ACL en WLC: 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 y reglas actuales, y proporciona ejemplos relevantes. Este documento no está pensado para sustituir las ACL en el Ejemplo de Configuración del Controlador de LAN Inalámbrica, sino para proporcionar información complementaria.

Nota: Para ACL de Capa 2 o flexibilidad adicional en reglas ACL de Capa 3, Cisco recomienda que configure ACL en el router de primer salto conectado al controlador.

El error más común ocurre cuando el campo de protocolo se configura en IP (protocol=4) en una línea ACL con la intención de permitir o denegar paquetes IP. Dado que este campo selecciona realmente lo que se encapsula dentro del paquete IP, como TCP, protocolo de datagramas de usuario (UDP) y protocolo de mensajes de control de Internet (ICMP), se traduce en bloquear o permitir paquetes IP en IP. A menos que desee bloquear paquetes de IP móvil, IP no debe seleccionarse en ninguna línea ACL. El ID de bug de Cisco CSCsh2975 (sólo para clientes registrados) cambia IP a IP en IP.

Prerequisites

Requirements

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Conocimiento de cómo configurar el WLC y el Lightweight Access Point (LAP) para el funcionamiento básico
- Conocimientos básicos sobre el protocolo de punto de acceso ligero (LWAPP) y los métodos de seguridad inalámbrica

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.

Comprensión de las ACL en un WLC

Las ACL se componen de una o más líneas ACL seguidas de un "deny any any" implícito al final de la ACL. Cada línea tiene estos campos:

- Número de secuencia
- Dirección:
- Dirección IP y máscara de origen
- Máscara y dirección IP de destino
- Protocolo
- Puerto Src
- Puerto de destino
- DSCP
- Acción

Este documento describe cada uno de estos campos:

- **Número de secuencia**: indica el orden en que se procesan las líneas ACL en el paquete. El paquete se procesa contra la ACL hasta que coincide con la primera línea ACL. También le permite insertar líneas ACL en cualquier lugar de la ACL incluso después de que se haya creado la ACL. Por ejemplo, si tiene una línea ACL con un número de secuencia de 1, puede insertar una nueva línea ACL al frente si coloca un número de secuencia de 1 en la nueva línea ACL. Esto mueve automáticamente la línea actual hacia abajo en la ACL.
- **Dirección**: indica al controlador en qué dirección aplicar la línea ACL. Hay 3 direcciones: Entrante, Saliente y Cualquiera. Estas direcciones se toman de una posición relativa al WLC y no al cliente inalámbrico.Entrantes: los paquetes IP originados en el cliente inalámbrico se inspeccionan para ver si coinciden con la línea ACL.Saliente: los paquetes IP destinados al cliente inalámbrico se inspeccionan para ver si coinciden con la línea ACL.Any (Cualquiera): los paquetes IP originados en el cliente inalámbrico y destinados al cliente inalámbrico se inspeccionan para ver si coinciden con la línea ACL. La línea ACL se aplica a las direcciones Entrante y Saliente.**Nota:** La única dirección y máscara que debe utilizarse al seleccionar Any (Cualquiera) para la dirección es 0.0.0.0/0.0.0.0 (Cualquiera). No debe especificar un host o una subred específicos con la dirección "Any" (Cualquiera) porque se requeriría una nueva

línea con las direcciones o subredes intercambiadas para permitir el tráfico de retorno.La opción Cualquier dirección sólo se debe utilizar en situaciones específicas en las que desee bloquear o permitir un puerto o protocolo IP específico en ambas direcciones, dirigiéndose a los clientes inalámbricos (Saliente) y viniendo de los clientes inalámbricos (Entrante).Cuando especifica direcciones IP o subredes, debe especificar la dirección como Entrante o Saliente y crear una segunda línea ACL nueva para el tráfico de retorno en la dirección opuesta. Si se aplica una ACL a una interfaz y no permite específicamente el tráfico de retorno de vuelta a través, el tráfico de retorno es denegado por el "deny any any" implícito al final de la lista ACL.

- **Dirección IP y máscara de origen**: Define las direcciones IP de origen desde un único host hasta varias subredes, que depende de la máscara. La máscara se utiliza junto con una dirección IP para determinar qué bits de una dirección IP se deben ignorar cuando se compara esa dirección IP con la dirección IP en el paquete.**Nota:** Las máscaras en un WLC ACL no son como el comodín o las máscaras inversas utilizadas en Cisco IOS® ACL. En las ACL del controlador, 255 significa que coincide exactamente con el octeto en la dirección IP, mientras que 0 es un comodín. La dirección y la máscara se combinan bit a bit.Un bit de máscara 1 significa verificar el valor de bit correspondiente. La especificación de 255 en la máscara indica que el octeto en la dirección IP del paquete que se inspecciona debe coincidir exactamente con el octeto correspondiente en la dirección ACL.Un bit de máscara 0 significa no verificar (ignorar) ese valor de bit correspondiente. La especificación de 0 en la máscara indica que se ignora el octeto en la dirección IP del paquete inspeccionado.0.0.0.0/0.0.0.0 equivale a "Cualquier" dirección IP (0.0.0.0 como dirección y 0.0.0.0 como máscara).
- **Dirección IP y máscara de destino**: sigue las mismas reglas de máscara que la dirección IP y la máscara de origen.
- **Protocolo**: especifica el campo de protocolo en el encabezado del paquete IP. Algunos de los números de protocolo se traducen para comodidad del cliente y se definen en el menú desplegable. Los diferentes valores son:Cualquiera (todos los números de protocolo coinciden)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 valor Any coincide con cualquier protocolo en el encabezado IP del paquete. Esto se utiliza para bloquear por completo o permitir paquetes IP hacia/desde subredes específicas. Seleccione IP para que coincida con los paquetes IP en IP. Las selecciones comunes son UDP y TCP, que permiten establecer puertos de origen y destino específicos. Si selecciona Otro, puede especificar cualquiera de los números de protocolo de paquete IP definidos por IANA .
- **Puerto Src**: solo se puede especificar para los protocolos TCP y UDP. 0-65535 es equivalente a Cualquier puerto.
- **Puerto de destino**: solo se puede especificar para los protocolos TCP y UDP. 0-65535 es equivalente a Cualquier puerto.
- **Punto de código de servicios diferenciados (DSCP)**: permite especificar los valores DSCP específicos que deben coincidir en el encabezado del paquete IP. Las opciones del menú desplegable son específicas de Any (Cualquiera). Si configura un valor específico, indique el valor en el campo DSCP. Por ejemplo, se pueden utilizar valores de 0 a 63.
- **Acción**: las 2 acciones son denegar o permitir. Denegar bloquea el paquete especificado. Permitir reenvía el paquete.

Reglas y limitaciones de ACL

Limitaciones de ACL Basadas en WLC

Estas son las limitaciones de las ACL basadas en WLC:

- No puede ver qué línea de ACL coincidió con un paquete (consulte el ID de error de Cisco CSCse36574 (sólo para clientes registrados)).
- No puede registrar paquetes que coincidan con una línea ACL específica (consulte la identificación de error de Cisco CSCse36574 (sólo para clientes registrados)).
- Los paquetes IP (cualquier paquete con un campo de protocolo Ethernet igual a IP [0x0800]) son los únicos paquetes inspeccionados por la ACL. Las ACL no pueden bloquear otros tipos de paquetes Ethernet. Por ejemplo, la ACL no puede bloquear ni permitir paquetes ARP (protocolo Ethernet 0x0806).
- Un controlador puede tener hasta 64 ACL configuradas; cada ACL puede tener hasta un máximo de 64 líneas.
- Las ACL no afectan al tráfico de multidifusión y difusión que se reenvía desde o hacia los puntos de acceso (AP) y los clientes inalámbricos (consulte la identificación de error de Cisco CSCse65613 (sólo para clientes registrados)).
- Antes de la versión 4.0 del WLC, las ACL se omiten en la interfaz de administración, por lo que no puede afectar el tráfico destinado a la interfaz de administración. Después de la versión 4.0 del WLC, puede crear las ACL de la CPU. Consulte Configuración de ACL de CPU para obtener más información sobre cómo configurar este tipo de ACL.**Nota:** Las ACL aplicadas a las interfaces de administración y de administrador de AP se ignoran. Las ACL en el WLC están diseñadas para bloquear el tráfico entre la red inalámbrica y cableada, no la red cableada y el WLC. Por lo tanto, si desea evitar que los AP en las subredes determinadas se comuniquen con el WLC completamente, necesita aplicar una lista de acceso en sus switches o router intermitentes. Esto bloqueará el tráfico LWAPP de esos AP (VLAN) al WLC.
- Las ACL dependen del procesador y pueden afectar el rendimiento del controlador bajo una carga pesada.
- Las ACL no pueden bloquear el acceso a la dirección IP virtual (1.1.1.1). Por lo tanto, DHCP no se puede bloquear para los clientes inalámbricos.
- Las ACL no afectan el puerto de servicio del WLC.

Reglas para ACL Basadas en WLC

Estas son las reglas para las ACL basadas en WLC:

- Solo puede especificar números de protocolo en el encabezado IP (UDP, TCP, ICMP, etc.) en las líneas ACL, porque las ACL están restringidas a paquetes IP solamente. Si se selecciona IP, esto indica que desea permitir o denegar paquetes IP en IP. Si se selecciona Any (Cualquiera), esto indica que desea permitir o denegar paquetes con cualquier protocolo IP.
- Si selecciona Cualquiera en la dirección, el origen y el destino deben ser Cualquiera (0.0.0.0/0.0.0.0).
- Si la dirección IP de origen o de destino no es Any (Cualquiera), se debe especificar la dirección del filtro. Además, se debe crear una sentencia inversa (con dirección/puerto IP de origen y dirección/puerto IP de destino intercambiados) en la dirección opuesta para el tráfico de retorno.
- Hay un "deny any any" implícito al final de la ACL. Si un paquete no coincide con ninguna línea en la ACL, el controlador lo descarta.

Configuraciones

Ejemplo de ACL con DHCP, PING, HTTP y DNS

En este ejemplo de configuración, los clientes sólo pueden:

- Recibir una dirección DHCP (DHCP no puede ser bloqueado por una ACL)
- Ping y be ping (cualquier tipo de mensaje ICMP; no se puede restringir a ping solamente)
- Establecer conexiones HTTP (de salida)
- Resolución del sistema de nombres de dominio (DNS) (saliente)

Para configurar estos requisitos de seguridad, la ACL debe tener líneas que permitan:

- Cualquier mensaje ICMP en cualquier dirección (no se puede restringir a ping solamente)
- Cualquier puerto UDP a DNS entrante
- DNS a cualquier puerto UDP saliente (tráfico de retorno)
- Cualquier puerto TCP a HTTP entrante
- HTTP a cualquier puerto TCP saliente (tráfico de retorno)

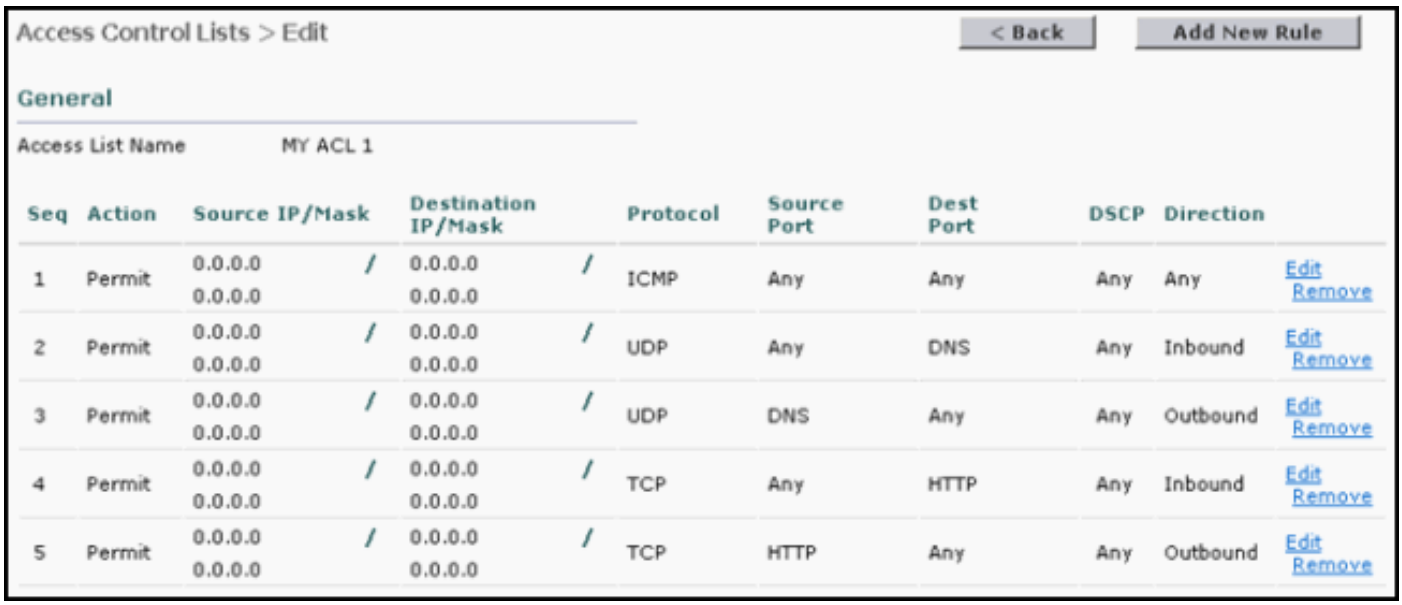
Así es como se ve la ACL en el resultado del comando **show acl detailed "MY ACL 1"** (las comillas solo son necesarias si el nombre de la ACL es más de 1 palabra):

```
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
```

La ACL puede ser más restrictiva si especifica la subred en la que se encuentran los clientes inalámbricos en lugar de Cualquier dirección IP en las líneas ACL de HTTP y DNS.

Nota: Las líneas ACL DHCP no pueden restringirse a una subred ya que el cliente recibe inicialmente su dirección IP utilizando 0.0.0.0 y luego renueva su dirección IP a través de una dirección de subred.

Así es como se ve la misma ACL en la GUI:



Ejemplo de ACL con DHCP, PING, HTTP y SCCP

En este ejemplo de configuración, los teléfonos IP 7920 sólo pueden:

- Recibir una dirección DHCP (no puede ser bloqueada por ACL)
- Ping y be ping (cualquier tipo de mensaje ICMP; no se puede restringir a ping solamente)
- Permitir resolución DNS (entrante)
- Conexión del teléfono IP al CallManager y viceversa (cualquier dirección)
- Conexiones del teléfono IP al servidor TFTP (CallManager utiliza el puerto dinámico después de la conexión TFTP inicial al puerto UDP 69) (Saliente)
- Permitir la comunicación del teléfono IP 7920 con el teléfono IP (en cualquier dirección)
- No permitir Web de teléfono IP o directorio telefónico (saliente). Esto se realiza a través de una línea de ACL implícita "deny any any" al final de la ACL.Esto permitirá las comunicaciones de voz entre los teléfonos IP, así como las operaciones normales de arranque entre el teléfono IP y el CallManager.

Para configurar estos requisitos de seguridad, la ACL debe tener líneas que permitan:

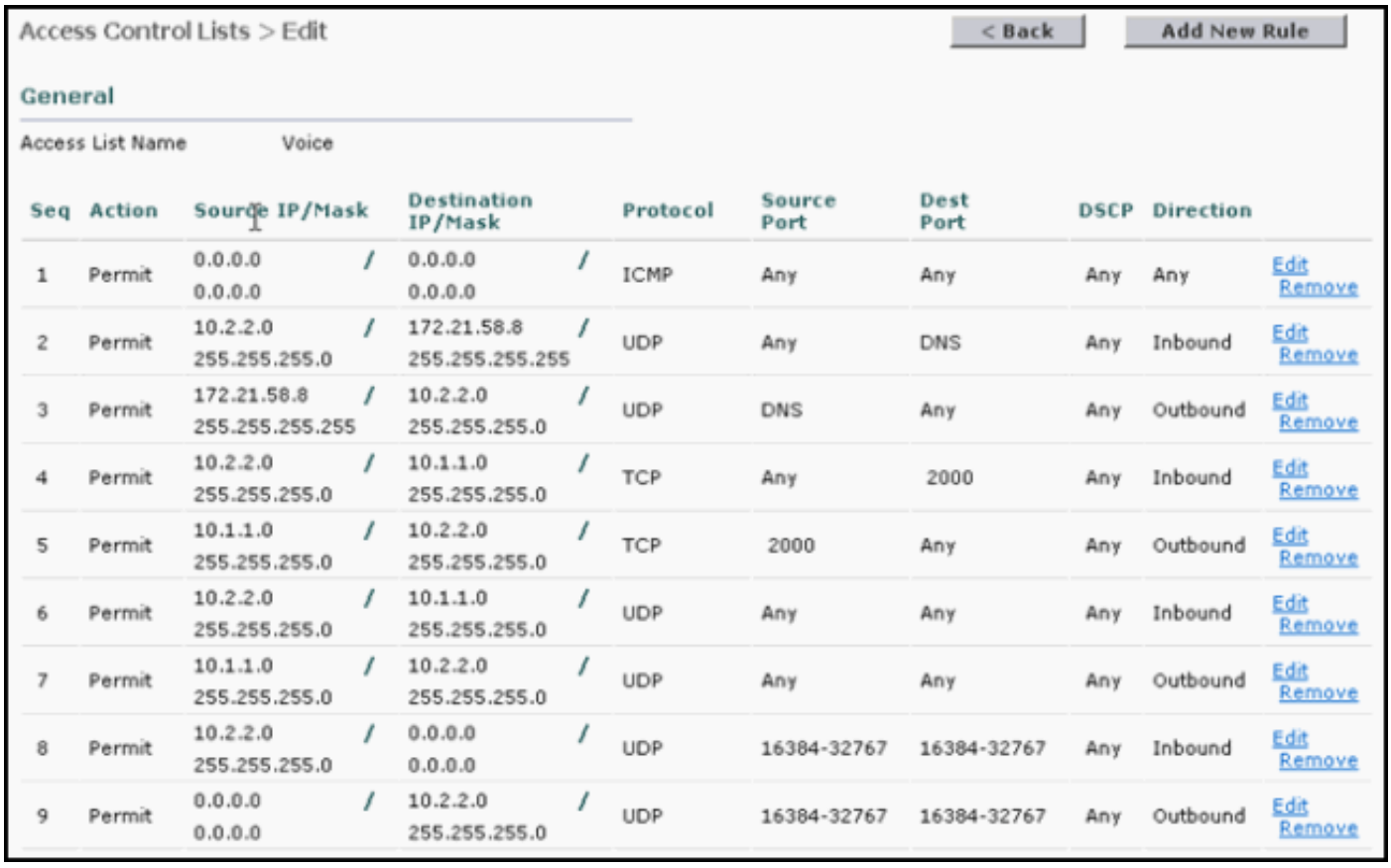
- Cualquier mensaje ICMP (no se puede restringir a ping solamente) (cualquier dirección)
- Teléfono IP al servidor DNS (puerto UDP 53) (entrante)
- El servidor DNS a los teléfonos IP (puerto UDP 53) (saliente)
- Puertos TCP del teléfono IP al puerto TCP 2000 de CallManager (puerto predeterminado) (entrante)
- Puerto TCP 2000 desde el CallManager a los teléfonos IP (Saliente)
- Puerto UDP del teléfono IP al servidor TFTP. Esto no puede restringirse al puerto TFTP estándar (69) porque CallManager utiliza un puerto dinámico después de la solicitud de conexión inicial para la transferencia de datos.
- Puerto UDP para tráfico de audio RTP entre teléfonos IP (puertos UDP 16384-32767) (en cualquier dirección)

En este ejemplo, la subred del teléfono IP 7920 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. Este es el resultado del comando **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
```

Así es como se ve en la GUI:



Access Control Lists > Edit

< Back | Add New Rule

General

Access List Name: Voice

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

Apéndice: Puertos del teléfono IP 7920

Estas son las descripciones resumidas de los puertos que el teléfono IP 7920 utiliza para comunicarse con Cisco CallManager (CCM) y otros teléfonos IP:

- Phone to CCM [TFTP] (puerto UDP 69 inicialmente y luego cambiar al puerto dinámico [Ephemeral] para la transferencia de datos): protocolo de transferencia de archivos trivial (TFTP) utilizado para descargar archivos de firmware y configuración.
- Phone to CCM [Web Services, Directory] (puerto TCP 80): direcciones URL del teléfono para aplicaciones XML, autenticación, directorios, servicios, etc. Estos puertos se pueden configurar por servicio.
- Teléfono a CCM [señalización de voz] (puerto TCP 2000): protocolo de control de cliente ligero (SCCP). Este puerto es configurable.
- Teléfono a CCM [señalización de voz segura] (puerto TCP 2443): protocolo de control de clientes skinny seguro (SCCPS)
- Teléfono a CAPF [Certificados] (puerto TCP 3804): puerto de escucha de función proxy de autoridad certificadora (CAPF) para emitir certificados de importancia local (LSC) a teléfonos IP.
- Portadora de voz a/desde el teléfono [llamadas telefónicas] (puertos UDP 16384 - 32768): protocolo en tiempo real (RTP), protocolo seguro en tiempo real (SRTP).**Nota:** CCM solo utiliza los puertos UDP 24576-32768, pero otros dispositivos pueden utilizar el rango completo.
- Teléfono IP a servidor DNS [DNS] (puerto UDP 53): los teléfonos utilizan DNS para resolver

el nombre de host de los servidores TFTP, CallManagers y los nombres de host del servidor Web cuando el sistema está configurado para utilizar nombres en lugar de direcciones IP.
- Teléfono IP al servidor DHCP [DHCP] (puerto UDP 67 [cliente] y 68 [servidor]): el teléfono utiliza DHCP para recuperar una dirección IP si no está configurada de forma estática.

Los puertos que CallManager 5.0 utiliza para comunicarse se pueden encontrar en Cisco Unified CallManager 5.0 TCP y UDP Port Usage. También tiene los puertos específicos que utiliza para comunicarse con el teléfono IP 7920.

Los puertos que CallManager 4.1 utiliza para comunicarse se pueden encontrar en Cisco Unified CallManager 4.1 TCP and UDP Port Usage. También tiene los puertos específicos que utiliza para comunicarse con el teléfono IP 7920.

Información Relacionada

- Ejemplo de configuración de ACL en controladores de LAN inalámbricas
- Guía de configuración del Controlador de LAN de la Red Inalámbrica Cisco, versión 4.0
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).