ЗАЩИТА ОТ ШИРОКОВЕЩАТЕЛЬНЫХ ШТОРМОВ В СЕТЯХ ПРОВАЙДЕРОВ

Раджабов Ф.Р. Email: Radzhabov 693@scientifictext.ru

Раджабов Фарид Рауфович – сервисный инженер,
АО «Nvision Business Solutions, г. Москва

Аннотация: *несмотря на интеллектуальность и эффективность современного сетевого оборудования, широковещательный шторм остается актуальной проблемой сетевого администрирования. Принимая во внимание «скудность теоретической базы, допускающей практическое применение», поиск прикладных методов на основе экспериментов для профилактики появления или обнаружения широковещательного шторма является востребованным в решении задачи повышения производительности сетей провайдеров.*

Целью настоящей работы является поиск, обзор и анализ практических методов обнаружения широковещательного трафика и поиск средств повышения безопасности и надежности сетей провайдеров на их основе.

Ключевые слова: *широковещательный шторм, сеть провайдера, мониторинг сети.*

PROTECTION AGAINST BROADCASTING STORMS IN NETWORK PROVIDERS

Radzhabov F.R.

Radzhabov Farid Raufovich – Service Engineer,
JSC "NVISION BUSINESS SOLUTIONS", MOSCOW

Abstract: *despite the intelligence and efficiency of modern network equipment, the broadcast storm remains an urgent problem of network administration. Taking into account the "scarcity of a theoretical base that allows practical application," the search for applied methods based on experiments to prevent the appearance or detection of a broadcast storm is in demand in solving the problem of increasing the productivity of provider networks.*

The aim of this work is to search, review and analyze practical methods for detecting broadcast traffic and to search for ways to increase the security and reliability of provider networks based on them.

Keywords: *broadcast storm, network provider, network monitoring.*

УДК 004.722.4

Широковещательный шторм возникает, когда сетевая система перегружена непрерывным многоадресным (*multicast*) или широковещательным (*broadcast*) трафиком. Когда различные узлы отправляют / транслируют данные по сетевому каналу, а другие сетевые устройства ретранслируют данные обратно в сетевой канал в ответ, это в конечном итоге приводит к понижению производительности сети и сбою сетевого взаимодействия. Отказаться от использования широковещательных пакетов в сети практически невозможно, так как они используются служебными протоколами всех известных стеков протоколов: TCP/IP, IPX/SPX, AppleTalk.

Существует много причин, по которым происходит широковещательный шторм, включая плохую технологию и неправильные конфигурации сети, приводящие к петлям коммутации, хакерские атаки на сеть, коммутаторы с неисправным портом или низкой скоростью порта, неисправность сетевой карты, зараженные ПК и пр. Следующие составляющие играют активную роль в создании широковещательного шторма:

- плохое управление сетью;
- плохой мониторинг сети;
- использование дешевых устройств, в том числе концентраторов, коммутаторов, маршрутизаторов, кабелей, разъемов и т. д.;
- неправильно поддерживаемая конфигурация сети и неопытные сетевые инженеры;
- отсутствие логической топологии сети, которая необходима для правильного управления и предоставления рекомендаций для всех маршрутов сетевого трафика.

Поэтому, широковещательный шторм является **актуальной проблемой** сетевого администрирования, несмотря на интеллектуальность и эффективность современного сетевого оборудования.

Предлагаемые в настоящее время решения: сегментирование сети посредством виртуальных сетей (*VLAN – Virtual Local Area Network*), использование специальных протоколов (*STP, RSTP, MSTP* и др.) для построения путей без петель для пакетов, контроль широковещательного трафика в программах – сетевых анализаторах, уже доказано, не обеспечивают гарантированной защиты от широковещательного шторма. Например, в [1] доказано, что проблема организации трафика, которая заключается в поиске

оптимальной логической топологии коммутируемых сетей Ethernet, реализующих протокол *MSTP*, является *NP*-трудной.

Следовательно, решение задачи выявления и уменьшения воздействий на сеть, приводящих к появлению широковещательного шторма и снижению производительности сетей провайдеров, является востребованным в практической деятельности поддержки работоспособности сети.

В [2] приводится пример образования широковещательного шторма в результате передачи сегмента (на транспортном уровне) с неверным параметром (например, номером порта назначения) широковещательным способом 10 000 машинам. Каждая машина может послать обратно сообщение об ошибке. Протокол *UDP* страдал от подобной проблемы, пока протокол *ICMP* (*Internet Control Message Protocol* – протокол межсетевых управляющих сообщений, входит в стек *TCP/IP*) не был изменен так, чтобы хосты воздерживались от отправки сообщений об ошибке в ответ на широковещательные сегменты *UDP*. Беспроводным сетям с их ограниченной пропускной способностью также важно не отвечать на непроверенные широковещательные пакеты.

Принимая во внимание, что «понимание производительности сетей – это скорее искусство, чем наука», и «скудность теоретической базы, допускающей практическое применение» [2], поиск на основе экспериментов практических методов повышения производительности сетей провайдеров, является востребованным.

Некоторые прикладные методы по снижению широковещательного шторма

- Контроль шторма и соответствующие протоколы позволяют ограничивать скорость широковещательных пакетов. Если у вашего коммутатора есть такой механизм, включите его.
- Убедитесь, что IP-трансляции широковещательных пакетов отключены на устройствах третьего уровня. Нет практически никаких причин, по которым можно допустить, чтобы широковещательные пакеты, поступающие из Интернета, направлялись в частное адресное пространство. Если шторм исходит из глобальной сети, отключение широковещательной IP-трансляции отключит его.
- Разделите ваш широковещательный домен. Создание новой VLAN и перенос в нее хостов приведет к балансировке нагрузки широковещательного трафика до более приемлемого уровня. Широковещательный трафик необходим и полезен, но слишком большое его количество в конечном итоге приводит к ухудшению производительности работы сети.
- Проверьте, как часто очищаются таблицы ARP. Чем чаще они обновляются, тем чаще выполняются ARP-широковещательные запросы.
- Иногда, когда у коммутаторов происходит сбой работы на физическом уровне, их порты начинают отправлять широковещательный трафик в сеть. Если у вас есть запасной коммутатор той же или аналогичной модели, скопируйте конфигурацию активного коммутатора на запасной и поменяйте местами оборудование и кабели во время технического обслуживания. Если шторм утих, то это была аппаратная проблема. Если нет, то мы должны искать причину дальше.
- Проверьте петлю коммутации (Bridging loop, Switching loop) [3]. Скажем, был неуправляемый коммутатор уровня 2, подключенный к неуправляемому коммутатору в восходящем направлении, и кто-то подключил кабель между двумя портами на одном и том же неуправляемом коммутаторе (скажем, порты 1 и 2). Неуправляемый коммутатор будет отвечать на все широковещательные рассылки несколько раз и заполнять широковещательный домен пакетами, вызывая атаку типа «отказ в обслуживании» в сети.
  - BPDU и PortFast или аналогичные функции опциональных настроек STP должны быть реализованы как лучший способ предотвращения циклов.
  - Не позволяйте пользователям подключать неуправляемые коммутаторы к портам управляемого коммутатора, применяя максимальное количество MAC-адресов на порт. Это может быть до двух MAC-адресов, если у пользователя есть компьютер, подключенный к IP-телефону, который, в свою очередь, подключен к коммутатору.

Список литературы / References

1. *Fortz Bernard, Gouveia Luís, Joyce-Moniz Martim.* Optimal design of switched Ethernet networks implementing the Multiple Spanning Tree Protocol, Discrete Applied Mathematics, Volume 234, 2018, Pages 114-130. [Электронный ресурс]. Режим доступа: http://www.sciencedirect.com/science/article/pii/S0166218X16303353)/ (дата обращения: 15.05.2020).
2. *Таненбаум Э., Уэзеролл Д.* Компьютерные сети. СПб.: Питер, 2012.
3. STP в Cisco. [Электронный ресурс]. Режим доступа: http://xgu.ru/wiki/STP_%D0%B2_Cisco/ (дата обращения: 3.05.2020).
4. *Магомедова Р.М., Раджабов Ф.Р.* Мобильное приложение поддержки ведения портфолио студентов // Проблемы современной науки и образования, 2014. № 4 (22). С. 10-11.