



Cisco UC500 SIP Trunking Configuration Guide for Qwest iQ SIP Trunking Service

Vern Carpenter
vecarpen@cisco.com
Cisco Systems, Inc.

TABLE OF CONTENTS

1	OVERVIEW	3
1.1	INTRODUCTION	3
1.2	SCOPE	3
1.3	REVISION CONTROL.....	3
1.4	USAGE	4
1.5	ASSUMPTIONS.....	4
2	UC500 SIP TRUNKING OVERVIEW	5
2.1	PRODUCT DESCRIPTION	5
2.2	UC500 SIP TRUNK QUALIFICATION AND TEMPLATES	5
2.4	SUPPORTED LINE-SIDE PROTOCOLS	6
2.5	SECURITY	6
2.6	TOPOLOGY FOR UC500 INSTALLATION.....	6
3	REQUIREMENTS	9
3.1	HARDWARE REQUIREMENTS.....	9
3.2	SOFTWARE REQUIREMENTS	9
3.3	QWEST SERVICE PROVIDER SIP TRUNK TEMPLATE	9
4	CONFIGURATION	10
4.1	INSTALLATION	10
4.2	INITIAL CONFIGURATION	10
4.3	USING CCA TO CONFIGURE THE UC500 FOR SIP TRUNKING.....	11
5	.XML CONFIGURATION	26

1 Overview

1.1 Introduction

SIP trunking is widely being used as the de facto standard for PSTN trunking for IP PBXs. The SIP connect forum builds on existing Internet Engineering Task Force (IETF) standards to define a model of interconnection between IP PBXs and VoIP service provider (SP) networks.

At this time the UC500 IP PBX platform has been validated to work with Qwest's SIP Trunking service but does not support a "Qwest Pull Down" menu.

This document details the topology and supporting configurations for VARs and customers who wish to install and operate the UC500 with SIP Trunking service. This document focuses mostly on the configuration of SIP Trunking parameters and does not focus on every feature of the UC500.

1.2 Scope

This document is intended to aid in the configuration and / or testing of UC500 for Qwest SIP Trunk SIP Trunking service. It addresses the appropriate SIP Trunking configuration items using the Cisco Configuration Assistant (CCA) for UC500.

It is assumed that the user has training and/or experience with the Cisco UC500 and CCA solution. For additional UC500 configuration and CCA tool information, refer to the following:

CCA:

http://www.cisco.com/en/US/products/ps7287/tsd_products_support_series_home.html

UC500:

http://www.cisco.com/en/US/products/ps7293/tsd_products_support_series_home.html

1.3 Revision Control

Release	Release Date	Changes to this Version
1.0	11/09/09	First draft

1.1	1/09/10	Second draft
-----	---------	--------------

1.4 Usage

This document details how to deploy the UC500 with Qwest's SIP Trunking service using the Cisco Configuration Assistant (CCA) graphical configuration tool.

1.5 Assumptions

It is assumed that the administrator has set up and knows the system settings, Phone extensions and features, LAN and WAN addressing as well and username/passwords. This document will address the set up of SIP Trunks and the associated dial plans settings but this is not intended to address every voice feature. Since the initial configuration is done, the Telephony Wizard should not come up when the CCA tool is launched, also the System Mode (PBX or Key System) as well as the extension length should be set.

2 UC500 SIP Trunking Overview

2.1 Product Description

Cisco's UC500 is a purpose built appliance for SMB solutions that provides IP PBX, voicemail, switching, VPN, firewall & optional wireless functionality. The IP PBX & voicemail features are based on Cisco Unified Communications Manager Express (CME) & Cisco Unity Express (CUE). The switching, VPN, firewall & wireless are based on IOS features while management is provided via the Cisco Configuration Assistant (CCA) tool.

UC500 provides the following benefits:

- Cost-effective, converged data and voice solution in an appliance.
- Key system/small PBX features plus innovative convergence applications for up to 104 users with the use of an optional expansion switch.
- Intuitive GUI for easy installation, adds, moves, and changes.
- Firewall & VPN support, based on US DoD certified IOS firewall technologies.
- Optional integrated Wireless LAN support for mobility with ability to extend wireless coverage

UC500 offers voice-mail and automated attendant capabilities for IP and analog phone users & these are fully integrated into the appliance.

2.2 UC500 SIP Trunk Qualification and Templates

The main focus of the document is to define guidelines in developing a UC500 configuration template & validate a configuration that works & enables communication between the UC500 and Qwest's SIP service. Customer- and site-specific features such as hunt-group definitions, paging groups are left to VARs and customers to configure. Basic voice features including on-net and off-net calling, call transfers and forwarding, voicemail access, and any other network-based voice services upon which a PBX/voicemail system have been tested.

2.3 Access Router

Cisco strongly recommends that providers have a well-defined demarcation point such as a Cisco IAD / ISR that is managed by the provider & provides network access services for IP voice and data traffic. The Managed Access router provides:

- NAT ALG functionality
- QoS for SIP Trunk calls & SLA guarantees
- WAN conversion to Ethernet on UC500
- Well defined point of troubleshooting for SP & customer

Any other equipment on the customer premises, including IP PBXs is the responsibility of the customer and a supporting VAR. The templates that resulted from the testing

efforts, particularly with respect to LAN topology, are tested recommendations that are subject to VAR and end-customer requirements. The only exceptions to this are required UC500 SIP trunking parameters that must be configured.

2.4 Supported Line-side Protocols

Line side protocol defines the communication protocol used between the IP phones and UC500. All IP phones supported on the UC500 can be deployed with SIP trunks – there may be caveats for certain specific configurations.

2.5 Security

Securing IP Telephony installations such UC500 is a topic that is beyond the scope of this document. Security is an area in which VARs may provide additional value to customers, if executed properly. Cisco's IOS firewall, for example, can be configured on UC500 to enable the appropriate access-lists and other elements of the firewall.

UC500's IOS cryptographic image may also be configured to enable SSH and HTTPS (SSL) access to the UC500 management interfaces. Administrative access to the UC500 management interfaces may also be configured through the use of local usernames and password, privilege levels, and the use of AAA servers such as Cisco's Access Control Server (ACS) which provides Radius and TACACS+ services. These configuration efforts may be performed by the VAR or end-customer through CCA.

The UC500 templates also include Class of Restriction (COR) to enable access control for different classes of users. International number dialing, for example, may be restricted to specific phones.

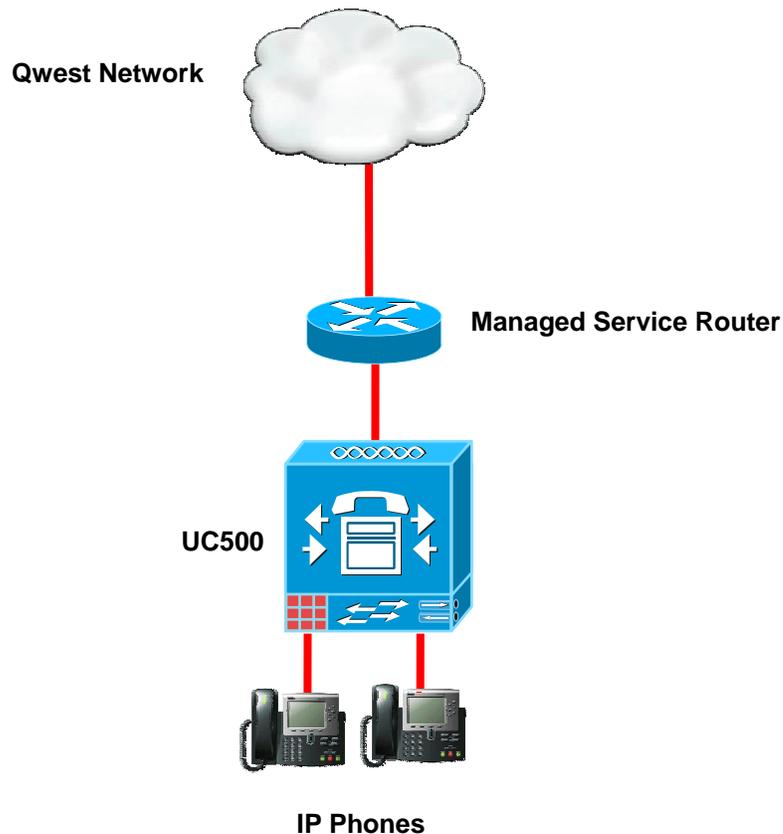
Care should be taken by the VAR or customer to avoid disabling call control, voicemail, and phone features when enabling security features manually. As an example, many security administrators will limit access to the HTTP server in IOS through the use of access control lists (ACLs). If those ACLs, however, inadvertently prevent IP phones from reaching the HTTP server imbedded in UC500 then features such as user directories and IP phone services will be disabled.

2.6 Topology for UC500 Installation

There are several ways in which a UC500 system can be integrated into a customer's local area network (LAN). The key factor to consider in the implementation, however, is that the "managed SIP Trunks" are generally not modified according to various CPE scenarios. These provide a SIP NAT ALG and NAT router for local private network addressing, but do not participate in local routing decisions for subnets and VLANs defined by the end-customer or VAR. This enables the SP to provide reliable, consistent, and supportable IAD configurations across a wide customer base.

Figure 1 depicts the topology that was used in this guide when connected up to the Qwest SIP Trunk service.

Figure 2.1 Topology



In this topology the UC500 is only serving the Voice Subnet and is not connected to the Data subnet network directly. UC500 becomes the default gateway, TFTP, and DHCP server for the phones only. The Voice subnet is only meant to pass Voice traffic, No data traffic should be routed over the Voice Subnet. The Data traffic will be on its own subnet and is maintained separate of the UC500.

Requirements for this configuration include:

- Two layer 2 Ethernet switches required to terminate fa0/0 and fa0/1 which are the voice and data subnets respectively. It is also possible to use a switch only for the Data subnet, while terminating the UC500 “WAN” port directly to the fa0/0 interface of the Managed Services Router.
 - A Layer 3 switch can be used to condense the required hardware, however configuration of the Layer 3 switch is the responsibility of the VAR/Customer

- A crossover cable also is required to be used between the UC500 WAN port and the fa0/0 interface of the Managed Services router to allow static full duplex and 100 Mbps speed settings to be enforced. Without the crossover cable both the UC500 and the Managed Services Router should have the interfaces set to Auto for speed and duplex. The Crossover cable is NOT supplied by Qwest or Cisco.
- Cisco UC500 appliance
- Cisco IP Phones, up to 48 with ESW500 expansion switches.
- Miscellaneous analog phones or other devices such as fax machines

3 Requirements

3.1 Hardware Requirements

The UC500 appliance, supported Cisco IP phones, and a service provider managed SIP Trunk (highly recommended). An Uninterruptible Power Supply (UPS) is strongly recommended for UC500, which runs the embedded Unity Express module. This appliance is fairly robust but nevertheless subject to errors in the event of sudden power loss.

3.2 Software Requirements

Below are the current minimum recommendations for software releases & versions for the various portions of the UC500, which will interact with the SIP trunk:

Component	Supported
IOS Release	uc500-advipservicesk9-mz.124-20.T2 or current release
UC500 Software Pack	7.0(3) or above
CUE Release	7.0.3 or above
CCA Release	2.2 or above

To download the above:

UC500 Software bundle files are at:

<http://www.cisco.com/cgi-bin/tablebuild.pl/UC520-files>

CCA Software is at:

<http://www.cisco.com/en/US/products/ps7287/index.html>

(Click on Download Software)

3.3 Qwest Service Provider SIP Trunk template

This is the custom XML template developed for Qwest that configures the appropriate SIP parameters. This file should reside on the technician's laptop in a known folder and it will be referenced to be selected as a step in the SIP Trunking setup. You will be able to get this template from Qwest Operations team.

4 Configuration

The UC500 may be configured with either the Cisco Configuration Assistant (CCA) or command line interface (CLI). This guide documents the CCA configurations tasks as far as possible with CLI used only to customize the template further to work with the provider.

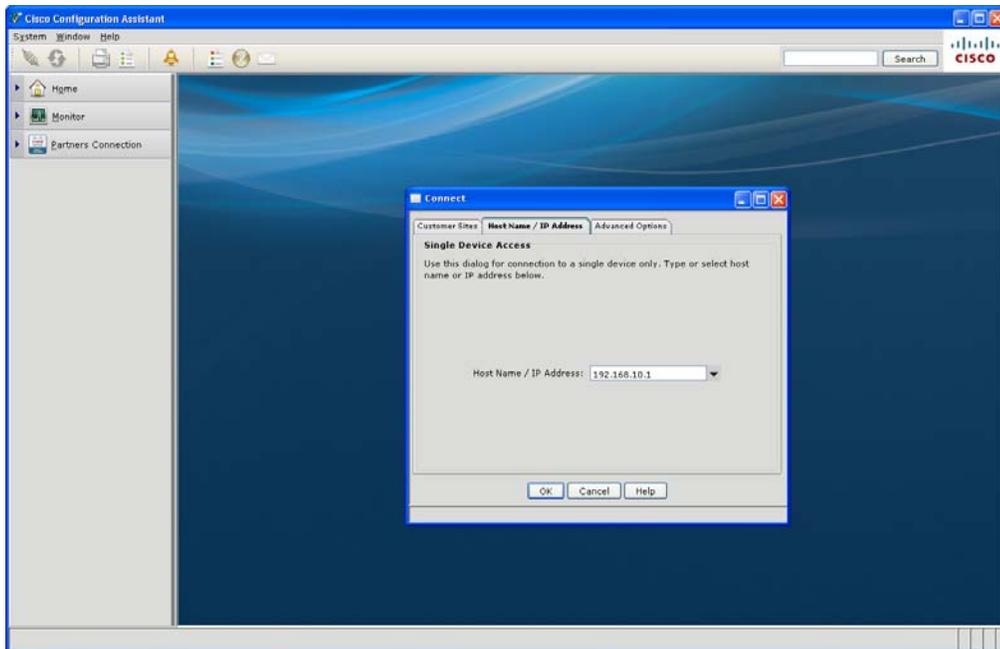
4.1 Installation

Please refer to the “Getting Started Guide” for instructions about physically connecting the UC500’s ports.

http://www.cisco.com/en/US/docs/net_mgmt/cisco_configuration_assistant/version2_0/quick/guide/English/ccags.html

4.2 Initial Configuration

Launch the CCA tool from the PC directly connected to the UC500. The Connect screen will be displayed. Select the “**Host Name/ IP Address**” tab to enter the UC500 IP address and start the configuration process. Figure 4.2.1 **Initial Launch and Connect Screen by default the Address is “192.168.10.1”**



4.3 Using CCA to configure the UC500 for SIP Trunking

New with CCA 2.1 release is the capability to set QoS and Traffic Shaping on the WAN interface. To do this, select the WAN interface and select Traffic Shaping. Set your desired Bandwidth settings.

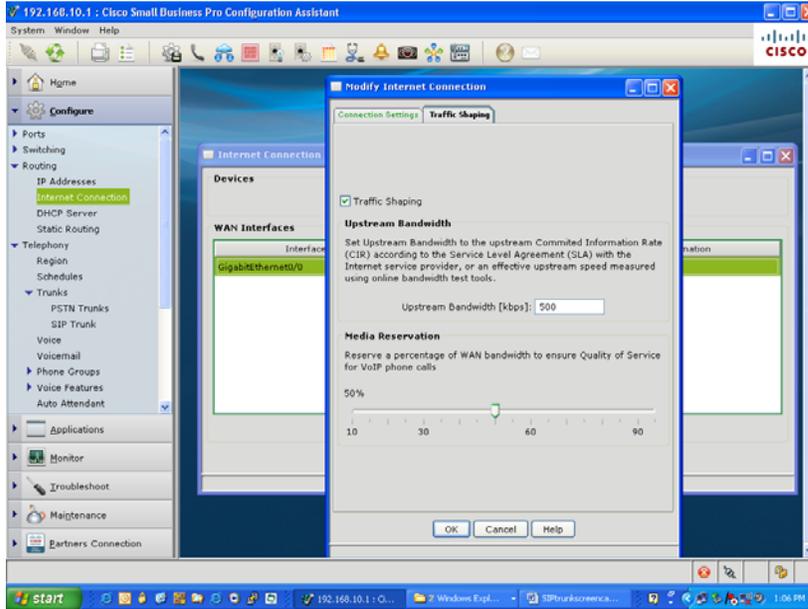


Figure 4.3.1 Traffic Shaping

Click “OK”

4.3.1 SIP Trunking

Under Telephony → Trunks → Select “SIP Trunk” tab and fill the parameters as required or supplied by the SP during customer provisioning.

Service Provider: Select from the dropdown menu, at the time of this documentation Qwest has not completed certification and will not show up as one of the Service Provider choices. Qwest is presently going thru the qualification steps to be one of these pull down selections. Until then select the “Add” menu and follow the steps on the next page.

Proxy Server (primary): Enter IP or domain name of proxy server; this information is noted on the customer work order.

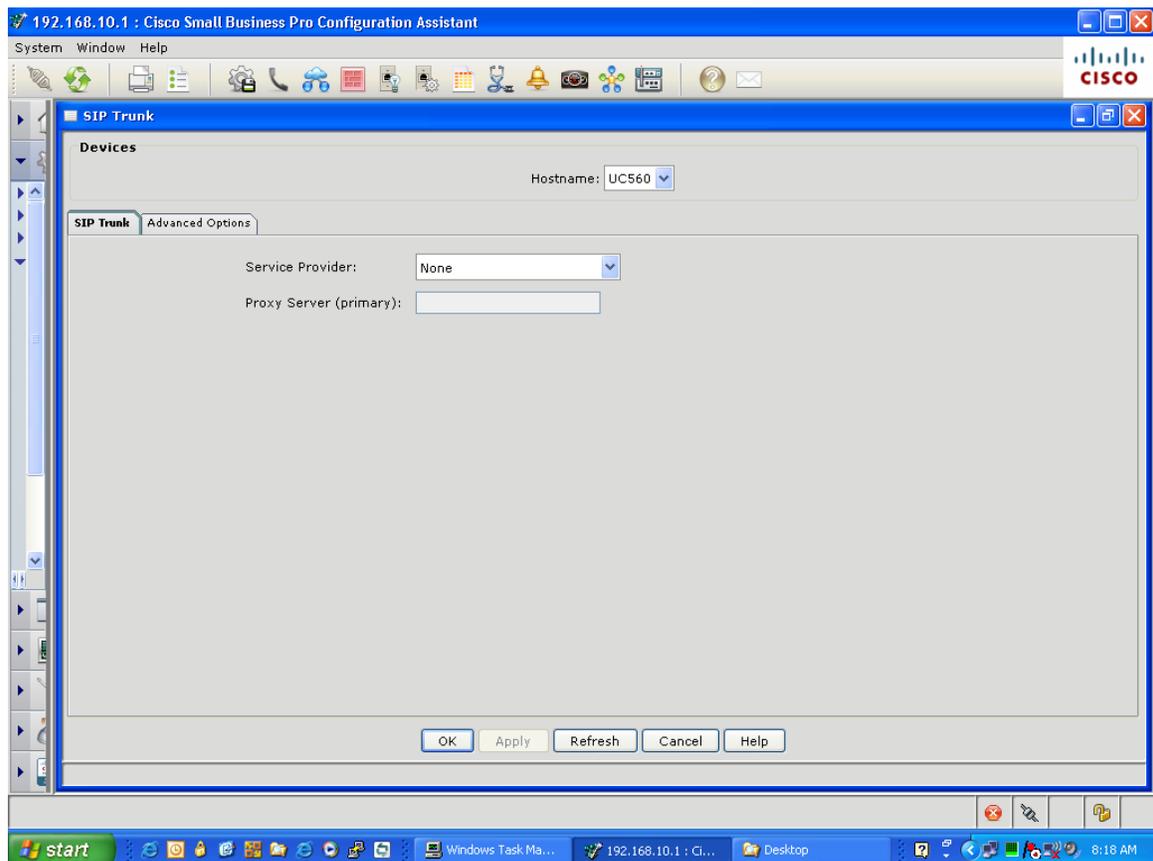


Figure 4.3.2 SIP Trunk parameters

Select the “Pull Down” arrow and scroll down to “Add”. This allows a person to select an externally generated XML file. The UC500 teams have generated this file for each specific service provider. It contains SIP parameters for this Service Providers network.

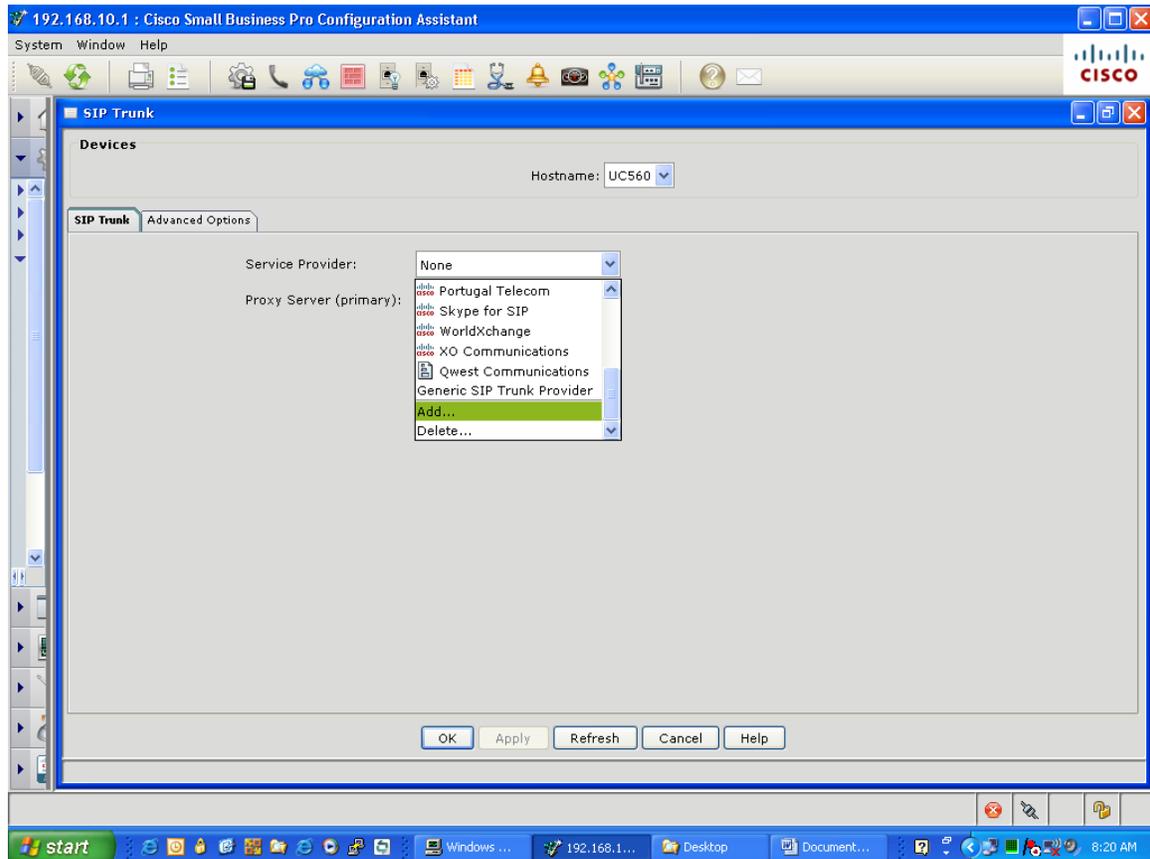


Figure 4.3.3 Select “Add” Template

“Browse” to the file location where the XML was previously saved and select the Qwest template.

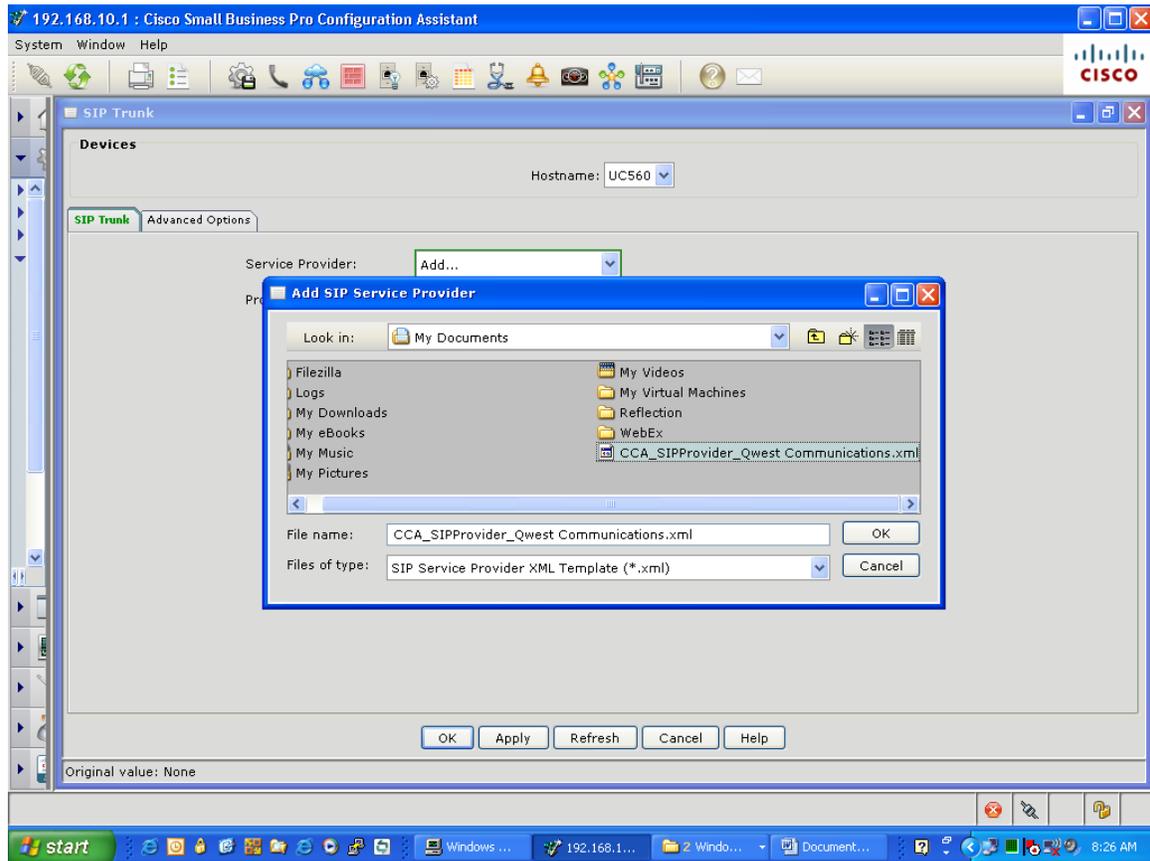


Figure 4.3.4 Select Template

Click “OK”

Enter the Proxy Server information. Qwest provides this information.

The screenshot shows a configuration window titled "SIP Trunk" with a sub-tab "Advanced Options". The "Devices" section at the top has a "Hostname" dropdown menu set to "SIPUC520". Below this, the "Service Provider" is set to "Qwest Communications" with a dropdown arrow, and the "Template" is "12/14/09, Rev1" with a "Browse..." button. The "Proxy Server (primary)" and "(secondary)" fields are both text boxes containing "0.0.0.0". At the bottom of the window, there are buttons for "OK", "Apply", "Refresh", "Cancel", and "Help". A status bar at the very bottom indicates "Original value: 10.182.3.40".

Figure 4.3.5 Proxy Server

Enter in any additional allowed IP address's that are permitted to access your VoIP network.

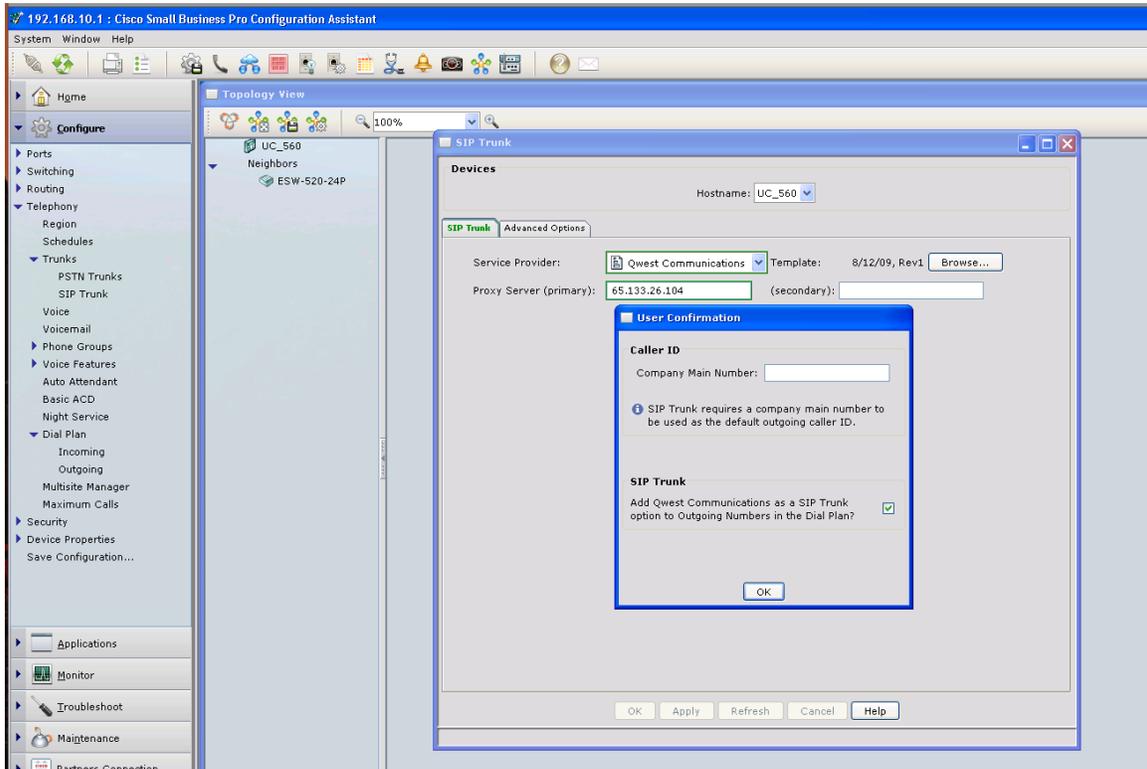
The screenshot shows a configuration window titled "SIP Trunk". At the top, there is a "Devices" section with a "Hostname" dropdown menu set to "SIPUC520". Below this, the "Advanced Options" tab is selected. Under "Advanced Options", there is a section titled "Additional Allowed IP Addresses" with an information icon and the text: "Specify any additional allowed IP address that is permitted to access your VoIP network. Verify the IP addresses with your Service Provider before configuring." Below this text is a table with the following structure:

IP Address
0.0.0.0
0.0.0.0

Below the table, it says "Total Rows: 2" and there are "Add" and "Delete" buttons. At the bottom of the window, there are "OK", "Apply", "Refresh", "Cancel", and "Help" buttons. At the very bottom, there is a field labeled "Original value:".

Figure 4.3.6 Additional Allowed IP Addresses

You will be asked to enter the Company Main Number for the CallerID, you should have received this from Qwest, Enter the number then hit “OK”



Once complete, hit **Apply** or **Ok**.

4.3.2 Dial Plan:

Steps to setting up Dial Plan after adding SIP Trunk

- Setting the Incoming Dial Plan – Direct Dialing, Map outside numbers to internal extensions.
- Outgoing Call Handling and Map Caller-ID from Outgoing numbers to PSTN numbers. You can choose to send a main number only if you like. This is where you set outgoing trunking preference.
- Setup Maximum Calls (Call Admission Control). Setup your SIP trunk to only allow a maximum number of calls.

4.3.2.1 Incoming Dial Plan – Direct Dialing:

You can map DID ranges from Qwest provided numbers to internal extensions for users, Auto attendant, Hunt Groups or Operator. You can add each one individually or by a Range.

The screenshot shows the 'Incoming Dial Plan' configuration window. At the top, there is a 'Devices' section with a 'Hostname' dropdown set to 'UC_560'. Below this, there are two tabs: 'Incoming FXO Calls' and 'Direct Dialing', with 'Direct Dialing' being the active tab. The main area is divided into two sections:

Direct Dial to Internal User Extensions

Description:	DID Range Start	DID Range End	Internal Number Start	Internal Number End	Trunks
--------------	-----------------	---------------	-----------------------	---------------------	--------

Total Rows: 0

Buttons: Add, Modify, Delete

Direct Dial to Auto-Attendant, Groups, Operator

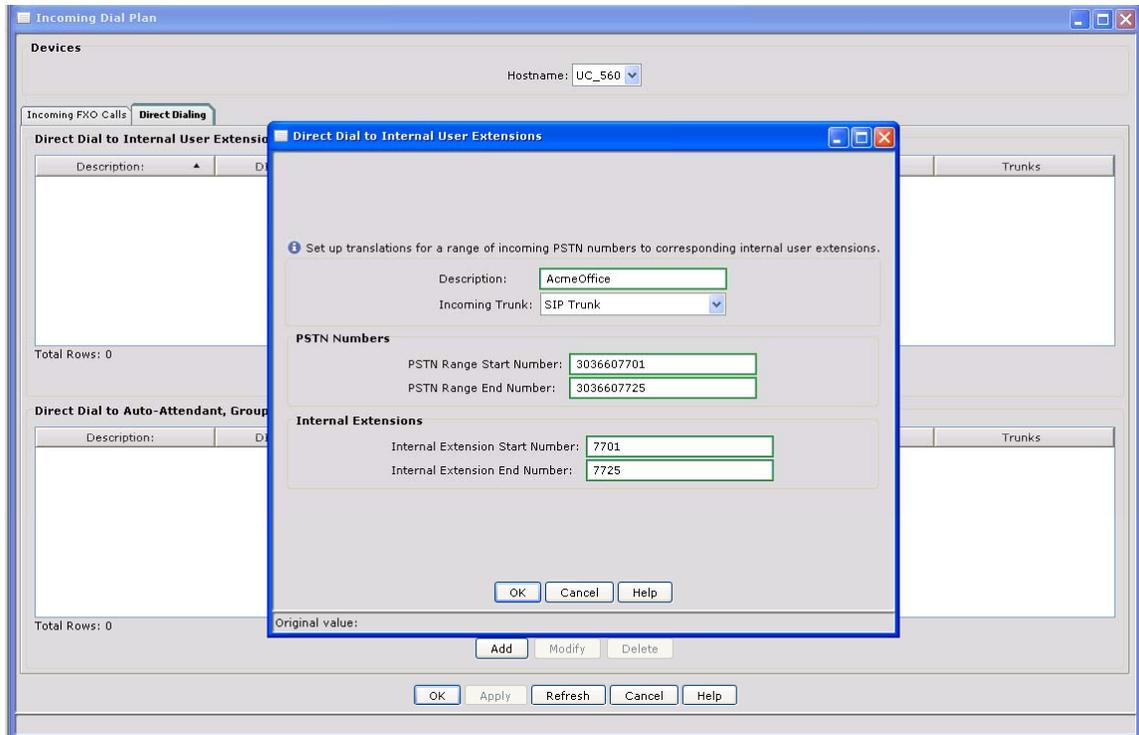
Description:	DID Range Start	DID Range End	Destination Type	Destination	Trunks
--------------	-----------------	---------------	------------------	-------------	--------

Total Rows: 0

Buttons: Add, Modify, Delete

Bottom navigation buttons: OK, Apply, Refresh, Cancel, Help

Begin by Selecting, Telephony → Dial Plan → Incoming → Direct Dialing



To do this select the “Add” button, enter a description, PSTN range and internal extension range. If you want to map one extension at a time you would enter the same number for starting and ending numbers.

Click “OK” and then “Apply” or “Ok”

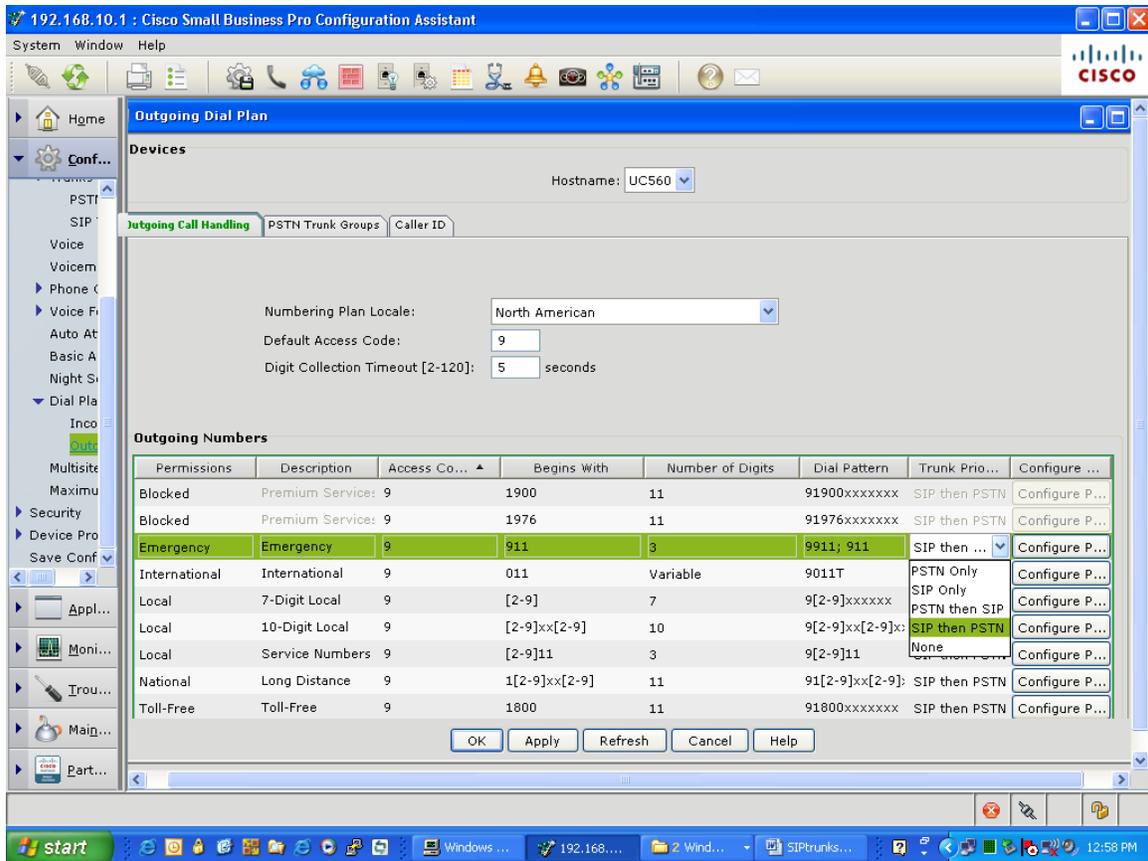
4.3.2.2 Outgoing Call Handling

Starting with CCA 2.1 release the Dial Plan configuration has it’s own tab under:

Configure→Telephony→Dial Plan→Outgoing

Select the Numbering Plan Locale – for example “North American” and select any dial plans you want to modify. Select the Trunk preference for each dial plan. You can even manually set the preference number by using the “Configure” Tab.

Figure 4.3.9a **Outgoing Call Handling**



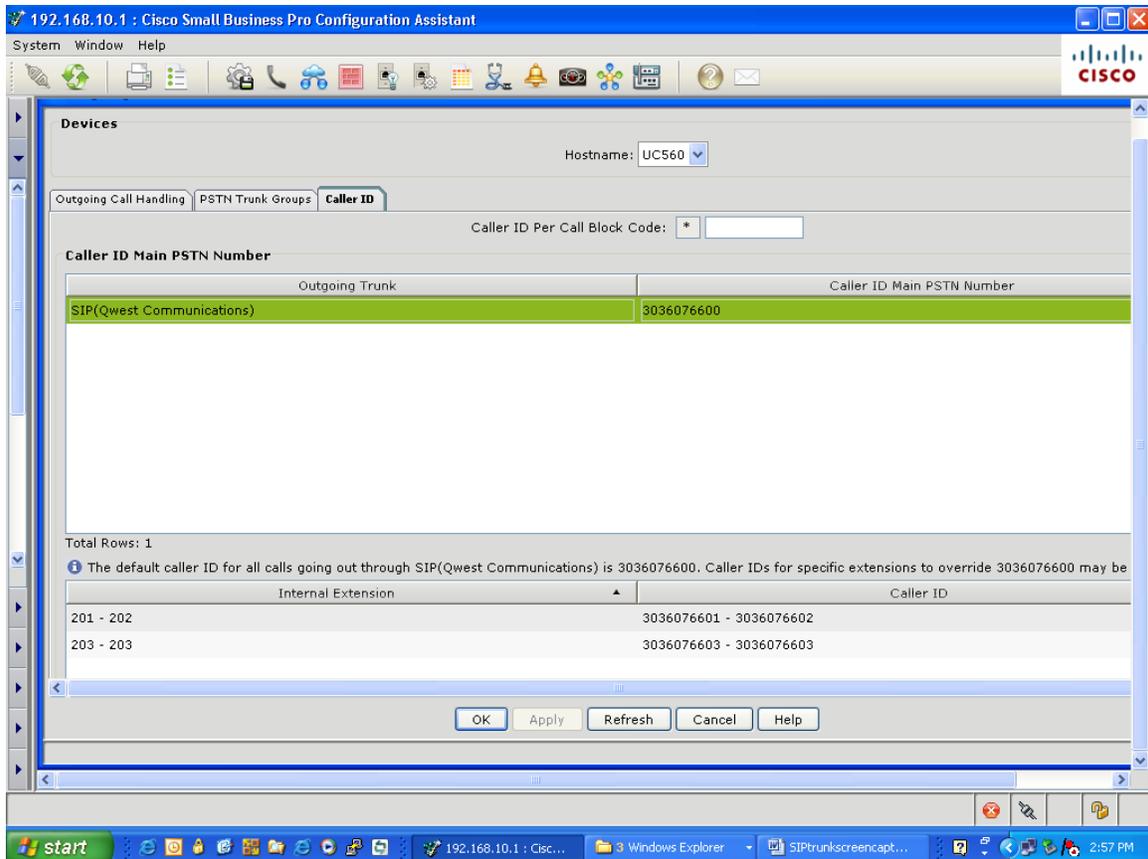
Click “Apply” or “Ok” when done with all Preference changes

4.3.2.3 Caller ID

Starting with CCA 2.1 release the Dial Plan configuration has it’s own tab under: Configure→Telephony→Dial Plan→Caller ID

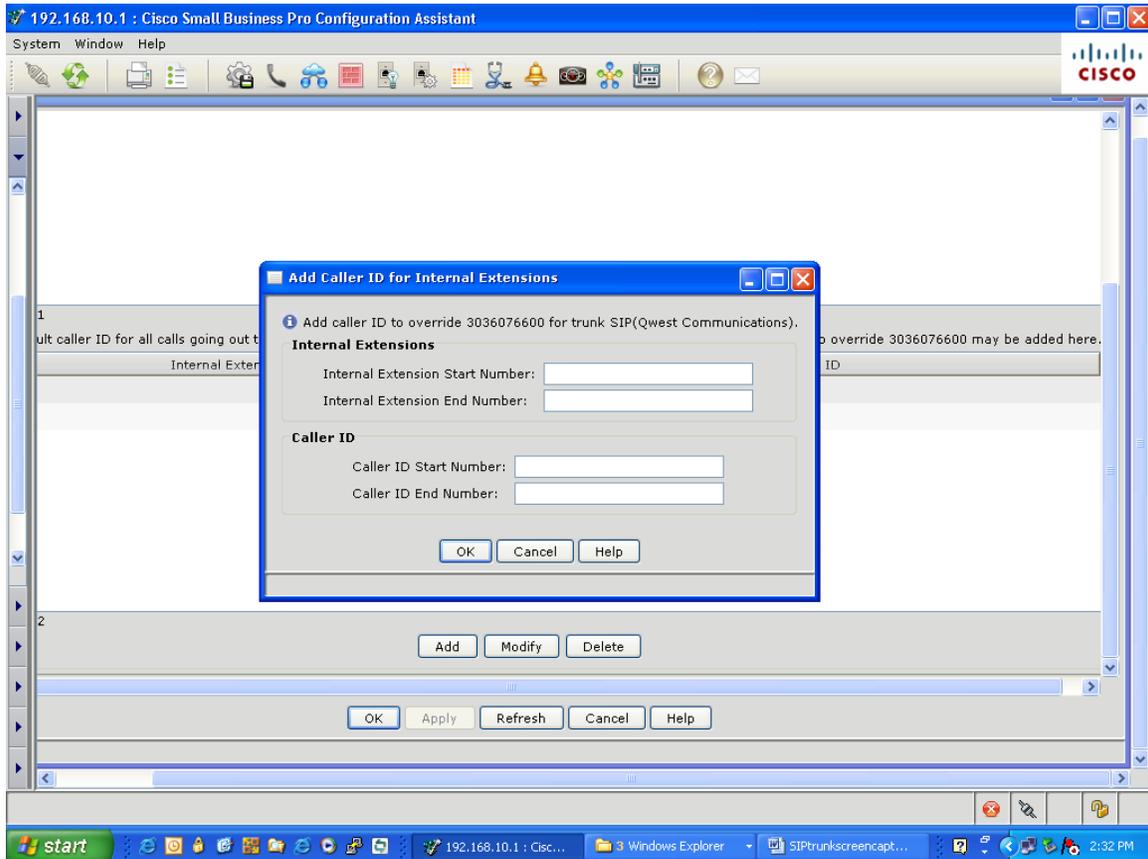
After you created a SIP Trunk you should have a SIP trunk to select (see figure below). You will see the main Caller ID in the right window. If you want to add individual Caller ID’s you can do it in two manners. 1) You can map multiple internal numbers to external numbers by using a beginning and ending number or 2) you can add a single Caller ID mapping by entering the same beginning and ending numbers.

Figure 4.3.9a Outgoing Call Handling



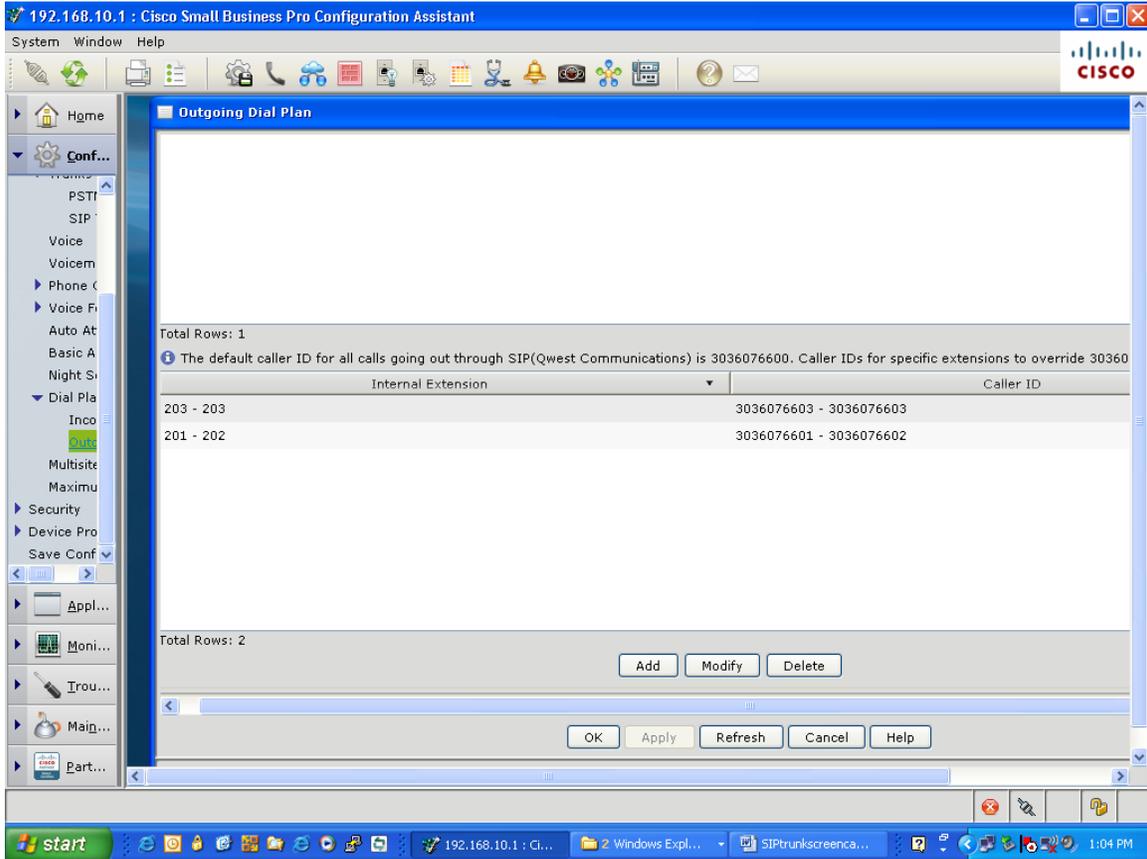
Click "Add" to enter Caller ID mapping

Figure 4.3.9b Caller ID Mapping entry



Enter individual or multiple Caller ID mappings and hit “OK”

Figure 4.3.9c Caller ID Mapping result

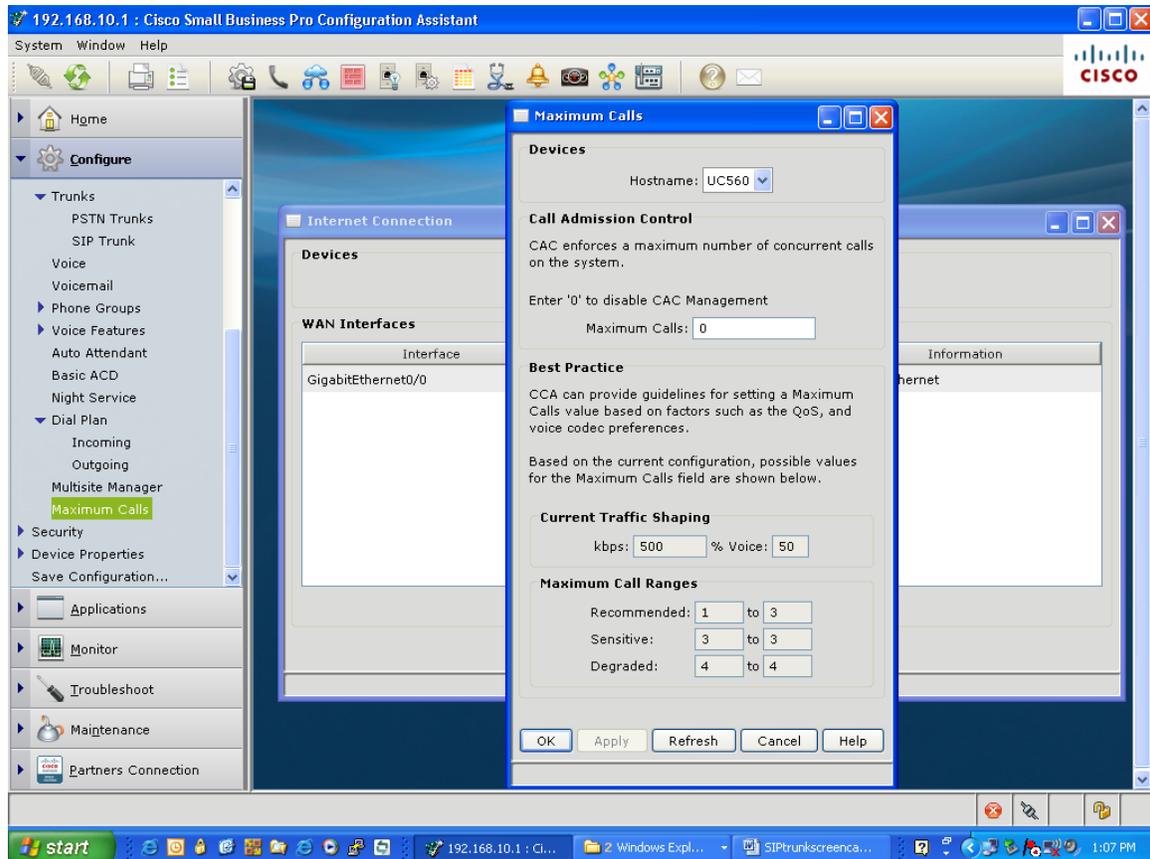


4.3.2.4 Maximum Calls (Call Admission Control)

Starting with CCA 2.1 release the Dial Plan configuration has it's own tab under:
Configure→Telephony→Maximum Calls

You can specify how many calls you want to allow over you SIP Trunk by using this parameter.

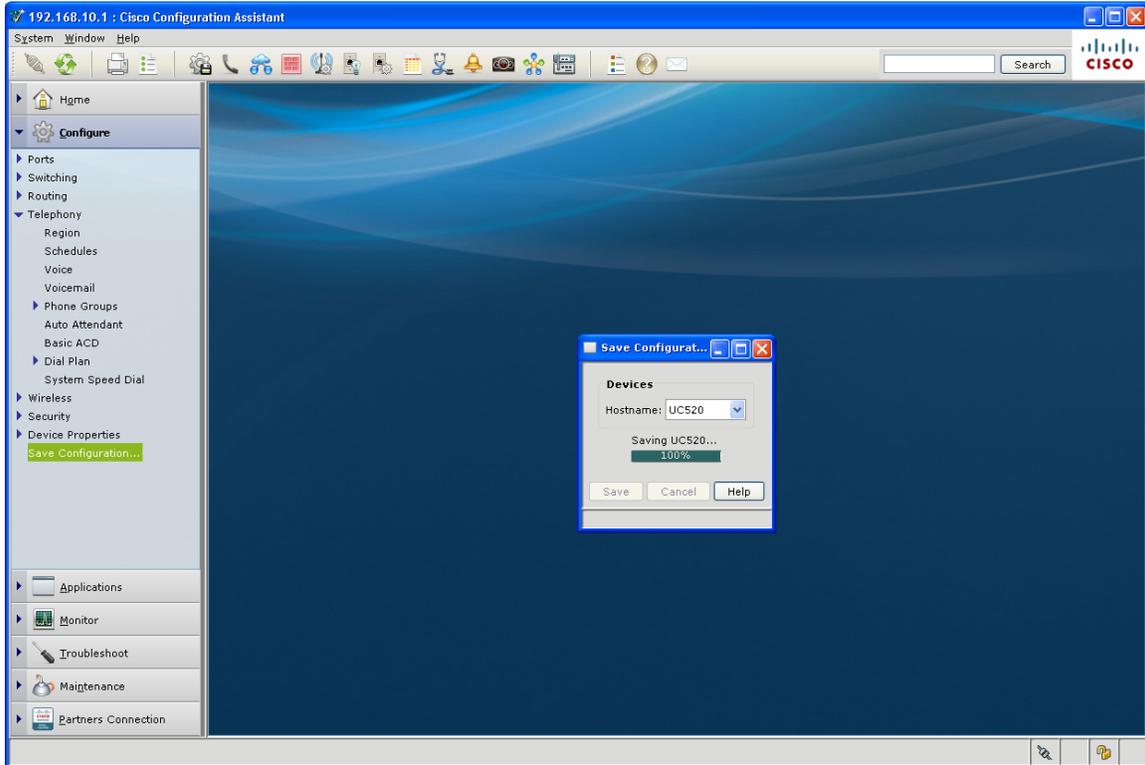
Figure 4.3.9d Maximum Calls



Select Maximum Calls and Click “OK” or “Apply”

After the configuration is applied – this is now part of the running configuration and will not survive a reload. To ensure the configuration is saved to NVRAM – navigate to, and click “Save Configuration”

Figure 4.3.10 Save Configuration



This completes the CCA configuration for the UC500 SIP trunking portion.

5 .XML Configuration

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
- <ns1:SIPProviderTemplate xmlns:ns1="SIPProviderXMLSchema">
- <ProviderName>Qwest Communications</ProviderName>
  <Revision>1</Revision>
- <Fields>
- <FieldInfo>
  <FieldName>Proxy Server</FieldName>
  <isDisplayed>true</isDisplayed>
  <isRequired>true</isRequired>
  </FieldInfo>
- <FieldInfo>
  <FieldName>Secondary Proxy Server</FieldName>
  <isDisplayed>true</isDisplayed>
  <isRequired>>false</isRequired>
  </FieldInfo>
- <FieldInfo>
  <FieldName>Registrar Server</FieldName>
  <isDisplayed>>false</isDisplayed>
  <isRequired>>false</isRequired>
  </FieldInfo>
- <FieldInfo>
  <FieldName>Outbound Proxy Server</FieldName>
  <isDisplayed>>false</isDisplayed>
  <isRequired>>false</isRequired>
  </FieldInfo>
- <FieldInfo>
  <FieldName>SIP Domain Name</FieldName>
  <isDisplayed>>false</isDisplayed>
  <isRequired>>false</isRequired>
  </FieldInfo>
- <FieldInfo>
  <FieldName>Digest Authentication</FieldName>
  <isDisplayed>>false</isDisplayed>
  <isRequired>>false</isRequired>
  </FieldInfo>
- <FieldInfo>
  <FieldName>User Credentials</FieldName>
  <isDisplayed>>false</isDisplayed>
  <isRequired>>false</isRequired>
  </FieldInfo>
- <FieldInfo>
  <FieldName>Call Admission Controls</FieldName>
  <isDisplayed>>false</isDisplayed>
  <isRequired>>false</isRequired>
  </FieldInfo>
- <FieldInfo>
  <FieldName>Company Name</FieldName>
  <isDisplayed>>false</isDisplayed>
```

```

<isRequired>false</isRequired>
  </FieldInfo>
</Fields>
<CredentialsRealm>Proxy Server</CredentialsRealm>
- <VoiceCodecPreference>
- <VoiceCodec>
  <VoiceCodecType>G729</VoiceCodecType>
  <Preference>1</Preference>
  </VoiceCodec>
  </VoiceCodecPreference>
  <FaxProtocol>T38</FaxProtocol>
  <DTMFMethod>RFC 2833</DTMFMethod>
  <RTPPayloadType>100</RTPPayloadType>
  <DSCPSignaling>cs3</DSCPSignaling>
  <DSCPMedia>cs5</DSCPMedia>
  <isHairpinCallTransfers>true</isHairpinCallTransfers>
  <isHairpinCallForwards>true</isHairpinCallForwards>
  <isPreserveCallerIDs>true</isPreserveCallerIDs>
  <Transport>udp</Transport>
  <SessionPort>Fixed</SessionPort>
  <DestinationPort>5060</DestinationPort>
  <RegistrarExpiry>3600</RegistrarExpiry>
  <isRegisterAllIDs>false</isRegisterAllIDs>
  <isSamePasswordForAllIDs>false</isSamePasswordForAllIDs>
  <ProvisionalACK>System</ProvisionalACK>
  <RetriesInvite>2</RetriesInvite>
  <RetriesRegister>10</RetriesRegister>
  <TimersConnect>100</TimersConnect>
  <isRemotePartyIDs>true</isRemotePartyIDs>
- <SupplementaryCommands>
- <SupplementaryCommand>
  <SubMode>sip-ua</SubMode>
  <Command />
  <Processing>Pre</Processing>
  </SupplementaryCommand>
</SupplementaryCommands>
</ns1:SIPProviderTemplate>

```