Устранение неполадок "дублирование IP-адреса 0.0.0.0" сообщения об ошибках

Содержание

Введение

Этот документ описывает проблему, с которой встречаются, когда **Дублирование IP-адреса, 0.0.0.0** сообщения об ошибках получены клиентами, которые выполняют Microsoft Windows Vista и более поздние версии. Методы, которые используются, чтобы решить и устранять проблему, также описаны.

Проблема

С Microsoft Windows Vista и более поздними версиями, Microsoft представила новый механизм, который используется для обнаружения дублирований адреса в сети, когда происходит процесс DHCP. Этот новый поток обнаружения описан в RFC 5227.

Один из триггеров для этого потока обнаружения определен в разделе 2.1.1:

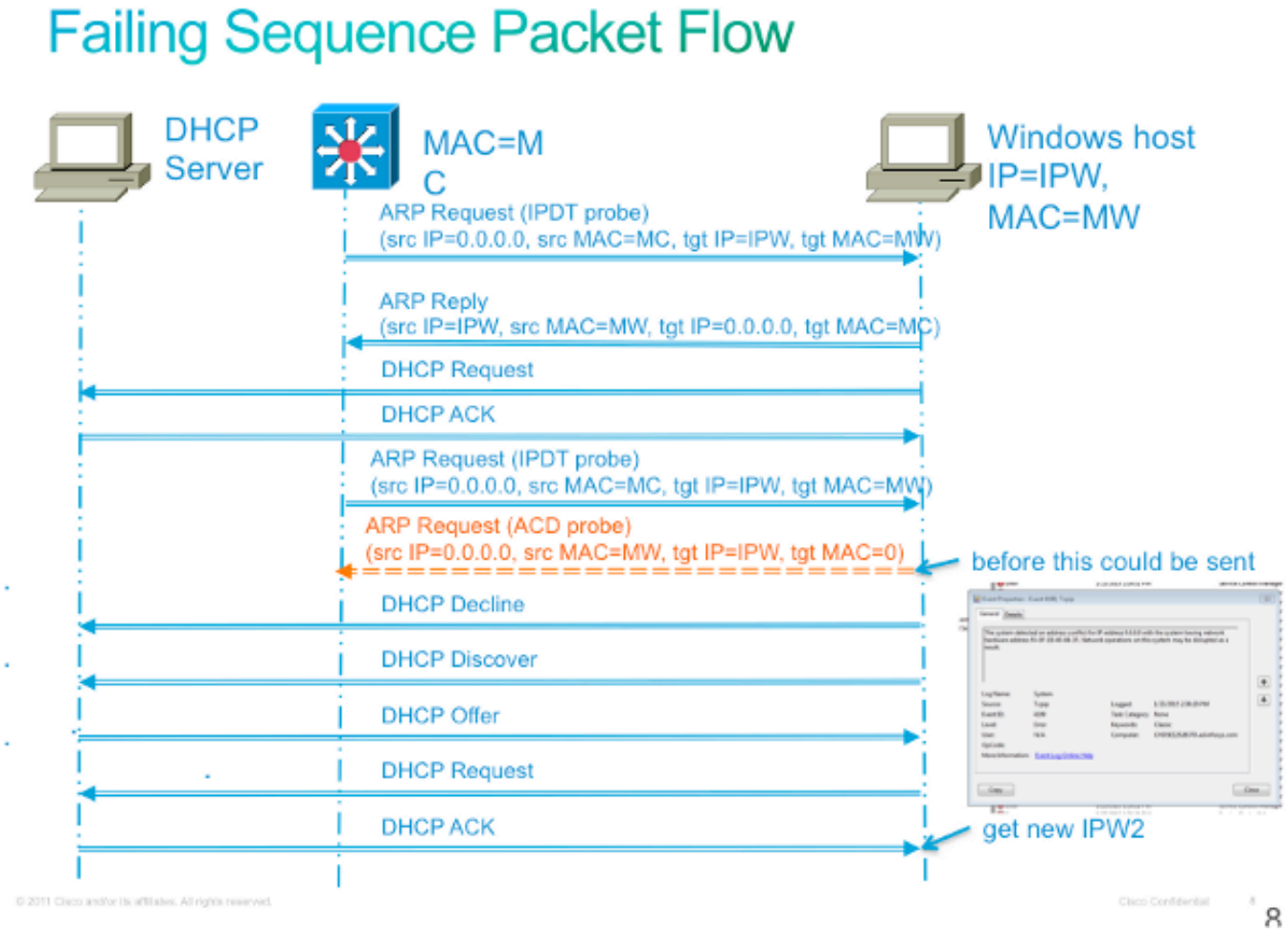
Кроме того, если в течение этого периода хост получает какой-либо Зонд ARP, где 'целевой IP - адрес' пакета является адресом, зондируемым для, и 'аппаратный адрес отправителя пакета' не является аппаратным адресом ни одного из интерфейсов хоста, тогда хост, SHOULD так же рассматривает это как конфликт адресов и сигнализирует ошибку агенту настройки как выше. Это может произойти, если два (или больше) хосты, по любой причине, были непреднамеренно настроены с тем же адресом, и оба находятся одновременно в процессе зондирования того адреса, чтобы видеть, может ли это безопасно использоваться.

Cisco IOS® использует Зонд Протокола ARP, который получен от адреса 0.0.0.0 для поддержания отслеживающего IP - устройство кэша во время отслеживания IP - устройства, и опция, которая использует его, активирована (такие как 802.1x) на коммутаторе Cisco IOS. Цель отслеживания IP - устройства для коммутатора, чтобы получить и вести список устройств, которые связаны с коммутатором через IP-адрес. Зонд не заполняет запись отслеживания. Это используется, чтобы активировать и поддержать запись в таблице после того, как это изучено. Этот IP-адрес тогда используется, когда Список контроля доступа (ACL) применен к интерфейсу для замены адресом источника в ACL с IP-адресом клиента. Эта функция важна каждый раз, когда списки доступа используются с 802.1x или любой другой функцией Flex-Auth на коммутаторах Cisco.

Причина дублирования IP-адреса

Если коммутатор отсылает Зонд ARP для клиента, в то время как Microsoft Windows PC находится в своей фазе обнаружения дублирования адреса, то Microsoft Windows обнаруживает зонд как дублирование IP-адреса и представляет сообщение, что дублирование IP-адреса было найдено в сети для 0.0.0.0. ПК не получает адрес, и пользователь должен или вручную освободить/возобновить адрес, разъединить и воссоединиться с сетью или перезагрузить ПК для получения доступа к сети.

Вот пример отказавшей пакетной последовательности:



Решение

Существуют несколька способов, которые используются для обхождения этой проблемы. Вот список возможных обходной путей:

- Большая часть эффективного способа, который используется для предотвращения этой проблемы должна настроить коммутатор так, чтобы это передало Зонд ARP не-RFC-совместимого для определения источника зонда от коммутируемого виртуального интерфейса (SVI) в VLAN, где находится ПК. Если SVI настроен для VLAN и любой из двух команд, которые придерживаются, используются, то IP-адрес отправителя в зондах IPDT никогда не будет 0.0.0.0. Таким образом точно ошибка дублирования IP-адреса не произойдет.

  Вот формат команды для более старых версий кода:

`ip device tracking probe use-svi`Эта конфигурация в настоящее время не инициирует сообщение об ошибках обнаружения дублирования адреса в Microsoft Windows предупреждении к этому методу, то, что SVI должен существовать на каждом коммутаторе в каждой VLAN, где находятся клиенты Microsoft Windows, которые выполняют DHCP. Этот метод трудно масштабировать, таким образом, Cisco рекомендует использовать отслеживающую IP - устройство тестовую задержку в качестве основного метода. SVI не в настоящее время доступен на платформе коммутатора серии "6500". Эта команда была внедрена в SE версии Cisco IOS 12.2 (55) на 2900, 3500, и Платформы коммутатора серии 3700, и в SG Версии 15.1 (1) на Платформе коммутатора серии 4500.

Вот формат команды для более новых версий кода:

`ip device tracking probe auto-source fallback <host-ip> <mask> [override]` Эта последняя команда CLI была представлена через идентификатор ошибки Cisco CSCtn27420 в версии Cisco IOS 15.2 (2) E. Это было добавлено, чтобы позволить определяемому пользователем IP - адресу источника запроса ARP вместо требования использовать IP - адрес источника по умолчанию 0.0.0.0. Новое **устройство ip** команды global**, отслеживающее тестовую автоисходную нейтрализацию 0.0.0.x 255.255.255.0 замен**, позволяет пользователю использовать адрес узла 0.0.0.x в подсети во избежание любых проблем дублирования IP-адресов. Если не будет никакого SVI для конкретной VLAN, то IP - адрес хоста нейтрализации будет использоваться для определения источника зонда вместо этого.

- Основная альтернатива не-SVI, которая используется для обхождения проблемы должна задержать зонд от коммутатора так, чтобы Microsoft Windows имел время для завершения обнаружения дублирования IP-адреса. Это эффективно только на сценариях установления соединения и портах доступа. Введите эту команду для отсрочки зонда:

  `ip device tracking probe delay 10`RFC задает десяти-секундное окно для обнаружения дублирования адреса, поэтому при отсрочке отслеживающего устройство зонда это решает вопрос в почти всех случаях. Когда коммутатор обнаруживает зонд от ПК, в дополнение к тестовой задержке задержка также перезагружает. Например, если тестовый таймер считал в обратном порядке к пяти секундам и обнаруживает Зонд ARP от ПК, сброс таймера назад к десяти секундам. Это окно может быть далее уменьшено при включении DHCP, snooping также поскольку это так же перезагружает таймер. В редких случаях ПК передает Зонду ARP миллисекунды, прежде чем коммутатор передаст свой зонд, который все еще инициирует сообщение дублирования адреса конечному пользователю. Эта команда была представлена в SE версии Cisco IOS 15.0 (1) на 2900, 3500, и Платформы коммутатора серии 3700, SG Версии 15.0 (2) на Платформе коммутатора серии 4500 и Версия 12.2 (33) SXI7 на платформе коммутатора серии "6500".

- Другой метод, который используется для решения этого вопроса включает устранение неполадок клиента для определения причины, что обнаружение дублирования адреса происходит настолько поздно после того, как ссылка подключается к сети. Коммутатор

не имеет никакого способа определить время, когда этот процесс происходит, таким образом, необходимо оценить время, которое установлено для тестовой задержки для предотвращения конфликта. Для эффективного устранения проблем причины, что обнаружение дублирования адреса происходит настолько поздно, дополнительная информация о поведении отслеживающего IP - устройство зонда полезна.

Зонд ARP передается при двух обстоятельствах:

Ссылка, которая привязана к текущей записи в шагах базы данных IPDT от ВНИЗ к Работоспособному состоянию.Ссылка уже в Работоспособном состоянии, которое привязано к записи в базе данных IPDT, имеет тестовый интервал с истекшим сроком.

Введите эту команду для установки отслеживающего IP - устройство тестового интервала:

`ip device tracking probe interval <seconds>` Интервал по умолчанию составляет тридцать секунд. Для просмотра этой информации введите эту команду:

`show ip device tracking all`

```
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
IP Device Tracking Probe Delay Interval = 0
------------------------------------------------------------
IP Address MAC Address Vlan Interface STATE
------------------------------------------------------------
10.0.0.1 a820.661b.b384 301 GigabitEthernet0/1 INACTIVE

Total number interfaces enabled: 1
Enabled interfaces:
```

`Gi0/1` После начальных шагов записи от ВНИЗ к Работоспособному состоянию, не передаются никакие дальнейшие зонды, пока коммутатор не видит трафик от того устройства для интервала тестовой задержки. Кроме того, как сообщили ранее, конфликт только происходит, если ПК отсылает миллисекунды Зонда ARP, прежде чем коммутатор передаст Зонд ARP (одновременно).

- Последний метод, который используется для обхождения проблемы, которая описана в этом документе, должен отключить обнаружение дублирования адреса на клиентской стороне. Эта процедура описана в статье How to Disable the Gratuitous ARP Function Microsoft Support-Base. Централизованно разверните это изменение для создания этой опции более масштабируемой.