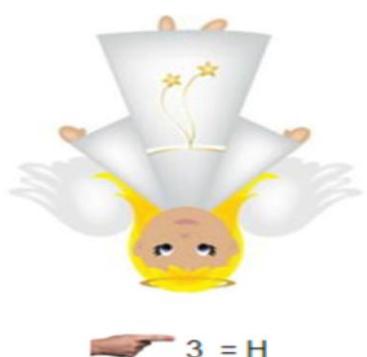


“ О ” Т
Я

Д д Я



3 = H

З ” Я



**ИЗМЕРЕНИЕ ЧИСЛА КОЛЛИЗИЙ В СЕТИ.
ИЗМЕРЕНИЕ ЧИСЛА ОШИБОК НА
КАНАЛЬНОМ УРОВНЕ СЕТИ.
МЕТОДИКА УПРЕЖДАЮЩЕЙ
ДИАГНОСТИКИ СЕТИ.**

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).

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.

ДЛЯ ВЫЯВЛЕНИЯ ПРИЧИНЫ КОЛЛИЗИЙ ИСПОЛЬЗУЮТСЯ СЛЕДУЮЩИЕ ПРАВИЛА.

ПРАВИЛО 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.
- ✘ Наиболее точно коллизии обнаруживают аппаратные измерительные приборы, например LANMeter компании Fluke.

ПРАВИЛО 2

Высокая утилизация канала связи не всегда сопровождается высоким уровнем коллизий.

- ✘ Уровень коллизий будет низким, если в сети одновременно работает не более двух станций 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 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).

ПРАВИЛО 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 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 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, то между корпусами компьютеров может возникать разность потенциалов.

-
- ✘ 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**.

ИЗМЕРЕНИЕ ЧИСЛА ОШИБОК НА КАНАЛЬНОМ УРОВНЕ СЕТИ

В сетях Ethernet наиболее распространенными являются следующие типы ошибок.

- ✘ **Короткий кадр** - кадр длиной менее 64 байт с правильной контрольной последовательностью. Наиболее вероятная причина появления коротких кадров - неисправная сетевая плата или неправильно сконфигурированный или испорченный сетевой драйвер.

✘ **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.

В соответствии с общепринятым стандартом де-факто число ошибок канального уровня не должно превышать **1%** от общего числа переданных по сети кадров.

ПРАВИЛО 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.

ПРАВИЛО 2

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

- ✘ При анализе локальной сети, 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.

ПРАВИЛО 3

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

ПРАВИЛО 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.

МЕТОДИКА УПРЕЖДАЮЩЕЙ ДИАГНОСТИКИ СЕТИ

- ✘ 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
 - + во-вторых, как они изменяются в течение длительного промежутка времени: рабочего дня, недели, месяца, квартала, года и т. д.

ПАРАМЕТРЫ НАБЛЮДЕНИЯ

- ✘ **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 администратора сети. Такая ситуация свидетельствует о наличии в сети проблемы.

KAb,,



, Yb



