Обзор технологии отслеживания устройств по IP (IPDT)

Содержание

Введение

В документе описывается функция отслеживания устройств по IP (IPDT), а также способы ее отключения и проверки ее работоспособности.

Обзор IPDT

Определение и применение

Основная задача функции IPDT состоит в отслеживании подключенных узлов (ассоциации MAC- и IP-адреса). Для этого она отправляет одноадресные зонды ARP с интервалом по умолчанию, равным 30 секундам; эти зонды отправляются на MAC-адрес узла, подключенного к противоположной стороне канала, и используют уровень 2 (L2) в качестве источника по умолчанию MAC-адрес физического интерфейса, из которого исходит ARP, а также IP-адрес отправителя 0.0.0.0 с учетом определения зонда ARP, приведенного в RFC 5227, отрывок из которого приведен здесь:

В этом документе термином «зонд ARP» обозначается пакет запроса ARP, передаваемый в

виде широковещательной рассылки в локальном канале с параметром sender IP address (IP-адрес отправителя), имеющим значение 0.0.0.0. Параметр sender hardware address (аппаратный адрес отправителя) ДОЛЖЕН содержать аппаратный адрес интерфейса, отправляющего пакет. В поле sender IP address (IP-адрес отправителя) ДОЛЖНЫ быть указаны только нули, чтобы не загрязнять кеши ARP на других узлах, подключенных к тому же каналу, в том случае, когда оказывается, что адрес уже используется другим узлом. В поле target IP address (целевой IP-адрес) ДОЛЖЕН быть указан зондируемый адрес. Зонд ARP передает вопрос («Использует ли кто-нибудь этот адрес? ») и подразумеваемое заявление («Это адрес, который я надеюсь использовать»).

Функция IPDT предназначена для того, чтобы коммутатор мог формировать и вести список устройств, подключенных к коммутатору через IP-адрес. Зонд не заполняет запись отслеживания; он просто используется для ведения записи в таблице, полученной посредством запроса ARP и ответа на него от хоста.

Когда функция IPDT включена, инспектирование IP ARP включается автоматически; оно обнаруживает присутствие новых узлов в ходе мониторинга пакетов ARP. Если динамическая проверка ARP включена, только пакеты ARP, прошедшие проверку, используются для обнаружения новых узлов, которые заносятся в таблицу отслеживания устройств.

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

Функция IPDT всегда была доступна. Однако в последних выпусках Cisco IOS® зависящие от нее функции включены по умолчанию (см. описание ошибки Cisco с идентификатором CSCuj04986). Это может быть чрезвычайно полезно, когда база данных ассоциаций IP- и MAC-адресов узлов используется для указания IP-адресов источника в динамических списках контроля доступа (ACL) или для поддержания привязки IP-адреса к метке группы безопасности.

Зонд ARP отправляется в двух ситуациях:

- Канал, связанный с текущей записью базы данных IPDT, переходит из состояния «Не работает» в состояние «Работает», а запись ARP уже заполнена.
- Для уже работающего соединения, которое связано с записью в базе данных IPDT, истек интервал отправки зонда.

Известная проблема

Зонд поддержки активности, передаваемый коммутатором, является проверкой L2. С точки зрения коммутатора как таковые IP-адреса, используемые в качестве источника в ARP, не важны: эту функцию можно использовать на устройствах, на которых вообще не задан IP-адрес, поэтому IP-адрес источника 0.0.0.0 не имеет значения.

Когда узел получает это сообщение, он отвечает и указывает в поле IP-адреса назначения единственный IP-адрес, имеющийся в полученном пакете, который является его собственным IP-адресом. Это может вызвать появление ложных предупреждений о дублировании IP-адреса, потому что узел, который отправляет ответ, видит собственный IP-адрес и как источник, и как назначение пакета; см. статью Дублирование IP-адреса 0.0.0.0. Поиск причины сообщения об ошибке, в которой приведена подробная информация о дублировании IP-адреса.

Состояние по умолчанию и использование

Важно отметить, что, даже если функция IPDT включена глобально, это еще не означает, что она выполняет мониторинг данного порта. В выпусках, где функция IPDT всегда включена и где ее можно глобально включать и выключать, когда функция IPDT включена глобально, другие функции определяют, будет ли она работать на определенном интерфейсе (см. раздел «Области функционирования»).

Области функционирования

Функция IPDT и ее зонды ARP, передаваемые из определенного интерфейса, используются для следующих функций:

- Протокол NMSP, версии 3.2.0E, 15.2(1)E, 3.5.0E и более поздние
- Датчик устройства, версии 15.2(1)E, 3.5.0E и более поздние
- 1X, функция MAC Authentication Bypass (MAB), диспетчер сеансов
- Web Based Authentication
- Auth-proxy
- IP Services Gateway (IPSG) для статических узлов
- Flexible NetFlow
- Cisco TrustSec (CTS)
- Mediatrace
- Перенаправления HTTP

Отключение IPDT

В выпусках, где функция IPDT по умолчанию выключена, ее можно выключить глобально с помощью следующей команды:

```
# no ip device tracking
```

В выпусках, где функция IPDT всегда включена, предыдущая команда недоступна или не позволяет отключать IPDT (идентификатор ошибки Cisco CSCuj04986). В этом случае есть несколько способов отключить отслеживание функцией IPDT определенного порта или выдачу ей предупреждений о дублирующихся IP-адресах.

Ввод команды ip device tracking probe delay 10

Эта команда не позволяет коммутатору отправлять зонд в течение 10 секунд, когда он обнаруживает включение/переключение канала, что сводит к минимуму возможность передачи зонда, пока узел на другом конце канала проверяет наличие дублирующихся IP-адресов. RFC задает 10-секундное окно для обнаружения дублирующихся IP-адресов, поэтому, если задержать отправку зонда для отслеживания устройства, проблема в большинстве случаев может быть решена.

Если коммутатор отправляет зонд ARP для клиента, пока узел (например, компьютер под управлением Microsoft Windows) находится на этапе обнаружения дублирующихся адресов,

узел обнаружит зонд как дублированный IP-адрес и выдаст пользователю сообщение о том, что в сети обнаружен дублированный IP-адрес. Компьютер мог не получить адрес, и пользователь должен будет вручную выпустить/продлить адрес, разорвать и снова установить соединение с сетью или перезагрузить компьютер, чтобы получить доступ к сети.

Помимо задержки зонда, задержка также сбрасывает себя, когда коммутатор обнаруживает зонд, отправленный с компьютера/узла. Например, если таймер зонда отсчитает пять секунд и обнаружит зонд ARP от компьютера или узла, таймер сбросится назад на 10 секунд.

Доступ к этой конфигурации был предоставлен посредством описания ошибки Cisco с идентификатором CSCtn27420.

Ввод команды ip device tracking probe use-svi. . . Команда

С помощью этой команды можно настроить в коммутаторе отправку зонда ARP, не соответствующего RFC; iP-адрес источника будет отличаться от 0.0.0.0, но это будет интерфейс Switch Virtual Interface (SVI) в сети VLAN, в которой находится узел. Компьютеры под управлением Microsoft Windows больше не рассматривают зонд как зонд, соответствующий определению RFC 5227, и не выявляют возможное дублирование IP-адреса.

Ввод команды ip device tracking probe auto-source [fallback <host-ip> <mask>] [override]

Для заказчиков, у которых нет предсказуемых/управляемых оконечных устройств, или для тех, у кого много коммутаторов в роли L2-only, настройка интерфейса SVI, который привносит к конструкцию переменную уровня 3, не является подходящим решением. Начиная с версии 15.2(2)E, было реализовано усовершенствование: возможность назначать произвольный IP-адрес, который не обязательно должен принадлежать коммутатору, в качестве адреса источника в зондах ARP, формируемых функцией IPDT. Это усовершенствование предоставляет возможность изменять автоматическое поведение системы следующими способами (в этом списке указано, какие действия система выполняет автоматически после использования каждой команды):

Ввод команды ip device tracking probe auto-source

1. Установите в качестве источника SVI сети VLAN (при наличии).
2. Выполните поиск пары «источник/MAC-адрес» в таблице IP-адресов хоста для той же подсети.
3. Передайте нулевой IP-адрес источника как в варианте по умолчанию.

Ввод команды ip device tracking probe auto-source fallback 0.0.0.1 255.255.255.0

1. Установите в качестве источника SVI сети VLAN (при наличии).
2. Выполните поиск пары «источник/MAC-адрес» в таблице IP-адресов хоста для той же подсети.
3. Вычислите IP-адрес источника по IP-адресу назначения с указанным битом и маской узла.

Ввод команды ip device tracking probe auto-source fallback 0.0.0.1 255.255.255.0 override

1. Установите в качестве источника SVI сети VLAN (при наличии).
2. Вычислите IP-адрес источника по IP-адресу назначения с указанным битом и маской узла.

Примечание. При переопределении выполнять поиск записи в таблице не нужно.

В качестве примера предыдущих вычислений предположим, что выполняется зондирование узла 192.168.1.200. По указанным битам маски и хоста формируется адрес источника 192.168.1.1.

При зондировании записи 10.5.5.20 был бы сформирован зонд ARP с адресом источника 10.5.5.1 и так далее.

Ввод команды ip device tracking maximum 0

Эта команда не совсем отключает функцию IPDT, но она все же ограничивает количество отслеживаемых узлов до нуля. Это нерекомендуемое решение, его следует использоваться с осторожностью, потому что оно влияет на все остальные функции, которые зависят от IPDT, в том числе конфигурацию портов и каналов (см. описание ошибки Cisco с идентификатором CSCun81556).

Выключение активных функций, которые запускают IPDT

В число функций, которые могут запускать функцию IPDT, входят NMSP, датчик устройства, dot1x/MAB, WebAuth и IPSG. Это решение зарезервировано для самых сложных ситуаций, в которых все доступные ранее решения либо не сработали, как ожидалось, либо создали дополнительные проблемы. Тем не менее это решение является единственным вариантом, обеспечивающим чрезвычайно высокую точность при отключении функции IPDT, потому что отключить можно только функции, связанные с IPDT, которые вызывают проблемы и оставляют все остальное как есть.

В последних выпусках Cisco IOS (начиная с версии 15.2(2)E) отображаются выходные данные, похожие на следующие:

```
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
```

Две строки, написанные заглавными буквами, внизу выходных данных — это функции, для работы которых требуется IPDT. Большинство проблем, создаваемых при отключении отслеживания устройства, можно избежать, если отключать отдельные сервисы, которые работают в интерфейсе.

В более ранних версиях Cisco IOS этот простой способ узнать, какие модули включены в интерфейсе, отсутствует. В связи с этим для получения таких же результатов необходимо выполнять более сложный процесс. **Необходимо включить debug ip device track interface, представляющий собой журнал с низкой частотой, использование которого является безопасным в большинстве конфигураций. Будьте осторожны, не включите debug ip device tracking all, поскольку в этом случае, наоборот, консоль будет переполнена в случаях сложных конфигураций.**

После включения отладки верните интерфейс в состояние по умолчанию, а затем добавьте сервис IPDT и удалите из конфигурации интерфейса. В результатах отладок можно будет видеть, какие сервисы были включены или отключены с помощью поданной команды.

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 То По выходным данным видно, что была включена функция 00000008 и новая функция имеет маску 0000004C.

Теперь удалите только что добавленную конфигурацию:

```
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)#
```

После удаления функции 00000008 в выходных данных указана маска 00000044, которая должна была быть исходной, заданной по умолчанию маской. Это значение 00000044 является ожидаемым, поскольку AIM равно 0x00000004, а SM — 0x00000040, а вместе они дают 0x00000044.

Есть несколько сервисов IPDT, которые могут работать в интерфейсе:

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 этом примере для IPDT настроены модули HOST_TRACK_CLIENT_SM (SESSION-MANAGER) и HOST_TRACK_CLIENT_ATTACHMENT (которые также называются AIM/NMSP). Для того чтобы выключить IPDT на этом интерфейсе, необходимо отключить оба этих модуля, потому что сервис IPDT отключается ТОЛЬКО после отключения всех использующих его функций.

После отключения этих функций на экране отобразятся выходные данные, аналогичные следующим:

```
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
-------------------------------------------
```

Этим способом сервис IPDT можно отключать точнее.

Вот несколько примеров команд, используемых для отключения некоторых функций, рассмотренных ранее:

- nmsp attach suppress
- no macro auto monitor

  Примечание. Последняя функция должна быть доступна только на платформах, которые поддерживают порты Smart Port (презентация SmartPort Flash), которые используются для активации функций и настроек с учетом местоположения коммутатора в сети и для массового развертывания конфигурация в сети.

Проверка работы IPDT

Для проверки статуса IPDT на устройстве используются следующие команды:

- show ip device tracking...

  Эта команда отображает интерфейсы, где функция IPDT включена и где связи MAC/IP/интерфейса в настоящее время отслеживаются.

- clear ip device tracking...

Эта команда удаляет записи, связанные с IPDT.

Примечание. Коммутатор отправляет зонды ARP узлам, которые были удалены. Если узел присутствует, он отвечает на зонд ARP, и коммутатор добавляет запись IPDT для этого узла. Необходимо отключить зонды ARP перед подачей команды очистки IPDT; таким образом, все записи ARP должны быть удалены. **Если включить зонды ARP после выполнения команды clear ip device tracking, все записи снова вернутся.**

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

Эта команда позволяет собирать данные отладки для отображения работы IPDT в реальном времени.