Устранение источников и причин появления нежелательного сетевого трафика

Ваша сеть может обладать пропускной способностью и всеми возможностями, которые имеет восьмирядная скоростная автострада в солнечное воскресное утро. Как и транспорт на этой слабо загруженной дороге, ваш трафик без «бутылочных горлышек» движется быстро: препятствий можно избежать, объездных путей мало и встречаются они редко, а возникающие время от времени скопления транспорта быстро рассасываются.

Но что делать, если некоторые машины крайне нуждаются в ремонте? В то время как другие мчатся по шоссе, плохо работающие машины начинают создавать заторы. Сама автострада в отличном состоянии, но по мере того, как машины, которые уже давно следовало отправить в автомастерскую, занимают всё больше рядов, движение по всему шоссе замедляется.

Нежелательный сетевой трафик происходит из нескольких источников и часто становится причиной его обработки устройствами в сети, что препятствует использованию «открытой автострады» вашими пользователями.

Например:

- Чрезмерный объем широковещательного трафика плохо воздействует на конечные станции, которые определяют, нужен ли им этот трафик
- Нежелательные протоколы могут свидетельствовать об устарелой или неправильной конфигурации устройств
- Использование заводских настроек портов коммутаторов может приводить к появлению значительных объемов нежелательного трафика и периодически замедлять работу сети

Обнаружение источников нежелательного трафика и принятие мер по исправлению либо устранению причин, лежащих в основе этого явления, может повысить производительность сети и поможет избежать дальнейших проблем. Однако без соответствующих инструментов и методов устранения неисправностей эта работа может затянуться надолго.

Для быстрого поиска нежелательного трафика и устройства или устройств, которые вызывают эту проблему, можно использовать сетевой помощник EtherScope™ компании Fluke Networks. EtherScope также предоставляет статистику, которая помогает установить степень отрицательного воздействия неполадки на вашу сеть, и тесты для определения того, имеют ли изменения конфигурации нужный эффект.

Чрезмерный объем широковещательного трафика

Широковещательный трафик – важная часть практически любой сети. Однако в связи с тем, что каждая конечная станция, получающая пакет широковещательного трафика, должна его обработать, желательно сократить общий объем такого трафика. Чрезмерное количество пакетов широковещательного трафика также может свидетельствовать о неисправности в оборудовании или конфигурации и даже об активности злоумышленников. В обычной сети число широковещательных пакетов может быть либо очень маленьким, либо перегружать сеть. В этом деле первым шагом должна стать проверка объема широковещательного трафика, а следующим – определение того, является ли он чрезмерным в вашей сети. Прибор EtherScope отслеживает трафик по его типу и MAC-адресам. Вы сможете быстро узнать, какие устройства генерируют наибольшее количество широковещательных пакетов. EtherScope имеет функцию автоматического обнаружения устройств и связывает

Рис. 1. Статистика трафика по типу и MAC-адресам

полученный сетевой трафик с устройством, которое является его источником, для создания списка «источников загрузки канала». С помощью этого списка, выбрав меню «Broadcasts» (Широковещательные пакеты), вы сможете моментально просмотреть главные источники широковещательного трафика.

Рис. 2. Окно «Top Talkers» (Источники загрузки)

EtherScope также обнаруживает топологию второго уровня в вашей сети. В процессе обнаружения EtherScope определяет комму-

татор и порт коммутатора, через который конечные устройства подключаются к сети, что позволяет вам принять соответствующие меры, в том числе временно отключить порт коммутатора для исследования неполадки.

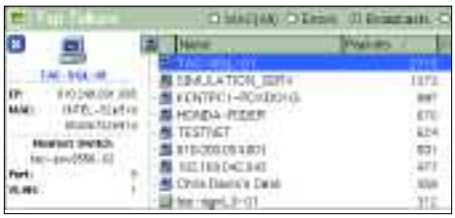

Рис. 3. Сведения о ближайшем к источнику загрузки коммутаторе

Ненужные протоколы

По мере развития сетей и сетевых служб и в процессе замены и модернизации серверов и клиентов растет вероятность того, что сеть будет перегружена ненужными, зачастую устаревшими протоколами. Каждая ситуация уникальна, но важно знать, где искать эти протоколы, и располагать устройством, которое показывает не только то, какие устройства используют какие протоколы, но и место их подключения к сети.

EtherScope контролирует весь сетевой трафик и автоматически создает статистику по протоколам на базе обширного списка типов протоколов и портов TCP и UDP. Сочетание статистики по протоколам и функции обнаружения устройств – самый легкий способ определить, какие протоколы действуют в вашей сети и кто их использует. Для обнаружения исходных устройств, использующих ненужный протокол, щелкните данный протокол. Затем щелкните устройство, чтобы найти источник в сети.

Рис. 4. Отслеживание коммутатора

Для упрощения работы EtherScope отображает только те протоколы, которые были обнаружены в процессе проверки. Если пакет невозможно приписать к номеру известного порта, устройство отправляет его в список «Другое», например, «Other TCP» (Другой TCP). Это способствует выявлению пользователей, на компьютерах которых могут быть запущены нежелательные приложения или действуют вирусы.

Функция EtherScope по обнаружению устройств содержит механизм, который может значительно повысить результативность работы в сетях, использующих управляющую или административную виртуальную локальную сеть для разделения данных пользователей и трафика инфраструктуры. Обычно устройства в другой виртуальной локальной сети не подлежат обнаружению. Давая пользователям возможность создавать список устройств в управляющей виртуальной сети, EtherScope предоставляет полную картину соединений второго уровня от коммутаторов до устройств конечных пользователей, тем самым облегчая поиск источников ненужных протоколов.

Рис. 5. Сведения об устройстве

Заводские конфигурации коммутаторов

Нежелательный сетевой трафик и даже временные неполадки в работе исправной сети могут быть побочным эффектом использования заводских настроек. Вам следует обратить внимание на протокол Spanning-Tree Protocol (STP, протокол связующего дерева), который используется почти в каждой коммутируемой сети. Большинство производителей по умолчанию включают протокол STP для каждого порта коммутатора. Это разумное решение, поскольку оно позволяет быстро подключать новые устройства и, кроме того, защищает сеть от возникновения перенаправляющих циклов при росте сети. Когда состояние интерфейса меняется, например, исчезает связь с другим коммутатором, STP использует специальный блок данных протокола моста (BPDU, Bridge Protocol Data Unit), который называется уведомлением об изменении топологии (TCN, Topology Change Notification). Данный механизм очень эффективно работает в стабильной сети, и присутствие уведомлений TCN обычно не является проблемой.

Проблема, которая может вызвать неожиданные последствия, возникает в ситуации, когда протокол STP включается для портов, которые действительно часто меняют состояние. Поскольку TCN создается в случае отказа порта, находившегося в состоянии перенаправления, или перехода порта в состояние перенаправления, в том числе всякий раз, когда конечный пользователь подключается к сети, начинается процесс TCN, который влияет на каждый мост в связующем дереве. В худшем случае, если в сети большое количество пользователей, которые подключаются и отключаются, сеть может практически непрерывно находиться в состоянии изменения топологии. Воздействие на сеть состоит в том, что время существования записи о перенаправлении в таблице моста (номинально 5 минут) сокращается до эффективных 15 секунд, что может привести к очень высокому уровню лавинной маршрутизации при повторном определении коммутаторами каждого соединения.

Если вы хотите изменить заводскую настройку портов коммутатора, то можете воспользоваться функцией Telnet или эмулятора терминалов EtherScope для получения доступа к коммутатору и настройки портов. Соответствующие команды для настройки коммутаторов см. в документации по коммутатору.

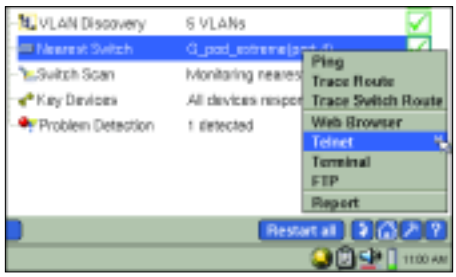

Рис. 6. Использование функции Telnet или эмулятора терминалов для изменения конфигурации коммутатора

Заключение

Нежелательный трафик не только причиняет неудобства для пользователей, но и приводит к путанице при устранении неисправностей сети, которые трудно обнаружить. Знание возможных причин и источников нежелательного трафика может быть важной составляющей содержания сети в хорошем состоянии и эффективной работы. Вооружившись автоматизированными инструментами, такими как сетевой помощник Fluke Networks EtherScope, и зная, где и что искать, вы выйдете победителем из борьбы с любой неисправностью.

Посетите веб-сайт **www.flukenetworks.com/etherscope**, чтобы посмотреть виртуальную демонстрацию работы EtherScope или заказать пробное тестирование в вашей сети.

NETWORKSUPERVISION

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

Fluke Networks работает более чем в 50 странах мира. За информацией о местных дистрибьюторах и представительствах обращайтесь на сайт **www.flukenetworks.com/contact**.

Напечатано в США. 2/2005 2671158 A-RUS-N Ред. A