума в кабеле с помощью кабельного сканера. При отсутствии сканера визуально убедитесь, что кабель не проходит вблизи сильных источников электромагнитного излучения: высоковольтных или сильноточных кабелей, люминесцентных ламп, электродвигателей, копировальной техники и т. п.

Правило # 3.8. Отсутствие ошибок на канальном уровне еще не гарантирует того, что информация в вашей сети не искажается.

В начале данного раздела уже упоминалось, что влияние ошибок канального уровня на работу сети сильно преувеличено. Следствием ошибок нижнего уровня является повторная передача кадров. Благодаря высокой скорости сети Ethernet (особенно Fast Ethernet) и высокой производительности современных компьютеров, ошибки нижнего уровня не оказывает существенного влияния на время реакции прикладного ПО.

Мы очень редко встречались со случаями, когда ликвидация только ошибок нижних (канального и физического) уровней сети позволяла существенно улучшить время реакции прикладного ПО. В основном проблемы были связаны с серьезными дефектами кабельной системы сети.

Значительно большее влияние на работу прикладного ПО в сети оказывают такие ошибки, как бесследное исчезновение или искажение информации в сетевых платах, маршрутизаторах или коммутаторах при полном отсутствии информации об ошибках нижних уровней. Мы употребляем слово "информация", так как в момент искажения данные еще не оформлены в виде кадра.

Причина таких дефектов в следующем. Информация искажается (или исчезает) "в недрах" активного оборудования - сетевой платы, маршрутизатора или коммутатора. При этом приемо-передающий блок этого оборудования вычисляет правильную контрольную последовательность (CRC) уже искаженной ранее информации, и корректно оформленный кадр передается по сети. Никаких ошибок в этом случае, естественно, не фиксируется. SNMP-агенты, встроенные в активное оборудование, здесь ничем помочь не могут.

Иногда кроме искажения наблюдается исчезновение информации. Чаще всего оно происходит на дешевых сетевых платах или на коммутаторах Ethernet-FDDI. Механизм исчезновения информации в последнем случае понятен. В ряде коммутаторов Ethernet-FDDI обратная связь быстрого порта с медленным (или наоборот) отсутствует, в результате другой порт не получает информации о перегруженности входных/выходных буферов быстрого (медленного) порта. В этом случае при интенсивном трафике информация на одном из портов может пропасть.

Опытный администратор сети может возразить, что кроме защиты информации на канальном уровне в протоколах IPX и TCP/IP возможна защита информации с помощью контрольной суммы.

В полной мере на защиту с помощью контрольной суммы можно полагаться, только если прикладное ПО в качестве транспортного протокола задействует TCP или UDP. Только при их использовании контрольной суммой защищается весь пакет. Если в качестве "транспорта" применяется IPX/SPX или непосредственно IP, то контрольной суммой защищается лишь заголовок пакета.

Даже при наличии защиты с помощью контрольной суммы описанное искажение или исчезновение информации вызывает существенное увеличение времени реакции прикладного ПО.

Если же защита не установлена, то поведение прикладного ПО может быть непредсказуемым.

Помимо замены (отключения) подозрительного оборудования выявить такие дефекты можно двумя способами.

Первый способ заключается в захвате, декодировании и анализе кадров от подозрительной станции, маршрутизатора или коммутатора. Признаком описанного дефекта служит повторная передача пакета IP или IPX, которой не предшествует ошибка нижнего уровня сети. Некоторые анализаторы протоколов и экспертные системы упрощают задачу, выполняя анализ трассы или самостоятельно вычисляя контрольную сумму пакетов.

Вторым способом является метод стрессового тестирования сети.

Выводы. Основная задача диагностики канального уровня сети - выявить наличие повышенного числа коллизий и ошибок в сети и найти взаимосвязь между числом ошибок, степенью загруженности канала связи, топологией сети и местом подключения измерительного прибора. Все измерения следует проводить на фоне генерации анализатором протоколов собственного трафика.

Если установлено, что повышенное число ошибок и коллизий не является следствием перегруженности канала связи, то сетевое оборудование, при работе которого наблюдается повышенное число ошибок, следует заменить.

Если не удается выявить взаимосвязи между работой конкретного оборудования и появлением ошибок, то проведите комплексное тестирование кабельной системы, проверьте уровень шума в кабеле, топологию линий заземления компьютеров, качество питающего напряжения.

Сергей Семенович Юдицкий - генеральный директор ЗАО "ПроЛАН", с ним можно связаться по адресу: ssy@testlab.ipu.rssi.ru. Владислав Витальевич Борисенко - системный инженер ЗАО "ПроЛАН", с ним можно связаться по адресу: slw@testlab.ipu.rssi.ru. Виктор Сергеевич Подлазов - эксперт ЗАО "ПроЛАН".

КАКИЕ ПАРАМЕТРЫ НЕОБХОДИМО ОТСЛЕЖИВАТЬ ПРИ ДИАГНОСТИКЕ СЕТИ?

Методика упреждающей диагностики сети

Методика упреждающей диагностики заключается в следующем. Администратор сети должен непрерывно или в течение длительного времени наблюдать за работой сети. Такие наблюдения желательно проводить с момента ее установки. На основании этих наблюдений администратор должен определить, во-первых, как значения наблюдаемых параметров влияют на работу пользователей сети и, во-вторых, как они изменяются в течение длительного промежутка времени: рабочего дня, недели, месяца, квартала, года и т. д.

Наблюдаемыми параметрами обычно являются:

- параметры работы канала связи сети - утилизация канала связи, число принятых и переданных каждой станцией сети кадров, число ошибок в сети, число широковещательных и многоадресных кадров и т. п.;
- параметры работы сервера - утилизация процессора сервера, число отложенных (ждущих) запросов к диску, общее число кэш-буферов, число "грязных" кэш-буферов и т. п.

Зная зависимость между временем реакции прикладного ПО и значениями наблюдаемых параметров, администратор сети должен определить максимальные значения параметров, допустимые для данной сети. Эти значения вводятся в виде порогов (thresholds) в диагностическое средство. Если в процессе эксплуатации сети значения наблюдаемых параметров превысят

пороговые, то диагностическое средство проинформирует об этом событии администратора сети. Такая ситуация свидетельствует о наличии в сети проблемы.

Наблюдая достаточно долго за работой канала связи и сервера, вы можете установить тенденцию изменения значений различных параметров работы сети (утилизации ресурсов, числа ошибок и т. п.). На основании таких наблюдений администратор может сделать выводы о необходимости замены активного оборудования или изменения архитектуры сети.

В случае появления в сети проблемы, администратор в момент ее проявления должен записать в специальный буфер или файл дамп канальной трассы и на основании анализа ее содержимого сделать выводы о возможных причинах проблемы.

Статья опубликована с разрешения журнала

Журнал сетевых решений/LAN

№07-08 1998 г

ОТКРЫТЫЕ СИСТЕМЫ