# Поведение WSA на обнаружении MTU-маршрута с использованием WCCP

## Содержание



## Введение

Этот документ описывает проблему, с которой встречаются, где маршрутизатор отбрасывает пакеты, когда ваша конфигурация включает и протокол WCCP и обнаружение Максимального размера передаваемого блока данных (MTU) пути, и это предоставляет решение проблемы.

## Общие сведения

### Предварительная фаза

Когда посмотрели на отдельно, много функций превосходны для решения определенной проблемы. Иногда, хотя при объединении двух или трех способов это производит некоторое неловкое поведение, и необходимо представить другую функцию или обходной путь, чтобы заставить его работать должным образом. Например, используйте связующее дерево и Протокол OSPF и Уровень 2 (L2), конвергенция берет дольше (20-е), чем OSPF (1 с, если минимальный интервал простоя используется), но связующее дерево замены с Многосвязным деревом (MST) и это функционирует должным образом снова.

То же поведение совместимости наблюдалось между WCCP и обнаружением MTU-маршрута; многие думают, что это - проблема заголовка Универсальной инкапсуляции маршрутизации (GRE). Однако этот документ объясняет реальную причину.

### Как MTU путь Dicovery и WCCP работает отдельно

## Обнаружение MTU маршрута

Каждая линия имеет свой предел на том, насколько большой пакет может быть. Если вы передаете больший пакет, чем поддерживается, то он отброшен. Одна из ролей устройств L3 (маршрутизаторы) на пути должна заботиться и прервать большие пакеты от одной из линий к другой, чтобы удостовериться, что сквозная связь очевидна для возможностей каждой линии.

Иногда, хотя, конечные хосты настроены таким способом, которым их пакеты не могут быть прерваны (например, зашифрованные файлы, голосовые вызовы). Эта информация передана через бит "Не фрагментировать" (DF) в IP - заголовке. Маршрутизаторы отбрасывают пакеты как они, но маршрутизатор пытается сообщить до конца, хост с помощью сообщения Протокола ICMP (введите C 3 назначениями недостижимый, код 4 - необходимая фрагментация, но Набор битов DF). Таким образом, хост знает для передачи пакетов меньшего размера в будущем.

Это - основа обнаружения MTU-маршрута. Можно передать большие пакеты с Набором битов DF, чтобы видеть, делают ли они его к концу или если вы получаете отчёт о ICMP, как ранее описано. Как только вы определяете максимальный осуществимый размер пакета, используйте его для дальнейшей связи. См. RFC 1191 для получения дополнительной информации.

Web Security Appliance (WSA) использует обнаружение MTU-маршрута по умолчанию. Таким образом все его генерируемые пакеты имеют Набор битов DF конфигурацией по умолчанию.

## WCCP

Если необходимо наложить безопасность в сеть на вебе - трафике без ведома других, вы выполняете их трафик через прокси, который не видим. WCCP является протоколом, который используется для передачи между устройством, которое перехватывает (маршрутизатор/межсетевой экран) и механизм/прокси веб-кэша, который является WSA в этом случае.

Эта схема иллюстрирует как трафики в этом сценарии:

Это работает как это:

1. Клиент передает GET HTTP с Источником IP, его IP-адрес (IP-адрес клиента) и IP-адрес сервера назначения.

2. Межсетевой экран или маршрутизатор перехватывают GET HTTP и вперед это через GRE WCCP или чистый L2 к веб-кэшу/WSA. Источник является все еще IP-адресом клиента, и назначением является все еще IP-адрес Web-сервера.

3. WSA осматривает запрос и, если это легитимно, зеркала это к Web-серверу. Здесь IP - адресом назначения является IP-адрес Web-сервера, и IP - адрес источника мог бы быть WSA или клиентом, на основе того, включили ли вы спуфинг IP-адреса клиента. Для данного примера это не имеет значения, потому что ответный трафик в обоих случаях должен поразить WSA.

4. Ответный трафик осмотрен в WSA.

5. WSA передает ответ клиенту с IP - адресом источника, ALWAYS IP-адрес Web-сервера (таким образом, клиент не становится подозрительным), и целевой IP-адрес клиента.

# Проблема

Если один из маршрутизаторов из схемы должен фрагментировать трафик, что происходит? WSA помещает бит DF на пакет номер 5, но это должно быть фрагментировано. Маршрутизатор отбрасывает его и говорит отправителю, что фрагментация необходима, но бит DF установлен (тип ICMP 3 кода 4). В конце концов, RFC 1191 должен работать теперь, и отправитель должен понизить свой размер пакета.

С WCCP IP - адресом источника является IP-адрес Web-сервера, таким образом, этот ICMP никогда не переходит к WSA; скорее это пытается перейти к реальному Web-серверу (помните, этот маршрутизатор на нижней части не знает о WCCP). Это - то, как WCCP и обнаружение MTU-маршрута вместе иногда ломают вашу организацию сети.

# Решение

Существует четыре способа решить эту проблему:

- Обнаружьте реальный MTU и затем используйте **etherconfig** на WSA для понижения MTU интерфейса. Помните, что заголовок TCP равняется 60, IP равняется 20, и когда вы используете ICMP, который добавляет 8 байтов к IP - заголовку.

- Отключите обнаружение MTU-маршрута (**pathmtudiscovery** команда CLI WSA). Это приводит к TCP MSS 536, который мог бы вызвать проблему производительности.

- Измените сеть, таким образом, нет никакой фрагментации L3 между WSA и клиентами.

- Используйте **IP tcp mss - отрегулировали 1360** (или другой расчетный номер) команда на каждом маршрутизаторе Cisco на пути на соответствующих интерфейсах.

# Дополнительные примечания

В то время как эта проблема расследовалась, она была обнаружена, что, если вы устанавливаете прокси явно в клиента в течение нескольких минут и затем удаляете его, вопрос решен в течение следующих четырех - пяти часов. Это - то, вследствие того, что, в явном режиме, механизме обнаружения MTU-маршрута между WSA и клиентом работает. Как только WSA обнаруживает MTU путь, он хранит его наряду с обнаруженным TCP MSS на внутреннюю таблицу для ссылки. Очевидно эта таблица обновляется каждые четыре - пять часов, который представляет решение не работать снова после такого большого количества времени.