IP - устройство, отслеживающий (IPDT) обзор

Содержание

Введение

Документ описывает IP - устройство, Отслеживающий (IPDT) и как отключить его и проверить его операцию.

Обзор IPDT

Определение и использование

Основная задача IPDT состоит в том, чтобы отслеживать подключенные узлы (ассоциация MAC и IP-адреса). Чтобы сделать это, это передает Протоколу разрешения одиночного адреса зонды (ARP) с интервалом по умолчанию 30 секунд; эти зонды передаются MAC-адресу хоста, связанного с другой стороны ссылки, и используют Уровень 2 (L2) в качестве источника по умолчанию MAC-адрес физического интерфейса, из которого ARP идет и IP-адрес отправителя 0.0.0.0, на основе определения Зонда ARP, перечисленного в RFC 5227, выбранном сюда:

В этом документе термин 'ARP Зонда' использован для обращения к Пакету запроса ARP, передан на локальной ссылке со все-нулевым 'IP-адресом отправителя'. 'Аппаратный адрес отправителя' MUST содержит аппаратный адрес интерфейса, передающего пакет. 'Поле MUST' IP-адреса отправителя быть установленным во все обнуляет, чтобы избежать загрязнять кэши ARP в других хостах на той же ссылке в случае, где адрес, оказывается, уже используется другим хостом. Поле MUST 'целевого IP - адреса' быть установленным в зондируемый адрес. Зонд ARP передает обоим вопрос ("Кто-либо использует этот адрес?") и подразумеваемый оператор ("Это - адрес, который я надеюсь использовать".).

Цель IPDT для коммутатора, чтобы получить и вести список устройств, которые связаны с коммутатором через IP-адрес. Зонд не заполняет запись отслеживания; это просто используется для поддержания записи в таблице после того, как это изучено через запрос ARP / ответ от хоста.

Когда IPDT включен, инспектирование IP ARP включено автоматически; это обнаруживает присутствие новых хостов, когда это контролирует пакеты ARP. Если динамическая проверка ARP включена, только пакеты ARP, которые она проверяет, используются для обнаружения новых хостов к таблице Отслеживания Устройства.

Функция отслеживания IP DHCP обнаруживает подключение или отключение узла при назначении или аннулировании DHCP IP-адресов.

IPDT является функцией, которая всегда была доступна. Однако на более свежих версиях Cisco IOS®, его взаимозависимости включены по умолчанию (см. идентификатор ошибки Cisco CSCuj04986). Может быть чрезвычайно полезно, когда его база данных ассоциаций хостов IP/MAC используется для начальной загрузки source IP динамических списков контроля доступа (ACL), или поддерживать привязку IP-адреса к метке группы безопасности.

Зонд ARP передается при двух обстоятельствах:

- Ссылка, привязанная к текущей записи в шагах базы данных IPDT от ВНИЗ к Работоспособному состоянию и Записи ARP, была заполнена.

- Ссылка уже в Работоспособном состоянии, которое привязано к записи в базе данных IPDT, имеет тестовый интервал с истекшим сроком.

Известные проблемы

Зонд 'поддержки активности', передаваемый коммутатором, является проверкой L2. Как таковой с точки зрения коммутатора, IP-адреса, используемые в качестве источника в ARPs, не важны: эта функция может быть использована на устройствах без IP-адреса, настроенного вообще, таким образом, Источник IP 0.0.0.0 не релевантен.

Когда хост получает, это обменивается сообщениями, он отвечает назад и заполняет поле IP - адреса назначения с единственным IP-адресом, доступным в полученном пакете, который является собственным IP-адресом. Это может вызвать ложные предупреждения дублирования IP-адреса, потому что хост, который ответы рассматривают собственный IP-адрес и как источник и как назначение пакета; обратитесь к Дублированию IP-адреса 0.0.0.0. Статья Error Message Troubleshoot для получения дополнительной информации о сценарии дублирования IP-адреса.

Состояние по умолчанию и операция

Следует отметить, что, даже если IPDT включен глобально, который не обязательно подразумевает, что IPDT активно контролирует данный порт. На версиях, где IPDT всегда включен и где IPDT может быть глобально переключенным выкл/вклом, когда IPDT включен глобально, другие функции фактически определяют, активно ли это на определенном интерфейсе (см. раздел областей Функциональности).

Области функциональности

IPDT и его зонды ARP, передаваемые из данного интерфейса, используются для этих функций:

- Протокол Network Mobility Services (NMSP), Версии 3.2.0E, 15.2 (1) E, 3.5.0E и позже
- Датчик устройства, Версии 15.2 (1) E, 3.5.0E и позже
- 1X, Обход проверки подлинности MAC (MAB), менеджер сеанса
- Web Based Authentication
- Auth-proxy
- IP-сервисы шлюз (IPSG) для статических хостов
- Гибкий netflow
- Cisco TrustSec (CTS)
- Трассировка сред
- Перенаправления HTTP

Отключите IPDT

На версиях, где IPDT не включен по умолчанию, IPDT может быть выключен глобально с этой командой:

```
# no ip device tracking
```

На версиях, где IPDT всегда включен, предыдущая команда не доступна, или это не позволяет вам отключать IPDT (идентификатор ошибки Cisco CSCuj04986). В этом случае существует несколько способов гарантировать, что IPDT не контролирует определенный порт, или он не генерирует предупреждения IP - адресации с дублированием.

Войдите IP устройство, отслеживающее зонд, задерживают 10 Команд

Эта команда не позволяет коммутатору передавать зонд в течение 10 секунд, когда она обнаруживает соединение / откидная створка, которая минимизирует возможность передать зонд в то время как хост с другой стороны проверок канала связи для дублирований IP-адреса. RFC задает 10-секундное окно для обнаружения дублирования адреса, поэтому при отсрочке отслеживающего устройство зонда проблема может быть решена в большинстве случаев.

Если коммутатор отсылает Зонд ARP для клиента, в то время как хост (например, Microsoft Windows PC) находится в его фазе Обнаружения Дублирования адреса, хост обнаруживает зонд как дублирование IP-адреса и предоставляет пользователю сообщение, что дублирование IP-адреса было найдено в сети. ПК не мог бы получить адрес, и

пользователь должен вручную освободить/возобновить адрес, разъединить и воссоединиться с сетью или перезагрузить ПК для получения доступа к сети.

Когда коммутатор обнаруживает зонд от ПК/хоста, в дополнение к тестовой задержке задержка также перезагружает себя. Например, если тестовый таймер считал в обратном порядке к пяти секундам и обнаруживает Зонд ARP от ПК/хоста, сброс таймера назад к 10 секундам.

Эта конфигурация была сделана доступной через идентификатор ошибки Cisco CSCtn27420.

Введите IP устройство, отслеживающее тестовое использование-svi... Команда

С этой командой можно настроить коммутатор для передачи Зонда ARP не-RFC-совместимого; Источник IP не будет 0.0.0.0, но это будет коммутируемый виртуальный интерфейс (SVI) в VLAN, где находится хост. Машины Microsoft Windows больше не рассматривают зонд как зонд, как определено RFC 5227 и не отмечают потенциального IP - адресацию с дублированием.

Введите IP устройство, отслеживающее тестовый автоисточник [нейтрализация <IP - адрес хоста> <mask>] [замена] Команда

Для клиентов, которые не имеют предсказуемыми / управляемые конечные устройства или для тех, у кого есть много коммутаторов в роли L2-only, конфигурации SVI, который представляет переменную Уровня 3 в дизайне, не подходящее решение. Усовершенствование представило, в Версии 15.2 (2) E и позже, возможность позволить произвольное присвоение IP-адреса, который не должен принадлежать коммутатору для использования в качестве адреса источника в зондах ARP, генерируемых IPDT. Это усовершенствование представляет шанс модифицировать автоматическое поведение системы этими способами (этот список показывает, как система автоматически ведет себя после того, как каждая команда используется):

Введите IP устройство, отслеживающее тестовую автоисходную Команду

1. Установите источник в SVI VLAN если подарок.
2. Ищите пару источника/MAC в таблице IP-узла для той же подсети.
3. Передайте нулевой Источник IP как в случае по умолчанию.

Введите IP устройство, отслеживающее тестовую автоисходную нейтрализацию 0.0.0.1 255.255.255.0 Команд

1. Установите источник в SVI VLAN если подарок.
2. Ищите пару источника/MAC в таблице IP-узла для той же подсети.

3. Вычислите source IP из IP - адреса назначения с битом узла и предоставленной маской.

Введите IP устройство, отслеживающее тестовую автоисходную нейтрализацию 0.0.0.1 255.255.255.0 Команд замены

1. Установите источник в SVI VLAN если подарок.

2. Вычислите source IP из IP - адреса назначения с битом узла и предоставленной маской.

Примечание: Замена заставляет вас пропустить поиск записи в таблице.

Как пример предыдущих вычислений, предположите зондирование хоста 192.168.1.200. С битами маски и битами узла, если, вы генерируете адрес источника 192.168.1.1.

При зондировании записи 10.5.5.20 вы генерировали бы зонд ARP с адресом источника 10.5.5.1 и так далее.

Введите ip device tracking maximum 0 Команд

Эта команда действительно не отключает IPDT, но это действительно ограничивает количество отслеженных хостов нуля. Это не рекомендуемое решение, и оно должно использоваться с осторожностью, потому что оно влияет на все другие функции, которые полагаются на IPDT, который включает конфигурацию port-channel, как описано в идентификатор ошибки Cisco CSCun81556.

Выключите Активные Функции тот Триггер IPDT

Некоторые функции, которые могли бы инициировать IPDT, включают NMSP, датчик устройства, dot1x/MAB, WebAuth и IPSG. Это решение зарезервировано для самого трудного или сложных ситуаций, где или все решения, ранее доступные, не работали как ожидалось, или они создали дополнительные проблемы. Это - однако, единственное решение, которое позволяет экстремальную глубину детализации, когда вы отключаете IPDT, потому что можно выключить только IPDT-связанные функции, которые вызывают проблемы и оставляют все остальное незатронутым.

В новой Cisco IOS, Versions15.2 (2) E и позже, вы видите выходные данные, подобные этому:

```
Switch#show ip device tracking interface gig 1/0/9
-----------------------------------------
Interface GigabitEthernet1/0/9 is: STAND ALONE
IP Device Tracking = Disabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 180000
IPv6 Device Tracking Client Registered Handle: 75
IP Device Tracking Enabled Features:
HOST_TRACK_CLIENT_ATTACHMENT
HOST_TRACK_CLIENT_SM
```

Эти две линии всеми заглавными буквами у основания выходных данных - те, которые

используют IPDT для работы. Большинства проблем, созданных при отключении отслеживания устройства, можно избежать, если вы отключаете одиночные сервисы, которые работают в интерфейсе.

В более ранних версиях Cisco IOS этот 'легкий' способ знать, какие модули включены под интерфейсом, еще не доступен, таким образом, необходимо пройти более включенный процесс для получения тех же результатов. Необходимо включить **track interface устройства ip отладки**, который является низкочастотным журналом, который должен быть безопасным в большинстве настроек. Бойтесь включать **устройство ip отладки, отслеживающее все**, потому что это, наоборот, лавинно рассылает консоль в ситуациях с масштабом.

Как только отладка идет, возвратите интерфейс, чтобы принять значение по умолчанию, и затем добавить и удалить сервис IPDT из конфигурации интерфейса. Результаты отладок говорят вам, которые сервис был позволен/отключен с командой, которую вы использовали.

Например:

```
Switch(config)#int gig 1/0/9
Switch(config-if)#ip device track max 10
Switch(config-if)#
*Mar 27 09:58:49.470: sw_host_track-interface:Feature 00000008 enabled on port
Gi1/0/9, mask now 0000004C, 65 ports enabled
*Mar 27 09:58:49.471: sw_host_track-interface:Gi1/0/9[L2 DOWN, IPHOST DIS]IP
host tracking max set to 10
Switch(config-if)#
```

То, что показывают выходные данные, - то, что вы активировали опцию **00000008**, и что маска новой характеристики является **0000004C**.

Теперь, удалите конфигурацию, которую вы просто добавили:

```
Switch(config-if)#no ip device track max 10
Switch(config-if)#
*Mar 27 10:02:31.154: sw_host_track-interface:Feature 00000008 disabled on port
Gi1/0/9, mask now 00000044, 65 ports enabled
*Mar 27 10:02:31.154: sw_host_track-interface:Gi1/0/9[L2 DOWN, IPHOST DIS]IP
host tracking max cleared
*Mar 27 10:02:31.154: sw_host_track-interface:Max limit has been removed from
the interface GigabitEthernet1/0/9.
Switch(config-if)#
```

Как только вы удаляете функцию **00000008**, вы видите **00000044** маски, которые, должно быть, были оригиналом, маской по умолчанию. Это значение **00000044** ожидается, так как AIM является **0x00000004**, и SM является **0x00000040**, которые вместе приводят к **0x00000044**.

Существует несколько сервисов IPDT, которые могут работать под интерфейсом:

Сервис IPDT	Interface
HOST_TRACK_CLIENT_IP_ADMISSIONS	= 0x00000001
HOST_TRACK_CLIENT_DOT1X	= 0x00000002
HOST_TRACK_CLIENT_ATTACHMENT	= 0x00000004
HOST_TRACK_CLIENT_TRACK_HOST_UPTO_MAX	= 0x00000008
HOST_TRACK_CLIENT_RSVP	= 0x00000010
HOST_TRACK_CLIENT_CTS	= 0x00000020
HOST_TRACK_CLIENT_SM	= 0x00000040
HOST_TRACK_CLIENT_WIRELESS	= 0x00000080

В примере HOST_TRACK_CLIENT_SM (МЕНЕДЖЕР СЕАНСА) и HOST_TRACK_CLIENT_ATTACHMENT (также известный как AIM/NMSP) модули настроены для IPDT. Для выключения IPDT на этом интерфейсе необходимо отключить обоих, потому что IPDT является отключенный ONLY, когда все функции, которые используют его, отключены также.

После того, как вы отключите те опции, у вас есть выходные данные, подобные этому:

```
Switch(config-if)#do show ip dev trac int gig 1/0/9
-----------------------------------------
Interface GigabitEthernet1/0/9 is: STAND ALONE
IP Device Tracking = Disabled IPDT is disabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 180000
IP Device Tracking Enabled Features:
? No active features
-----------------------------------------
```

Таким образом IPDT отключен с большим количеством глубины детализации.

Вот некоторый пример команд, используемых для отключения некоторых функций, обсужденных ранее:

- **присоединение nmsp подавляет**
- **никакой макро-автоматический монитор**

  Примечание: Последняя функция должна быть доступной только на платформах, которые поддерживают Умные порты (Презентация Flash SmartPort), которые используются для активации опций и параметров настройки на основе местоположения коммутатора в сети и для массовых развертываний конфигурации по сети.

Проверьте операцию IPDT

Используйте эти команды для проверки статуса IPDT на устройстве:

- **show ip device tracking...**

  Эта команда отображает интерфейсы, где IPDT включен и где в настоящее время отслеживаются ассоциации MAC/IP/интерфейса.

- **clear ip device tracking...**

  Эта команда очищает IPDT-связанные записи.

  Примечание: Коммутатор передает зонды ARP к хостам, которые были удалены. Если хост присутствует, он отвечает на зонд ARP, и коммутатор добавляет запись IPDT для хоста. Необходимо отключить зонды ARP перед ясной командой IPDT; таким образом все Записи ARP должны закончиться. Если зонды ARP включены после **команды clear ip device tracking** все записи возвращаются снова.

- **debug ip device tracking...**

  Эта команда позволяет вам собирать отладки для отображения действия IPDT в в реальном времени.