ACL на контроллерах беспроводных LAN: "Правила, ограничения и примеры"

Содержание

Введение

Этот документ содержит сведения о списках управления доступом (ACL) на контроллерах беспроводных локальных сетей (WLC). Этот документ объясняет существующие ограничения и правила, и дает соответствующие примеры. Этот документ не предназначен, чтобы быть заменой для ACL на Примере конфигурации Контроллера беспроводной локальной сети, но предоставить дополнительную информацию.

Примечание: Для ACL Уровня 2 или дополнительной гибкости в правилах списка прав доступа (ACL) Уровня 3, Cisco рекомендует настроить ACL на первом маршрутизаторе перехода, связанном с контроллером.

Когда поле протокола установлено в IP (protocol=4) в строке ACL с намерением разрешить или запретить пакеты IP, наиболее распространенная ошибка происходит. Поскольку это поле фактически выбирает то, что инкапсулируется в пакете IP, таком как TCP, Протокол UDP и Протокол ICMP, это преобразовывает в блокирование или разрешение пакетов IPINIP. Пока вы не хотите заблокировать пакеты Мобильного IP, IP не должен быть выбран ни в какой строке ACL. Идентификатор ошибки Cisco CSCsh22975 (только зарегистрированные клиенты) изменяет IP на IPINIP.

Предварительные условия

Требования

Убедитесь, что вы обеспечили выполнение следующих требований, прежде чем попробовать эту конфигурацию:

- Знание того, как настроить WLC и Облегченную точку доступа (LAP) для главной операции
- Базовые знания о Протоколе LWAPP и методах безопасности беспроводной связи

Используемые компоненты

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

Условные обозначения

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

Поймите ACL на WLC

ACL составлены из одной или более строк ACL, придерживавшихся неявным, "запрещают любого любой" в конце ACL. Каждая линия имеет эти поля:

- Порядковый номер
- Направление
- IP - адрес источника и маска
- IP - адрес назначения и маска
- Протокол
- Порт src
- Конечный порт
- DSCP
- Действие

Этот документ описывает каждое из этих полей:

- **Порядковый номер** — Указывает на заказ, что строки ACL обработаны против пакета. Пакет обработан против ACL, пока это не совпадает с первой строкой списка контроля доступа. Это также позволяет вам вставлять строки ACL где угодно в ACL даже после того, как будет создан ACL. Например, если у вас есть строка ACL с порядковым номером 1, можно вставить новую строку ACL впереди если это путем включения порядкового номера 1 в новой строке ACL. Это автоматически перемещает текущую линию вниз в ACL.
- **Направление** — Говорит контроллер в который направление принудить строку ACL. Существует 3 направления: Входящий, Исходящий, и Любой. Эти направления взяты от позиции относительно WLC а не беспроводного клиента.Входящий — пакеты из источника IP от беспроводного клиента осмотрены, чтобы видеть, совпадают ли они со строкой ACL.Исходящий — пакеты IP, предназначенные беспроводному клиенту, осмотрены, чтобы видеть, совпадают ли они со строкой ACL.Любой — пакеты из

источника IP от беспроводного клиента и предназначенный беспроводному клиенту осмотрены, чтобы видеть, совпадают ли они со строкой ACL. Строка ACL применена и к Входящему и к Исходящие направления.**Примечание:** Единственный адрес и маска, которая должна использоваться при выборе Any для направления являются 0.0.0.0/0.0.0.0 (Любой). Вы не должны задавать определенный хост или подсеть ни с "Каким" направлением, потому что новая линия требовалась бы с адресами или подсетями, подкачанными для учета ответного трафика.Любое направление должно только использоваться в определенных ситуациях, где вы хотите заблокировать или позволить определенный Протокол "IP" или порт в обоих направлениях, переходя к (Исходящим) беспроводным клиентам и приезжая от (Входящих) беспроводных клиентов.При определении IP-адресов или подсетей необходимо задать направление как Входящее или Исходящее и создать вторую новую строку ACL для ответного трафика в противоположном направлении. Если ACL применен к интерфейсу и в частности не позволяет ответный трафик назад через, ответный трафик запрещен неявным, “запрещают любого любой” в конце списка ACL.

- **IP - адрес источника и Маска** — Определяют IP - адреса источника от одного хоста до нескольк подсетей, который зависит от маски. Маска используется в сочетании с IP-адресом для определения, какие биты в IP-адресе должны быть проигнорированы, когда тот IP-адрес по сравнению с IP-адресом в пакете.**Примечание:** Маски в ACL WLC не походят на подстановочный знак или обратные маски, используемые в Cisco IOS® ACLs. В то время как 0 подстановочный знак, в ACL контроллера 255 средств совпадают с октетом в IP-адресе точно. Адрес и маска объединены поразрядно.Бит маски 1 средство проверяет соответствующее разрядное значение. Спецификация 255 в маске указывает на октет в IP-адресе пакета, который осмотрен, должен совпасть точно с соответствующим октетом в адресе ACL.Бит маски, который не проверяют 0 средств (игнорирует) то соответствующее разрядное значение. Спецификация 0 в маске указывает на октет в IP-адресе пакета, который осмотрен, проигнорирован.0.0.0.0/0.0.0.0 эквивалентен “Любому” IP-адресу (0.0.0.0 как адрес и 0.0.0.0 как маска).
- **IP - адрес назначения и Маска** — Придерживаются тех же правил маски как IP - адрес источника и маска.
- **Протокол** — Задает поле протокола в Заголовке IP - пакете. Некоторые количества по протоколу преобразованы для удобства клиента и определены в выпадающее меню. Другие значения:Любой (со всеми количествами по протоколу совпадают),TCP (Протокол "IP" 6)UDP (Протокол "IP" 17)ICMP (Протокол "IP" 1)ESP (Протокол "IP" 50)AH (Протокол "IP" 51)GRE (Протокол "IP" 47)IP (Протокол "IP" 4 IPINIP [CSCsh22975])Eth По IP (Протокол "IP" 97)OSPF (Протокол "IP" 89)Другой (Задавать)Любое значение совпадает с любым протоколом в IP-заголовке пакета. Это используется, чтобы полностью заблокировать или позволить пакетному к/оту IP определенные подсети. Выберите IP для соответствия с пакетами IPINIP. Общие выборы являются UDP и TCP, которые обеспечивают установку определенного источника и портов назначения. При выборе Other можно задать любой из номеров пакетного протокола IP, определенных IANA.
- **Порт src** — Может только быть задан для TCP и протокола UDP. 0-65535 эквивалентно Любому порту.
- **Конечный порт** только быть задан для TCP и протокола UDP. 0-65535 эквивалентно Любому порту.
- **Кодовая точка дифференцированных сервисов (DSCP)** — Позволяет вам задавать

определенные DSCP-значения для соответствия в Заголовке IP - пакете. Выборы в выпадающее меню являются определенными или Любой. Если вы настраиваете определенный, вы указываете на значение в поле DSCP. Например, значения от 0 до 63 могут использоваться.
- **Действие** — Эти 2 действия, запрещают или разрешают. Запретите блокирует указанный пакет. Разрешение передает пакет.

Правила списка прав доступа (ACL) и ограничения

Ограничения WLC базирующиеся ACL

Это ограничения основанных на WLC ACL:

- Вы не видите, с какой строкой ACL совпал пакет (обратитесь к идентификатору ошибки Cisco CSCse36574 (только зарегистрированные клиенты)).
- Вы не можете регистрировать пакеты, которые совпадают, определенная строка ACL (обратитесь к идентификатору ошибки Cisco CSCse36574 (только зарегистрированные клиенты)).
- Пакеты IP (любой пакет с полем протокола ethernet, равным IP [0x0800]), являются единственными пакетами, осмотренными ACL. Другие типы пакетов Ethernet не могут быть заблокированы ACL. Например, пакеты ARP (протокол Ethernet 0x0806) не могут быть заблокированы или позволены ACL.
- Контроллер может иметь до 64 настроенных ACL; каждый ACL может иметь максимум до 64 линий.
- ACL не влияют на групповую адресацию и широковещательный трафик, который передан от или до точек доступа (AP), и беспроводные клиенты (обратитесь к идентификатору ошибки Cisco CSCse65613 (только зарегистрированные клиенты)).
- Перед версией 4.0 WLC ACL обойдены на Интерфейсе управления, таким образом, вы не можете влиять на трафик, предназначенный к Интерфейсу управления. После версии 4.0 WLC можно создать ACL ЦП. См. Настраивают ACL ЦП для получения дополнительной информации о том, как настроить этот тип ACL.**Примечание:** ACL применились к менеджменту, и Интерфейсы менеджера точки доступа проигнорированы. ACL на WLC разработаны для блокирования трафика между проводной и беспроводной сетью, не проводной сетью и WLC. Поэтому, если вы хотите предотвратить AP в определенных подсетях от связи с WLC полностью, необходимо применить список доступа на неустойчивые коммутаторы или маршрутизатор. Это заблокирует трафик LWAPP от тех AP (VLAN) к WLC.
- ACL являются зависимым процессора и могут повлиять на производительность контроллера под нагрузкой большая.
- ACL не могут блокировать доступ к виртуальному IP - адресу (1.1.1.1). Поэтому DHCP не может быть заблокирован для беспроводных клиентов.
- ACL не влияют на сервисный порт WLC.

Правила для WLC базирующиеся ACL

Это правила для основанных на WLC ACL:

- Можно только задать количества по протоколу в IP - заголовке (UDP, TCP, ICMP, и т.д.) в строках ACL, потому что ACL ограничены пакетами IP только. Если IP выбран, это указывает, что вы хотите позволить или запретить пакеты IPINIP. Если Кто-либо выбран, это указывает, что вы хотите позволить или запретить пакеты с любым Протоколом "IP".
- Если вы выбираете Any для направления, источник и назначение должны быть Любым (0.0.0.0/0.0.0.0).
- Если или источник или IP - адрес назначения не Никто, направление фильтра должно быть задано. Кроме того, обратный оператор (c/port IP - адреса источника и подкачанным/port IP - адреса назначения) в противоположном направлении должен быть создан для ответного трафика.
- Существует неявное, "запрещают любого любой" в конце ACL. Если пакет не совпадает ни с какими линиями в ACL, он отброшен контроллером.

Конфигурации

Пример ACL с DHCP, PING, HTTP и DNS

В этом примере конфигурации клиенты только быть в состоянии к:

- Получите адрес DHCP (DHCP не может быть заблокирован ACL),
- Эхо-запрос и быть пропингованным (любой Тип сообщения ICMP - не может быть ограничен для прозванивания только),
- Сделайте соединения HTTP (исходящими)
- (Исходящее) разрешение Системы доменных имен (DNS)

Для настройки этих требований безопасности ACL должен иметь линии для разрешения:

- Любое сообщение ICMP в любом направлении (не может быть ограничен для прозванивания только),
- Любой порт UDP к входящему DNS
- DNS к любому порту UDP, исходящему (ответный трафик)
- Любой порт TCP к входящему HTTP
- HTTP к любому порту TCP, исходящему (ответный трафик)

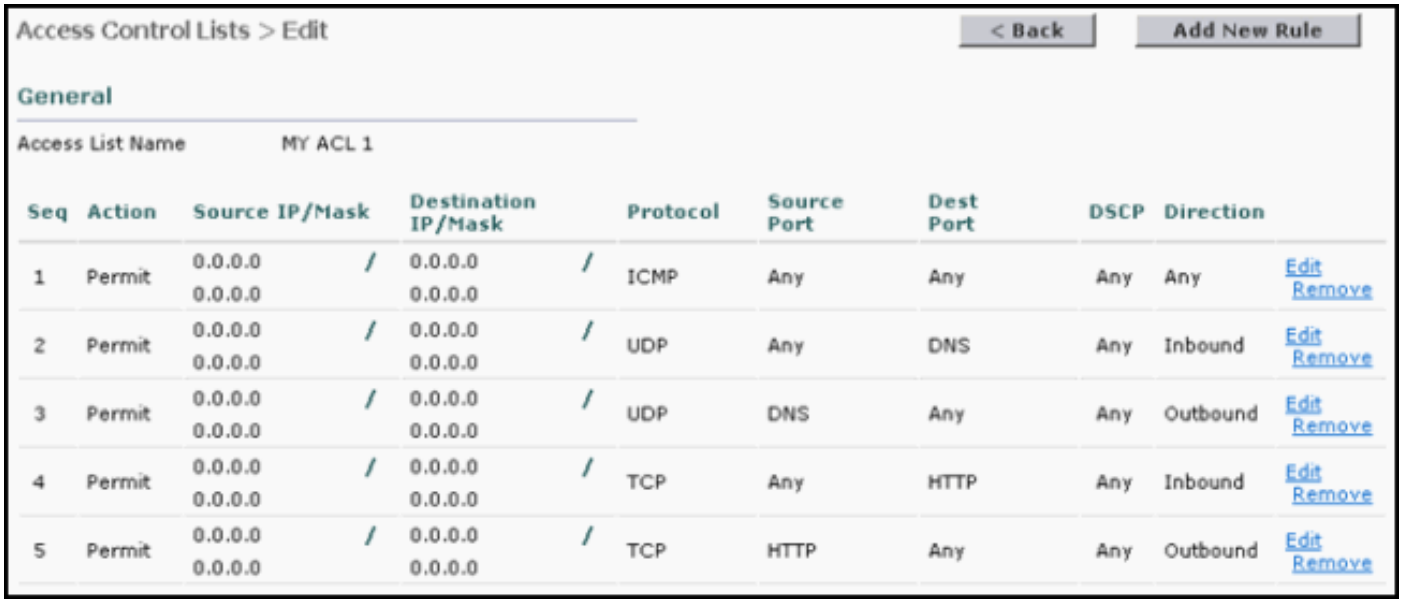
Это - то, на что ACL похож в **подробном "MY ACL 1" show acl** (кавычки только необходимы, если название ACL является больше чем 1 словом), выходные данные команды:

```
Seq  Direction  Source IP/Mask   Dest IP/Mask     Protocol  Src Port  Dest Port  DSCP  Action
---  ---------  ---------------  ---------------  --------  --------  ---------  ----  ------
1      Any      0.0.0.0/0.0.0.0  0.0.0.0/0.0.0.0     1      0-65535   0-65535     Any  Permit
2      In       0.0.0.0/0.0.0.0  0.0.0.0/0.0.0.0     17     0-65535   53-53       Any  Permit
3      Out      0.0.0.0/0.0.0.0  0.0.0.0/0.0.0.0     17     53-53     0-65535     Any  Permit
```

ACL может быть более строгим при определении подсети, что беспроводные клиенты идут вместо Любого IP-адреса в строках ACL HTTP и DNS.

Примечание: Строки ACL DHCP не могут быть подсетью, ограниченной, поскольку клиент первоначально получает ее IP-адрес с помощью 0.0.0.0, затем возобновляет ее IP-адрес через адрес подсети.

Это - то, на что тот же ACL похож в GUI:



Пример ACL с DHCP, PING, HTTP и SCCP

В этом примере конфигурации 7920 IP-телефонов только быть в состоянии к:

- Получите адрес DHCP (не может быть заблокирован ACL),
- Эхо-запрос и быть пропингованным (любой Тип сообщения ICMP - не может быть ограничен для прозванивания только),
- Позвольте (Входящее) Разрешение DNS
- Соединение IP-телефона с CallManager и наоборот (Любое Направление)
- Соединения IP-телефона с сервером TFTP (CallManager использует динамический порт после начального соединения TFTP к порту 69 UDP) (Исходящий)
- Позвольте 7920 IP-телефонов связи IP-телефона (Любое Направление)
- Запретите IP-телефону веб-или Телефонный (Исходящий) Каталог. Это сделано через неявное, "запрещают любую любую" строку ACL в конце ACL.Это позволит голосовую связь между IP-телефонами, а также обычной начальной загрузкой операции между IP-телефоном и CallManager.

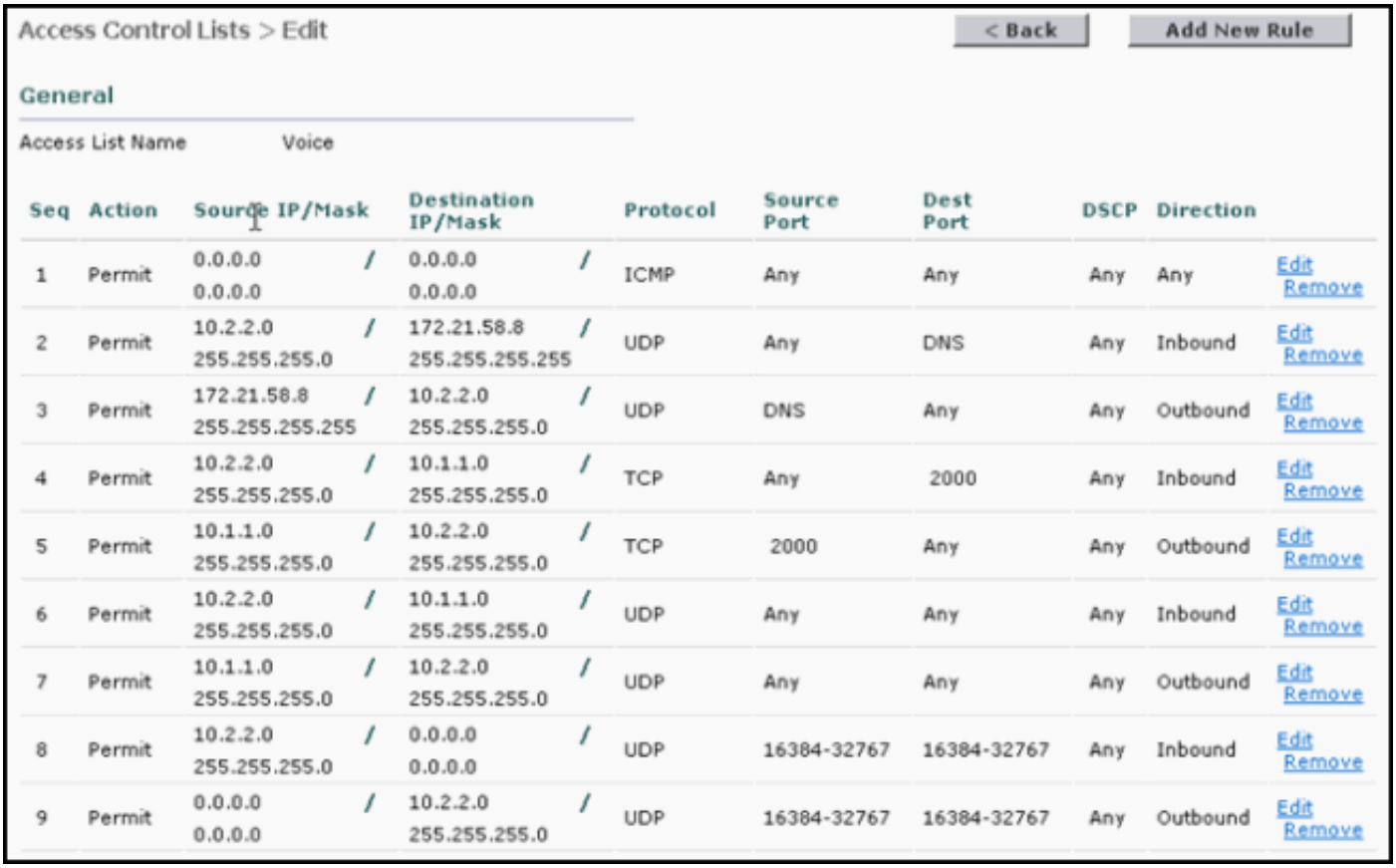
Для настройки этих требований безопасности ACL должен иметь линии для разрешения:

- Любое сообщение ICMP (не может быть ограничен для прозванивания только) (Любое направление)
- IP-телефон к серверу DNS (порт 53 UDP) (Входящий)
- Сервер DNS к IP-телефонам (порт 53 UDP) (Исходящий)
- Порты TCP IP-телефона к Порту TCP CallManager 2000 (Входящий) (порт по умолчанию)
- Порт TCP 2000 от CallManager до (Исходящих) IP-телефонов
- Порт UDP от IP-телефона до сервера TFTP. Это не может быть ограничено стандартным портом (69) TFTP, потому что CallManager использует динамический порт после запроса первоначального подключения о передаче данных.
- Порт UDP для RTP аудиотрафика между IP-телефонами (UDP ports16384-32767) (Любое направление)

В данном примере 7920 подсетей IP-телефона являются 10.2.2.0/24, и подсеть CallManager является 10.1.1.0/24. Сервер DNS 172.21.58.8. Это - выходные данные от **команды show acl detail Voice**:

```
Seq Direction Source IP/Mask          Dest IP/Mask            Protocol Src Port  Dest Port  DSCP
Action
--- --------- --------------          ---------------         -------- --------  ---------  ----
------
1     Any     0.0.0.0/0.0.0.0         0.0.0.0/0.0.0.0            1     0-65535   0-65535    Any
Permit
2     In      10.2.2.0/255.255.255.0 172.21.58.8/255.255.255.255 17    0-65535   53-53      Any
Permit
3     Out     172.21.58.8/255.255.255.255 10.2.2.0/255.255.255.0 17    53-53     0-65535    Any
Permit
4     In      10.2.2.0/255.255.255.0  10.1.1.0/255.255.255.0     6     0-65535   2000-2000  Any
Permit
5     Out     10.1.1.0/255.255.255.0  10.2.2.0/255.255.255.0     6     2000-2000 0-65535    Any
Permit
6     In      10.2.2.0/255.255.255.0  10.1.1.0/255.255.255.0     17    0-65535   0-65535    Any
Permit
7     Out     10.1.1.0/255.255.255.0  10.2.2.0/255.255.255.0     17    0-65535   0-65535    Any
Permit
8     In      10.2.2.0/255.255.255.0  0.0.0.0/0.0.0.0            17 16384-32767 16384-32767 Any
Permit
9     Out     0.0.0.0/0.0.0.0         10.2.2.0/255.255.255.0     17 16384-32767 16384-32767 Any
Permit
```

Это - то, на что это похоже в GUI:



Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	ICMP	Any	Any	Any	Any	Edit Remove
2	Permit	10.2.2.0 / 255.255.255.0	172.21.58.8 / 255.255.255.255	UDP	Any	DNS	Any	Inbound	Edit Remove
3	Permit	172.21.58.8 / 255.255.255.255	10.2.2.0 / 255.255.255.0	UDP	DNS	Any	Any	Outbound	Edit Remove
4	Permit	10.2.2.0 / 255.255.255.0	10.1.1.0 / 255.255.255.0	TCP	Any	2000	Any	Inbound	Edit Remove
5	Permit	10.1.1.0 / 255.255.255.0	10.2.2.0 / 255.255.255.0	TCP	2000	Any	Any	Outbound	Edit Remove
6	Permit	10.2.2.0 / 255.255.255.0	10.1.1.0 / 255.255.255.0	UDP	Any	Any	Any	Inbound	Edit Remove
7	Permit	10.1.1.0 / 255.255.255.0	10.2.2.0 / 255.255.255.0	UDP	Any	Any	Any	Outbound	Edit Remove
8	Permit	10.2.2.0 / 255.255.255.0	0.0.0.0 / 0.0.0.0	UDP	16384-32767	16384-32767	Any	Inbound	Edit Remove
9	Permit	0.0.0.0 / 0.0.0.0	10.2.2.0 / 255.255.255.0	UDP	16384-32767	16384-32767	Any	Outbound	Edit Remove

Приложение: 7920 портов IP-телефона

Это итоговые описания портов 7920 использования IP-телефона для передачи с Cisco CallManager (CCM) и другие IP-телефоны:

- Телефон к CCM [TFTP] (порт 69 UDP первоначально тогда изменяются на динамический порт [Эфемерный] для передачи данных) — Протокол TFTP использовал загружать микропрограммное обеспечение и файлы конфигурации.

- Телефон к CCM [веб-сервисы, Каталог] (порт TCP 80) — Телефонные URL для приложений XML, аутентификации, каталогов, сервисов, и т.д. Эти порты конфигурируемы на на сервисное основание.
- Телефон к CCM [Голосовая сигнализация] (порт TCP 2000) — Skinny Client Control Protocol (SCCP). Этот порт конфигурируем.
- Телефон к CCM [Безопасная Голосовая сигнализация] (порт TCP 2443) — Безопасный Skinny Client Control Protocol (SCCP)
- Телефон к CAPF [Сертификаты] (порт TCP 3804) — порт прослушивания функции представительства сертифицирующей организации (CAPF) для запуска Локально Значительных Сертификатов (LSC) к IP-телефонам.
- Телефон к/ота Речевого информационного канала [Телефонные звонки] (порты 16384 - 32768 UDP) — Протокол RTP, Безопасный протокол реального времени (SRTP).**Примечание:** CCM только использует порты 24576-32768 UDP, но другие устройства могут использовать полный диапазон.
- Когда система настроена для использования названий, а не IP-адресов, IP-телефон к Серверу DNS [DNS] (порт 53 UDP) — телефоны используют DNS для решения имени хоста серверов TFTP, CallManagers и имен хоста Web-сервера.
- IP-телефон к серверу DHCP [DHCP] (порт 67 UDP [клиент] и 68 [сервер]) — телефон использует DHCP для получения IP-адреса если не статически настроенный.

Порты 5.0 использования CallManager для передачи с могут быть найдены в Cisco Unified CallManager 5.0 TCP и Использованием порта UDP. Это также имеет определенные порты, которые это использует для передачи с 7920 IP-телефонами.

Порты 4.1 использования CallManager для передачи с могут быть найдены в Cisco Unified CallManager 4.1 TCP и Использованием порта UDP. Это также имеет определенные порты, которые это использует для передачи с 7920 IP-телефонами.

Дополнительные сведения

- Пример конфигурации ACL на контроллере беспроводных LAN
- Руководство по конфигурированию контроллера Cisco Wireless LAN, выпуск 4.0
- Cisco Systems – техническая поддержка и документация