Cisco UC500 SIP Trunking

Configuration Guide

SBCS Product Marketing team
Cisco Systems, Inc.
Date: June 08, 2008
Version 2.1

TABLE OF CONTENTS

© 2008 Cisco Systems, Inc. All rights reserved.

1 Overview

1.1 Introduction

SIP trunking is widely being used as the de facto standard for PSTN trunking for IP PBXes. The SIPconnect 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.[1]

This document details the topology and supporting configurations for VARs and customers who wish to install and operate the UC500 with SIP Trunking service.

1.2 Scope

This document is intended to aid SP integration teams & Cisco partners (VARs) responsible for configuring and / or testing UC500 for SIP Trunking services. It addresses the Cisco Configuration Assistant (CCA) for UC500 & some CLI configurations on the UC500 for the most common deployments – there may be certain features that are not covered in the guide.

1.3 Revision Control

Release	Release Date	Changes to this Version
2.0	04/24/08	Updates for CCA 1.6, UC500 4.2.7 software pack & CLI configurations (section 4.4)
2.1	06/08/08	Updates for section 4.4

1.4 Usage

This document details how to deploy the UC500 using the Cisco Configuration Assistant (CCA) graphical configuration tool. A specific example is provided that must be adapted to customer parameters and other requirements.

1.5 Revision

Please send any suggestions or error reports related to this document via

http://supportwiki.cisco.com/wiki/feedback.php .

[1] See http://www.sipforum.org/sipconnect

© 2008 Cisco Systems, Inc. All rights reserved.

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 48 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 abilty 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 service provider's SIP call agent. 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 depends would be the more common ones tested. More customer-specific features such as hunt-group definitions, paging groups are left to VARs and customers to configure.

2.3 Managed 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

© 2008 Cisco Systems, Inc. All rights reserved.

Any other equipment on the customer premise, 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.

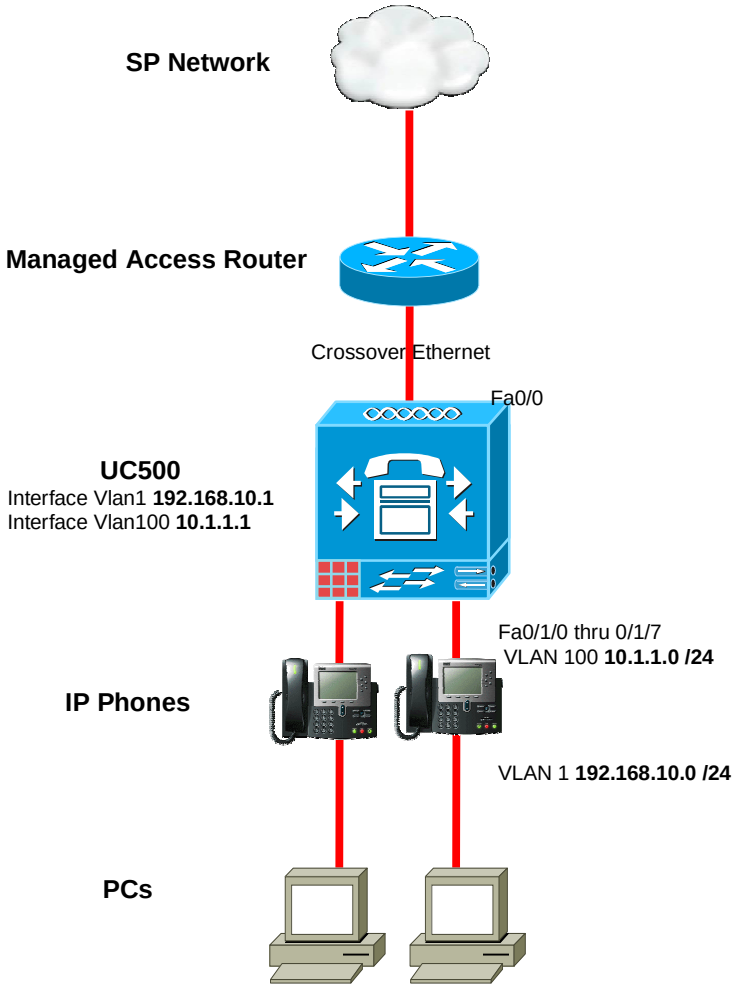
2.6 Topology for UC500 Installation

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 access routers" 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.

© 2008 Cisco Systems, Inc. All rights reserved.

Figure 1 depicts the topology that was used in this guide

Figure 2.1 Topology



In this topology, UC500 is placed inline between the managed access router and CPE devices including IP phones and personal computers. UC500 becomes the default gateway, TFTP, and DHCP server for the phones and PCs. Requirements for this configuration include:

- A layer 2 Ethernet switch or cross over cable between the Managed Access Router and UC500
- Cisco UC500 appliance
- Cisco IP Phones, up to 48 with CE520 expansion switches.
- Miscellaneous analog phones or other devices such as fax machines

© 2008 Cisco Systems, Inc. All rights reserved.

This template for a LAN topology also supports running the IOS firewall feature set on the UC500 platform although the firewall configuration is not covered in this document.

Considerations for this topology include:

- The “WAN” segment between the Managed Access Router and the UC500 is assumed to be in the 1.1.100.0/24 subnet but can be modified based on deployment options. The subnet can be modified by the VAR or end-customer so long as the subnet changes are addressed in the UC500 “WAN” interface and routing configuration.
- Some providers may also provide a publicly routable address for UC500 rather than use a private IP address. This has the benefit of avoiding “NATing” for IP traffic at the Managed Access Router and can simplify remote access to the UC500, via VPN or SSH or telnet.
- “VLAN 1”, “Voice VLAN 100”, and the subnets depicted can be modified by the VAR or end-customer to suit customer requirements.
- PCs may or may not be attached through Cisco IP phones according to customer preference, but the maximum number of ports supported by UC500 is 48.
- Inline power support for the IP phones is provided by UC500.
- The UC500 provides routing for all devices in VLANs 1 and 100, and also NATs the 192.168.10.0/24 subnet for the data VLAN 1 to allow access to the internet.

© 2008 Cisco Systems, Inc. All rights reserved.

3 Requirements

3.1 Hardware Requirements

The UC500 appliance, supported Cisco IP phones, and a service provider managed access router (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.124-11.XW7**
UC500 Software Pack	**4.2.7**
CUE Release	**3.0.3**
CCA Release	**1.6(1)**

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)

© 2008 Cisco Systems, Inc. All rights reserved.

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" located at http://www.cisco.com/en/US/products/ps7293/products_getting_started_guide09186a0080824095.html for instructions about physically connecting the UC500's ports. To summarize:

- Connect the "WAN" port to the same Ethernet segment as the inside interface of the Managed Access Router. This may be accomplished either with a crossover cable or with a LAN switch.
- Connect IP phones to the FastEthernet ports on the front of the UC500.
- PCs should generally be connected to the switch port on the phones.
- Any analog devices (such as faxes) may be connected to the FXS ports on the UC500.

Install CCA on a PC connected to one of the FastEthernet ports on the front of the UC500. Make sure this PC is configured for DHCP to receive an IP address from UC500.

4.2 Initial Configuration

If the UC500 platform has been configured for testing or other purposes prior to the customer installation, be sure to reset it to the factory default configuration. UC500 ships with the factory default configuration files on its compact flash, for example "UC500-16U-4FXO-K9-factory-4.2.5.cfg". The exact name of this file depends on the UC500 model but the procedure to restore the configuration to the factory default is the same: Using a console connection, copy this file to the startup-config in NVRAM. For example:

```
UC500#copy flash:UC500-16U-4FXO-K9-factory-4.2.5.cfg startup-config
Destination filename [startup-config]?
[OK]
11553 bytes copied in 2.340 secs (4937 bytes/sec)
UC500#
```

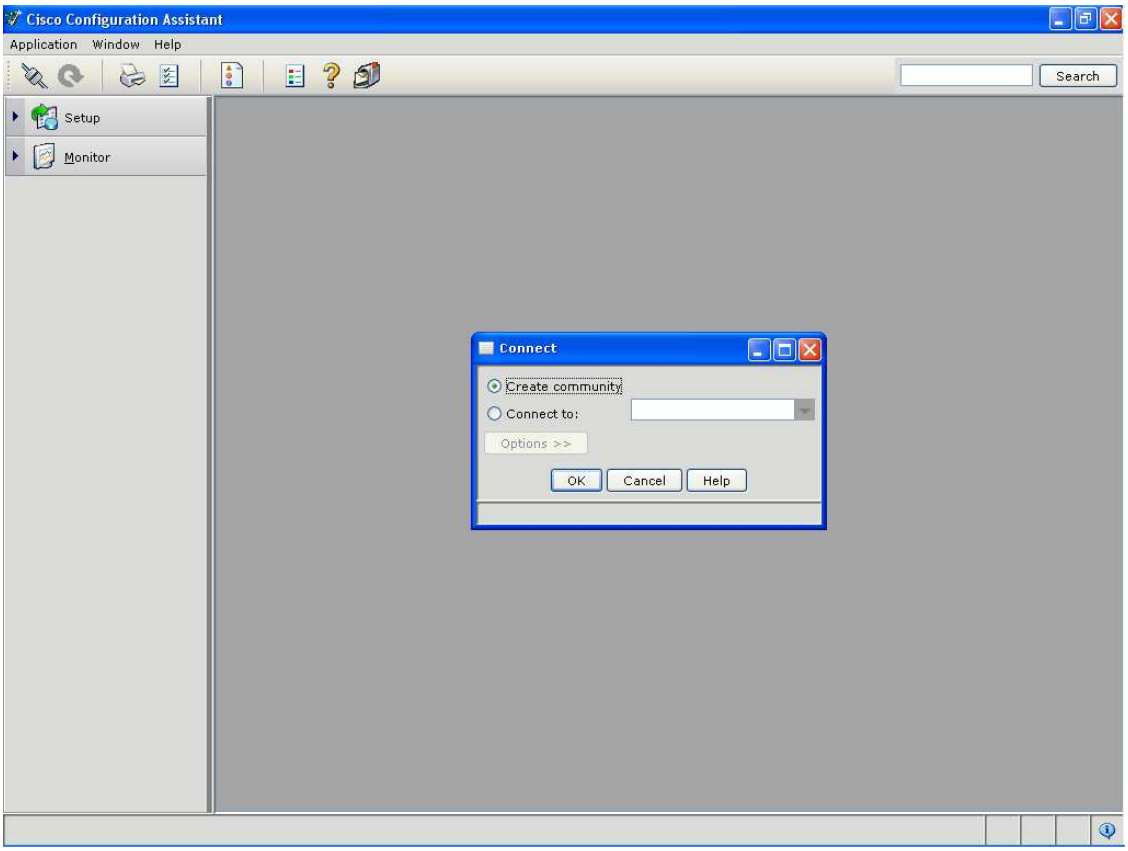
Then reload the UC500.

© 2008 Cisco Systems, Inc. All rights reserved.

4.3 Using CCA to configure the UC500 for SIP Trunking

4.3.1 With the UC500 in a default configuration, launch CCA on the workstation attached to a FastEthernet port. CCA begins with a prompt to connect. Select "Create Community" to add this UC500 to a new community as follows:

Figure 4.3.1 Create community for CCA

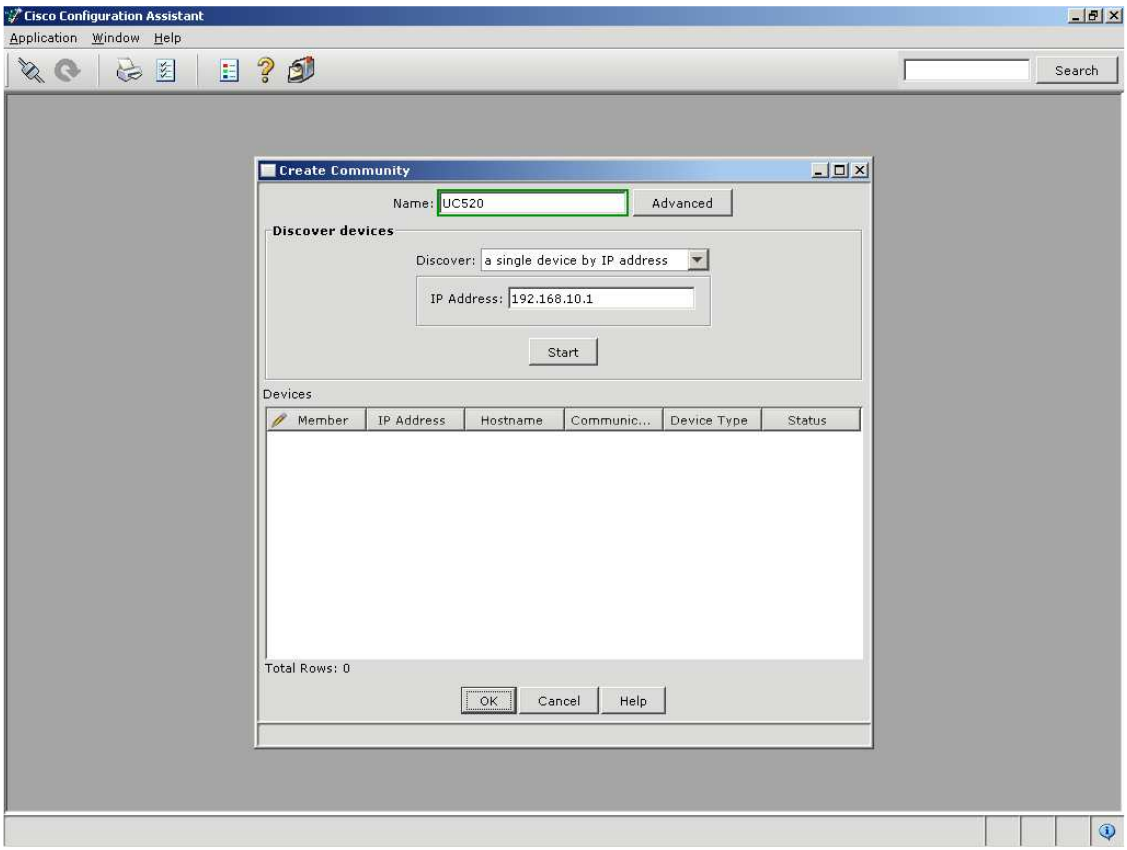


© 2008 Cisco Systems, Inc. All rights reserved.

4.3.2 This should pop up a new window - add the below:

Name: whatever name you need for the community (usually the customer name)
Discover: Choose “a single device by IP address” option from the dropdown
IP address: Enter 192.168.10.1
Click on Start

Figure 4.3.2 Community Setup



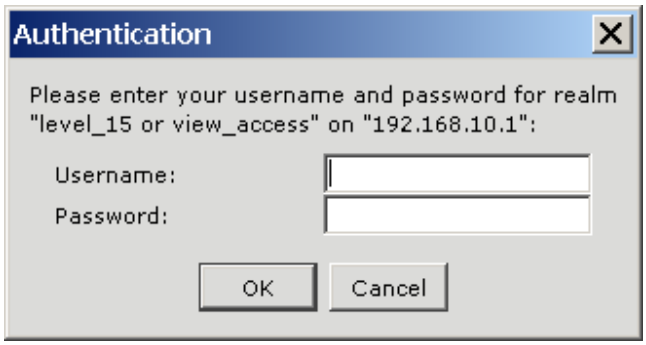
© 2008 Cisco Systems, Inc. All rights reserved.

4.3.3 An SSH certificate warning may appear:

Figure 4.3.3a Certificate Warning

Select “Yes” or “Always” to continue to a login prompt:

Figure 4.3.3b Login



Enter the below defaults

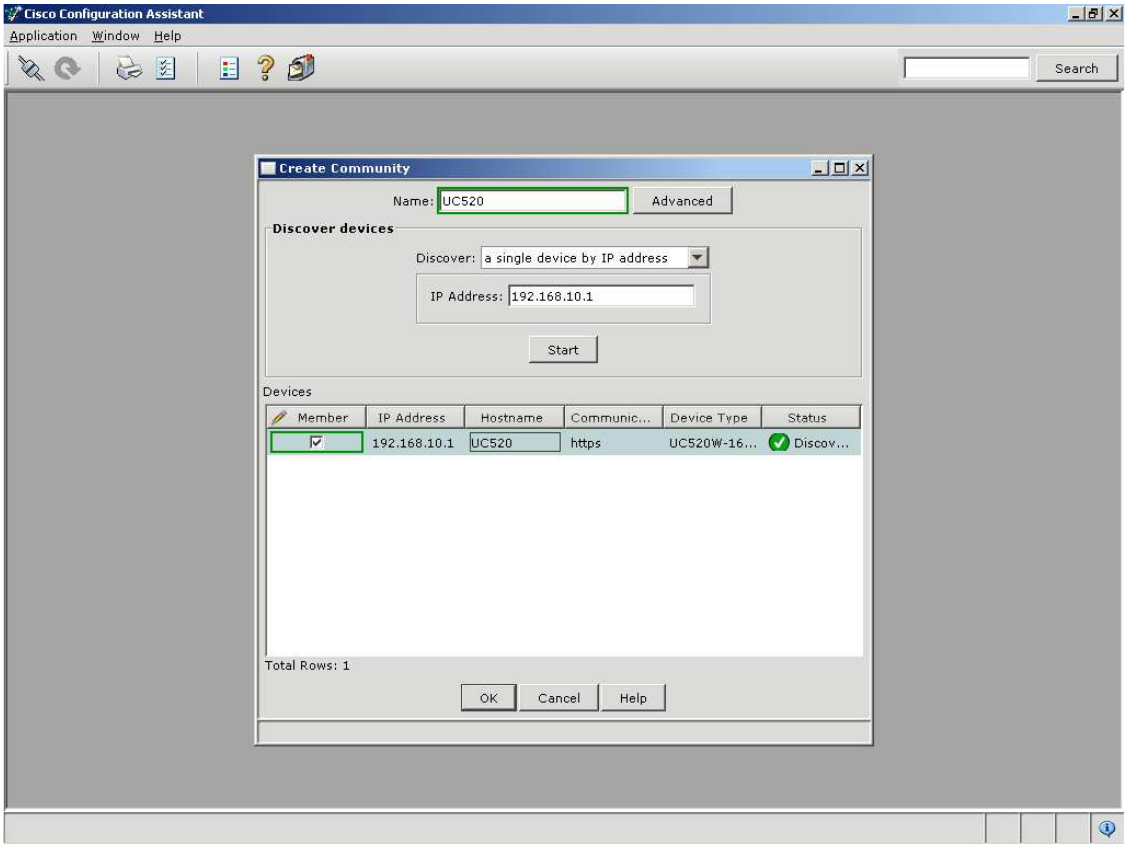
Username: “cisco”

Password: “cisco”

© 2008 Cisco Systems, Inc. All rights reserved.

4.3.4 Now it should show the UC500 that was discovered as below – select that and hit "Ok"

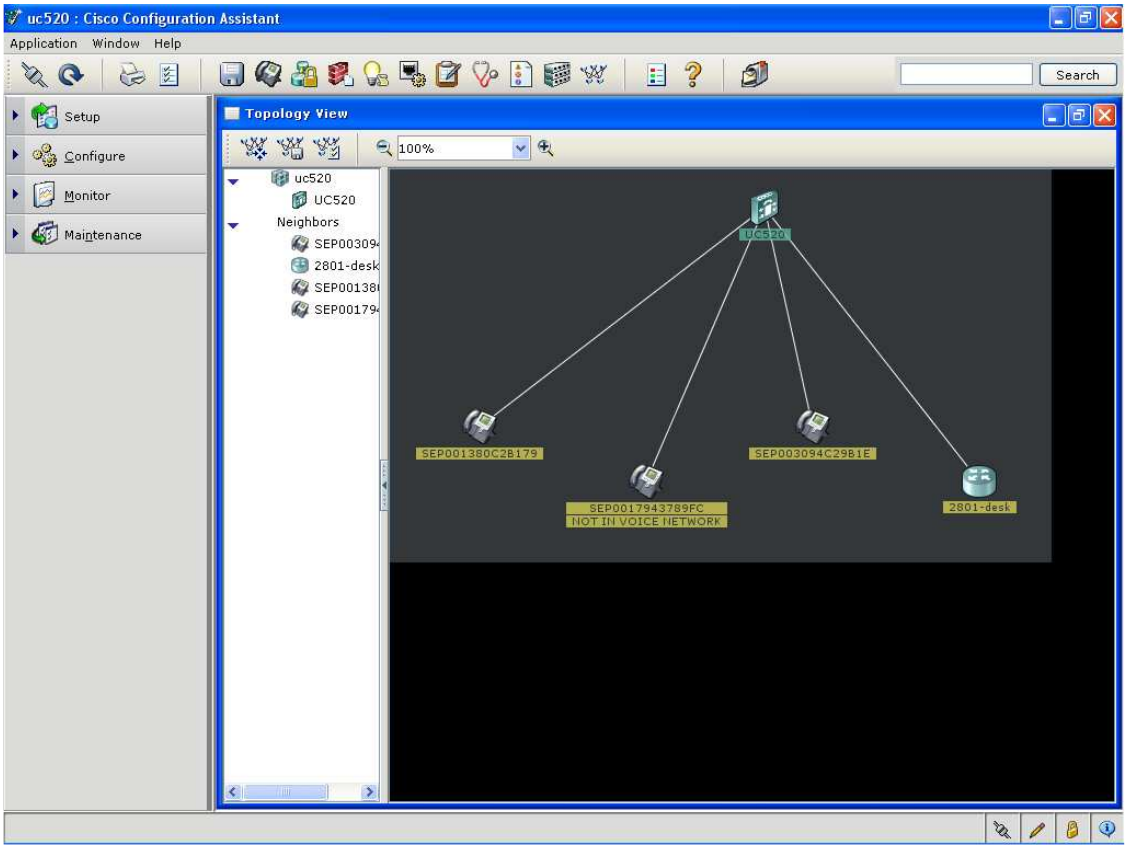
Figure 4.3.4 Discover device



© 2008 Cisco Systems, Inc. All rights reserved.

4.3.5 The CCA will go through a network discovery process for about 1-2 minutes (please be patient at this step) – then a Topology view will show up as below showing all the connected device(s):

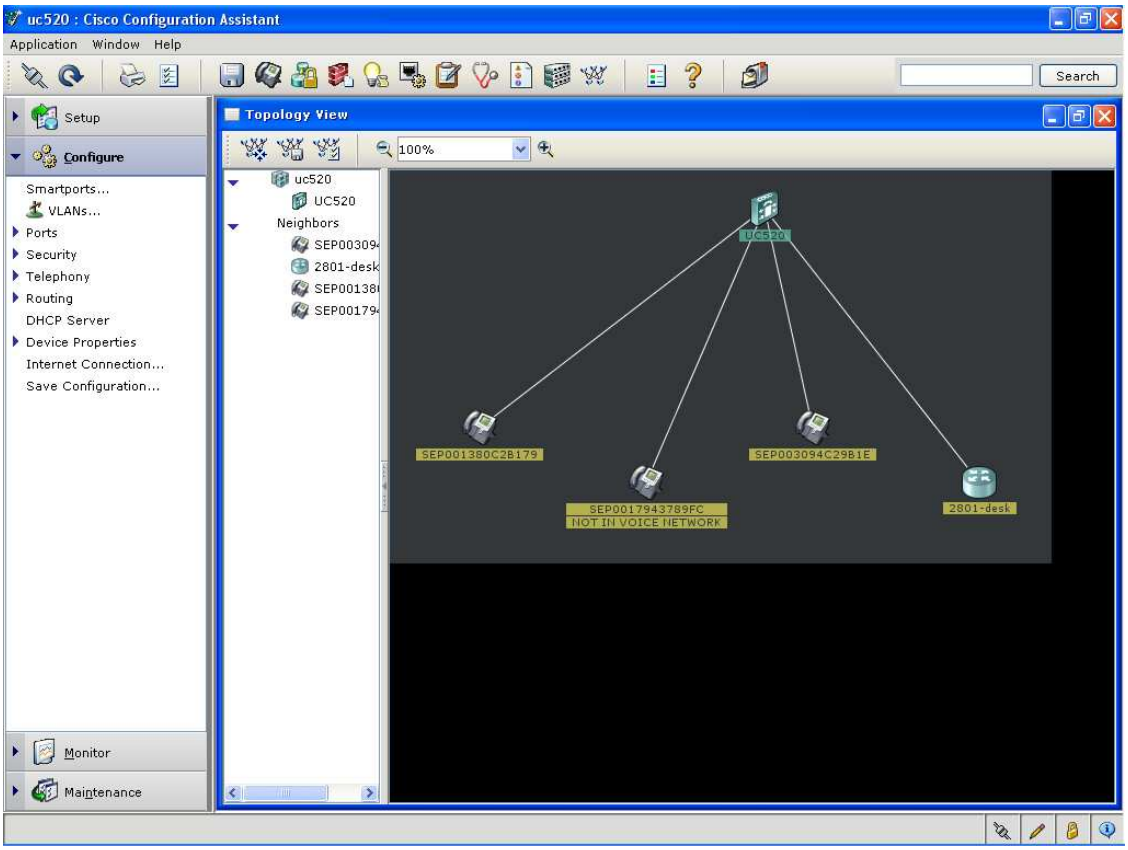
Figure 4.3.5 Topology view



© 2008 Cisco Systems, Inc. All rights reserved.

4.3.6 In this setup – there is a single phone connected to the UC500. To configure the UC500 – click on "Configure" on the Left pane – this should show up as below:

Figure 4.3.6 Left pane showing Configure options



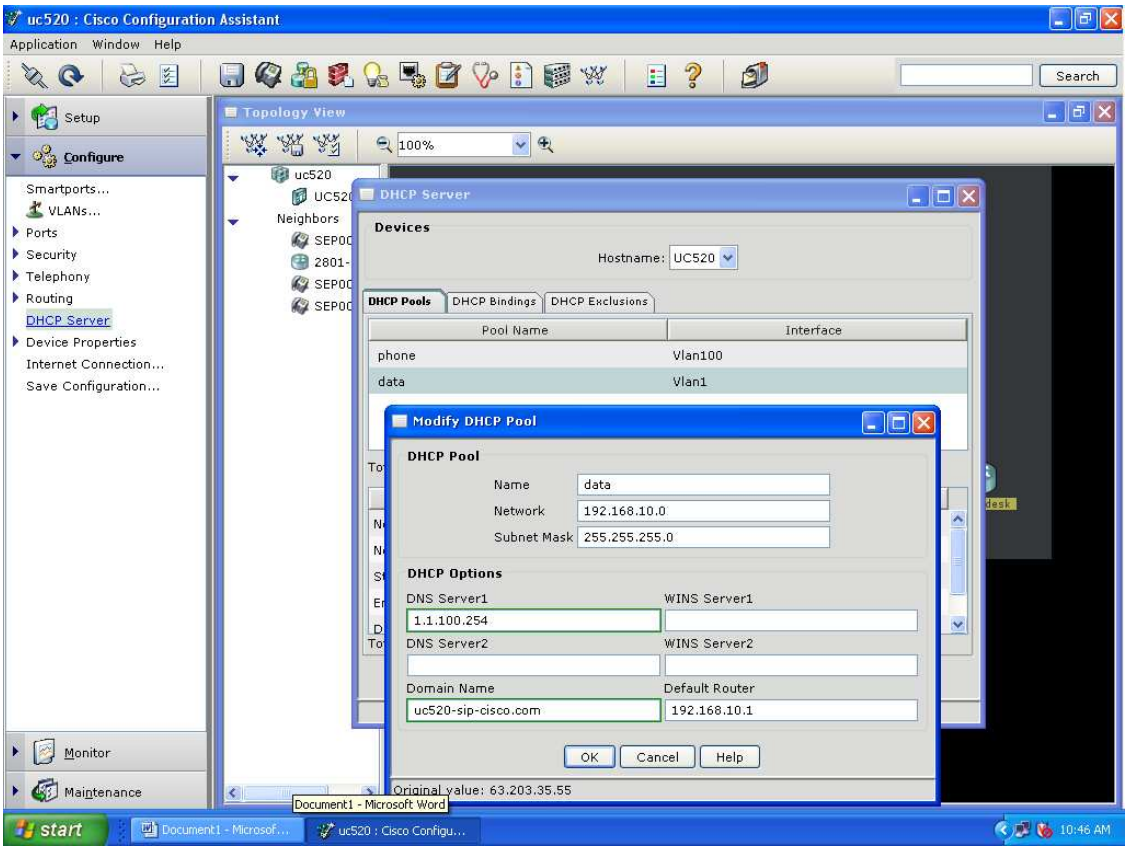
The configuration elements that need to be modified or kept at default from now on are defined per the VAR / customer. The focus for now will be on common SIP Trunk configuration features that need to be changed.

"Smartports" configuration option allows changing data and voice VLAN assignments from the recommended defaults that are assumed in this document to something else.
"Ports" allows the assignment of static duplex and speed settings, power management, and enablement.
"Security" allows the creation or modifications of NAT, VPN server and Firewall options. This will not be addressed in this document but are discussed in the UC500 product documentation.
"Telephony" is where the majority of configuration for SIP Trunking takes place, and will be addressed in the next section of this document.
Cisco recommends that VARs leave the "Switching", "Routing", "Smartports" & "Ports" portions at their default settings unless integration into the provider network requires the addition of IP interfaces, VLANs or static routing decisions etc.

© 2008 Cisco Systems, Inc. All rights reserved.

4.3.7 "DHCP Server" may be selected so that appropriate DNS settings are applied for PCs based on the SP requirement or if the VAR / customer intend to change the default DHCP configuration. Cisco recommends that VARs leave this alone unless there is a compelling need for this.

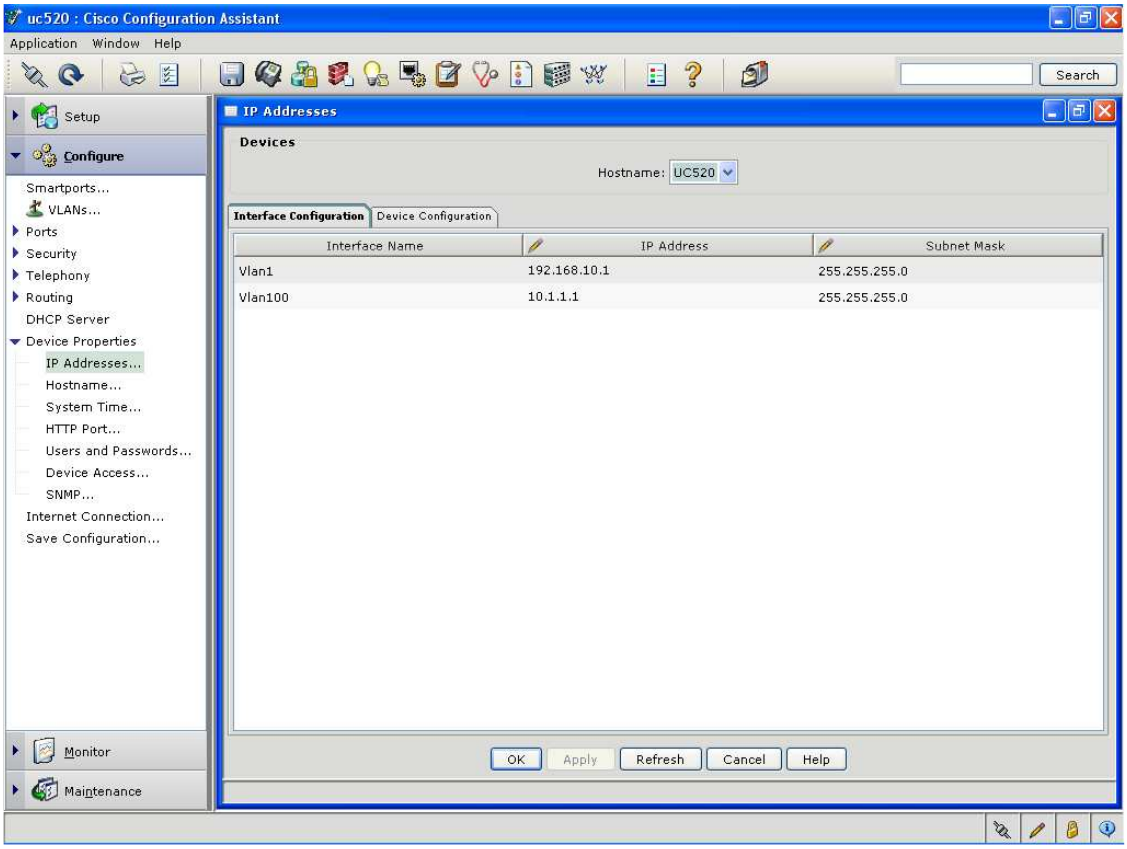
Figure 4.3.7 Changing DNS in the "data" DHCP pool settings



© 2008 Cisco Systems, Inc. All rights reserved.

4.3.8 To change the DNS settings for the UC500 – click on "Device Properties -> IP addresses" – this is particularly relevant if the SIP Trunking provider uses domain names instead of IP addresses to route SIP calls between devices

Figure 4.3.8 default DNS settings for UC500

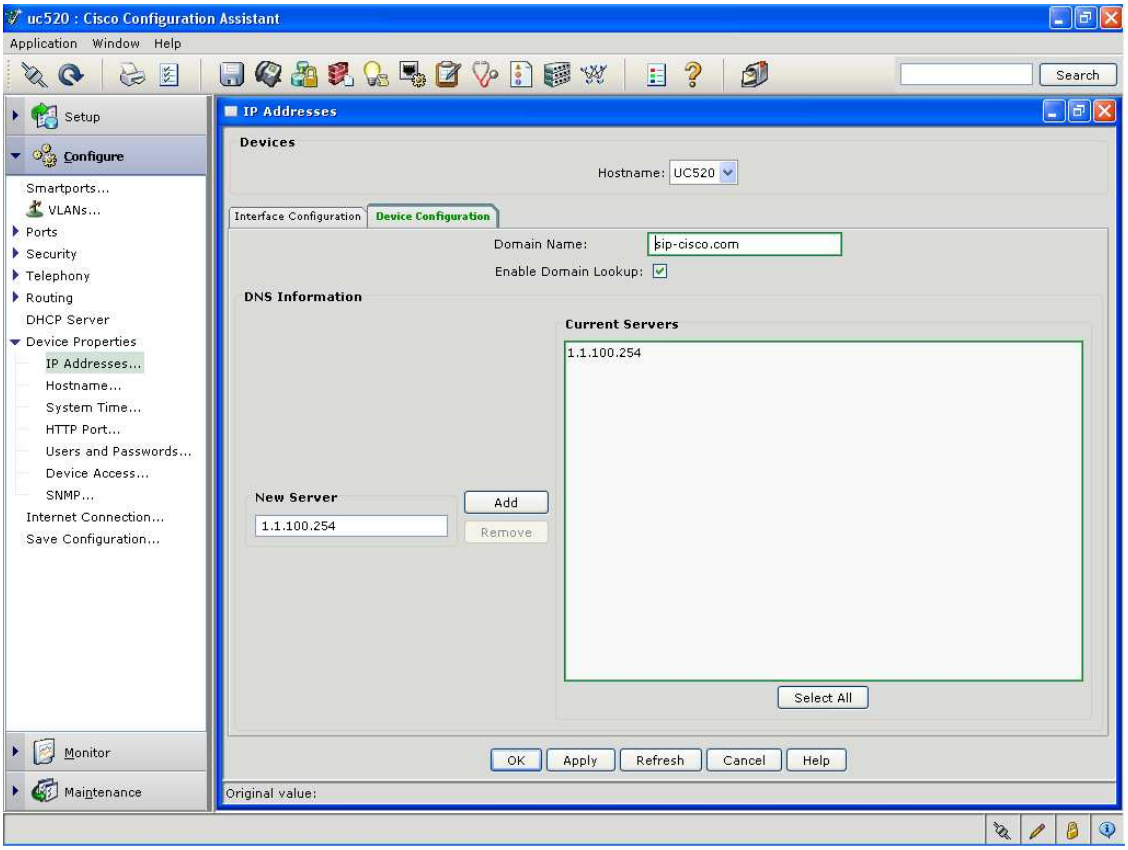


© 2008 Cisco Systems, Inc. All rights reserved.

4.3.9 Click on the "Device Configuration" tab on the right pane & do the below:

Domain name: name the provider requires the UC500 to have
Enable Domain Lookup: should be checked
Remove any old DNS servers in the config
New Server: Enter IP address of DNS server & click Add
Click "OK" at the bottom to continue

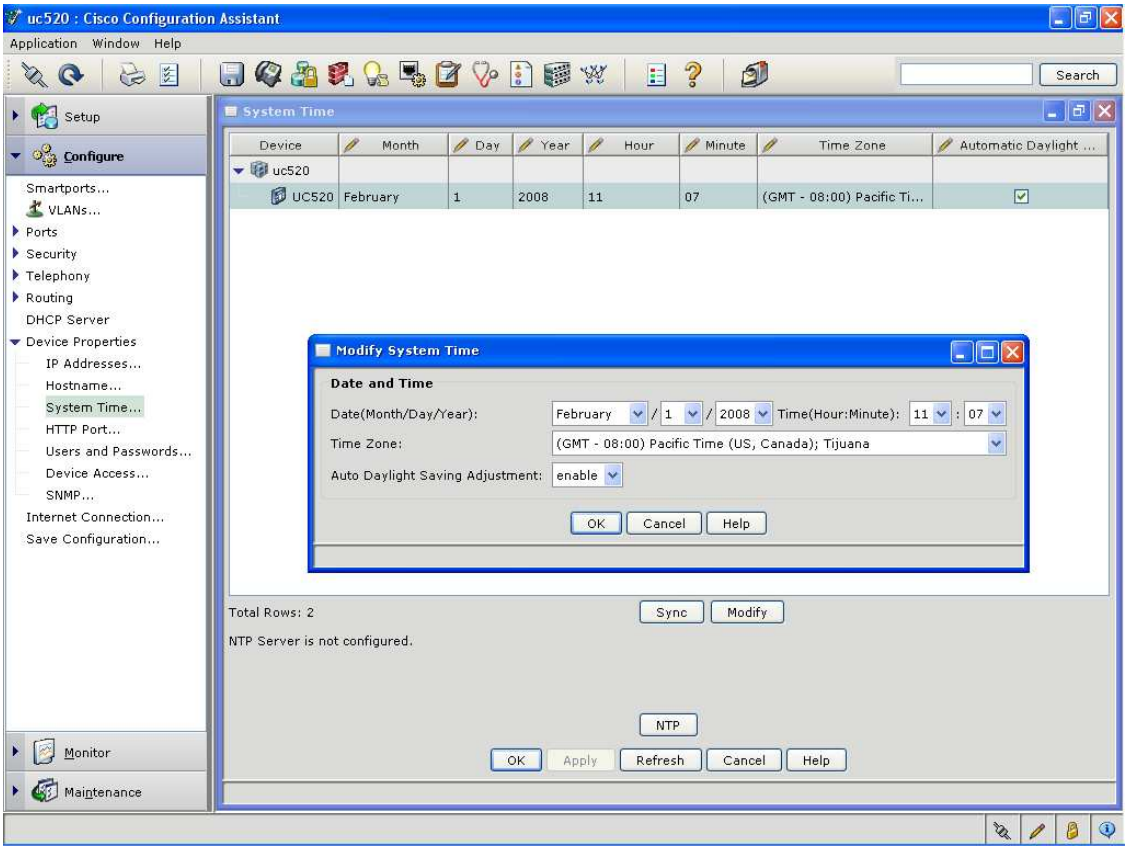
Figure 4.3.9 updated DNS settings for UC500



© 2008 Cisco Systems, Inc. All rights reserved.

4.3.10 Click on "Device Properties -> System Time" to set the system clock. Click the Device name (e.g. "UC520") and then the "Modify" button. Make the appropriate selections and click "OK":

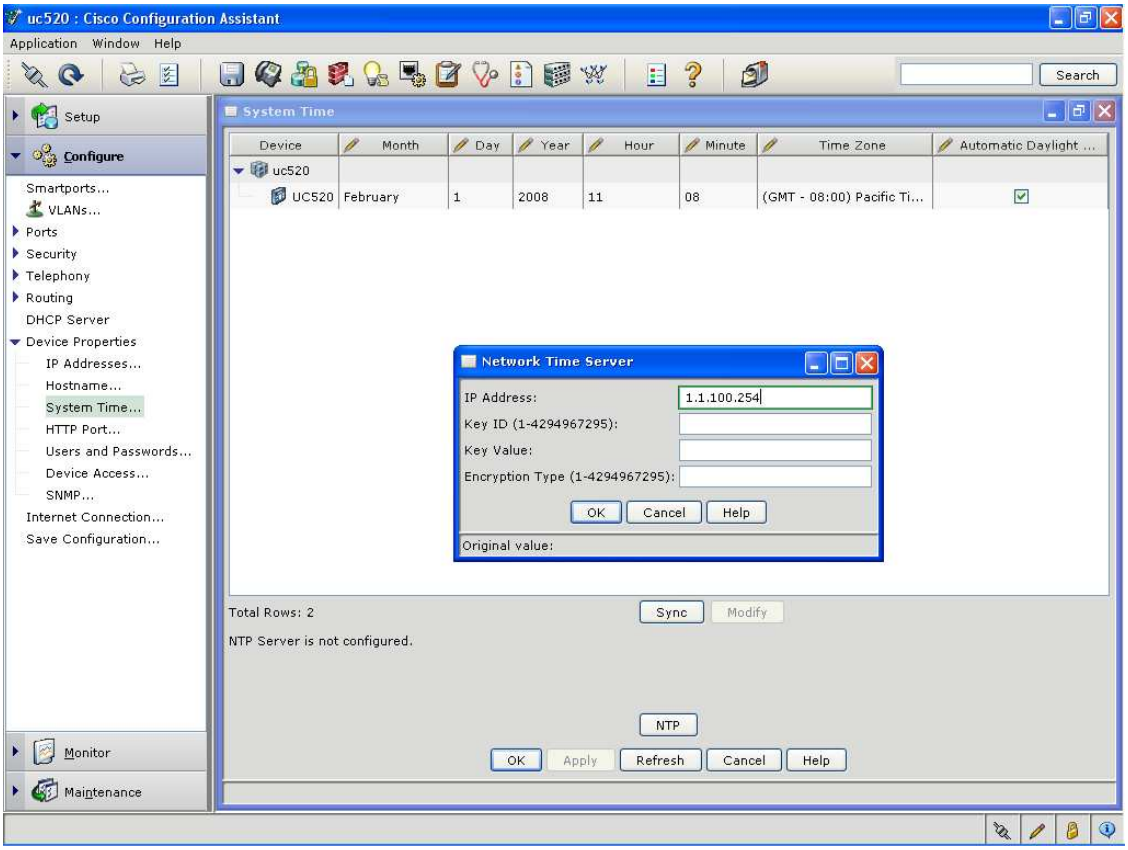
Figure 4.3.10 Setting System Time



© 2008 Cisco Systems, Inc. All rights reserved.

4.3.11 If the provider supplies NTP server information that can be configured in UC500 as well. Click on "NTP" at the bottom of the right pane & enter the IP address(es), Keys & Encryption as defined by the provider – then click "OK". This configuration is optional if no NTP is provided – in this case the UC500 clock is the system clock.

Figure 4.3.11 NTP settings

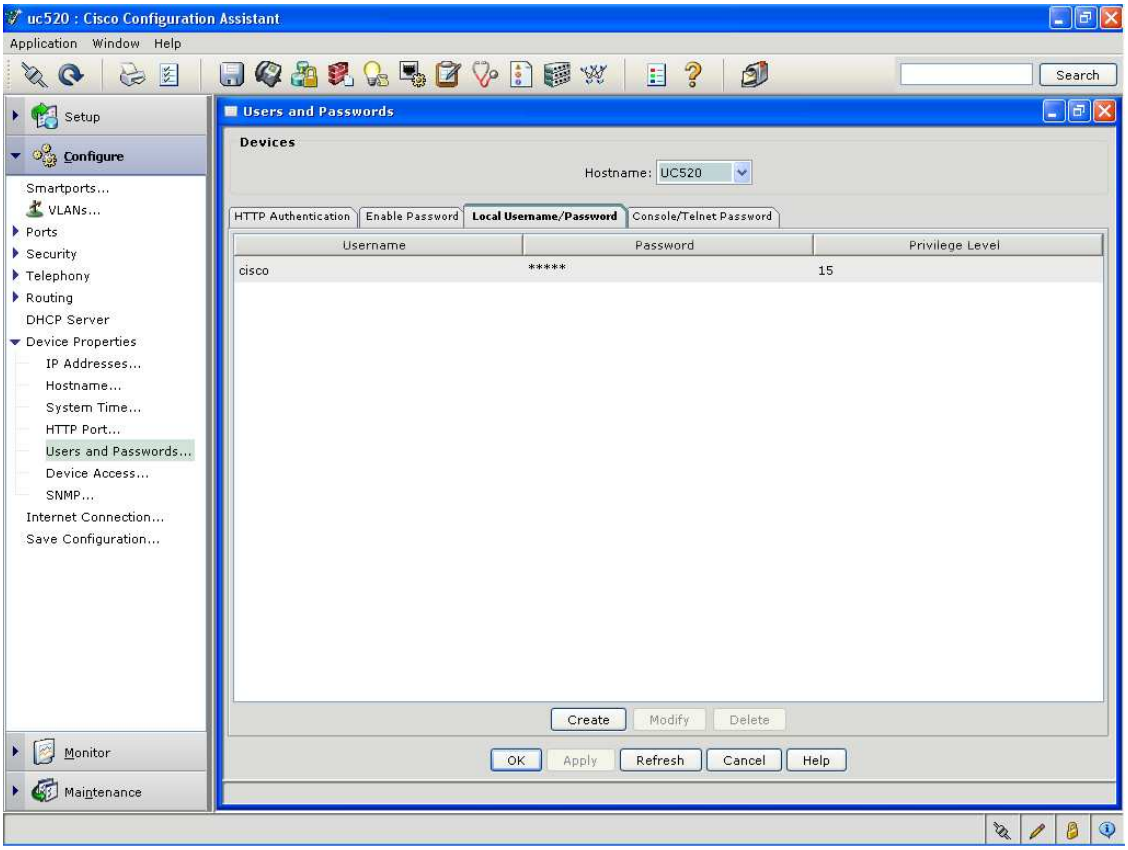


Click "OK" at the bottom of the pane – if a pop up comes up which states there is a need to reload CUE – hit "OK" and disregard this for now.

© 2008 Cisco Systems, Inc. All rights reserved.

4.3.12 Click on "Device Properties/Users and Password" to configure an administrative username and password for access to the UC500 system. Choose the device from the Hostname dropdown at the top & then change the options that are required. The Local Username / Password tab should be where you change this username / password combination. Click "OK" to continue once done.

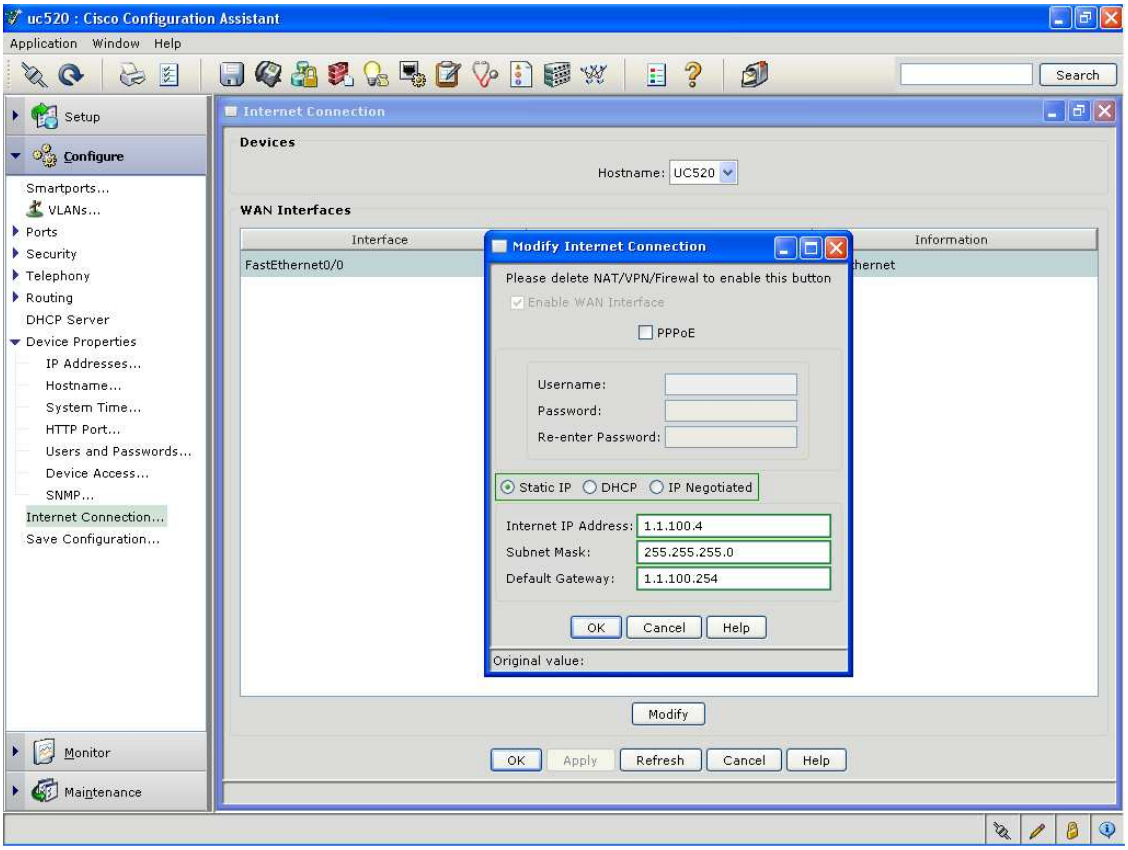
Figure 4.3.12 Username / Password Settings:



© 2008 Cisco Systems, Inc. All rights reserved.

4.3.13a Click "Internet Connection" from the left panel to configure the WAN interface with a appropriate WAN IP address option. This is a ***mandatory*** step when using CCA for UC500 configuration. Click the "FastEthernet 0/0" interface and then the "Modify" button. In this example – a static IP is being used (1.1.100.4). However, based on the network setup, DHCP can also be used as well as PPPoE for DSL. Click "OK" to go back to the Internet Connection pane.

Figure 4.3.13a WAN connection

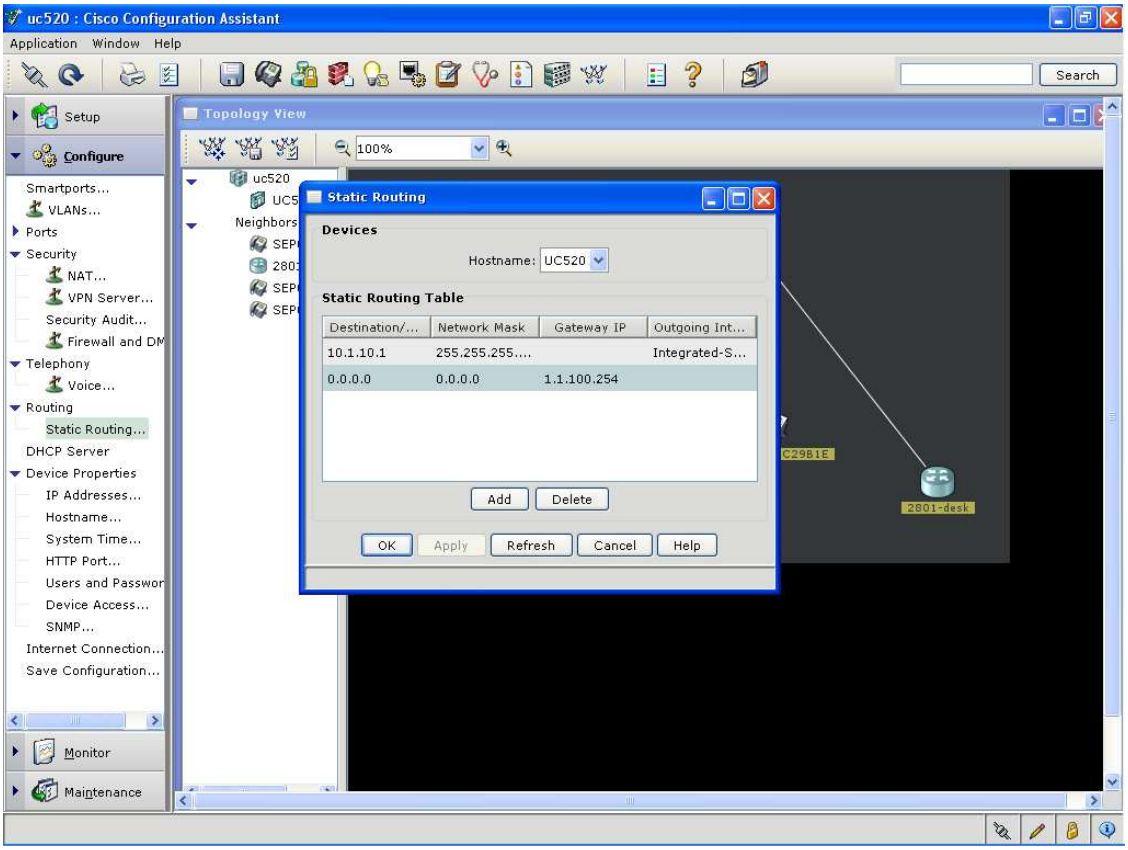


Click "OK" to continue.

© 2008 Cisco Systems, Inc. All rights reserved.

4.3.13b Click "Routing" from the left panel and configure the IP routing with the appropriate default gateway for UC500. Click the "FastEthernet 0/0" interface and then the "Modify" button. In this example – the default gateway is 1.1.100.254.

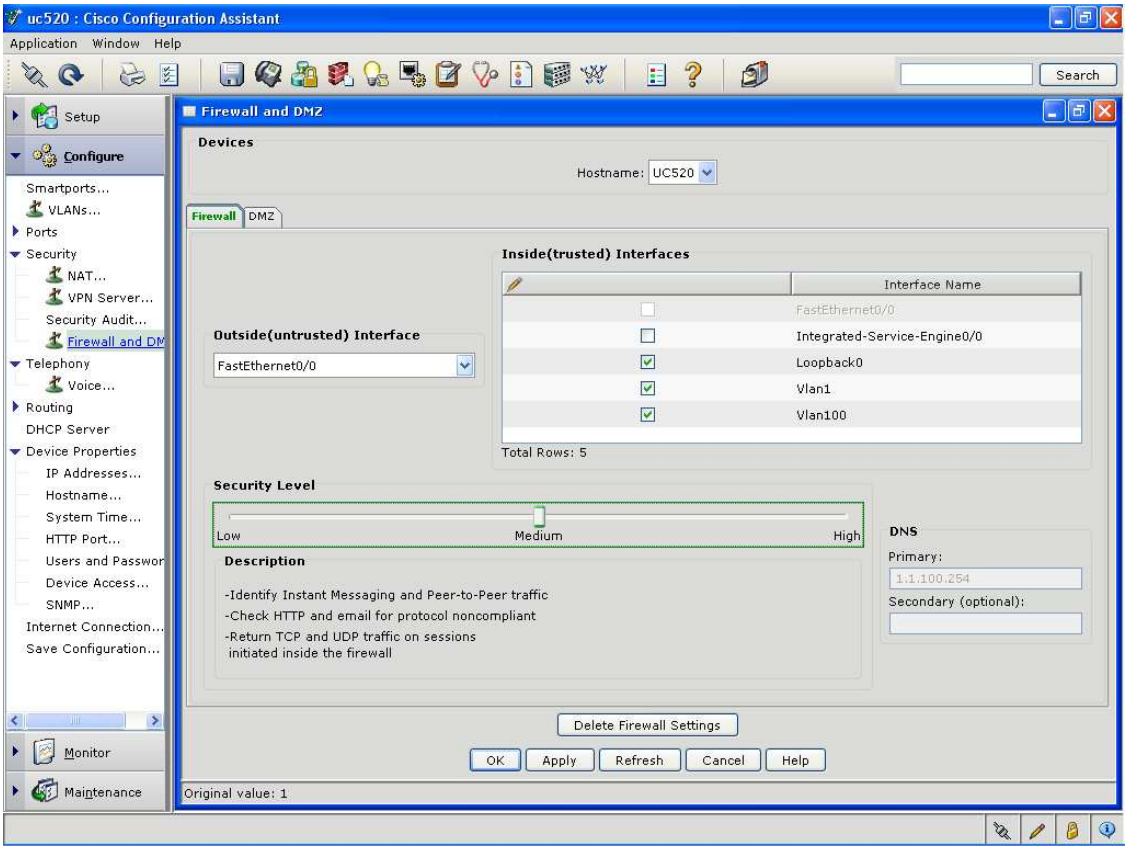
Figure 4.3.13a Routing



© 2008 Cisco Systems, Inc. All rights reserved.

4.3.14 Click on Security on the left and then go to Firewall. The Firewall settings can be set via CCA to either HIGH, MEDIUM or LOW levels based on the desired customer / VAR requirement. In this example, the user sets it to MEDIUM.

Figure 4.3.14 Security



NOTE: If using CCA 1.1 or earlier, then you will need to follow the below steps to ensure SIP traffic goes through. Check the WAN interface configuration (note if using PPPoE then this interface would be Dialer0, not FastEthernet0/0):

```
UC500#show run interface FastEthernet 0/0
interface FastEthernet0/0
ip verify unicast reverse-path
ip inspect SDM_MEDIUM out
```

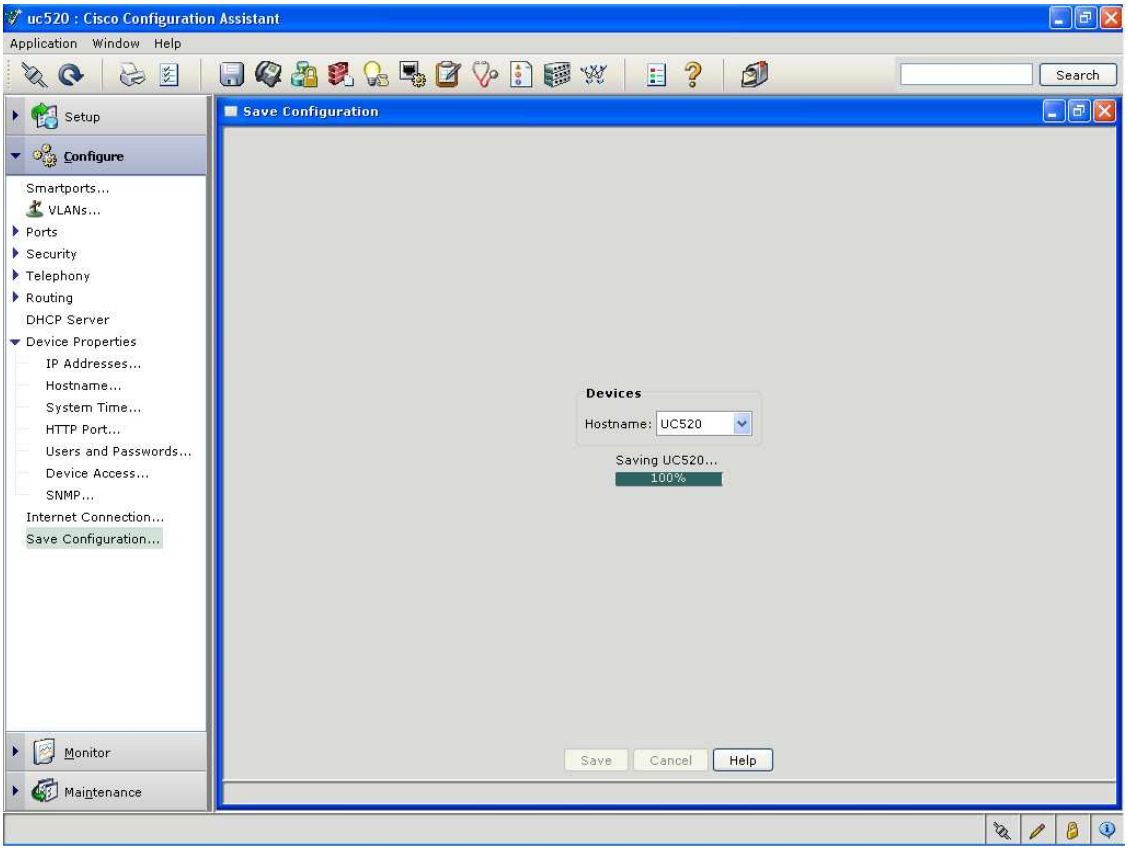
Add the below CLI :

```
UC500#config t
UC500(config)#interface FastEthernet 0/0
UC500(config-if)#no ip verify unicast reverse-path
UC500(config)#interface Integrated-Service-Engine 0/0
UC500(config-if)#no ip access-group 100 in
UC500(config-if)#interface Loopback 0
UC500(config-if)#no ip access-group 101 in
UC500(config)#ip inspect name SDM_MEDIUM udp router-traffic timeout 300
UC500(config)#end
```

© 2008 Cisco Systems, Inc. All rights reserved.

4.3.15 At this point, saving the configuration of the UC500 is strongly recommended:

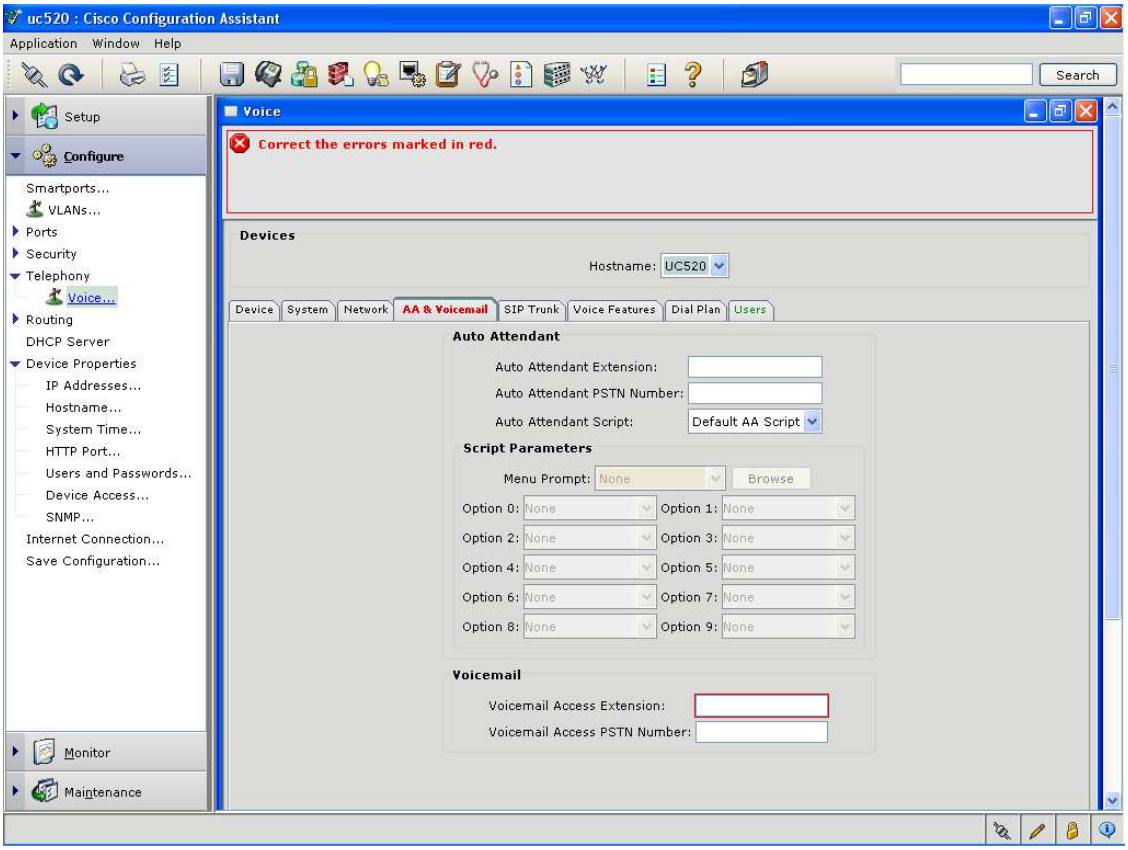
Figure 4.3.15 Saving configuration



© 2008 Cisco Systems, Inc. All rights reserved.

4.3.16 Once the configuration has been saved – go to the "Telephony -> Voice" on the left pane – after a minute or two you will automatically see the "AA & Voicemail" tab on the right with fields highlighted in red which imply these are mandatory to fill.

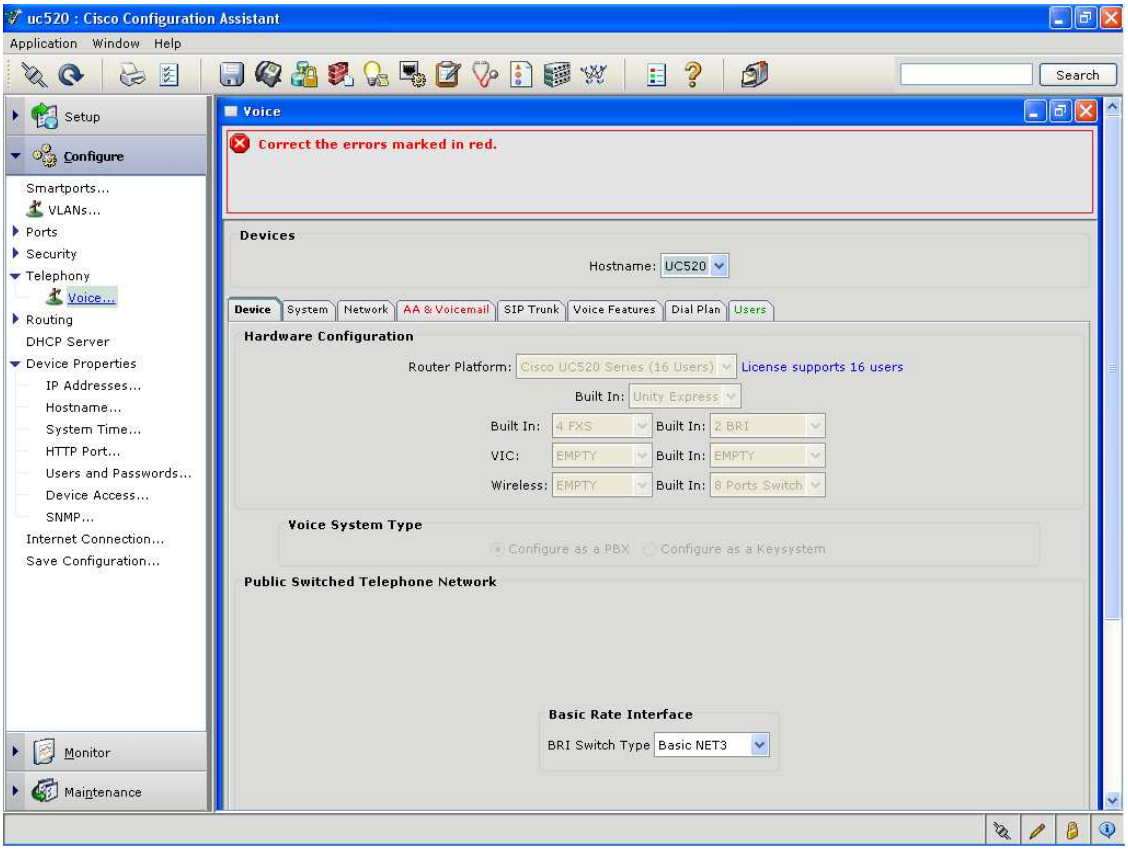
Figure 4.3.16 Voice Configuration Tab



© 2008 Cisco Systems, Inc. All rights reserved.

4.3.17 Click on the "Device" tab in CCA. This is more informational & shows if the UC500 is an 8, 16, 32 or 48 user system, the hardware installed & the system type. Make sure you select "Configure as a PBX" as your Voice System Type for SIP Trunking.

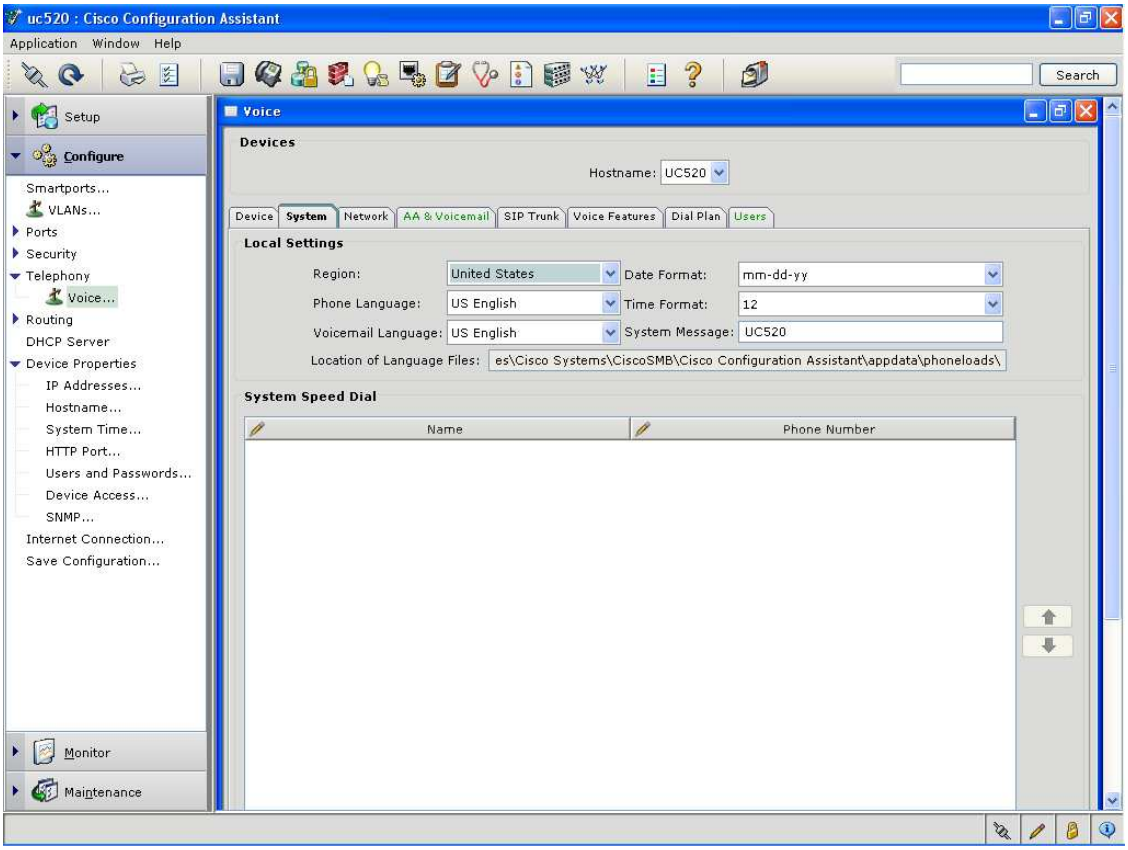
Figure 4.3.17 Device



© 2008 Cisco Systems, Inc. All rights reserved.

4.3.18 Click on the "System" tab – this has information on the system level information such as region, date & time format, language setup & system message. You can also add system level speed dials

Figure 4.3.18 System



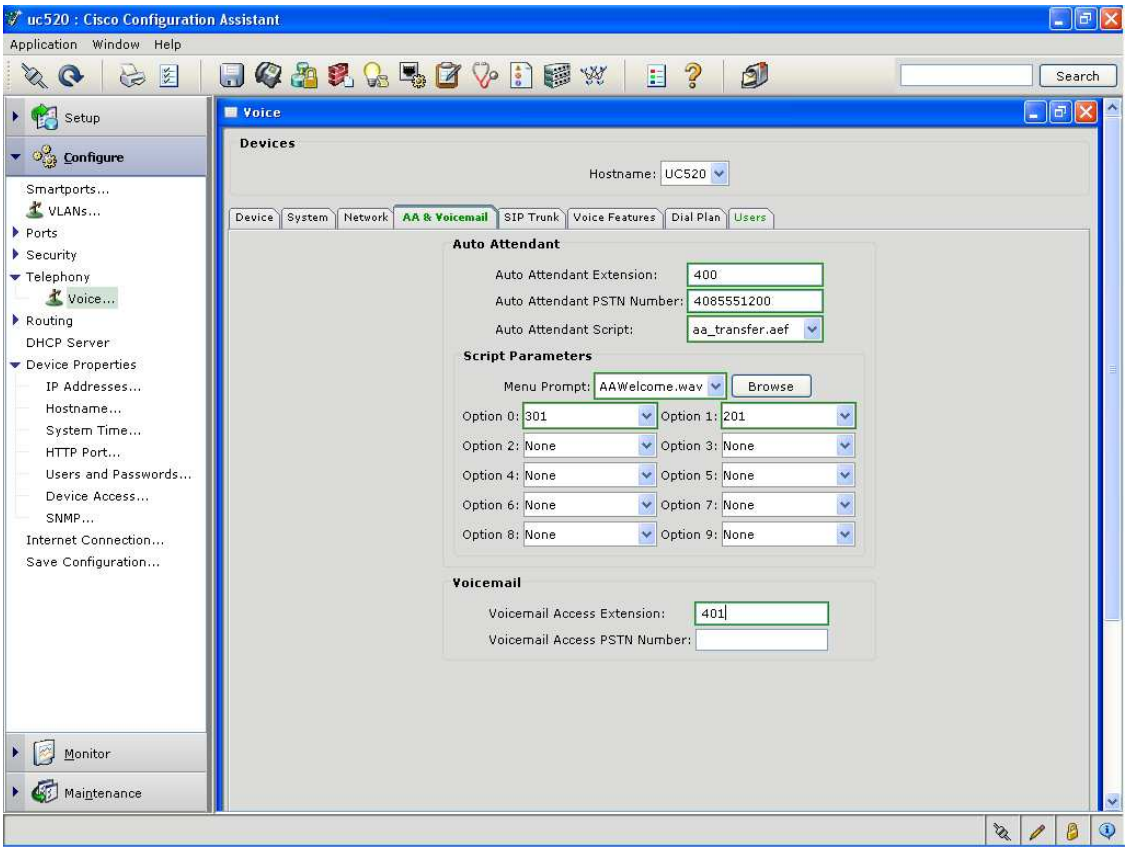
© 2008 Cisco Systems, Inc. All rights reserved.

4.3.19 Click on the AA & Voicemail tab and complete the fields as desired. Note that the number of digits in the AA & Voicemail extensions must be the same as all the other tabs to ensure consistent extension numbering. In this example -

Auto Attendant Extension: 400
Auto Attendant PSTN number: 4085551200 (This is the Main Number DID from SP)
Auto Attendant Script: Choose aa_transfer.aef
Menu Prompt: Choose AAWelcome.wav (or you can record your own prompt and upload)
Enter Options for each digit to route to an extension etc.
Voicemail Access Extension: 401

These can be changed to meet the requirements of the VAR / customer network.

Figure 4.3.19 Updated AA & Voicemail settings



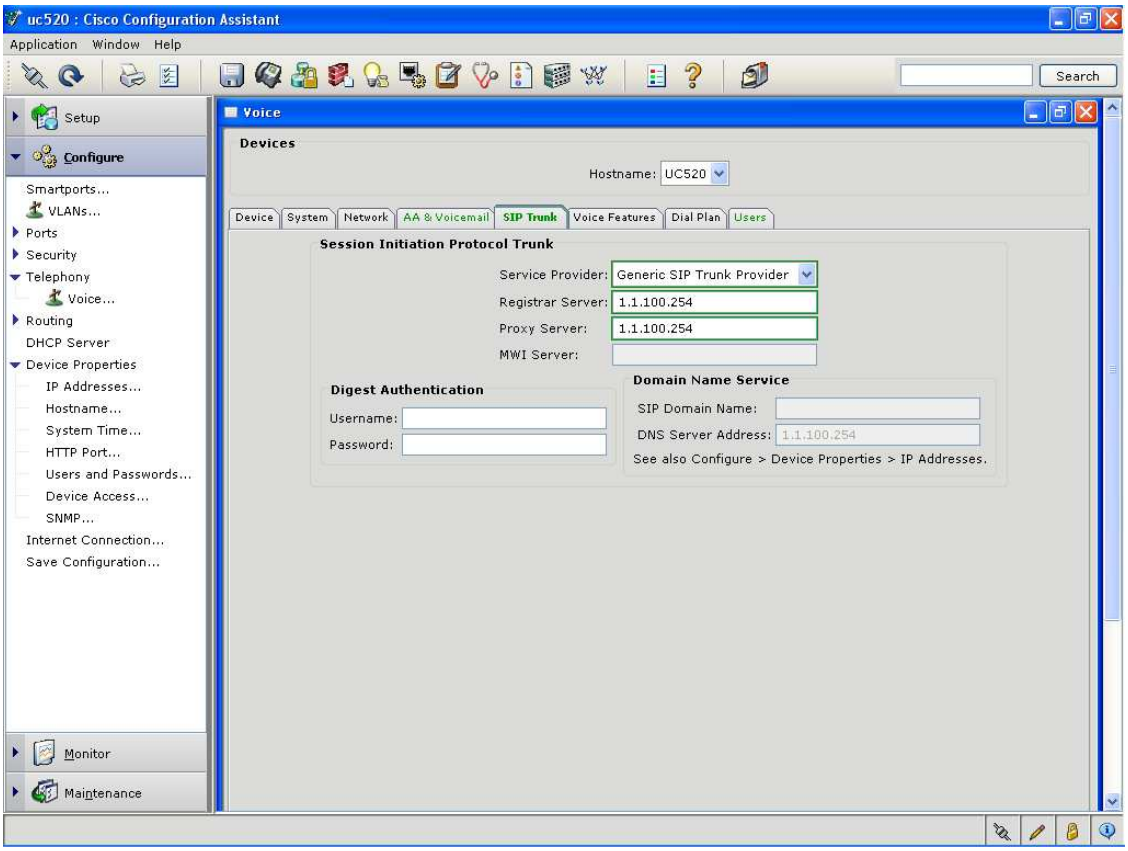
Do NOT click "OK" (scroll to the bottom to see this) for now until the entire Voice configuration is complete else you will get an error.

© 2008 Cisco Systems, Inc. All rights reserved.

4.3.20 Click on the "SIP Trunk Parameters" and fill the parameters as required or supplied by the SP during customer provisioning. In this example – the below are entered:

Service Provider: Choose "Generic SIP Trunk Provider" from the dropdown
Registrar Server: Enter IP or domain name of registrar server if any (this is where the SIP register messages would be sent to)
MWI Server: Fill this only if you need centralized voicemail.
Proxy Server: Enter IP or domain name of proxy server (this is where the SIP INVITE messages would be sent to – can be the same as Registrar server)
Digest Authentication: Enter username / password supplied by the SP if any. Typically the username is the main DID number (such as the Auto Attendant)

Figure 4.3.20 SIP Trunk parameters

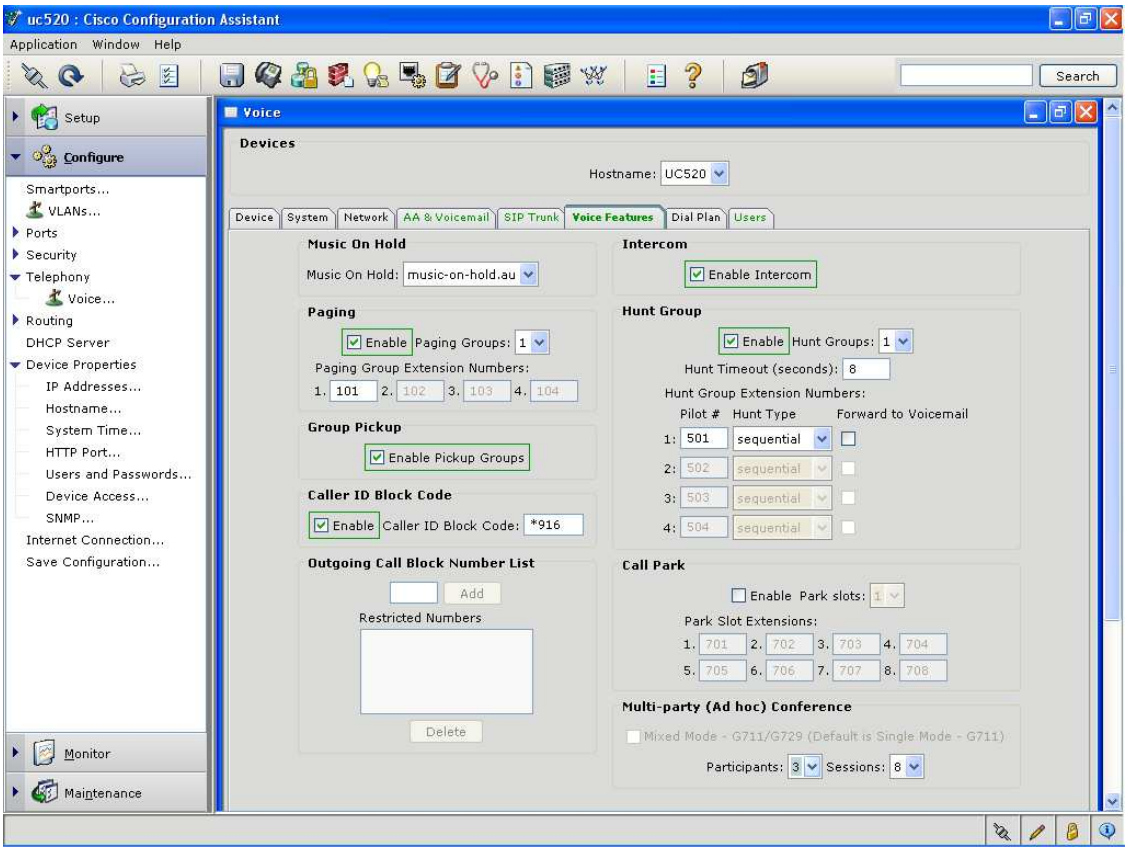


© 2008 Cisco Systems, Inc. All rights reserved.

4.3.21 Click on the "Voice System Features" tab to continue. This is where you configure the system wide features (if required) such as Paging, Intercom etc. It is strongly recommended that the default extensions provided for each feature are NOT changed, to avoid conflicts with other extensions, and more importantly with dial plan elements that are "built in" and not visible through CCA.

In this example - Paging, Group Pickup, Caller ID Block Code, Intercom and Hunt Group features are enabled.

Figure 4.3.21 Voice System Features tab

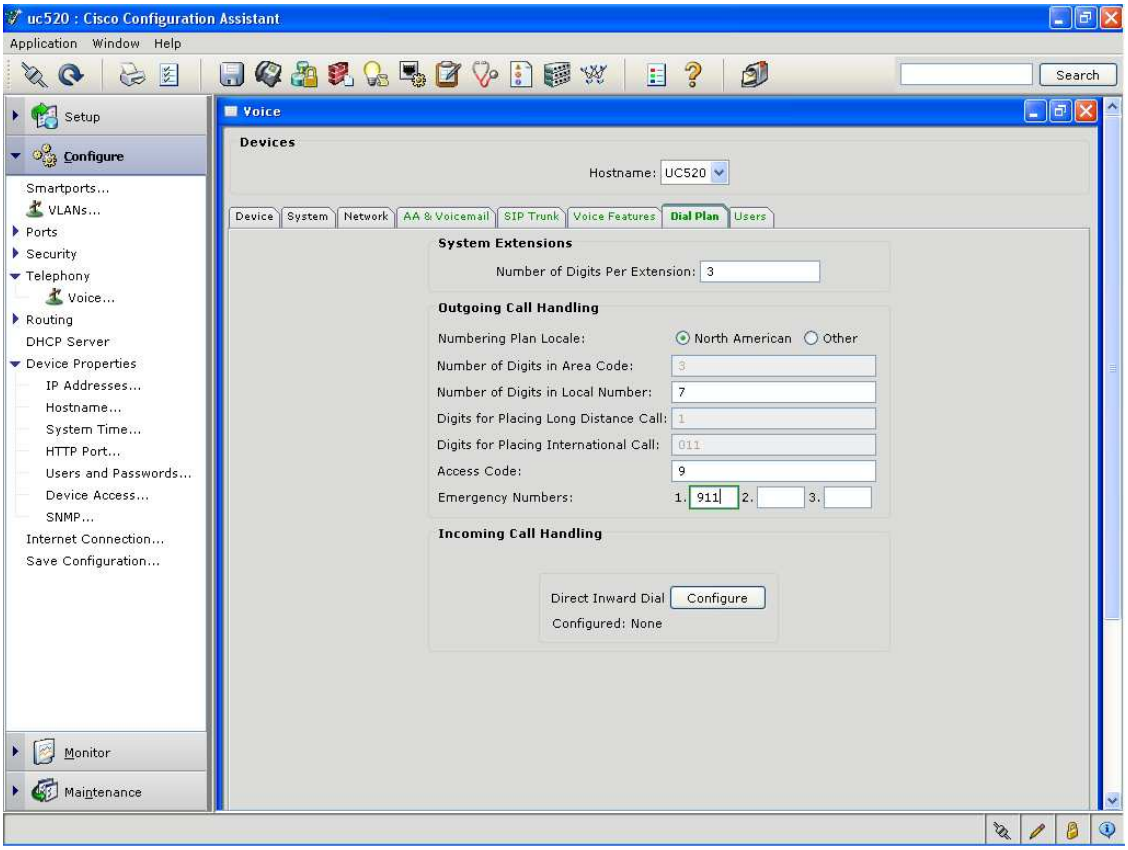


© 2008 Cisco Systems, Inc. All rights reserved.

4.3.22 Click on the “Dial Plan” tab to add dialplan specific parameters. This is used to define the numbering plan for outbound calls and also define the Access Code to dial out. On this screen – there is also the option to configure DIDs which implies mapping the external10 digit PSTN numbers to internal extensions on IP phones (section **4.3.23**)

Number of digits per Extension: 3
Numbering plan Locale: North American
Emergency Numbers: 911
the rest of the parameters are left as default in this example.

Figure 4.3.22 Dial Plan



© 2008 Cisco Systems, Inc. All rights reserved.

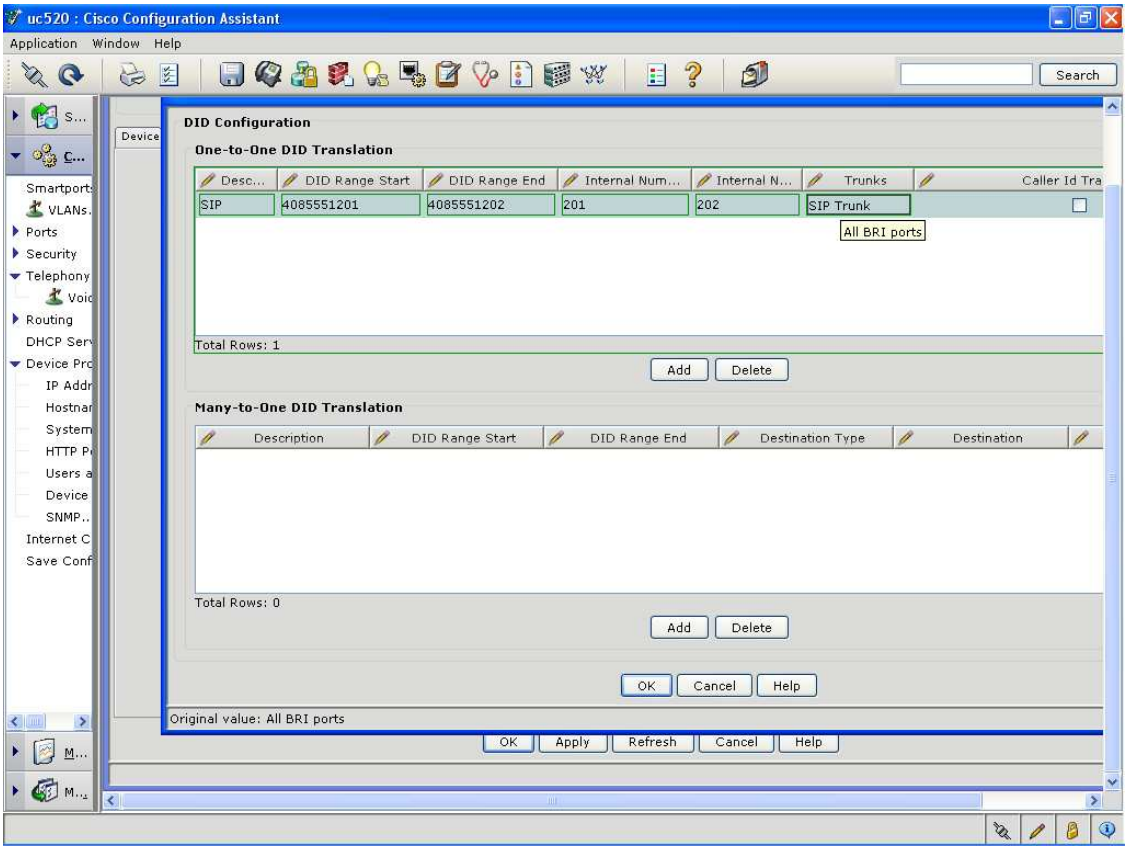
4.3.23 Now click on Configure button next to Direct Inward Dial (DID). Clicking on that button launches another pop up which is for DID configuration. This has 2 sections:

1. One to One DID translation – which is direct mapping between external PSTN number and internal extension
2. Many to One DID translation – which is mapping multiple external PSTN numbers to a single internal extension (say operator)

This example goes over configuring the DIDs for 2 extensions as below

Click on Add range for "One-to-One DID Translation"
Enter a description such as SIP
Enter DID range start as 4085551201 and end as 4085551202
Enter Internal Number Extension start as 201 and end as 202
Choose SIP Trunk from the trunk pulldown
Do not Check Caller ID and then click OK[1]

Figure 4.3.23 DID Configuration

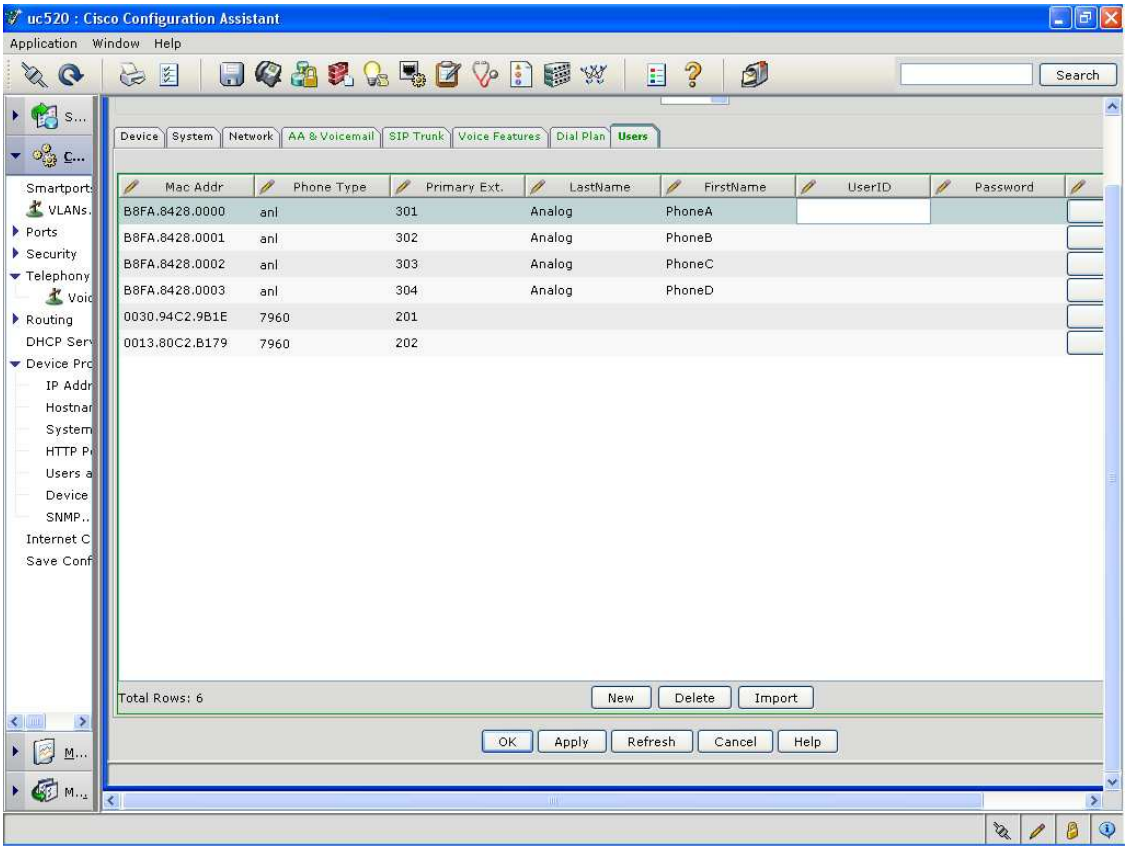


Note 1: The following are the rules for implementation of caller-id in CCA1.5:
1. If the caller-id check box is selected and the last few digits of the extension match that of the DID, then the outbound number would be the DID configured as above.
2. If the caller-id check box is selected and the last few digits of the extension DONOT match that of the DID, then an error is shown. The workaround is not check the box.
3. If caller-id check box is not selected, outbound caller ID for all calls would be the AA PSTN number.
4. For any internal extension without a DID mapped to it, outbound caller ID would be AA PSTN number.

© 2008 Cisco Systems, Inc. All rights reserved.

4.3.24 Click on the "User Parameters" tab to continue. This is where each of the phones (IP or analog) is configured and assigned names, user IDs & passwords. These userIDs & passwords are used by the UC500 to authenticate the users for XML / TAPI applications such as UCC etc. They also will be used for the CME user GUI logon to update speed dials etc.

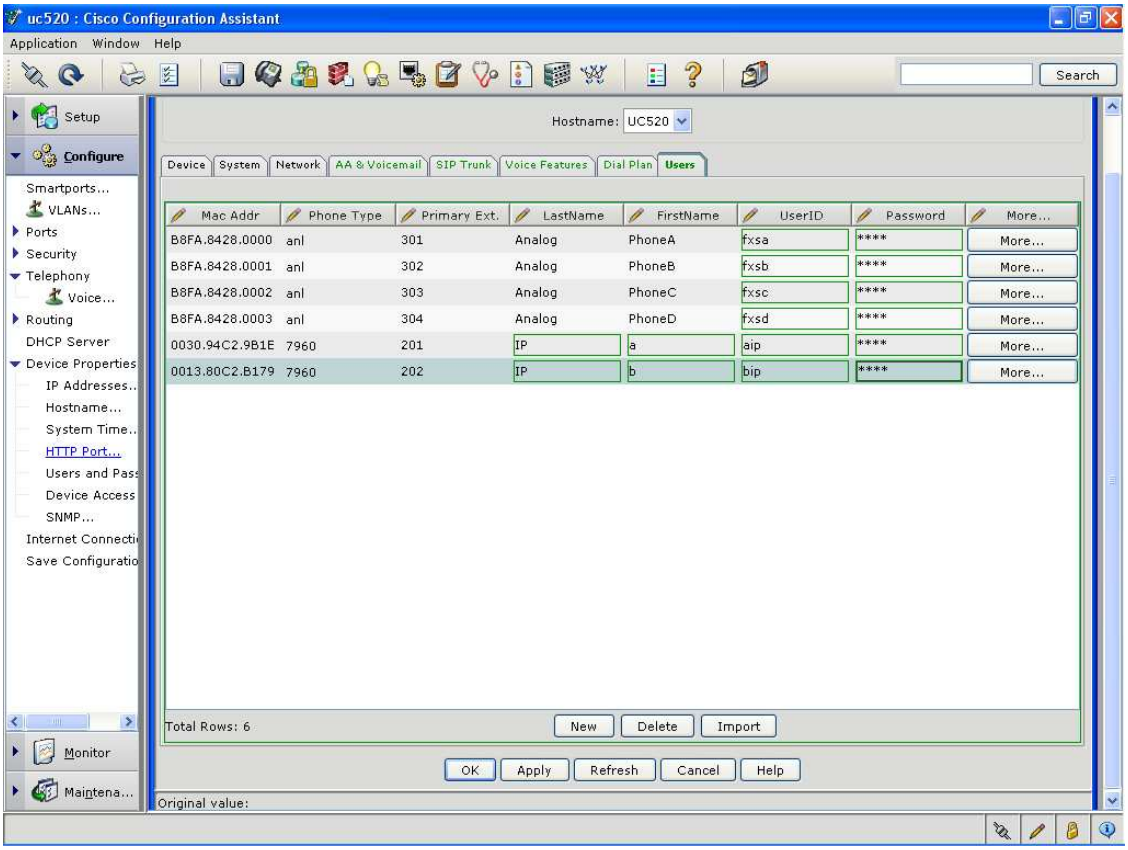
Figure 4.3.24 User parameters



© 2008 Cisco Systems, Inc. All rights reserved.

4.3.25 Enter the LastName, FirstName, UserID & Password for each phone. If the analog ports (FXS) are not needed – you can select each port with Phone type as “anl” & hit “Delete” (scroll down to the bottom to see this).

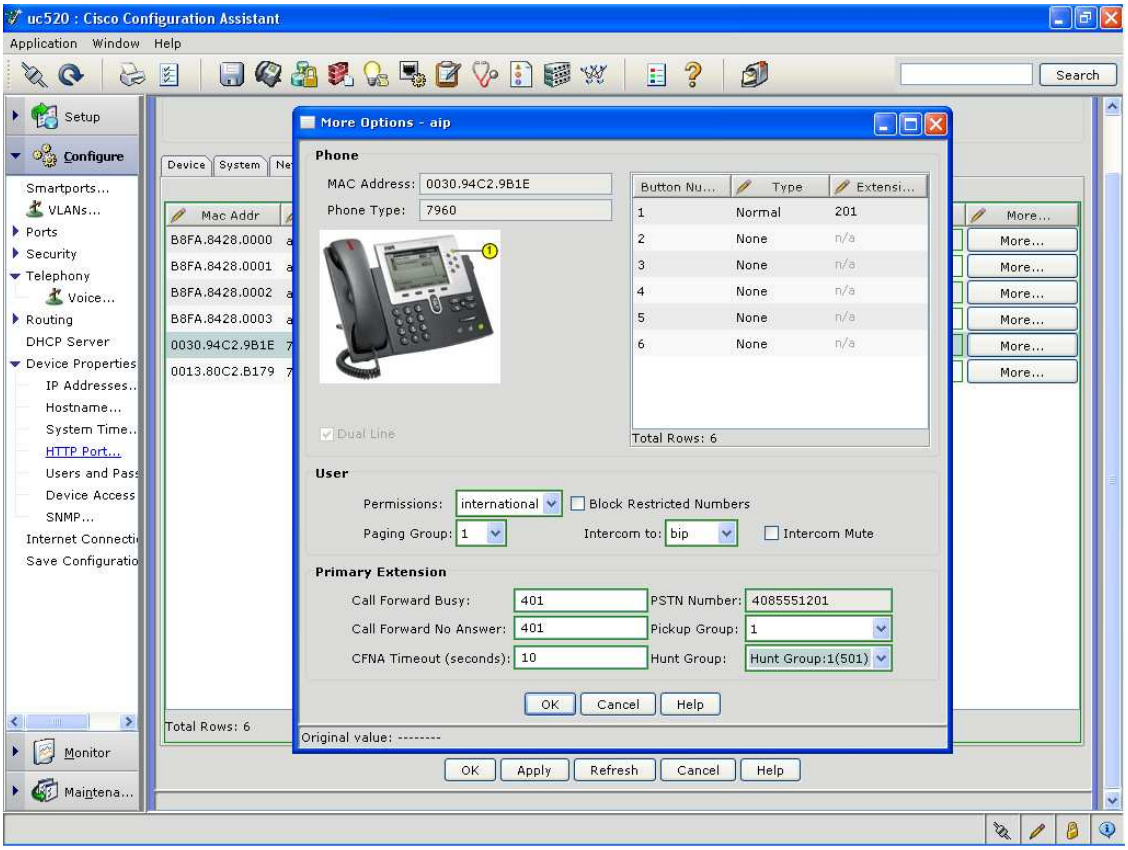
Figure 4.3.25 User parameters continued



© 2008 Cisco Systems, Inc. All rights reserved.

4.3.26 Configuration additional phone features requires the user click on "More" at the extreme right for a given phone – a pop up window as below will show up where you can add dialing permissions (COR), CFNA timeout, Hunt Group, Intercom, Paging group etc. You should also check to make sure the PSTN number field shows the DID you configured in step 4.3.23 for that extension.

Figure 4.3.26 User parameters continued

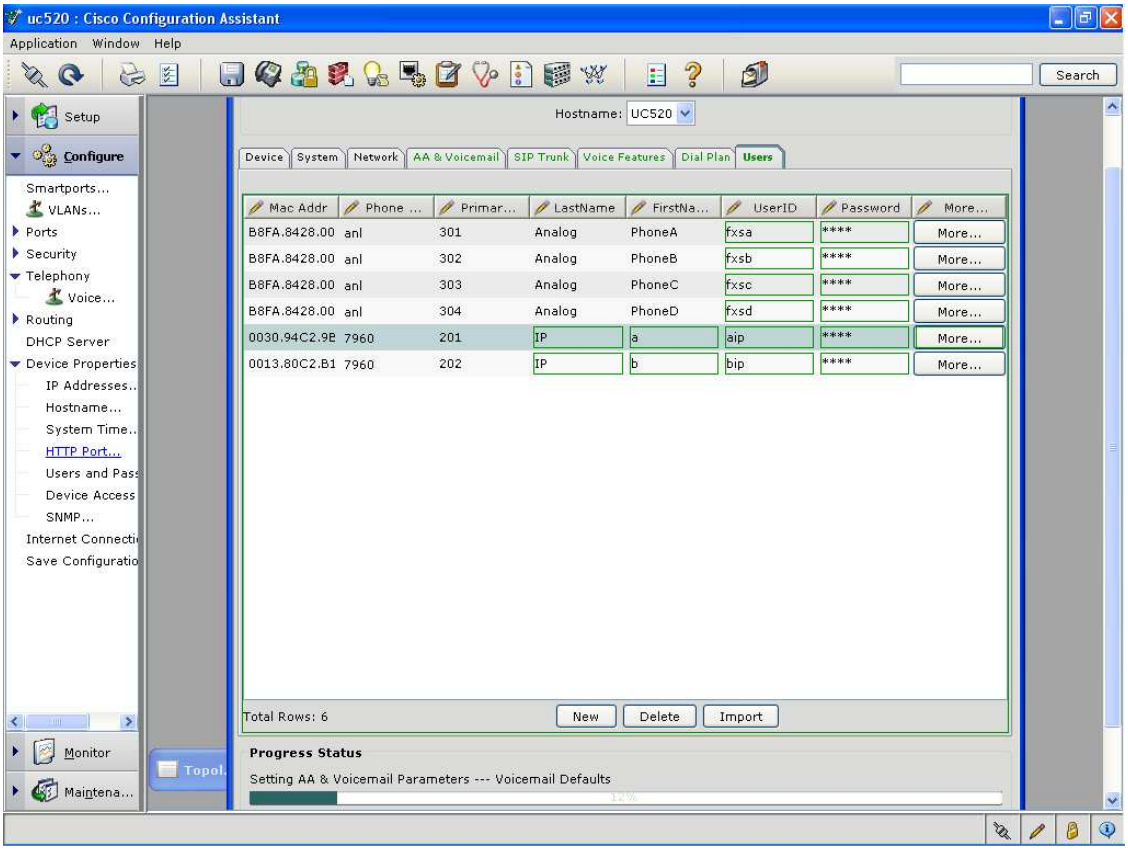


Click "OK" to continue configuring each phone.

© 2008 Cisco Systems, Inc. All rights reserved.

4.3.27 Once done – hit "Apply" at the bottom. Now you should see a progress bar at the bottom of the right pane (Scroll down if you cannot see this) which shows the various stages of the configuration.

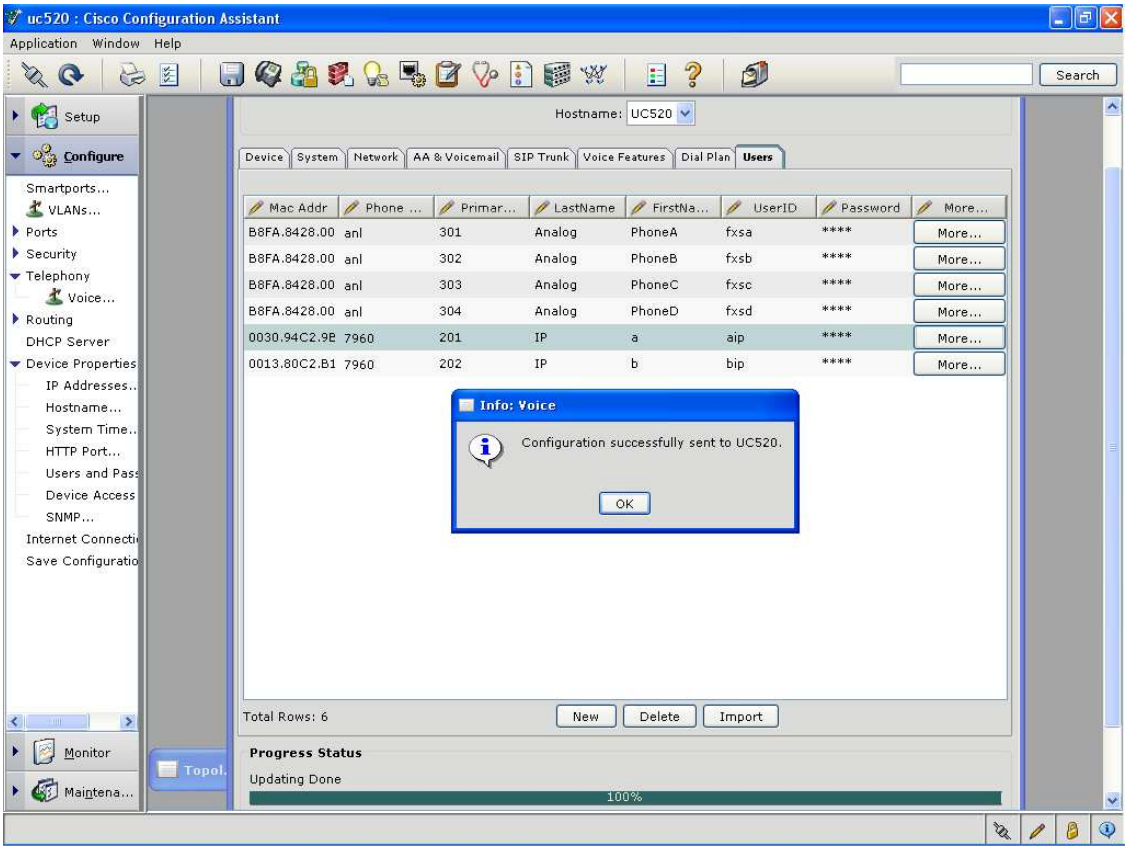
Figure 4.3.27 Status of Configuration



© 2008 Cisco Systems, Inc. All rights reserved.

4.3.28 Once configuration is applied – you should see the below pop up confirming the same

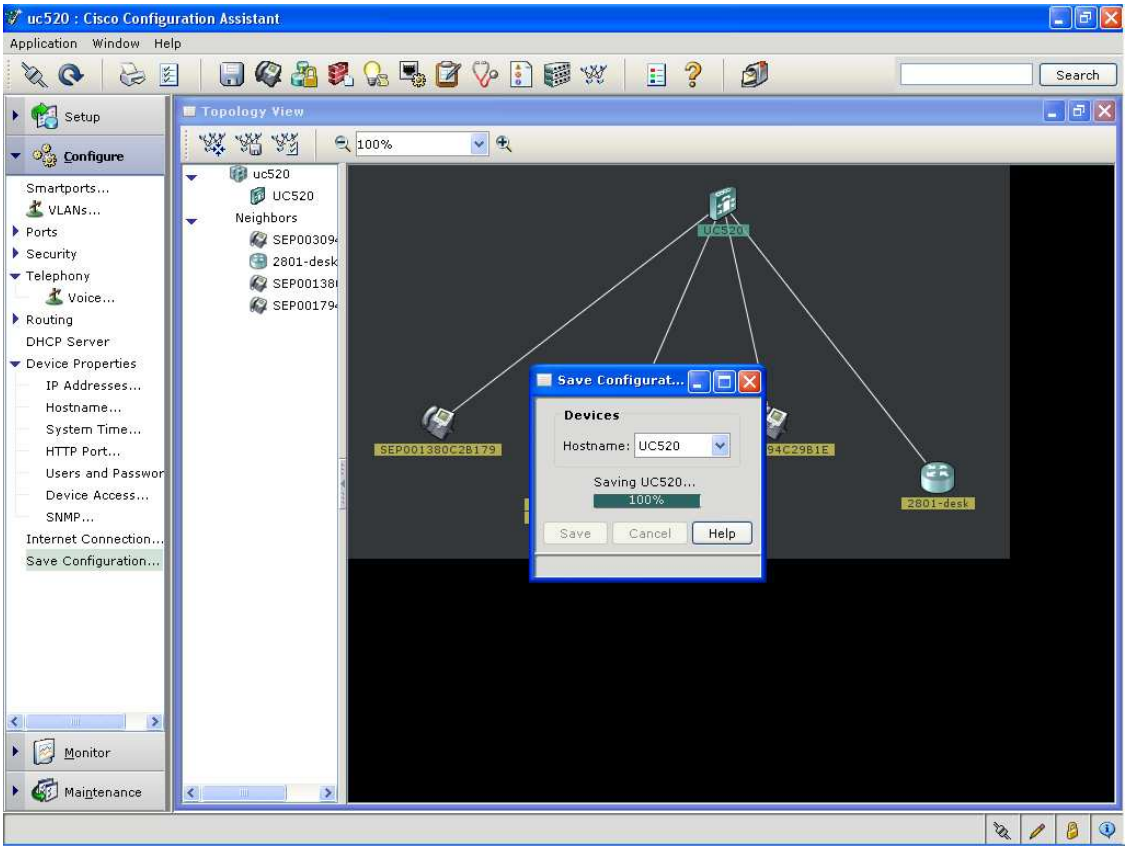
Figure 4.3.28 Configuration Successful



© 2008 Cisco Systems, Inc. All rights reserved.

4.3.29 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 – click on "Save Configuration" on the left as shown previously

Figure 4.3.29 Saving configuration



This completes the CCA configuration for the UC500 SIP trunking portion. There are a few commands that need to be entered via CLI depending on call flows that do not work. Please see the CLI section below.

4.4 CLI configuration

This is an optional step if calls do not work. This section will cover some of the more common scenarios or call flows that config will need to added / changed via CLI on the UC500. Please note that there are efforts underway to add some of these options into the CCA tool in which case the below CLIs will not be required.

4.4.1 Access UC500 via CLI

Open an ssh or telnet session to 192.168.10.1 (using an application such as Putty from the same PC that CCA was launched from). The username / password should be what you

© 2008 Cisco Systems, Inc. All rights reserved.

configured in step **4.3.12.** Once logged in you should be able to use the regular IOS CLI commands.

4.4.2 Securing the UC500 for SIP trunk calls

The Generic SIP trunk configuration pushed via CCA is not sure of the exact SIP devices it will talk to – hence by default the firewall (i.e. access-list) on the WAN interface is kept open. If the IP address(es) of the SIP devices that the UC500 will talk to are known or you want to restrict access to the SIP port (UDP 5060) – please do the below:

a. Find the correct access-list number applied to WAN interface (in this case it is FastEthernet 0/0):

```
UC520#sh run int fa0/0
interface FastEthernet0/0
 description $FW_OUTSIDE$
 ip address 1.1.100.1 255.255.255.0
 ip access-group 104 in
 ip nat outside
 ip inspect SDM_LOW out
 ip virtual-reassembly
 duplex auto
 speed auto
end
```

b. From above, the access-list 104 is the one in question – do the below

```
UC520#show ip access-list 104
Extended IP access list 104
    10 deny ip 10.1.10.0 0.0.0.3 any
    20 deny ip 10.1.1.0 0.0.0.255 any
    30 deny ip 192.168.10.0 0.0.0.255 any
    40 permit icmp any host 1.1.100.1 echo-reply
    50 permit icmp any host 1.1.100.1 time-exceeded
    60 permit icmp any host 1.1.100.1 unreachable
    70 permit udp any any eq 5060
    80 permit udp any eq 5060 any
    90 permit udp any any range 16384 32767
    100 permit udp host 63.203.35.55 eq domain any
    110 deny ip 10.0.0.0 0.255.255.255 any
    120 deny ip 172.16.0.0 0.15.255.255 any
    130 deny ip 192.168.0.0 0.0.255.255 any
    140 deny ip 127.0.0.0 0.255.255.255 any
    150 deny ip host 255.255.255.255 any
    160 deny ip host 0.0.0.0 any
    170 deny ip any any log
```

c. The lines in red are what you need to change to make it secure and allow only SIP signaling to / from IP addresses or domain names that the UC500 talks to. In most cases you will either have a SIP proxy server or softswitch, SIP registrar server or an SBC (outbound proxy). In this example, the SIP proxy & registrar IP address are the same – 1.1.100.254. Knowing this information – you can add the below in config mode:

```
ip access-list extended 104
 no 70 permit udp any any eq 5060
```

© 2008 Cisco Systems, Inc. All rights reserved.

```
 no 80 permit udp any eq 5060 any
70 permit udp host 1.1.100.254 any eq 5060
80 permit udp host 1.1.100.254 eq 5060 any
end
```

d. Make sure the changes have taken affect by looking at the access-list again – you should see the IP address of SIP proxy / registrar in there.

```
UC520#show ip access-list 104
Extended IP access list 104
    10 deny ip 10.1.10.0 0.0.0.3 any
    20 deny ip 10.1.1.0 0.0.0.255 any
    30 deny ip 192.168.10.0 0.0.0.255 any
    40 permit icmp any host 1.1.100.1 echo-reply
    50 permit icmp any host 1.1.100.1 time-exceeded
    60 permit icmp any host 1.1.100.1 unreachable
    70 permit udp  host 1.1.100.254 any eq 5060
    80 permit udp host 1.1.100.254 eq 5060 any
    90 permit udp any any range 16384 32767
    100 permit udp host 63.203.35.55 eq domain any
    110 deny ip 10.0.0.0 0.255.255.255 any
    120 deny ip 172.16.0.0 0.15.255.255 any
    130 deny ip 192.168.0.0 0.0.255.255 any
    140 deny ip 127.0.0.0 0.255.255.255 any
    150 deny ip host 255.255.255.255 any
    160 deny ip any any log
```

If you are using domain names instead of IP addresses, that will also work. Be aware that there may be an outage if the DNS server is not reachable which means the UC500 firewall cannot resolve the domain name to an IP address. This will become the default firewall configuration when using CCA 1.7 coming out in July 2008.

4.4.3 VOIP Codec used on SIP Trunk calls

By default the VoIP codecs configured on the UC500 for SIP trunking are G.711ulaw & G.729 (in that order). Deciding which codec to use depends on the below factors primarily:

a. DSP resources on the UC500 which is the limiting factor for lower bandwidth (hence more complex) voice codecs

b. Bandwidth of IP access link from UC500 to SP which is the limiting factor for higher bandwidth (hence less complex) voice codecs

4.4.3.1 Using G.711 as the codec on SIP trunk

UC500 Model	Bandwidth per call	MOH port	Voice (G711)	T.38 Fax	Transcoding	HW Conferencing
8/16 User (PVDM2-32)	80 Kbps	1	8/16	4	NA	8 sessions (64 conferees)
24/32/48 User (PVDM2-64)	80 Kbps	1	24/32/48	8	NA	8 sessions (64 conferees)

© 2008 Cisco Systems, Inc. All rights reserved.

NOTE: All values listed are the maximum for each function – you must mix & match to get the optimum # of calls that can be supported over the SIP trunk.

4.4.3.2 Using G.729 as the codec on the SIP trunk

UC500 Model	Bandwidth per call	MOH port	Voice (G729)	T.38 Fax	Transcoding	HW Conferencing
8/16 User (PVDM2-32)	24 Kbps	1	8/16	4	6	2 sessions (16 conferees)
24/32/48 User (PVDM2-64)	24 Kbps	1	24/32/48	8	10	2 sessions (16 conferees)

NOTE: All values listed are the maximum for each function – you must mix & match to get the optimum # of calls that can be supported over the SIP trunk.

If there is a need by the SP to only use G.729 then below is the CLI you would need to enter the below in config mode:

```
voice class codec 1
  no codec preference 1 g711ulaw
  no codec preference 2 g729r8
  codec preference 1 g729r8
sip-ua
  g729-annexb override
```

Also, transcoding is required in this case especially when going to voicemail (Cisco Unity Express) as that only supports G711ulaw. A sample transcoding configuration on UC500 can be done as shown below:

a. Find the MAC address to be used for transcoder:

```
UC500#sh int vlan 100 | inc bia
  Hardware is EtherSVI, address is 001b.8fa8.4282 (bia 001b.8fa8.4282)
```

b. Configure the DSPs for transcoding:

```
voice-card 0
  dsp services dspfarm
```

c. Disable SCCP services (affects only analog ports)

```
no sccp ccm group 1
Removing this CCM group will result the associated profiles (SCCP appl services) to
unregister with the active CCM or to bring down those appl services.
Do you want to continue...[y/n]? [no]: y
no sccp ccm 10.1.1.1 identifier 1
sccp ccm 10.1.1.1 identifier 1 version 4.1
```

d. Re enable SCCP services and add transcoder MAC address from above. Note the number of sessions is 6 in this case. This can change based on requirements for calls and also is based on any other features that use DSPs being turned on or off:

```
sccp ccm group 1
  associate ccm 1 priority 1
  associate profile 2 register mtp001b8fa84282
```

© 2008 Cisco Systems, Inc. All rights reserved.

e. Configure transcoding profile and allow specific codecs

```
dspfarm profile 2 transcode
  no codec ilbc
  no codec g723r63
  no codec g723r53
  no codec gsmamr-nb
  no codec g729br8
  maximum sessions 6
  associate application SCCP
  no shut
```

f. Register the transcoder to the UC500

```
telephony-service
 sdspfarm units 3
 sdspfarm tag 2 mtp001b8fa84282
 sdspfarm transcode sessions 6
 sdspfarm unregister force
```

4.4.4 Fax / Modem Calls

The UC500 can support Fax calls via T.38 (SIP re-Invite) or pass-through (G.711 SIP re-Invite) over the SIP trunk.

4.4.4.1 If the SP only supports T.38 – then the below changes need to be made to enable this to work:

- Delete the FXS port where the fax machine is connected from the CCA interface.
- In the CLI – remove sccp configuration for the FXS port in question (in this example using port 0/0/0):

```
dial-peer voice 1 pots
  no service ← Remove SCCP control
  destination-pattern 4085551010 ← Fax DID or PSTN number
```

- Enable T.38 support globally:

```
voice service voip
 fax protocol t38
```

- Add T.38 support on the inbound & outbound SIP trunk dial-peers (note there may be more than just 1000 shown below)

```
dial-peer voice 1000 voip
 fax protocol t38
```

4.4.4.2 If the SP supports fax and modem via G.711 passthrough, then this should work without any changes if the VOIP codec is G.711. If the VOIP Codec is G.729, then UC500 can be configured such that only fax calls use G711 codec and VOIP calls use G.729. Assume in this case the fax is on FXS port 0/0/0 which is extension 301 and this is mapped to PSTN DID 4085551010.

```
voice service voip
  fax protocol none
  no fax-relay sg3-to-g3
!
dial-peer cor list call-fax
  member PSTN-fax
```

© 2008 Cisco Systems, Inc. All rights reserved.

```
!
dial-peer voice 11100 voip
 corlist outgoing call-fax
 description ** Outgoing fax call to SIP trunk **
 translation-profile outgoing PSTN_Outgoing
 answer-address 301
 destination-pattern 9T
 session protocol sipv2
 session target sip-server
 dtmf-relay rtp-nte
 codec g711ulaw
 no vad
!
dial-peer voice 11101 voip
 description *****Incoming Fax call from SIP Trunk *****
 session protocol sipv2
 session target sip-server
 incoming called-number 4085551010
 dtmf-relay rtp-nte
 codec g711ulaw
 no vad
!
  ephone-dn  5  dual-line
  number 301 secondary 4085551010 no-reg both
  corlist incoming call-fax
```

4.4.4.3 For modem support – the UC500 supports G.711 upspeed via proprietary methods – support is being added to Cisco IOS to upspeed to G.711 via a SIP re-Invite as proposed in SIPConnect forum.

4.4.5 Outbound proxy support

This feature allows the UC500 to send all SIP packets to a specific IP address or DNS instead of the IP / DNS of the proxy server defined in section 4.3.20. This is a common method used in case the SP has an SBC (Session Border Controller) which interfaces with all customer IP PBXes from the SP point of view.

```
voice service voip
  sip
    outbound-proxy dns:sipconnect.cisco.com
```

Note: If outbound proxy is used, you cannot use SIP phones (such as Cisco 3911 or 3951) till UC520 software pack is upgraded to 4.3.x. Also, since the interface between UC500 & CUE (voicemail / AA) is also SIP – make sure all VOIP dial-peers on UC500 pointing to CUE have the below added:

```
dial-peer voice 2000 voip
  description ** cue voicemail pilot number **
  voice-class sip outbound-proxy  ipv4:10.1.10.1
```

4.4.6 Call Admission Control (CAC) & QoS

Since calls over SIP Trunk are using the IP interconnect, there is no implicit CAC setup like you would have with TDM trunks such as timeslots on a T1 PRI. To allow for this

© 2008 Cisco Systems, Inc. All rights reserved.

the UC500 has an option to define maximum calls out the WAN interface (FastEthernet 0/0) using the below example which limits to 3 total calls:

```
call threshold interface FastEthernet 0/0 int-calls low 3 high 3
```

For QoS (Quality of Service) by default the UC500 is setup to mark SIP packets (signaling) as cs4 and RTP (media or audio) packets as cs5. This can be changed via the below CLI on all VOIP dial peers used for the SIP Trunk:

```
dial-peer voice 1000 voip
 ip qos dscp ef media
 ip qos dscp af31 signaling
```

4.4.7 Call forward caller ID (calling-number local)

When calls get forwarded from the UC500 to the SP, the caller ID field is by default set to the original calling number. For example if PSTN A (4084441234) calls IP phone A (4085551001) & phone A is set up for CFA (Call Fwd All) to another cell phone on the PSTN (4083331234) – the INVITE for the second call will have the caller ID of PSTN A → 4084441234. Some SP soft switches will not process the INVITE as the From header in the INVITE is not a DID on the UC500 – to overcome this you can setup the caller ID for call forward or transfer to be the UC500 phone that initiates the feature as below:

```
telephony-service
 calling-number local
```

4.4.8 Creating a specific Dial Plan for outbound calls

The default dialplan when using a generic SIP Trunk provider template sends all calls out a single dial-peer which implies that Class of Restrictions (COR) do not apply. This can be changed using “dial-peers” as desired. An example using the North American Numbering plan (NANP) is shown below:

```
dial-peer voice 11001 voip
 corlist outgoing call-local
 description ** Outgoing Local call to SIP trunk **
 destination-pattern 9[2-9].....
 session protocol sipv2
 session target sip-server
 dtmf-relay rtp-nte
 no vad
!
dial-peer voice 11002 voip
 corlist outgoing call-domestic
 description ** Outgoing Long Distance call to SIP trunk **
 destination-pattern 91[2-9]..[2-9].....
 session protocol sipv2
 session target sip-server
 dtmf-relay rtp-nte
no vad
!
dial-peer voice 11003 voip
 corlist outgoing call-international
 description ** Outgoing International call to SIP trunk **
 destination-pattern 9011T
 session protocol sipv2
```

© 2008 Cisco Systems, Inc. All rights reserved.

```
 session target sip-server
 dtmf-relay rtp-nte
 no vad
!
dial-peer voice 11004 voip
 corlist outgoing call-local
 description ** 911/411 call to SIP trunk **
 destination-pattern 9[2-9]11
 session protocol sipv2
 session target sip-server
 dtmf-relay rtp-nte
 no vad
```

4.4.9 Adding a secondary or backup server for call routing & registration

For redundancy purposes, the SP may require a backup registrar server or proxy server for SIP calls in case the primary server(s) goes down.

4.4.9.1 Adding backup registrar server for SIP registration

For certain scenarios, the provider may have a backup SIP registrar server – below is an example of adding a backup server with IP address 10.1.100.253.

```
sip-ua
  registrar ipv4:10.1.100.253 secondary
```

4.4.9.2 Adding backup proxy server for inbound / outbound calls:

This implies duplicating the outbound dial-plan on the UC500 via dial-peers. This is similar to section 4.4.8 and will not repeat all the config here. The key addition would be to create new dial-peers (new tags) pointing to the backup proxy server (in the example below it is 10.1.100.253):

```
dial-peer voice 12001 voip
 corlist outgoing call-local
 description ** Outgoing Local call to SIP trunk **
 destination-pattern 9[2-9].....
 session target ipv4:10.1.100.253
 dtmf-relay rtp-nte
 no vad
```

4.4.10 Registration of Multiple DID numbers with unique credentials

There may be a requirement to register all DID numbers for a UC520 to the SP instead of the parent – child registration method. This is possible on the UC520 and also allows for unique credentials (username, password, realm) per DID. Below is an example for this:

```
sip-ua
   registrar ipv4:10.1.100.253
   credentials username 4085551201 password 123 realm Cisco.com
   credentials username 4085551202 password 456 realm Cisco.com
   credentials username 4085551203 password 789 realm Cisco.com
```

© 2008 Cisco Systems, Inc. All rights reserved.

4.4.11 Changing RTP payload type for RFC2833 DTMF

The default RTP payload type for RFC2833 on the UC520 is 101. If this needs to be changed to something within the dynamic RTP payload type range (96 – 127), below is the CLI needed under each dial-peer (incoming & outbound) for the SIP trunk dial-peers.

```
dial-peer voice 11001 voip
 description ** Outgoing Local call to SIP trunk **
 dtmf-relay rtp-nte
 rtp payload-type nte 103
```

In case of certain payload types in this range that are already assigned to other functions on the UC520, you need to change the payload type for these functions first. Here is a list of payload types that are already pre configured:

Function	Payload type
cisco-codec-fax-ind	96
cisco-codec-fax-ack	97
nse	100
cisco-codec-ilbc	116
cisco-codec-gsmamrnb	117
cisco-codec-video-h263+	118
cisco-codec-video-h264	119
cisco-rtp-dtmf-relay	121
cisco-fax-relay	122
cisco-cas-payload	123
cisco-clear-channel	125

To change the preconfigured value – you need to follow the below example which requires RFC2833 (nte) to use payload type of 100 which is used by nse.

```
dial-peer voice 11001 voip
 description ** Outgoing Local call to SIP trunk **
 dtmf-relay rtp-nte
 rtp payload-type nse 104
 rtp payload-type nte 100
```

4.4.12 Changing transport information for SIP traffic

If the provider requires that SIP traffic be sent using TCP instead of the default UDP – this can be changed at the system level as below:

```
voice service voip
  sip
    transport session tcp
```

If the provider requires that SIP traffic be sent to a TCP or UDP port other than 5060 which is the default; this can be changed at a system level as below:

```
sip-ua
   sip-server ipv4:10.1.1.254:5065
```

If the provider requires that SIP traffic always be sourced from the UC520 using TCP or UDP port 5060, this can be changed at a system level as below:

© 2008 Cisco Systems, Inc. All rights reserved.

```
sip-ua
  connection-reuse
```

5 Troubleshooting

The most common issues with SIP trunking on the UC500 are misconfiguration errors. Some common issues are listed below along with the best practices for troubleshooting:

5.1 Best practices when troubleshooting the UC500:

There are essentially 3 ways in which to gather information – most times you would need a combination of all 3 methods to get to the root of the issue

a. Using show commands on CLI to check the configuration & status – these are non intrusive commands. Common examples would be:

show run **← configuration on UC500**
show version **← IOS software version on the UC500**

b. Using debugs commands on CLI to check message exchanges for active calls – these can be intrusive commands and care must be taken that these are run during a low number of calls in testing. Common example would be:

debug ccsip messages **← to look at SIP messages sent / received by the UC500**

To ensure the debugs do not cause a CPU hog and adversely affect the UC500 performance – a common set of CLI to add is as below:

```
UC500#config terminal
UC500#(config)logging console informational
UC500#(config)logging buffer 100000 debug
UC500#(config)service sequence-number
UC500#(config)service timestamp debug date msec
UC500#(config)end
```

Before you start a call – enable the debugs you need & clear the log:

```
UC500#clear log
Clear logging buffer [confirm]
```

To view debugs once the call has completed:

```
UC500#terminal length 0
UC500# show logging
```

c. Using other tools such as a network sniffer (http://www.ethereal.com) to look at the SIP message exchange is also extremely useful as it provides insight into the IP addressing piece as well.

5.2 Troubleshooting SIP registration issues over the SIP trunk

This applies if the SP requires SIP registration for certain numbers from the UC500.

- Show commands:

```
UC500#show sip-ua register status ← to check the registered numbers
Line         peer         expires(sec)  registered
============ ============ ============
4085552001   20006        1559          yes
```

© 2008 Cisco Systems, Inc. All rights reserved.

- Debug commands:

  debug ccsip message ← **to check the SIP Register message**

- Common areas to check:
  - Check ephone-dns / hunt groups / dialplan patterns / POTS dial peers to ensure registration of only required numbers is done
  - Make sure registrar server CLI under sip-ua is correct
  - Make sure the authentication CLI under sip-ua is correct
  - Make sure the registrar server can be reachable (especially if using DNS)

5.3 Troubleshooting SIP inbound or outbound calls on the UC500

If calls are not being able to be placed to / from the UC500 to the SIP – the below would be useful to look at:

- Show commands:

  show ephone registered ← **Ensure the SCCP phones are registered**

  show voip rtp connection ← **Check the RTP streams & IP address / port numbers**

  show sip-ua call ← **Check if the active SIP calls are up**

  show call active voice brief ← **Check if there are SIP & SCCP call legs up**

- Debug commands:

  debug ccsip message ← **for SIP messages in & out**

  debug voip ccapi inout ← **for generic IOS voice stack – dialpeers etc**

  debug voice translation ← **for IOS voice translation rules**

  debug ephone detail mac-address <mac of phone> ← **for SCCP phone**

  debug voip rtp session named-events ← **for RFC 2833 DTMF**

  debug sccp message ← **for Xcoder if that is involved in call flow**

- Common areas to check:
  - If no inbound or outbound calls are successful DNS resolution may not be working
    - From the CLI, attempt to ping the DNS
    - Check “ip nameserver” addresses.
    - Make sure that “no ip domain-lookup” is NOT configured
  - If no inbound or outbound calls are successful DNS resolution may not be working or registration may have failed

© 2008 Cisco Systems, Inc. All rights reserved.

6 Test plan & verification

After configuring the above – the installer or integrator must make calls to ensure the configuration does work fine. If this is being used for testing to a specific SP (service provider), it is strongly recommended that a capture of the traces for various test cases be done. These traces can be sniffer traces got from the WAN port of the UC500 (using Wireshark software on a PC).

7 Technical Assistance

The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.

If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com. http://www.cisco.com/techsupport

8 Disclaimer:

This configuration guide is offered as a convenience only, and any specifications and information regarding the product in this guide are subject to change at any time. All statements, information, and recommendations in this guide are believed to be accurate at the time of publication but are presented without warranty of any kind, express or implied, and are provided “AS IS”. Users take full responsibility for the application of the specifications and information in this guide. In no event shall Cisco or its suppliers be liable for any indirect, special, consequential, or incidental damages, including, without limitation, lost profits or loss or damage arising out of the use or inability to use this guide, even if Cisco or its suppliers have been advised of the possibility of such damage.

© 2008 Cisco Systems, Inc. All rights reserved.