Содержание

Введение

Этот документ поясняет, как читать и создавать списки доступа (ACL) сервисных точек доступа (SAP) в маршрутизаторах Cisco. Хотя существует несколько типов ACL, в данном документе рассматриваются лишь те, в которых используется фильтрация на основе значений SAP. Числовой диапазон для этого типа ACL 200 - 299. Эти ACL могут быть применены к Интерфейсам Token Ring для фильтрации трафика Source Route Bridge (SRB) к Интерфейсам Ethernet для фильтрации трафика Прозрачного моста (TB), или к Коммутации соединения передачи данных (DLSw) равные маршрутизаторы.

Основная трудность при использовании списков ACL SAP – нужно точно знать, какие SAP разрешены или запрещены определенной записью ACL. Будем анализировать четыре различных сценария с фильтрацией отдельного протокола.

Перед началом работы

Условные обозначения

Дополнительные сведения об условных обозначениях в документах см. Cisco Technical Tips Conventions.

Предварительные условия

Для данного документа отсутствуют предварительные условия.

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

Сетевая архитектура систем отбора

Использование трафика Системной сетевой архитектуры (SNA) IBM SAP в пределах от 0x00 к 0xFF. Виртуальный телекоммуникационный метод доступа (VTAM) версии V3R4 и более поздних поддерживает значения SAP в диапазоне от 4 до 252 (или от 0x04 до 0xFC в шестнадцатеричной системе), где 0xF0 зарезервировано для трафика NetBIOS. SAP должны быть кратны 0x04, начиная с 0x04. **Следующий список ACL допускает наиболее распространенные протоколы SAP SNA и отклоняет все остальные (подразумевая неявный запрет всего трафика в конце каждого списка ACL):**

```
access-list 200 permit 0x0000 0x0D0D
```

Шестнадцатеричный	Двоичные файлы
0x0000 0x0D0D	`access-list 200 permit 0x0000 0x0D0D`

Определите, какие именно SAP включаются этой конкретной записью ACL, при помощи битов групповой маски. Используйте следующие правила при интерпретации разрядов шаблона маски:

- 0 = Полное соответствие требуется. Это означает, что разрешенный SAP должен иметь то же значение как SAP, настроенный в ACL. Дополнительные сведения см. в приведенной ниже таблице.
- 1 = разрешенный SAP может иметь либо 0, либо 1 в этом двоичном разряде, позиция "do not care".

Разрешенные ACL точки доступа к службам, где X=0 или X=1	Маска символа подстановки	SAP, настроенный в ACL
0	0	0
0	0	0
0	0	0
0	0	0
X	1	0
X	1	0
0	0	0
X	1	0

Используя результаты предыдущей таблицы, список SAP, отвечающий приведенному выше шаблону, приведен далее.

Позволенные соки (двоичные файлы)								Допустимые SAP (шестнадцатеричные)
0	0	0	0	0	0	0	0	0x00
0	0	0	0	0	0	0	1	0x01
0	0	0	0	0	1	0	0	0x04
0	0	0	0	0	1	0	1	0x05
0	0	0	0	1	0	0	0	0x08

0	0	0	0	1	0	0	1	0x09
0	0	0	0	1	1	0	0	0x0C
0	0	0	0	1	1	0	1	0x0D

Как вы можете видеть от вышеупомянутой таблицы, не весь возможный SNA SAP, включены в этот ACL. Эти SAP, однако, действуют в наиболее типичных случаях.

Другой вопрос для рассмотрения при разработке ACL - то, что SAP оценивает изменение в зависимости от того, если они - команды или ответы. Точка доступа к исходной службе включает в себя бит команды/ответа, чтобы различать их. Для параметра C/R задается значение 0 для команд и 1 для ответов. ACL должен пропускать или блокировать команды и ответы. Например, SAP 0x05 (используемый для ответов) является SAP 0x04 с набором C/R к 1. То же применяется к SAP 0x09 (SAP 0x08 с набором C/R к 1), 0x0D, и 0x01.

Фильтрация NetBIOS

Трафик NetBIOS использует значения SAP 0xF0 (для команд) и 0xF1 (для ответов). Обычно администраторы сети используют эти значения SAP для фильтрации этого протокола. Запись списка доступа, показанная ниже Трафика NetBIOS разрешений и, запрещает все остальное (помните, что неявные **запрещают все** в конце каждого ACL):

```
access-list 200 permit 0xF0F0 0x0101
```

Используя ту же процедуру, описанную в предыдущем разделе, можно определить, разрешает ли вышеприведенный ACL SAP 0xF0 и 0xF1.

Если, наоборот, требуется блокировать NetBIOS и разрешить остальную часть трафика, используйте следующий список ACL:

```
access-list 200 deny 0xF0F0 0x0101access-list 200 permit 0x0000 0xFFFF
```

Фильтрация IPX

По умолчанию маршрутизаторы Cisco передают IPX-трафик через мостовое соединение. **Чтобы изменить это поведение, необходимо выполнить на маршрутизаторе команду ipx routing.** IPX при помощи инкапсуляции 802.2 использует SAP 0xE0 в качестве точки доступа к службе назначения (DSAP) и SSAP. Поэтому, если маршрутизатор Cisco соединяет IPX, и требование должно разрешить только этот тип трафика, использовать следующий ACL:

```
access-list 200 permit 0xE0E0 0x0101
```

Наоборот, следующий ACL блокирует IPX и разрешает остальной трафик:

```
access-list 200 deny 0xE0E0 0x0101access-list 200 permit 0x0000 0xFFFF
```

Разрешить или запретить весь трафик

Каждый ACL включает неявное условие "deny all". Необходимо знать об этой записи при анализе поведения настроенного ACL. Последняя запись ACL, показанная ниже, запрещает весь трафик.

```
access-list 200 permit ....access-list 200 permit ....access-list 200 deny 0x0000 0xFFFF
```

Во время чтения маски символа подстановки (в двоичной системе), помните, что 1

считается позицией разряда "do not care". Шаблон маски all 1s в двоичном представлении преобразуется в 0xFFFF в шестнадцатеричном представлении.

Дополнительные сведения

- Страница технической поддержки DLSw
- Списки управления доступом: краткий обзор и инструкции
- Методы фильтрации DLSw+ SAP/MAC
- Техническая поддержка - Cisco Systems