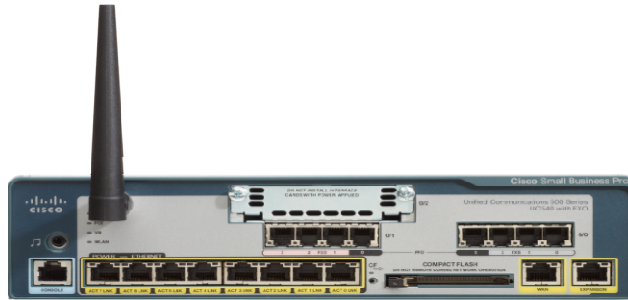


Cisco Small Business

Smart Business Communication System



Technical Enablement Lab

ACL Configuration

11/01/12

Mario Zaccone

Contents

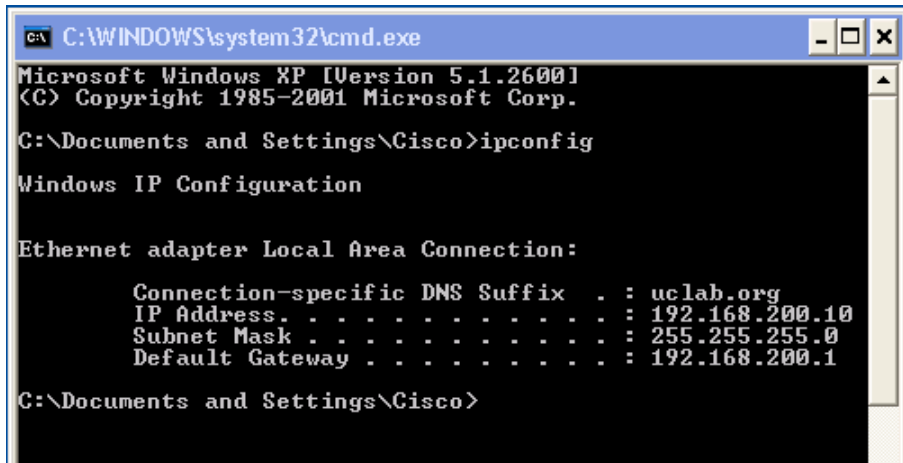
Introduction.....	3
Configuration.....	3

Introduction

In this lab we will use the “Access List Manager” feature of CCA to block the guest network from having access to another network.

Configuration

We will assume a guest VLAN exists but that we want to keep users on this guest VLAN from being able to access other existing VLANs. In this lab we have one user on the guest network with IP address 192.168.200.10.



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

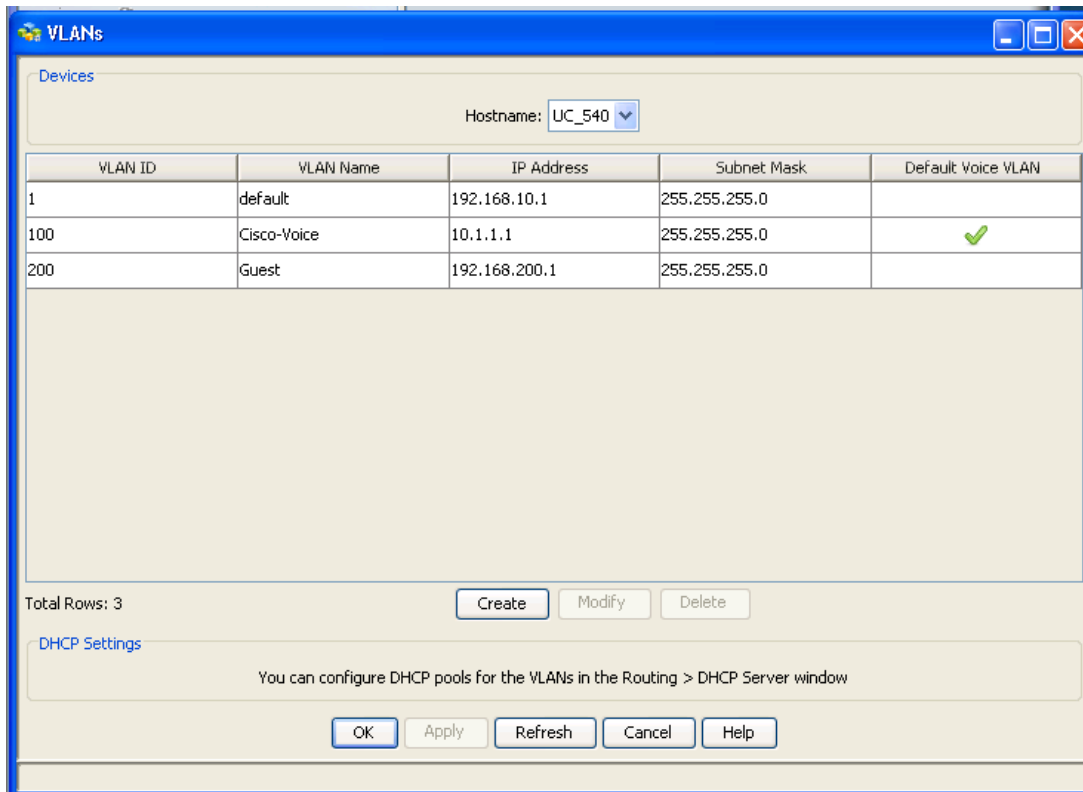
C:\Documents and Settings\Cisco>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : uclab.org
    IP Address. . . . .               : 192.168.200.10
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         : 192.168.200.1

C:\Documents and Settings\Cisco>
```



The screenshot shows a window titled "VLANs" with a "Devices" section where the hostname is set to "UC_540". Below this is a table with 5 columns: VLAN ID, VLAN Name, IP Address, Subnet Mask, and Default Voice VLAN. There are 3 rows of data. At the bottom of the table, there are buttons for "Create", "Modify", and "Delete". Below the table, there is a "DHCP Settings" section with a message and buttons for "OK", "Apply", "Refresh", "Cancel", and "Help".

VLAN ID	VLAN Name	IP Address	Subnet Mask	Default Voice VLAN
1	default	192.168.10.1	255.255.255.0	
100	Cisco-Voice	10.1.1.1	255.255.255.0	✓
200	Guest	192.168.200.1	255.255.255.0	

```

C:\WINDOWS\system32\cmd.exe - ping 10.1.1.14 -t
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Cisco>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : uclab.org
    IP Address. . . . . : 192.168.200.10
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.200.1

C:\Documents and Settings\Cisco>ping 10.1.1.14 -t

Pinging 10.1.1.14 with 32 bytes of data:

Reply from 10.1.1.14: bytes=32 time=1ms TTL=63
Reply from 10.1.1.14: bytes=32 time=1ms TTL=63
Reply from 10.1.1.14: bytes=32 time=1ms TTL=63
Reply from 10.1.1.14: bytes=32 time=1ms TTL=63

```

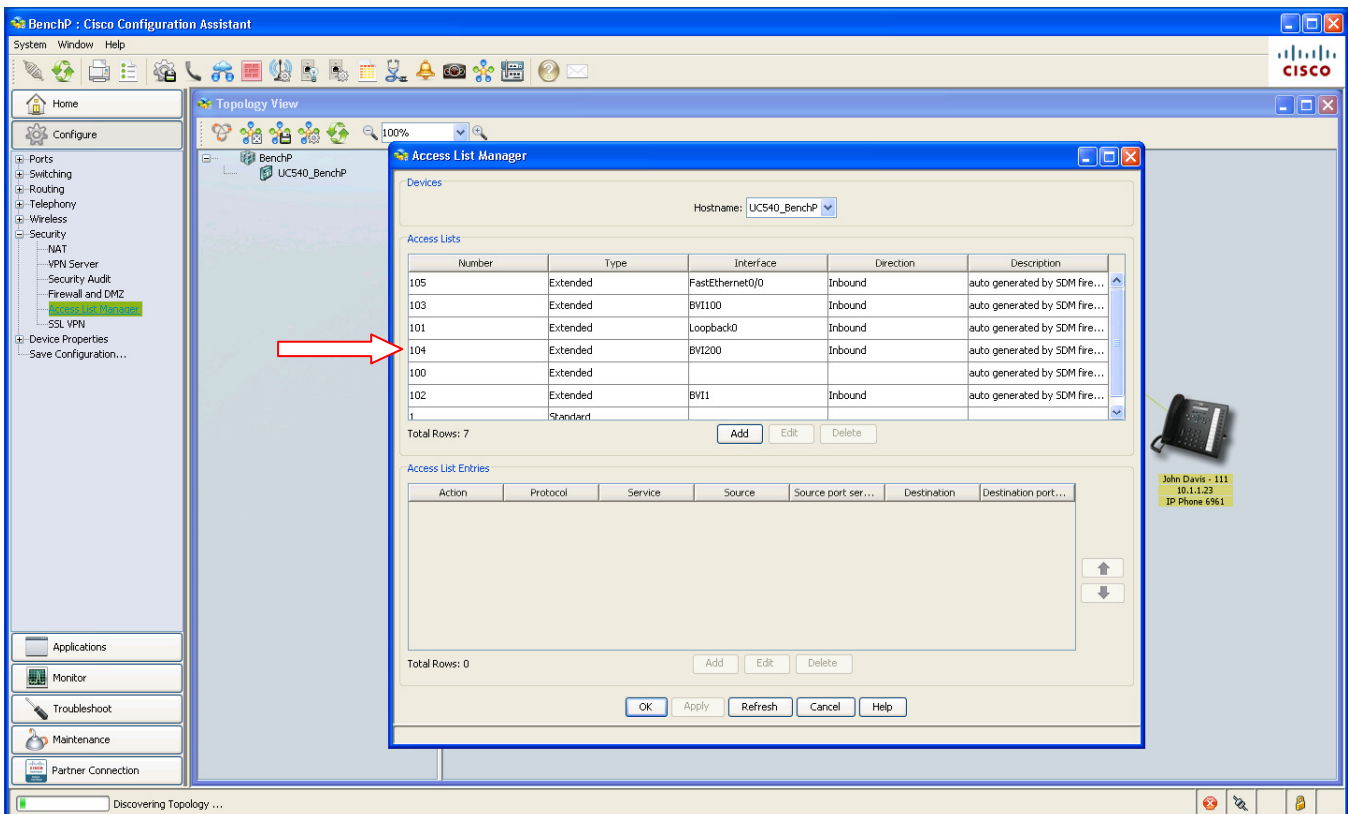
The guest client is able to ping a phone on the voice VLAN as shown in the screenshot to the left. A networking savvy user could easily intercept calls to that phone and listen in on conversations.

We will next configure ACLs to keep users on the guest network from being able to access the voice VLAN.

To do this we are going to modify ACL 104 which is bound to the guest VLAN interface BVI200 in the Inbound direction.

In CCA, navigate to the following location to get to the Access List Manager:

Configure-->Security-->Access List Manager



Access List Manager

Devices

Hostname: UC_540

Access Lists

Number	Type	Interface	Direction	Description
105	Extended	FastEthernet0/0	Inbound	auto generated by SD
103	Extended	BVI100	Inbound	auto generated by SD
101	Extended	Loopback0	Inbound	auto generated by SD
104	Extended	BVI200	Inbound	auto generated by SD
100	Extended			auto generated by SD
102	Extended	BVI1	Inbound	auto generated by SD
1	Standard			

Total Rows: 7

Add Edit Delete

Access List Entries

Action	Protocol	Service	Source	Source port ser...	Destination	Destination port...
Deny	0(ip)		10.1.10.0/0.0.0.3		any	
Deny	0(ip)		10.1.1.0/0.0.0.255		any	
Deny	0(ip)		192.168.10.0/0.0...		any	
Deny	0(ip)		255.255.255.255		any	
Deny	0(ip)		127.0.0.0/0.255....		any	
Permit	0(ip)		any		any	

Total Rows: 6

Add Edit Delete

OK Apply Refresh Cancel Help

Clicking on the "Add" button on the Access List Entries window brings up the window below.

Add Extended Access List Entry

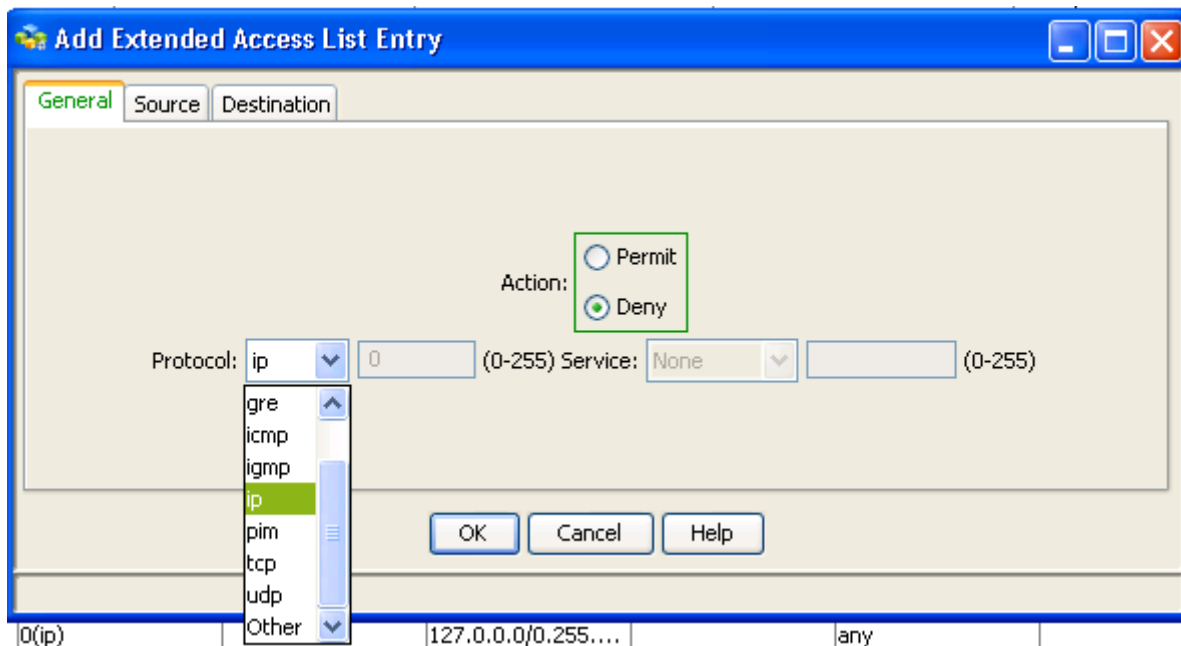
General Source Destination

Action: Permit Deny

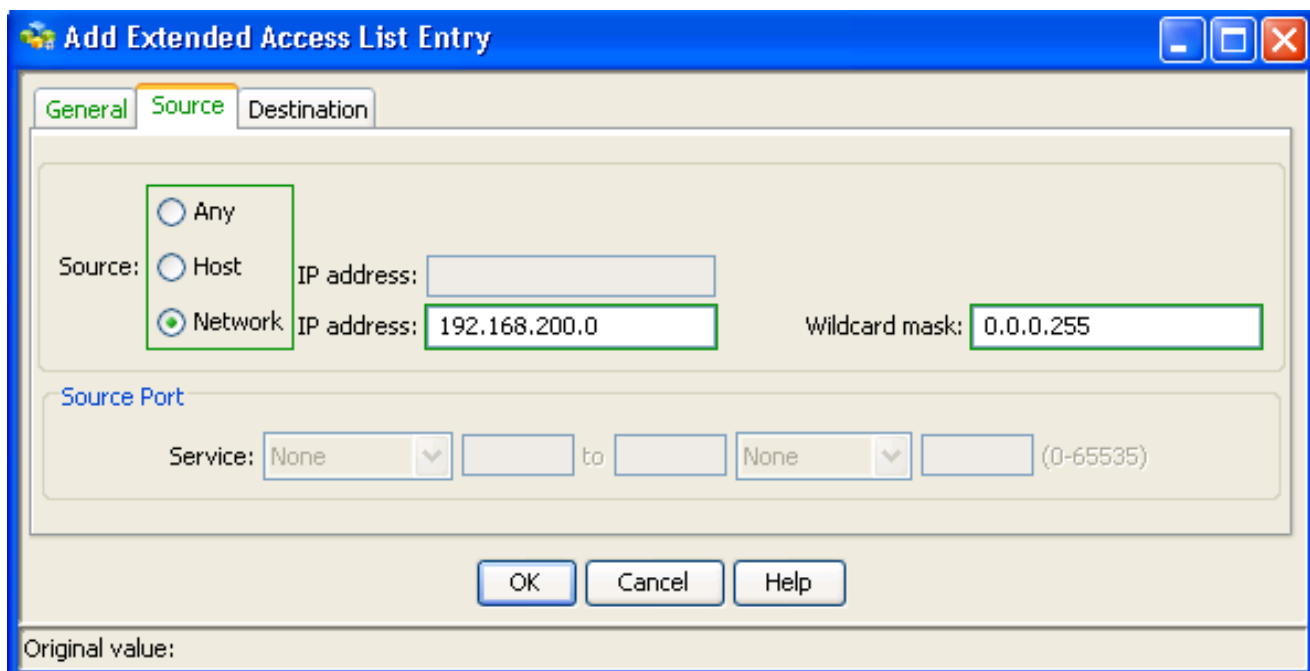
Protocol: ip 0 (0-255) Service: None (0-255)

OK Cancel Help

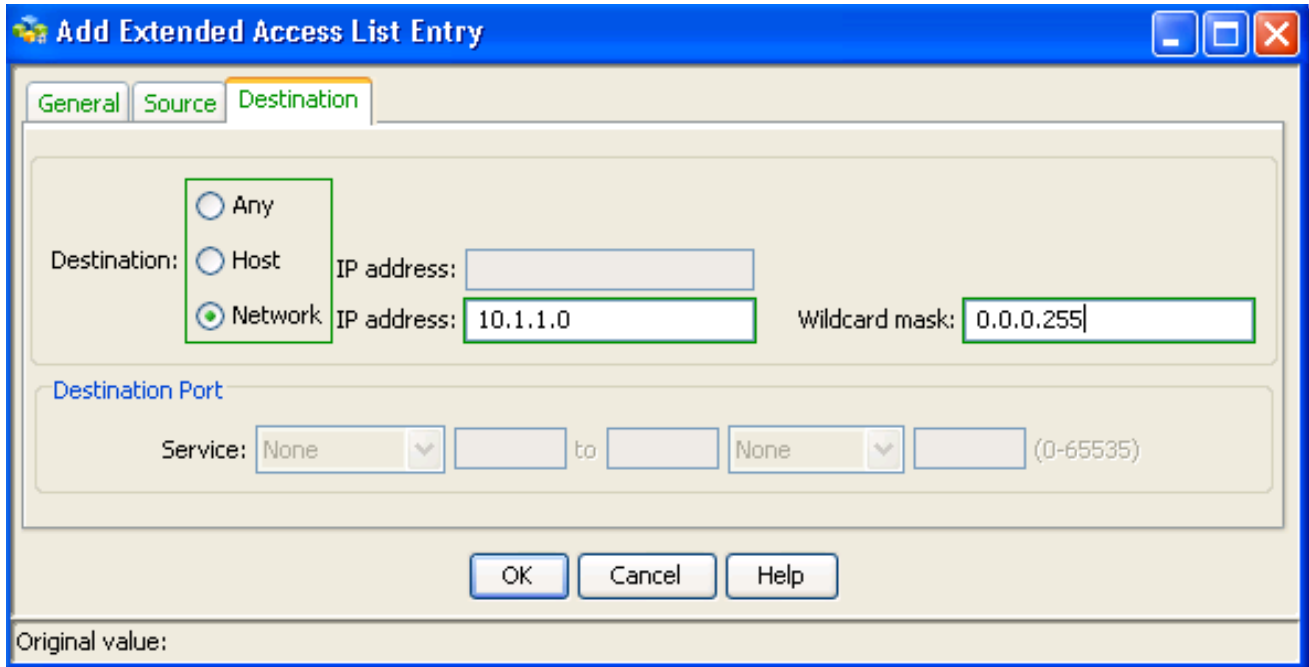
In order to block the guest VLAN from accessing the voice VLAN we are going to “Deny” the guest VLAN. In this example we are going to deny the IP protocol so that any and all IP traffic from the guest VLAN can deny other protocols as well. (see screenshot).



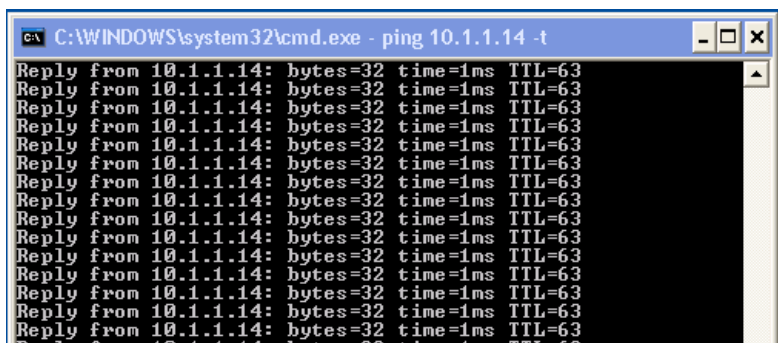
We are going to block access from the guest network 192.168.200.0 by specifying it as the “Source” network. The Wildcard mask indicates which parts of the IP address to match by using 0. Therefore, any IP address with 192.168.200.X will be matched as a source address.



We are blocking access from the guest network to the voice VLAN by configuring the voice VLAN network as the "Destination" network. The Wildcard mask here indicates matches any IP address with 10.1.1.X as a destination address.

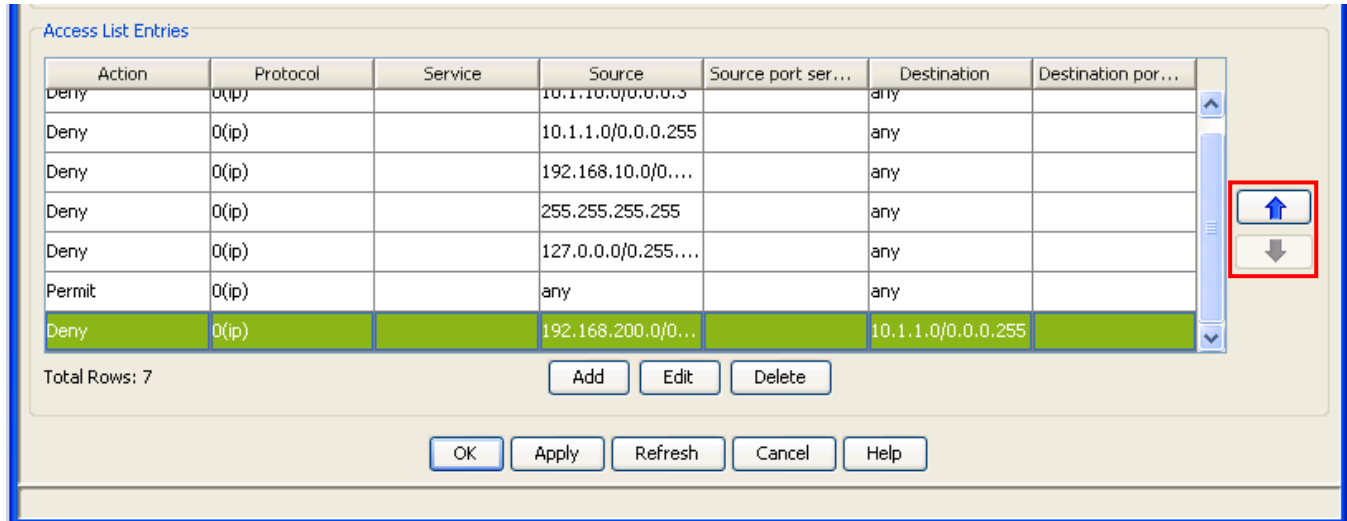


Once we apply this you will notice that the guest VLAN user is still able to ping the phone on the voice VLAN (screenshot below). Guest VLAN user with IP address 192.168.200.10 is able to ping the phone with IP address 10.1.1.14 because the Access List Entry we created needs to be moved. The access list entries in the access list are matched from top to bottom and because the entry we added currently falls after the Permit Any Any entry the ping is still allowed.



```
UC540_BenchP#show run | sec access-list 104
access-list 104 remark auto generated by SDM firewall configuration###NO_ACES_6##
access-list 104 remark SDM_ACL Category=1
access-list 104 deny ip 10.1.10.0 0.0.0.3 any
access-list 104 deny ip 10.1.1.0 0.0.0.255 any
access-list 104 deny ip 192.168.10.0 0.0.0.255 any
access-list 104 deny ip host 255.255.255.255 any
access-list 104 deny ip 127.0.0.0 0.255.255.255 any
access-list 104 permit ip any any
access-list 104 deny ip 192.168.200.0 0.0.0.255 10.1.1.0 0.0.0.255 ← Entry we added
```

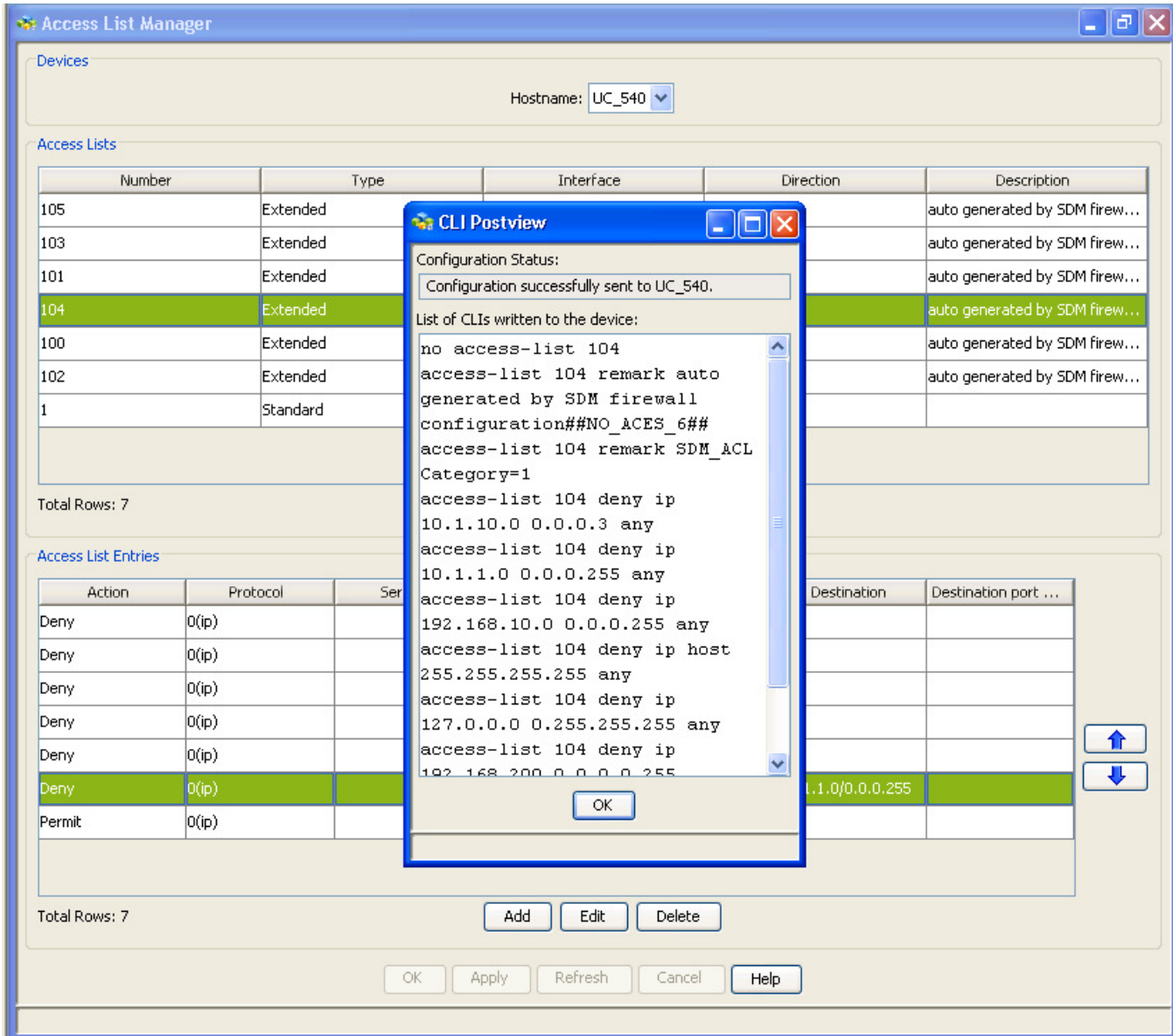
This is how it looks in CCA as opposed to the CLI view on the previous page. Notice that in both the CLI and the CCA view the entry we created is below the Permit Any Any entry.



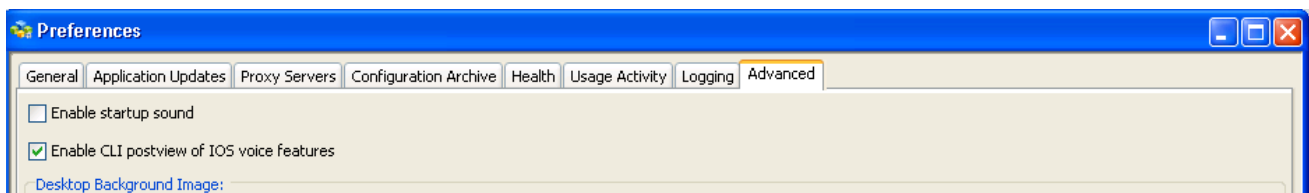
Once the access list entry we created is moved above the Permit Any Any entry using the arrow button to the right of the Access List Entries table and applied the guest VLAN user should then be denied access to the phone on the voice VLAN.

```
UC540_BenchP#show run | sec access-list 104
access-list 104 remark auto generated by SDM firewall configuration##NO_ACES_6##
access-list 104 remark SDM_ACL Category=1
access-list 104 deny ip 10.1.10.0 0.0.0.3 any
access-list 104 deny ip 10.1.1.0 0.0.0.255 any
access-list 104 deny ip 192.168.10.0 0.0.0.255 any
access-list 104 deny ip host 255.255.255.255 any
access-list 104 deny ip 127.0.0.0 0.255.255.255 any
access-list 104 deny ip 192.168.200.0 0.0.0.255 10.1.1.0 0.0.0.255 ← Entry we added is now above the Any Any
access-list 104 permit ip any any
```


Below is a screenshot of how it looks in CCA after the entry we added is moved above the Permit Any Any entry and applied:




Notice how CCA shows the CLI Postview. The CLI Postview window shows the commands CCA sends to the UC via telnet. You can enable the CLI Postview through the CCA preferences by going to System→Preferences and checking the Enable CLI postview of IOS voice features.



The screenshot below shows a continuous ping sourced from the guest VLAN user to the IP phone on the voice VLAN being denied after the access list entry is applied properly.

```
Reply from 10.1.1.14: bytes=32 time=1ms TTL=63
Reply from 10.1.1.14: bytes=32 time=1ms TTL=63
Reply from 10.1.1.14: bytes=32 time=1ms TTL=63
Reply from 10.1.1.14: bytes=32 time=1ms TTL=63
Reply from 10.1.1.14: bytes=32 time=1ms TTL=63
Reply from 10.1.1.14: bytes=32 time=1ms TTL=63
Reply from 10.1.1.14: bytes=32 time=1ms TTL=63
Reply from 10.1.1.14: bytes=32 time=1ms TTL=63
Reply from 10.1.1.14: bytes=32 time=1ms TTL=63
Reply from 192.168.200.1: Destination net unreach
Reply from 192.168.200.1: Destination net unreach
Reply from 192.168.200.1: Destination net unreach
Reply from 192.168.200.1: Destination net unreach
Reply from 192.168.200.1: Destination net unreach
Reply from 192.168.200.1: Destination net unreach
Reply from 192.168.200.1: Destination net unreach
```



This lab give a very simple example but the Access List Manager in CCA can be used in a variety of scenarios.