Содержание

Введение

Этот документ объясняет, как использовать фильтры Ethertype для блокирования трафика Межсетевого пакетного обмена (IPX) на точке доступа Cisco Aironet. Типичная ситуация, в которой это полезно, - когда широковещательные сообщения сервера IPX дросселируют беспроводное соединение, как это иногда происходит в большой корпоративной сети.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Этот документ применяется к точкам доступа Cisco Aironet, которые выполняют или VxWorks или программное обеспечение Cisco IOS.

Сведения, содержащиеся в данном документе, были получены с устройств в специальной лабораторной среде. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. Перед выполнением любых команд в активной сети необходимо осознавать потенциальные последствия их применения.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Соединитесь с точкой доступа

Можно открыть систему управления точки доступа через web-браузер или через последовательный порт точки доступа с эмулятором терминала. Если вы незнакомы с тем, как соединиться с точкой доступа, обратитесь к Использованию Интерфейса веба - обозревателя для направлений о том, как соединиться с точкой доступа, которая выполняет VxWorks или Использование Интерфейса веба - обозревателя для соединения с точкой доступа, которая выполняет программное обеспечение Cisco IOS.

!--- конфигурацию

Точки доступа, который VxWorks Выполнения

Как только вы установили соединение через браузер к точке доступа, выполните эти шаги, чтобы настроить и применить фильтр для блокирования трафика IPX.

Создайте фильтр

Выполните следующие действия:

1. В соответствии с Меню программы установки, выберите **Ethertype Filters**.
2. В Поле имени Набора введите имя фильтра (например, "BlockIPX") и **нажмите Add New**.
3. На следующей странице вы видите Расположение По умолчанию. Эти две опции *вперед* и *блок*. Выберите **вперед** от раскрывающегося меню.
4. В поле Special Cases введите **0x8137** и **нажмите Add New**.
5. Новое окно отображено с этими опциями:РасположениеПриоритетВремя существования индивидуальной рассылкиВремя существования групповой адресации.alertДля Расположения выберите **Block**. Оставьте другие опции при их настройках по умолчанию. **Нажмите кнопку OK.**Вы возвращены к экрану Ethertype Filter Set. Повторите Шаг 4 и Шаг 5, и добавьте **типы 0x8138, 0x00ff** и **0x00e0**.

Примените фильтр

Как только фильтр создан, это должно быть, применился к интерфейсу для вступления в силу.

1. Возвратитесь к Странице настройки. Под разделом Сетевых портов по отмеченной Ethernet строки нажмите **Filters**.
2. Вы видите, что EtherType с Получают и Прямые параметры настройки. От каждого раскрывающегося меню выберите фильтр, который вы создали в Шаге 2 процедуры Create a Filter, и нажмите **OK**. Этот шаг активирует фильтр, который вы создали.

Точки доступа, который программное обеспечение Cisco IOS Выполнения

Создайте фильтр

Выполните следующие действия:

1. Нажмите **Services** в панели навигации страницы.

2. В списке страницы Services нажмите **Filters**.
3. На странице Apply Filters нажмите вкладку **Ethertype Filters** в верхней части страницы.
4. Удостоверьтесь**, что NEW** (по умолчанию) выбран в меню Create/Edit Filter Index. Если вы хотите отредактировать существующий фильтр, выберите filter number из меню Create/Edit Filter Index.
5. В Поле индекса Фильтра назовите фильтр с номером от 200 до 299. Номер, который вы назначаете, создает список контроля доступа (ACL) для фильтра.
6. Введите **0x8137 дюймов** поле Add Ethertype.
7. Оставьте маску для Ethertype в поле Mask в значении по умолчанию.
8. Выберите **Block** из Меню Действие.
9. **Нажмите кнопку Add.** Ethertype появляется в поле Filters Classes.
10. Для удаления Ethertype из списка Классов Фильтров выберите его и нажмите **Delete Class**. Повторите Шаг 6 посредством Шага 9 и добавьте **типы 0x8138, 0x00ff** и **0x00e0** к фильтру.
11. Выберите **Forward All** из меню Default Action. Поскольку вы блокируете все пакеты IPX с этим фильтром, у вас должно быть действие по умолчанию, которое применяется ко всем другим пакетам.
12. **Щелкните "Применить".**

Примените фильтр

Фильтр был, на этом этапе, сохранен на точке доступа, но это не включено, пока вы не применяете его на странице Apply Filters.

1. Нажмите вкладку **Apply Filters** для возврата к странице Apply Filters.
2. Выберите filter number от одного из раскрывающихся меню Ethertype. Можно применить фильтр или к или к и Ethernet и радиопорты, и или к или и поступление и исходящие пакеты.
3. **Щелкните "Применить".** Фильтр включен на выбранных портах.

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.

Дополнительные сведения

- Поддержка продукта беспроводной локальной сети
- Поддержка технологии беспроводной локальной сети
- Программное обеспечение беспроводной локальной сети
- Cisco Systems – техническая поддержка и документация