ACL em controladores do Wireless LAN: Regras, limitações, e exemplos

Índice

Introdução

Este documento fornece informações sobre as lista de controle de acesso (ACL) nos Controllers de LAN Wireless (WLC). Este documento explica as limitações atual e as regras, e dá exemplos relevantes. Este documento não é significado ser uma substituição para ACL no exemplo da configuração de controle do Wireless LAN, mas fornecer a informação suplementar.

Note: Para a camada 2 ACL ou a flexibilidade adicional em regras ACL da camada 3, Cisco recomenda que você configura ACL no primeiro roteador de salto conectado ao controlador.

A maioria de erro comum ocorre quando o campo do protocolo está ajustado a IP (protocol=4) em uma linha ACL com a intenção de permitir ou de negar pacotes IP. Porque este campo seleciona realmente o que é encapsulado dentro do pacote IP, tal como o TCP, o User Datagram Protocol (UDP), e o Internet Control Message Protocol (ICMP), traduz em obstruir ou em permitir pacotes do IP in IP. A menos que você quiser obstruir pacotes IP Móveis, o IP não deve ser selecionado em nenhuma linha ACL. A identificação de bug Cisco CSCsh22975 (clientes registrados somente) muda o IP ao IP in IP.

Pré-requisitos

Requisitos

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- Conhecimento de como configurar o WLC e o Access point de pouco peso (REGAÇO) para a operação básica
- Conhecimento básico de métodos de pouco peso do protocolo (LWAPP) e da segurança Wireless do Access point

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Compreenda ACL em um WLC

Os ACL são compostos de umas ou várias linhas ACL seguidas por um implícito “negam todos os alguns” no fim do ACL. Cada linha tem estes campos:

- Número de seqüência
- Direção
- Endereço IP de origem e máscara
- Endereço IP de destino e máscara
- Protocolo
- Porta de Src
- Porta Dest
- DSCP
- Ação

Este documento descreve cada um destes campos:

- **Número de sequência** — Indica a ordem que as linhas ACL estão processadas contra o pacote. O pacote está processado contra o ACL até que combine a primeira linha ACL. Igualmente permite que você introduza linhas ACL em qualquer lugar no ACL mesmo depois que o ACL é criado. Por exemplo, se você tem uma linha ACL com um número de sequência de 1, você pode introduzir uma linha ACL nova na parte dianteira se ele pondo em um número de sequência de 1 na linha ACL nova. Isto move automaticamente a linha atual para baixo no ACL.
- **Sentido** — Diz o controlador em que sentido para reforçar a linha ACL. Há 3 sentidos: De entrada, de partida, e algum. Estes sentidos são tomados de uma posição relativo ao WLC e não ao cliente Wireless.De entrada — Os pacotes IP originado do cliente Wireless estão inspecionados para ver se combinam a linha ACL.De partida — Os pacotes IP destinados ao cliente Wireless estão inspecionados para ver se combinam a linha ACL.Alguns — Os pacotes IP originado do cliente Wireless e destinados ao cliente Wireless estão inspecionados para ver se combinam a linha ACL. A linha ACL é aplicada a de entrada e às direções externas.**Note**: O únicos endereço e máscara que devem ser usados quando você seleciona alguns para o sentido são 0.0.0.0/0.0.0.0 (alguns). Você não deve especificar um

host ou uma sub-rede específica com “nenhum” sentido porque uma nova linha seria exigida com os endereços ou as sub-redes trocada para permitir o tráfego de retorno.Todo o sentido deve somente ser usado nas situações específicas onde você quer obstruir ou permitir um protocolo IP ou uma porta específica nos ambos sentidos, indo aos clientes Wireless (de partida) e vindo dos clientes Wireless (de entrada).Quando você especifica endereços IP de Um ou Mais Servidores Cisco ICM NT ou sub-redes, você deve especificar o sentido como de entrada ou de partida e criar uma segunda linha ACL nova para o tráfego de retorno na direção oposta. Se um ACL é aplicado a uma relação e não permite especificamente a parte traseira do tráfego de retorno completamente, o tráfego de retorno está negado pelo implícito “nega todos os alguns” na extremidade da lista ACL.

- **Endereço IP de origem e máscara** — Define os endereços IP de origem de um host único aos sub-rede múltipla, que dependa da máscara. A máscara é usada conjuntamente com um endereço IP de Um ou Mais Servidores Cisco ICM NT a fim determinar que bit em um endereço IP de Um ou Mais Servidores Cisco ICM NT devem ser ignorados quando esse endereço IP de Um ou Mais Servidores Cisco ICM NT é comparado com o endereço IP de Um ou Mais Servidores Cisco ICM NT no pacote.**Note**: As máscaras em um WLC ACL não são como o convite ou as máscaras inversas usado em Cisco IOS® ACL. No controlador ACL, 255 significam o fósforo o octeto no endereço IP de Um ou Mais Servidores Cisco ICM NT exatamente, quando 0 forem um convite. O endereço e a máscara são combinados pouco a pouco.Um bit de máscara 1 significa a verificação o valor do bit correspondente. A especificação de 255 na máscara indica que o octeto no endereço IP de Um ou Mais Servidores Cisco ICM NT do pacote que é inspecionado deve combinar exatamente com o octeto corresponder no endereço ACL.Um bit de máscara 0 significa não verifica (para ignorar) isso valor do bit correspondente. A especificação de 0 na máscara indica que o octeto no endereço IP de Um ou Mais Servidores Cisco ICM NT do pacote que é inspecionado é ignorado.0.0.0.0/0.0.0.0 são equivalente a “todo o” endereço IP de Um ou Mais Servidores Cisco ICM NT (0.0.0.0 como o endereço e 0.0.0.0 como a máscara).
- **Endereço IP de destino e máscara** — Segue as mesmas regras da máscara que o endereço IP de origem e a máscara.
- **Protocolo** — Especifica o campo do protocolo no cabeçalho do pacote IP. Alguns dos números de protocolo são traduzidos para a conveniência do cliente e definidos no menu da tração para baixo. Os valores diferentes são:Alguns (todos os números de protocolo são combinados)TCP (protocolo IP 6)UDP (protocolo IP 17)ICMP (protocolo IP 1)ESP (50 pés do protocolo IP)AH (protocolo IP 51)GRE (protocolo IP 47)IP (IP in IP [CSCsh22975] do protocolo IP 4)Eth sobre IP (protocolo IP 97)OSPF (protocolo IP 89)Outro (especifique)O alguns avaliam fósforos todo o protocolo no cabeçalho IP do pacote. Isto é usado para obstruir ou permitir completamente pacotes IP para/desde sub-redes específicas. Selecione o IP para combinar pacotes do IP in IP. As seleções comuns são UDP e TCP que preveem ajustando portas de origem e de destino específicas. Se você seleciona outro, você pode especificar alguns dos números de protocolo do pacote IP definidos pelo IANA .
- **Porta de Src** — Pode somente ser especificado para o TCP e o protocolo UDP. 0-65535 é equivalente a toda a porta.
- **Porta Dest** — Pode somente ser especificado para o TCP e o protocolo UDP. 0-65535 é equivalente a toda a porta.
- **Differentiated Services Code Point (DSCP)** — Permite que você especifique valores específicos DSCP para combinar no cabeçalho do pacote IP. As escolhas no menu da tração para baixo são específicas ou algumas. Se você configura o específico, você indica o valor no campo DSCP. Por exemplo, os valores de 0 a 63 podem ser usados.

- **Ação** — As 2 ações são negam ou permitem. Negue a blocos o pacote especificado. Permita para a frente o pacote.

Regras ACL e limitações

As limitações do WLC basearam ACL

Estas são as limitações de ACL WLC-baseados:

- Você não pode ver que linha ACL foi combinada por um pacote (refira a identificação de bug Cisco CSCse36574 (clientes registrados somente)).
- Você não pode registrar os pacotes que combinam uma linha ACL específica (refira a identificação de bug Cisco CSCse36574 (clientes registrados somente)).
- Os pacotes IP (algum pacote com um campo do protocolo dos Ethernet igual a IP [0x0800]) são os únicos pacotes inspecionados pelo ACL. Outros tipos de pacotes de Ethernet não podem ser obstruídos por ACL. Por exemplo, os pacotes ARP (protocolo de Ethernet 0x0806) não podem ser obstruídos ou permitido pelo ACL.
- Um controlador pode ter até 64 ACL configurados; cada ACL pode ter até um máximo de 64 linhas.
- Os ACL não afetam o Multicast e o tráfego de broadcast de que é enviado ou aos Access point (AP) e aos clientes Wireless (refira a identificação de bug Cisco CSCse65613 (clientes registrados somente)).
- Antes da versão 4.0 WLC, os ACL são contorneados na interface de gerenciamento, assim que você não pode afetar o tráfego destinado à interface de gerenciamento. Após a versão 4.0 WLC, você pode criar CPU ACL. Consulte para configurar CPU ACL para obter mais informações sobre de como configurar este tipo de ACL.**Note**: Os ACL aplicados ao Gerenciamento e as relações do gerenciador AP são ignorados. Os ACL no WLC são projetados obstruir o tráfego entre o Sem fio e a rede ligada com fio, não a rede ligada com fio e o WLC. Consequentemente, se você quer impedir que os AP nas determinadas sub-redes se comuniquem com o WLC inteiramente, você precisa de aplicar uma lista de acessos em seu Switches ou roteador intermitente. Isto obstruirá o tráfego LWAPP daqueles AP (VLAN) ao WLC.
- Os ACL são processador dependente e podem impactar o desempenho do controlador sob a carga pesada.
- Os ACL não podem obstruir o acesso ao endereço IP de Um ou Mais Servidores Cisco ICM NT virtual (1.1.1.1). Consequentemente, o DHCP não pode ser obstruído para clientes Wireless.
- Os ACL não afetam a porta do serviço do WLC.

As regras para o WLC basearam ACL

Estas são as regras para ACL WLC-baseados:

- Você pode somente especificar números de protocolo no cabeçalho IP (UDP, TCP, ICMP, etc.) nas linhas ACL, porque os ACL são restringidos aos pacotes IP somente. Se o IP é selecionado, este indica que você quer permitir ou negar pacotes do IP in IP. Se algum é selecionado, este indica que você quer permitir ou negar pacotes com todo o protocolo IP.

- Se você seleciona alguns para o sentido, a fonte e o destino devem ser alguma (0.0.0.0/0.0.0.0).
- Se a fonte ou o endereço IP de destino não são alguma, o sentido do filtro deve ser especificado. Também, uma indicação inversa (com a /porta do endereço IP de origem e a /porta do endereço IP de destino trocadas) na direção oposta deve ser criada para o tráfego de retorno.
- Há um implícito “nega todos os alguns” no fim do ACL. Se um pacote não combina nenhuma linhas no ACL, está deixado cair pelo controlador.

Configurações

Exemplo de ACL com DHCP, PING, HTTP, e DNS

Neste exemplo de configuração, os clientes são possam somente:

- Receba um endereço de DHCP (o DHCP não pode ser obstruído por um ACL)
- Sibile e é sibilado (nenhum tipo de mensagem ICMP - não pode ser restringido para sibilar somente)
- Faça as conexões de HTTP (de partida)
- Definição do Domain Name System (DNS) (de partida)

A fim configurar estes requisitos de segurança, o ACL deve ter as linhas a reservar:

- Algum mensagem ICMP em um ou outro sentido (não pode ser restringido para sibilar somente)
- Alguma porta UDP ao DNS de entrada
- DNS a alguma porta UDP de partida (tráfego de retorno)
- Alguma porta TCP ao HTTP de entrada
- HTTP a alguma porta TCP de partida (tráfego de retorno)

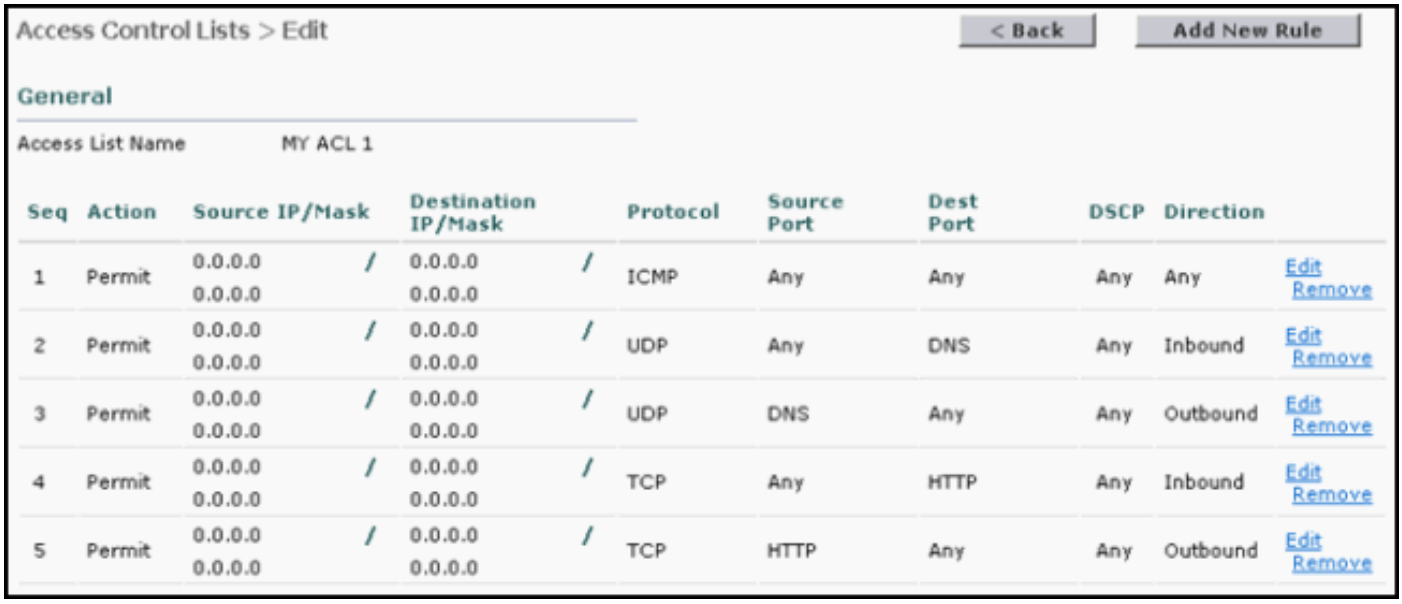
Este é o que o ACL olha como na **mostra acl detalhada “MEU** comando **ACL 1"** (as citações são somente necessárias se o nome ACL é mais de 1 palavra) output:

```
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
```

O ACL pode ser mais restritivo se você especifica a sub-rede que os clientes Wireless são sobre em vez de todo o endereço IP de Um ou Mais Servidores Cisco ICM NT nas linhas ACL DNS e HTTP.

Note: As linhas ACL DHCP não podem ser sub-rede restringidas como o cliente inicialmente recebem seu endereço IP de Um ou Mais Servidores Cisco ICM NT usando 0.0.0.0, a seguir renovam seu endereço IP de Um ou Mais Servidores Cisco ICM NT através de um endereço de sub-rede.

Este é o que o mesmo ACL olha como no GUI:



Exemplo de ACL com DHCP, PING, HTTP, e SCCP

Neste exemplo de configuração, 7920 Telefones IP são possam somente:

- Receba um endereço de DHCP (não pode ser obstruído pelo ACL)
- Sibile e é sibilado (nenhum tipo de mensagem ICMP - não pode ser restringido para sibilar somente)
- Permita a resolução de DNS (de entrada)
- Conexão do telefone IP ao CallManager e vice-versa (algum sentido)
- Conexões do telefone IP ao servidor TFTP (o CallManager usa a porta dinâmica após a conexão inicial TFTP à porta 69 UDP) (de partida)
- Permita o telefone IP 7920 a uma comunicação do telefone IP (algum sentido)
- Recuse a Web do telefone IP ou o diretório do telefone (de partida). Isto é feito através de um implícito “nega toda a qualquer” linha ACL no fim do ACL.Isto permitirá comunicações de voz entre Telefones IP assim como a bota normal acima das operações entre o telefone IP e o CallManager.

A fim configurar estes requisitos de segurança, o ACL deve ter as linhas a reservar:

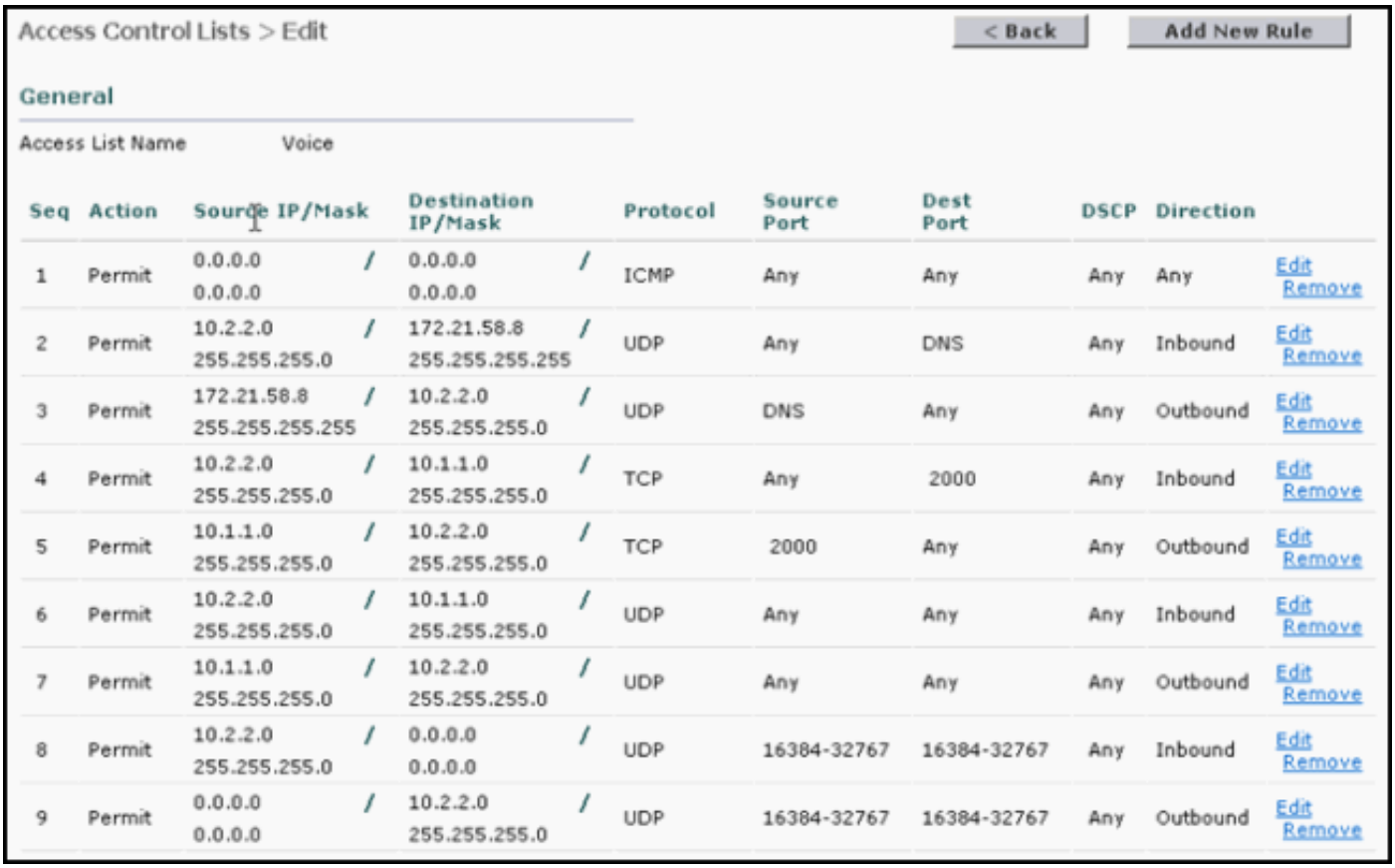
- Algum mensagem ICMP (não pode ser restringido para sibilar somente) (algum sentido)
- Telefone IP ao servidor DNS (porta 53 UDP) (de entrada)
- O servidor DNS aos Telefones IP (porta 53 UDP) (de partida)
- Portas TCP do telefone IP à porta TCP 2000 do CallManager (porta padrão) (de entrada)
- Porta TCP 2000 do CallManager aos Telefones IP (de partida)
- Porta UDP do telefone IP ao servidor TFTP. Isto não pode ser restringido à porta do padrão TFTP (69) porque o CallManager usa uma porta dinâmica após o pedido de conexão inicial para transferência de dados.
- Porta UDP para o tráfego de áudio RTP entre os Telefones IP (UDP ports16384-32767) (algum sentido)

Neste exemplo, a sub-rede de 7920 telefones IP é 10.2.2.0/24 e a sub-rede do CallManager é 10.1.1.0/24. O servidor DNS é 172.21.58.8. Esta é a saída do comando da **Voz do detalhe acl da mostra**:

```
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
```

Este é o que olha como no GUI:



Anexo: 7920 portas do telefone IP

Estas são as descrições sumárias das portas os 7920 usos do telefone IP comunicar-se com o CallManager da Cisco (CCM) e outros Telefones IP:

- Telefone ao [TFTP] CCM (a porta 69 UDP inicialmente muda então ao [Ephemeral] da porta dinâmica para transferência de dados) — Trivial File Transfer Protocol (TFTP) usado para transferir o firmware e os arquivos de configuração.
- Telefone ao [Web Services, Directory] CCM (porta TCP 80) — telefonam a URL para

aplicativos XML, autenticação, diretórios, serviços, etc. Estas portas são configuráveis na pela base de serviço.
- Telefone ao [Voice Signaling] CCM (porta TCP 2000) — ao protocolo skinny client control (SCCP). Esta porta é configurável.
- Telefone [Secure Voice Signaling] ao seguro CCM (porta TCP 2443) — ao protocolo skinny client control (os SCCP)
- Telefone ao [Certificates] CAPF (porta TCP 3804) — porta de escuta da função do proxy do Certificate Authority (CAPF) para emitir localmente - os Certificados significativos (LSC) aos Telefones IP.
- Exprima o portador para/desde o [Phone Calls] do telefone (Real-Time Protocol (RTP) das portas 16384 – 32768 UDP) —, o protocolo em tempo real seguro (SRTP).**Note**: O CCM usa somente portas UDP 24576-32768, mas os outros dispositivos podem usar a gama completa.
- O telefone IP ao [DNS] do servidor DNS (porta 53 UDP) — os telefones usa o DNS para resolver o nome de host dos servidores TFTP, dos CallManagers, e dos nomes de host do servidor de Web quando o sistema é configurado para usar nomes um pouco do que endereços IP de Um ou Mais Servidores Cisco ICM NT.
- O telefone IP ao [DHCP] do servidor DHCP ([client] da porta 67 UDP & 68 [server]) — o telefone usa o DHCP para recuperar um endereço IP de Um ou Mais Servidores Cisco ICM NT se não configurado estaticamente.

As portas os 5.0 usos do CallManager comunicar-se com podem ser encontradas em Cisco Unified CallManager 5.0 TCP e uso de porta UDP. Igualmente tem o específico move-o usa-se para comunicar-se com o telefone IP 7920.

As portas os 4.1 usos do CallManager comunicar-se com podem ser encontradas em Cisco Unified CallManager 4.1 TCP e uso de porta UDP. Igualmente tem o específico move-o usa-se para comunicar-se com o telefone IP 7920.

Informações Relacionadas

- ACL no exemplo da configuração de controle do Wireless LAN
- Guia de Configuração da Cisco Wireless LAN Controller Release 4.0
- Suporte Técnico e Documentação - Cisco Systems