ACLs on Wireless LAN Controllers: Rules, Limitations, and Examples

Document ID: 81733

Contents

Introduction
Prerequisites
Requirements
Components Used
Conventions
Understand ACLs on a WLC
ACL Rules and Limitations
Limitations of WLC Based ACLs
Rules for WLC Based ACLs
Configurations
ACL Example with DHCP, PING, HTTP, and DNS
ACL Example with DHCP, PING, HTTP, and SCCP
Appendix: 7920 IP Phone Ports
Related Information

Introduction

This document provides information about access control lists (ACLs) on Wireless LAN Controllers (WLCs). This document explains the current limitations and rules, and gives relevant examples. This document is not meant to be a replacement for ACLs on Wireless LAN Controller Configuration Example, but to provide supplemental information.

Note: For Layer 2 ACLs or additional flexibility in Layer 3 ACL rules, Cisco recommends that you configure ACLs on the first hop router connected to the controller.

The most common mistake occurs when the protocol field is set to IP (protocol=4) in an ACL line with the intention of permitting or denying IP packets. Because this field actually selects what is encapsulated inside the IP packet, such as TCP, User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP), it translates into blocking or allowing IP−in−IP packets. Unless you want to block Mobile IP packets, IP must not be selected in any ACL line. Cisco bug ID CSCsh22975 (registered customers only) changes IP to IP−in−IP.

Prerequisites

Requirements

Ensure that you meet these requirements before you attempt this configuration:

- Knowledge of how to configure the WLC and Lightweight Access Point (LAP) for basic operation
- Basic knowledge of Lightweight Access Point Protocol (LWAPP) and wireless security methods

Components Used

This document is not restricted to specific software and hardware versions.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Understand ACLs on a WLC

ACLs are made up of one or more ACL lines followed by an implicit "deny any any" at the end of the ACL. Each line has these fields:

- Sequence Number
- Direction
- Source IP Address and Mask
- Destination IP Address and Mask
- Protocol
- Src Port
- Dest Port
- DSCP
- Action

This document describes each of these fields:

- **Sequence Number** Indicates the order that ACL lines are processed against the packet. The packet is processed against the ACL until it matches the first ACL line. It also allows you to insert ACL lines anywhere in the ACL even after the ACL is created. For example, if you have an ACL line with a sequence number of 1, you can insert a new ACL line in front if it by putting in a sequence number of 1 in the new ACL line. This automatically moves the current line down in the ACL.
- **Direction** Tells the controller in which direction to enforce the ACL line. There are 3 directions: Inbound, Outbound, and Any. These directions are taken from a position relative to the WLC and not the wireless client.

    - Inbound IP packets sourced from the wireless client are inspected to see if they match the ACL line.
    - Outbound IP packets destined to the wireless client are inspected to see if they match the ACL line.
    - Any IP packets sourced from the wireless client and destined to the wireless client are inspected to see if they match the ACL line. The ACL line is applied to both Inbound and Outbound directions.

      Note: The only address and mask that should be used when you select Any for the direction is 0.0.0.0/0.0.0.0 (Any). You must not specify a specific host or subnet with the "Any" direction because a new line would be required with the addresses or subnets swapped to allow for return traffic.

      The Any direction should only be used in specific situations where you want to block or allow a specific IP protocol or port in both directions, going to the wireless clients (Outbound) and coming from the wireless clients (Inbound).

      When you specify IP addresses or subnets, you must specify the direction as Inbound or Outbound and create a second new ACL line for return traffic in the opposite direction. If an

ACL is applied to an interface and does not specifically allow return traffic back through, the return traffic is denied by the implicit deny any any at the end of the ACL list.

- **Source IP Address and Mask** Defines the source IP addresses from a single host to multiple subnets, which depends on the mask. The mask is used in conjunction with an IP address in order to determine which bits in an IP address should be ignored when that IP address is compared with the IP address in the packet.

  Note: Masks in a WLC ACL are not like the wildcard or inverse masks used in Cisco IOS® ACLs. In controller ACLs, 255 means match the octet in the IP address exactly, while 0 is a wildcard. The address and mask are combined bit by bit.

  - A mask bit 1 means check the corresponding bit value. The specification of 255 in the mask indicates the octet in the IP address of the packet that is inspected must match exactly with the corresponding octet in the ACL address.
  - A mask bit 0 means do not check (ignore) that corresponding bit value. The specification of 0 in the mask indicates the octet in the IP address of the packet that is inspected is ignored.
  - 0.0.0.0/0.0.0.0 is equivalent to Any IP Address (0.0.0.0 as the address and 0.0.0.0 as the mask).
- **Destination IP Address and Mask** Follows the same mask rules as the source IP address and mask.
- **Protocol** Specifies the protocol field in the IP packet header. Some of the protocol numbers are translated for customer convenience and are defined in the pull down menu. The different values are:

  - Any (all protocol numbers are matched)
  - TCP (IP protocol 6)
  - UDP (IP protocol 17)
  - ICMP (IP protocol 1)
  - ESP (IP protocol 50)
  - AH (IP protocol 51)
  - GRE (IP protocol 47)
  - IP (IP protocol 4 IP−in−IP [CSCsh22975])
  - Eth Over IP (IP protocol 97)
  - OSPF (IP protocol 89)
  - Other (Specify)

  The Any value matches any protocol in the IP header of the packet. This is used to completely block or allow IP packets to/from specific subnets. Select IP to match IP−in−IP packets. Common selections are UDP and TCP which provide for setting specific source and destination ports. If you select Other, you can specify any of the IP packet protocol numbers defined by IANA .
- **Src Port** Can only be specified for the TCP and UDP protocol. 0−65535 is equivalent to Any port.
- **Dest Port** Can only be specified for the TCP and UDP protocol. 0−65535 is equivalent to Any port.
- **Differentiated Services Code Point (DSCP)** Allows you to specify specific DSCP values to match in the IP packet header. The choices in the pull down menu are specific or Any. If you configure specific, you indicate the value in the DSCP field. For example, values from 0 to 63 can be used.
- **Action** The 2 actions are deny or permit. Deny blocks the specified packet. Permit forwards the packet.

ACL Rules and Limitations

Limitations of WLC Based ACLs

These are the limitations of WLC−based ACLs:

- You cannot see what ACL line was matched by a packet (refer to Cisco bug ID CSCse36574 (registered customers only)).

- You cannot log packets that match a specific ACL line (refer to Cisco bug ID CSCse36574 (registered customers only)).
- IP packets (any packet with an ethernet protocol field equal to IP [0x0800]) are the only packets inspected by the ACL. Other types of ethernet packets cannot be blocked by ACLs. For example, ARP packets (Ethernet Protocol 0x0806) cannot be blocked or allowed by the ACL.
- A controller can have up to 64 ACLs configured; each ACL can have up to a maximum of 64 lines.
- ACLs do not affect multicast and broadcast traffic that is forwarded from or to the access points (APs) and wireless clients (refer to Cisco bug ID CSCse65613 (registered customers only)).
- Before WLC version 4.0, ACLs are bypassed on the Management Interface, so you cannot affect traffic destined to the Management Interface. After WLC version 4.0, you can create CPU ACLs. Refer to Configure CPU ACLs for more information on how to configure this type of ACL.

  Note: ACLs applied to the Management and AP−Manager Interfaces are ignored. ACLs on the WLC are designed to block traffic between the wireless and wired network, not the wired network and the WLC. Therefore, if you want to prevent APs in the certain subnets from communicating with the WLC entirely, you need to apply an access list on your intermittent switches or router. This will block LWAPP traffic from those APs (VLANs) to the WLC.
- ACLs are processor dependent and can impact the performance of the controller under heavy load.
- ACLs cannot block access to the virtual IP address (1.1.1.1). Therefore, DHCP cannot be blocked for wireless clients.
- ACLs do not affect the service port of the WLC.

Rules for WLC Based ACLs

These are the rules for WLC−based ACLs:

- You can only specify protocol numbers in the IP header (UDP, TCP, ICMP, etc.) in ACL lines, because ACLs are restricted to IP packets only. If IP is selected, this indicates that you want to allow or deny IP−in−IP packets. If Any is selected, this indicates that you want to allow or deny packets with any IP protocol.
- If you select Any for the direction, the source and destination should be Any (0.0.0.0/0.0.0.0).
- If either the source or destination IP address is not Any, the direction of the filter must be specified. Also, an inverse statement (with source IP address/port and destination IP address/port swapped) in the opposite direction must be created for return traffic.
- There is an implicit "deny any any" at the end of the ACL. If a packet does not match any lines in the ACL, it is dropped by the controller.

Configurations

ACL Example with DHCP, PING, HTTP, and DNS

In this configuration example, clients are only be able to:

- Receive a DHCP address (DHCP cannot be blocked by an ACL)
- Ping and be pinged (any ICMP message type − cannot be restricted to ping only)
- Make HTTP connections (outbound)
- Domain Name System (DNS) resolution (outbound)

In order to configure these security requirements, the ACL must have lines to allow:

- Any ICMP message in either direction (cannot be restricted to ping only)
- Any UDP port to DNS inbound
- DNS to any UDP port outbound (return traffic)

- Any TCP port to HTTP inbound
- HTTP to any TCP port outbound (return traffic)

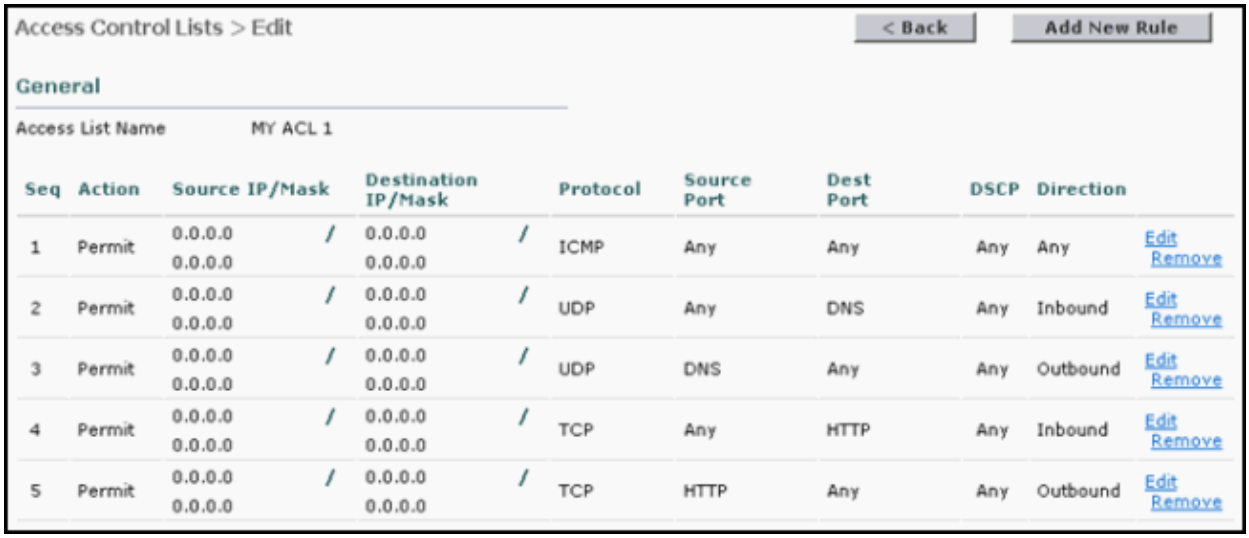
This is what the ACL looks like in the **show acl detailed "MY ACL 1"** (quotes are only necessary if the ACL name is more than 1 word) command output:

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

The ACL can be more restrictive if you specify the subnet that the wireless clients are on instead of Any IP address in the DNS and HTTP ACL lines.

Note: The DHCP ACL lines cannot be subnet restricted as the client initially receives its IP address using 0.0.0.0, then renews its IP address via a subnet address.

This is what the same ACL looks like in the GUI:



ACL Example with DHCP, PING, HTTP, and SCCP

In this configuration example, 7920 IP phones are only be able to:

- Receive a DHCP address (cannot be blocked by ACL)
- Ping and be pinged (any ICMP message type − cannot be restricted to ping only)
- Allow DNS resolution (Inbound)
- IP phone connection to the CallManager and vice versa (Any Direction)
- IP phone connections to TFTP server (CallManager uses dynamic port after initial TFTP connection to UDP port 69) (Outbound)
- Allow 7920 IP phone to IP phone communication (Any Direction)
- Disallow IP phone web or Phone Directory (Outbound). This is done via an implicit "deny any any" ACL line at the end of the ACL.

  This will allow voice communications between IP phones as well as normal boot up operations between the IP phone and the CallManager.

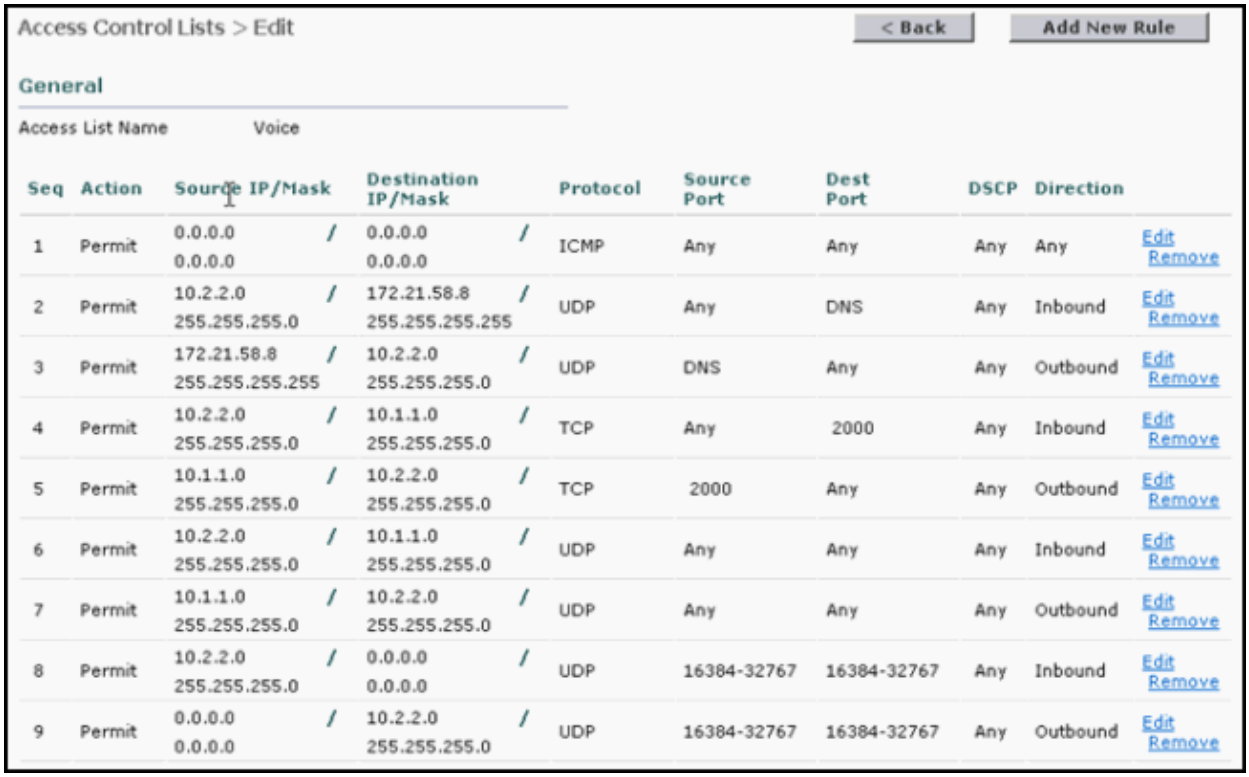
In order to configure these security requirements, the ACL must have lines to allow:

- Any ICMP message (cannot be restricted to ping only) (Any direction)
- IP phone to the DNS server (UDP port 53) (Inbound)
- The DNS server to IP phones (UDP port 53) (Outbound)
- IP phone TCP ports to the CallManager TCP Port 2000 (default port) (Inbound)
- TCP port 2000 from the CallManager to the IP phones (Outbound)
- UDP port from the IP phone to the TFTP server. This cannot be restricted to the standard TFTP port (69) beacuse the CallManager uses a dynamic port after the initial connection request for data transfer.
- UDP port for audio traffic RTP between IP phones (UDP ports16384−32767) (Any direction)

In this example, the 7920 IP phone subnet is 10.2.2.0/24 and the CallManager subnet is 10.1.1.0/24. The DNS server is 172.21.58.8. This is the output from the **show acl detail Voice** command:

```
Seq Direction Source IP/Mask          Dest IP/Mask            Protocol Src Port  Dest Port
--- --------- --------------          ---------------         -------- --------  ---------
1     Any     0.0.0.0/0.0.0.0         0.0.0.0/0.0.0.0            1     0-65535   0-65535
2     In      10.2.2.0/255.255.255.0 172.21.58.8/255.255.255.255 17    0-65535   53-53
3     Out     172.21.58.8/255.255.255.255 10.2.2.0/255.255.255.0 17    53-53     0-65535
4     In      10.2.2.0/255.255.255.0  10.1.1.0/255.255.255.0     6     0-65535   2000-2000
5     Out     10.1.1.0/255.255.255.0  10.2.2.0/255.255.255.0     6     2000-2000 0-65535
6     In      10.2.2.0/255.255.255.0  10.1.1.0/255.255.255.0     17    0-65535   0-65535
7     Out     10.1.1.0/255.255.255.0  10.2.2.0/255.255.255.0     17    0-65535   0-65535
8     In      10.2.2.0/255.255.255.0  0.0.0.0/0.0.0.0            17 16384-32767 16384-3276
9     Out     0.0.0.0/0.0.0.0         10.2.2.0/255.255.255.0     17 16384-32767 16384-3276
```

This is what it looks like in the 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

Appendix: 7920 IP Phone Ports

These are the summary descriptions of the ports the 7920 IP phone uses to communicate with the Cisco CallManager (CCM) and other IP phones:

- Phone to CCM [TFTP] (UDP port 69 initially then change to dynamic port [Ephemeral] for data transfer) Trivial File Transfer Protocol (TFTP) used to download firmware and configuration files.
- Phone to CCM [Web Services, Directory] (TCP port 80) Phone URLs for XML applications, authentication, directories, services, etc. These ports are configurable on a per service basis.
- Phone to CCM [Voice Signaling] (TCP port 2000) Skinny Client Control Protocol (SCCP). This port is configurable.
- Phone to CCM [Secure Voice Signaling] (TCP port 2443) Secure Skinny Client Control Protocol (SCCPS)
- Phone to CAPF [Certificates] (TCP port 3804) Certificate Authority Proxy Function (CAPF) listening port for issuing Locally Significant Certificates (LSCs) to IP phones.
- Voice Bearer to/from Phone [Phone Calls] (UDP ports 16384 32768) Real−Time Protocol (RTP), Secure Real Time Protocol (SRTP).

  Note: CCM only uses UDP ports 24576−32768, but other devices can use the full range.
- IP Phone to DNS Server [DNS] (UDP port 53) The phones use DNS to resolve the host name of TFTP servers, CallManagers, and web server host names when the system is configured to use names rather than IP addresses.
- IP Phone to DHCP server [DHCP] (UDP port 67 [client] & 68 [server]) The phone uses DHCP to retrieve an IP address if not statically configured.

The ports the 5.0 CallManager uses to communicate with can be found at Cisco Unified CallManager 5.0 TCP and UDP Port Usage. It also has the specific ports it uses to communicate with the 7920 IP phone.

The ports the 4.1 CallManager uses to communicate with can be found at Cisco Unified CallManager 4.1 TCP and UDP Port Usage. It also has the specific ports it uses to communicate with the 7920 IP phone.

Related Information

- **ACLs on Wireless LAN Controller Configuration Example**
- **Cisco Wireless LAN Controller Configuration Guide, Release 4.0**
- **Technical Support & Documentation − Cisco Systems**

Contacts & Feedback | Help | Site Map
© 2014 − 2015 Cisco Systems, Inc. All rights reserved. Terms & Conditions | Privacy Statement | Cookie Policy | Trademarks of Cisco Systems, Inc.

Updated: Mar 05, 2008 Document ID: 81733