ACL en los reguladores del Wireless LAN: Reglas, limitaciones, y ejemplos

Contenido

Introducción

Este documento proporciona información sobre las listas de control de acceso (ACL) en Controladores de LAN Inalámbricos (WLC). Este documento explica las limitaciones actuales y las reglas, y da los ejemplos relevantes. Este documento no se significa para ser un reemplazo para los ACL en el ejemplo de la configuración de controlador del Wireless LAN, pero para proporcionar la información suplemental.

Nota: Para la capa 2 ACL o la flexibilidad adicional en las reglas ACL de la capa 3, Cisco recomienda que usted configura los ACL en el primer router de saltos conectado con el regulador.

La mayoría del error común ocurre cuando el campo del protocolo se fija a IP (protocol=4) en una línea ACL con la intención de permitir o de negar los paquetes del IP. Porque este campo selecciona realmente qué se encapsula dentro del paquete del IP, tal como TCP, User Datagram Protocol (UDP), y Internet Control Message Protocol (ICMP), traduce a bloquear o a permitir los paquetes del IP en IP. A menos que usted quiera bloquear los paquetes del IP móvil, el IP no se debe seleccionar en ninguna línea ACL. El Id. de bug Cisco CSCsh22975 (clientes registrados solamente) cambia el IP al IP en IP.

prerrequisitos

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Conocimiento de cómo configurar el WLC y el Lightweight Access Point (REVESTIMIENTO) para la operación básica
- Conocimiento básico de los métodos del protocolo (LWAPP) y de la seguridad de red inalámbrica del Lightweight Access Point

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Entienda los ACL en un WLC

Los ACL se componen de una o más líneas ACL seguidas por un implícito “niegan cualquier ninguno” en el final del ACL. Cada línea tiene estos campos:

- Número de secuencia
- Dirección:
- Dirección IP de origen y máscara
- IP Address de destino y máscara
- Protocolo
- Puerto del src
- Puerto Dest
- DSCP
- Acción

Este documento describe cada uno de estos campos:

- **Número de secuencia** — Indica la orden que las líneas ACL están procesadas contra el paquete. El paquete se procesa contra el ACL hasta que haga juego la primera línea ACL. También permite que usted inserte las líneas ACL dondequiera en el ACL incluso después se crea el ACL. Por ejemplo, si usted tiene una línea ACL con un número de secuencia de 1, usted puede insertar una nueva línea ACL en el frente si él poniendo en un número de secuencia de 1 en la nueva línea ACL. Esto mueve automáticamente la línea actual abajo en el ACL.
- **Dirección** — Dice el regulador en el cual dirección para aplicar la línea ACL. Hay 3 direcciones: Entrante, saliente, y ninguno. Estas direcciones se toman de una posición en relación con el WLC y no el cliente de red inalámbrica.Entrante — Los paquetes del IP originados del cliente de red inalámbrica se examinan para ver si corresponden con la línea ACL.Saliente — Los paquetes del IP destinados al cliente de red inalámbrica se examinan para ver si hacen juego la línea ACL.Ningunos — Los paquetes del IP originados del cliente de red inalámbrica y destinados al cliente de red inalámbrica se examinan para ver si corresponden con la línea ACL. La línea ACL se aplica a entrante y a las direcciones

salientes.**Nota:** El únicos direccionamiento y máscara que deben ser utilizados cuando usted selecciona ningunos para la dirección es 0.0.0.0/0.0.0.0 (ningunos). Usted no debe especificar un host o una subred específico con la “ninguna” dirección porque una línea nueva sería requerida con los direccionamientos o las subredes intercambiada para tener en cuenta el tráfico de retorno.La cualquier dirección se debe utilizar solamente en las situaciones específicas donde usted quiere bloquear o permitir un específico protocolo IP o virar hacia el lado de babor en las ambas direcciones, yendo a los clientes de red inalámbrica (salientes) y viniendo de los clientes de red inalámbrica (entrantes).Cuando usted especifica los IP Addresses o las subredes, usted debe especificar la dirección como entrante o saliente y crear una segunda nueva línea ACL para el tráfico de retorno en la dirección opuesta. Si un ACL se aplica a una interfaz y no permite específicamente la parte posterior del tráfico de retorno a través, el tráfico de retorno es negado por el implícito “niega cualquier ninguno” en el extremo de la lista ACL.

- **Dirección IP de origen y máscara** — Define las dirección IP de origen de un solo host a las subredes múltiples, que depende de la máscara. La máscara se utiliza conjuntamente con un IP Address para determinar qué bits en un IP Address deben ser ignorados cuando ese IP Address se compara con el IP Address en el paquete.**Nota:** Las máscaras en un WLC ACL no son como el comodín o las máscaras inversas usadas en Cisco IOS® ACL. En el regulador ACL, 255 significa la coincidencia el octeto en la dirección IP exactamente, mientras que 0 es un comodín. El direccionamiento y la máscara se combinan poco a poco.Un Mask Bit 1 significa el control el valor en bits correspondiente. La especificación de 255 en la máscara indica que el octeto en la dirección IP del paquete se examina que debe hacer juego exactamente con el octeto la correspondencia en el direccionamiento ACL.Un Mask Bit 0 significa no marca (ignorar) eso valor en bits correspondiente. La especificación de 0 en la máscara indica que el octeto en la dirección IP del paquete se examina que se ignora.0.0.0.0/0.0.0.0 es equivalente a “cualquier” dirección IP (0.0.0.0 como el direccionamiento y 0.0.0.0 como la máscara).
- **IP Address de destino y máscara** — Sigue las mismas reglas de la máscara que la dirección IP de origen y la máscara.
- **Protocolo** — Especifica el campo del protocolo en encabezado del paquete IP. Algunos de los números de protocolo se traducen para la conveniencia del cliente y se definen en el menú de la extracción abajo. Los diversos valores son:Ningunos (se corresponden con todos los números de protocolo)TCP (protocolo IP 6)UDP (protocolo IP 17)ICMP (protocolo IP 1)ESP (protocolo IP 50)AH (protocolo IP 51)GRE (protocolo IP 47)IP (protocolo IP 4 IP en IP [CSCsh22975])Eth sobre IP (protocolo IP 97)OSPF (protocolo IP 89)Otro (especifique)El cualquier valor hace juego cualquier protocolo en el encabezado IP del paquete. Esto se utiliza para bloquear o para permitir totalmente los paquetes del IP a/desde las subredes específicas. Seleccione el IP para hacer juego los paquetes del IP en IP. Las selecciones comunes son UDP y el TCP que preven fijar los puertos de origen y de destino específicos. Si usted selecciona otro, usted puede especificar los números de protocolo uces de los del paquete del IP definidos por el IANA .
- **Puerto del src** — Puede ser especificado solamente para el TCP y el protocolo UDP. 0-65535 es equivalente a cualquier puerto.
- **Puerto Dest** — Puede ser especificado solamente para el TCP y el protocolo UDP. 0-65535 es equivalente a cualquier puerto.
- **Differentiated Services Code Point (DSCP)** — Permite que usted especifique los valores específicos DSCP para hacer juego en encabezado del paquete IP. Las opciones en el menú de la extracción abajo son específicas o ningunas. Si usted configura el específico, usted

indica el valor en el campo DSCP. Por ejemplo, los valores a partir de la 0 a 63 pueden ser utilizados.
- **Acción** — Las 2 acciones son niegan o permiten. Niegue a bloques el paquete especificado. Permita adelante el paquete.

Reglas ACL y limitaciones

Las limitaciones del WLC basaron los ACL

Éstas son las limitaciones de los ACL WLC-basados:

- Usted no puede ver qué línea ACL fue correspondida con por un paquete (refiera al Id. de bug Cisco CSCse36574 (clientes registrados solamente)).
- Usted no puede registrar los paquetes que hacen juego una línea ACL específica (refiera al Id. de bug Cisco CSCse36574 (clientes registrados solamente)).
- Los paquetes del IP (cualquier paquete con un campo del protocolo de los Ethernetes igual a IP [0x0800]) son los únicos paquetes examinados por el ACL. Otros tipos de paquetes Ethernet no pueden ser bloqueados por los ACL. Por ejemplo, los paquetes ARP (protocolo Ethernet 0x0806) no se pueden bloquear o permitir por el ACL.
- Un regulador puede tener hasta 64 ACL configurados; cada ACL puede tener hasta un máximo de 64 líneas.
- Los ACL no afectan al Multicast y al tráfico de broadcast de los cuales se remite o al (APS) y a los clientes de red inalámbrica de los Puntos de acceso (refiera al Id. de bug Cisco CSCse65613 (clientes registrados solamente)).
- Antes de la versión 4.0 del WLC, los ACL se desvían en la interfaz de administración, así que usted no puede afectar al tráfico destinado a la interfaz de administración. Después de la versión 4.0 del WLC, usted puede crear CPU ACL. Refiera a la configuración CPU ACL para más información sobre cómo configurar este tipo de ACL.**Nota:** Los ACL aplicados a la Administración y las interfaces del AP manager se ignoran. Los ACL en el WLC se diseñan para bloquear el tráfico entre la Tecnología inalámbrica y la red alámbrica, no la red alámbrica y el WLC. Por lo tanto, si usted quiere evitar que los AP en las ciertas subredes comuniquen con el WLC totalmente, usted necesita aplicar una lista de acceso en su Switches o router intermitente. Esto bloqueará el tráfico del LWAPP de esos AP (VLA N) al WLC.
- Los ACL son procesador dependiente y pueden afectar el funcionamiento del regulador bajo carga pesada.
- Los ACL no pueden bloquear el acceso a la dirección IP virtual (1.1.1.1). Por lo tanto, el DHCP no se puede bloquear para los clientes de red inalámbrica.
- Los ACL no afectan al puerto del servicio del WLC.

Las reglas para el WLC basaron los ACL

Éstas son las reglas para los ACL WLC-basados:

- Usted puede especificar solamente los números de protocolo en el encabezado IP (UDP, TCP, ICMP, etc.) en las líneas ACL, porque los ACL se restringen a los paquetes del IP solamente. Si se selecciona el IP, éste indica que usted quiere permitir o negar los paquetes del IP en IP. Si se selecciona ninguno, éste indica que usted quiere permitir o negar los

paquetes con protocolo IP.
- Si usted selecciona ningunos para la dirección, la fuente y el destino deben ser ninguna (0.0.0.0/0.0.0.0).
- Si la fuente o el IP Address de destino no es ninguna, la dirección del filtro debe ser especificada. También, una declaración inversa (con el /port de la dirección IP de origen y el /port del IP Address de destino intercambiados) en la dirección opuesta se debe crear para el tráfico de retorno.
- Hay un implícito “niega cualquier ninguno” en el final del ACL. Si un paquete no hace juego ninguna líneas en el ACL, es caído por el regulador.

Configuraciones

Ejemplo de ACL con el DHCP, el PING, el HTTP, y el DNS

En este ejemplo de configuración, los clientes son puedan solamente:

- Reciba un DHCP Address (el DHCP no se puede bloquear por un ACL)
- Haga ping y hagase ping (ningún tipo de mensaje de ICMP - no puede ser restringido para hacer ping solamente)
- Haga las conexiones HTTP (salientes)
- Resolución del Domain Name System (DNS) (saliente)

Para configurar estos requerimientos de seguridad, el ACL debe tener líneas a permitir:

- Cualquier mensaje ICMP en cualquier dirección (no puede ser restringido para hacer ping solamente)
- Cualquier puerto UDP al DNS entrante
- DNS a cualquier puerto UDP saliente (tráfico de retorno)
- Cualquier puerto TCP al HTTP entrante
- HTTP a cualquier puerto TCP saliente (tráfico de retorno)

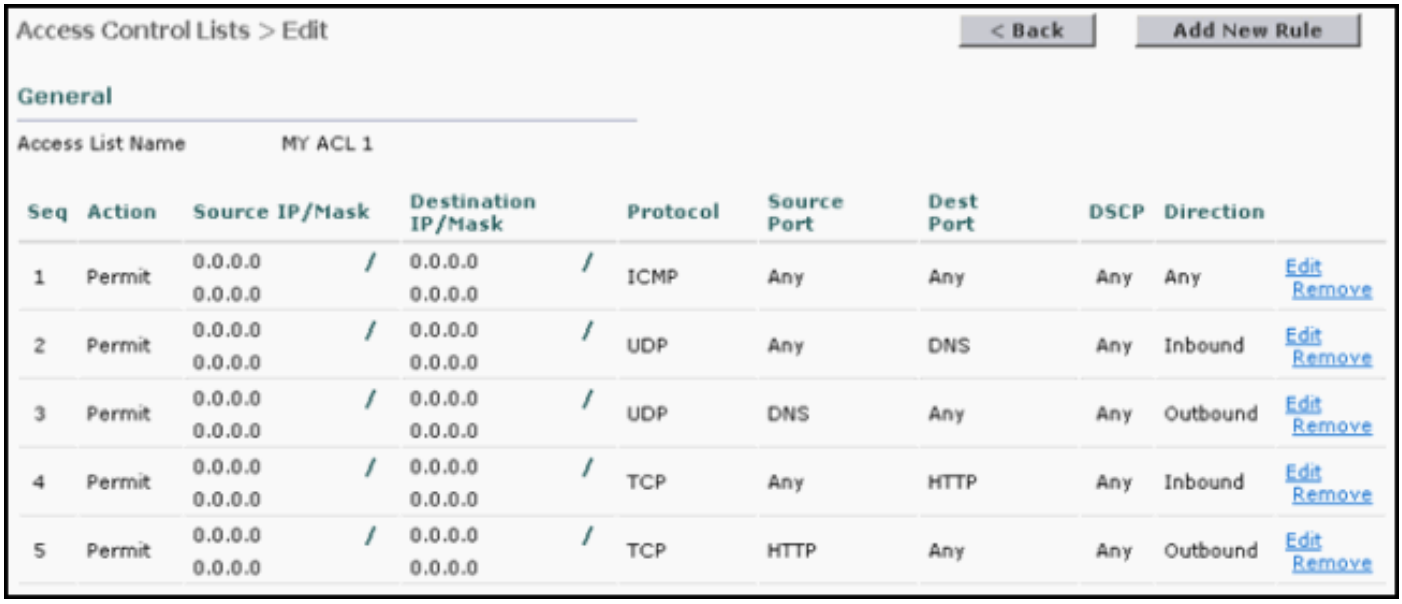
Esto es lo que parece el ACL en la **demostración acl detallada “MI** salida de comando **ACL el 1"** (las citas son solamente necesarias si el nombre ACL es más de 1 palabra):

```
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
```

El ACL puede ser más restrictivo si usted especifica la subred que los clientes de red inalámbrica están encendido en vez de cualquier dirección IP en las líneas ACL DNS y HTTP.

Nota: Las líneas ACL del DHCP no pueden ser subred restringidas como el cliente reciben su dirección IP usando 0.0.0.0, después renuevan inicialmente su dirección IP vía una dirección de subred.

Esto es lo que parece el mismo ACL en el GUI:



Ejemplo de ACL con el DHCP, el PING, el HTTP, y el SCCP

En este ejemplo de configuración, 7920 Teléfonos IP son puedan solamente:

- Reciba un DHCP Address (no puede ser bloqueado por el ACL)
- Haga ping y hagase ping (ningún tipo de mensaje de ICMP - no puede ser restringido para hacer ping solamente)
- Permita la resolución de DNS (entrante)
- Conexión del teléfono del IP al CallManager y vice versa (cualquier dirección)
- Conexiones del teléfono del IP al servidor TFTP (el CallManager utiliza el puerto dinámico después de la conexión inicial TFTP al puerto 69 UDP) (saliente)
- Permita el teléfono del IP 7920 a la comunicación del teléfono del IP (cualquier dirección)
- Rechace la red del teléfono del IP o el directorio del teléfono (saliente). Esto se hace vía un implícito “niega cualquier cualquier” línea ACL en el final del ACL.Esto permitirá las comunicaciones por voz entre los Teléfonos IP así como el inicio normal encima de las operaciones entre el teléfono del IP y el CallManager.

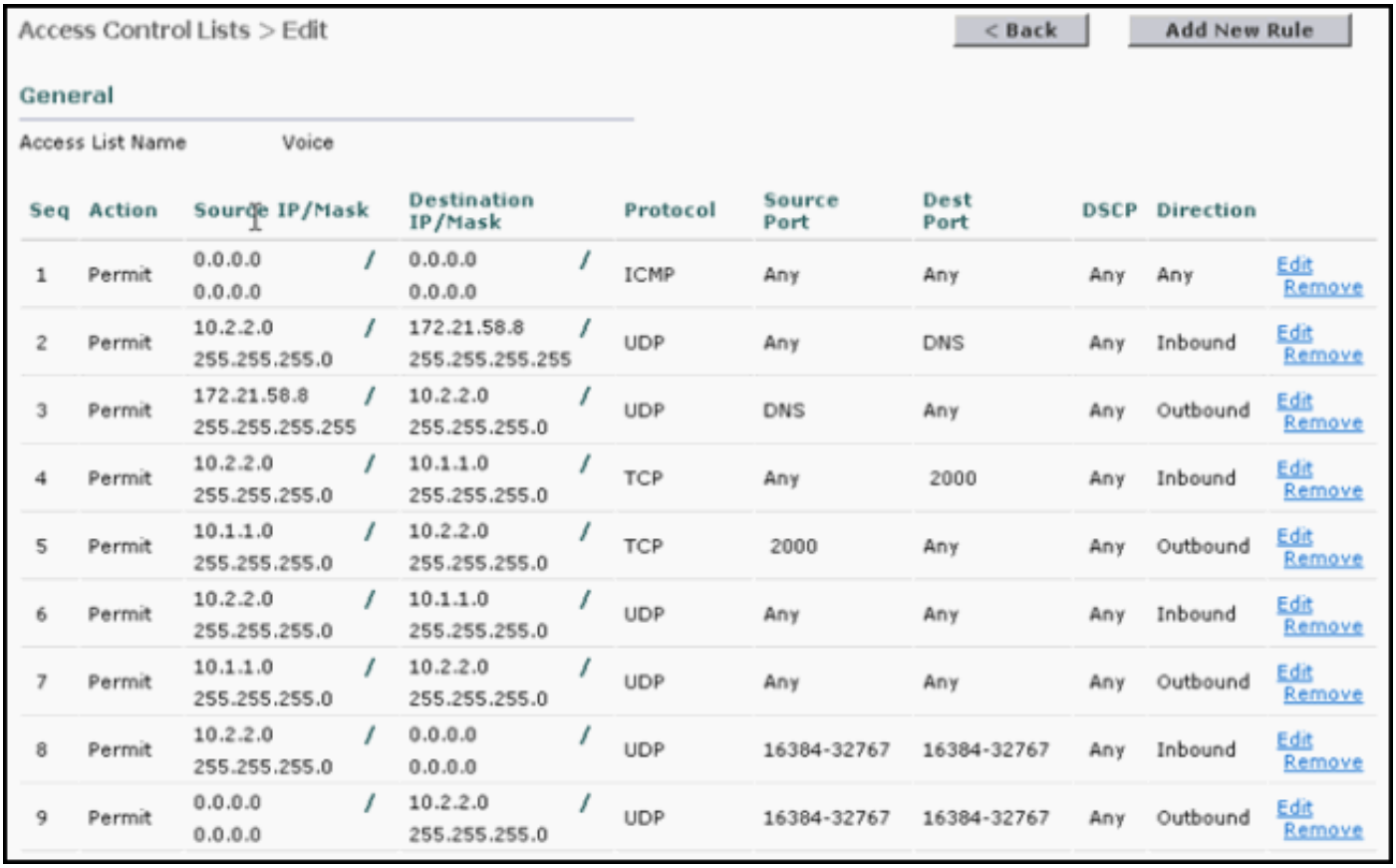
Para configurar estos requerimientos de seguridad, el ACL debe tener líneas a permitir:

- Cualquier mensaje ICMP (no puede ser restringido para hacer ping solamente) (cualquier dirección)
- Teléfono del IP al servidor DNS (puerto 53 UDP) (entrante)
- El servidor DNS a los Teléfonos IP (puerto 53 UDP) (saliente)
- Puertos TCP del teléfono del IP al puerto TCP 2000 (puerto predeterminado) del CallManager (entrante)
- Puerto TCP 2000 del CallManager a los Teléfonos IP (salientes)
- Puerto UDP del teléfono del IP al servidor TFTP. Esto no se puede restringir al puerto estándar TFTP (69) porque el CallManager utiliza un puerto dinámico después de la petición de conexión inicial la Transferencia de datos.
- Puerto UDP para el tráfico de audio RTP entre los Teléfonos IP (UDP ports16384-32767) (cualquier dirección)

En este ejemplo, la subred de 7920 teléfonos del IP es 10.2.2.0/24 y la subred del CallManager es 10.1.1.0/24. El servidor DNS es 172.21.58.8. Ésta es la salida del **control por voz del detalle acl de la demostración**:

```
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
```

Esto es lo que parece en el GUI:



Apéndice: 7920 puertos del teléfono del IP

Éstas son las descripciones sumarias de los puertos las 7920 aplicaciones del teléfono del IP de comunicar con el Cisco CallManager (CCM) y otros Teléfonos IP:

- Llame por teléfono a CCM al [TFTP] (el puerto 69 UDP entonces cambia inicialmente al [Ephemeral] del puerto dinámico para la Transferencia de datos) — Trivial File Transfer Protocol (TFTP) usado para descargar el firmware y los archivos de configuración.

- Llame por teléfono a CCM al [Web Services, Directory] (puerto TCP 80) — llaman por teléfono a los URL para las aplicaciones XML, la autenticación, los directorios, los servicios, el etc. Estos puertos son configurables en a por la base de servicio.
- Llame por teléfono al [Voice Signaling] de CCM (puerto TCP 2000) — al protocolo skinny client control (SCCP). Este puerto es configurable.
- Llame por teléfono [Secure Voice Signaling] al seguro de CCM (puerto TCP 2443) — al protocolo skinny client control (SCCPS)
- Llame por teléfono al CAPF al [Certificates] (puerto TCP 3804) — puerto de escucha de la función de proxy del Certificate Authority (CAPF) para publicar localmente - los Certificados significativos (LSC) a los Teléfonos IP.
- Exprese el portador a/desde el [Phone Calls] del teléfono (Real-Time Protocol (RTP) de los puertos 16384 – 32768 UDP) —, el protocolo de tiempo real seguro (SRTP).**Nota:** CCM utiliza solamente los puertos UDP 24576-32768, pero los otros dispositivos pueden utilizar el alcance total.
- El teléfono del IP al [DNS] del servidor DNS (puerto 53 UDP) — los teléfonos utiliza el DNS para resolver el nombre del host de los servidores TFTP, de los CallManageres, y de los nombres del host del servidor Web cuando el sistema se configura para utilizar los nombres bastante que los IP Addresses.
- El teléfono del IP al [DHCP] del servidor DHCP ([client] del puerto 67 UDP y 68 [server]) — el teléfono utiliza el DHCP para extraer una dirección IP si no configurada estáticamente.

Los puertos las 5.0 aplicaciones del CallManager de comunicar con se pueden encontrar en el Cisco Unified CallManager 5.0 TCP y el uso del puerto UDP. También tiene el específico lo vira hacia el lado de babor utiliza para comunicar con el teléfono del IP 7920.

Los puertos las 4.1 aplicaciones del CallManager de comunicar con se pueden encontrar en el Cisco Unified CallManager 4.1 TCP y el uso del puerto UDP. También tiene el específico lo vira hacia el lado de babor utiliza para comunicar con el teléfono del IP 7920.

Información Relacionada

- ACL en el ejemplo de la configuración de controlador del Wireless LAN
- Guía de configuración del Controlador de LAN de la Red Inalámbrica Cisco, versión 4.0
- Soporte Técnico y Documentación - Cisco Systems