Cisco Unified Communications 500 Series SIP Trunking

Configuration Guide for AT&T IP Flexible Reach Service

April 23, 2008
Version 1.2

Contents

1. Overview

1.1 Introduction

This document details how to install and operate the Cisco® Unified Communications 500 Series for Small Business (Cisco Unified 500 Series) with the AT&T IP Flexible Reach SIP trunking service.

1.2 Scope

This guide describes how to configure the Cisco Unified 500 Series, using the Cisco Configuration Assistant and the command-line interface, to support the AT&T IP Flexible Reach Service. It provides an example configuration that you must adapt to the parameters appropriate for your system.

General IP PBX administration is not covered here and should be completed before you configure AT&T IP Flexible Reach.

Note: The actual AT&T border element IP addresses will be provided by AT&T Customer Care. Please contact your Customer Care representative for the AT&T IP border element IP addresses for your specific Cisco Unified 500 Series configuration.

1.3 Special Notes

Emergency 911/E911 Services Limitations

The AT&T IP Flexible Reach Service supports E911/911 calling capabilities in certain circumstances. There are significant limitations on how these capabilities are delivered. Please review the AT&T IP Flexible Reach Service Guide in detail to understand these limitations and restrictions.

Calling Number Restricted / Privacy Not Supported

For calls from the Cisco Unified 500 Series to AT&T, the calling party number cannot be marked as restricted. This function is not supported.

1.4 Revision

Please send any suggestions related to this document to uc500-att-ccg@external.cisco.com

2. Cisco Unified 500 Series SIP Trunking Overview

2.1 Product Description

The Cisco Unified 500 Series is a purpose-built appliance for small and medium-sized businesses that provides IP PBX, voicemail, switching, VPN, firewall, and optional wireless capability. The IP PBX and voicemail features are based on Cisco Unified Communications Manager Express and Cisco Unity® Express. The switching, VPN, firewall, and wireless are based on Cisco IOS® Software features, while management is provided via the Cisco Configuration Assistant tool.

The Cisco Unified 500 Series provides the following:

- Cost-effective, converged data and voice solution in an appliance
- Key system/small PBX features plus innovative convergence applications
- Intuitive GUI for easy installation, adds, moves, and changes
- Firewall and VPN support, based on U.S. Department of Defense certified Cisco IOS Firewall technologies
- Optional integrated wireless LAN support for mobility, with the ability to extend wireless coverage

  The Cisco Unified 500 Series offers voicemail and automated attendant capabilities for IP and analog phone users. These features are fully integrated into the appliance.

2.2 Cisco Unified 500 Series SIP Trunk Qualification and Templates

The main focus of this document is to provide a defined configuration template for the Cisco Unified 500 Series and a validated configuration that enables communication between the Cisco Unified 500 Series and the AT&T IP Flexible Reach Service.

2.3 Managed Access Router

The AT&T IP Flexible Reach Service provides a well-defined demarcation point with a Cisco integrated services router that is managed by AT&T and provides network access services for IP voice and data traffic. The managed access router provides:

- Network Address Translation application-layer gateway (NAT ALG) capability
- Quality of service (QoS) for Session Initiation Protocol (SIP) trunk calls and service-level agreement (SLA) guarantees
- WAN conversion to Ethernet on the Cisco Unified 500 Series
- Well-defined point of troubleshooting for AT&T and the customer

Any other equipment on the customer premise, including IP PBXs, is the responsibility of the customer and a supporting VAR. The templates that result from the testing efforts, particularly with respect to LAN topology, are tested recommendations that are subject to VAR and customer requirements. The only exceptions to this are required Cisco Unified 500 Series SIP trunking parameters that must be configured for the AT&T IP Flexible Reach Service.

2.4 Supported Line-Side Protocols

Although the Cisco Unified 500 Series can also support SIP on the line side to SIP phones, this document does not address such configurations. Future versions of the Cisco Unified 500 Series templates will support this capability.

At present, the Cisco Unified 500 Series acts as a SIP user agent between the SIP trunk to the service provider call agent and Cisco Unified IP Phones running Skinny Client Control Protocol (SCCP) images.

2.5 Security

Techniques for securing IP telephony installations such as the Cisco Unified 500 Series are beyond the scope of this document. Security is an area in which VARs may provide additional value to customers. The Cisco IOS Firewall, for example, can be configured on the Cisco Unified 500 Series to enable the appropriate access lists and other elements of the firewall. See step 8 in section 4.2 for more information.

The Cisco IOS Software cryptographic image may also be configured to enable Secure Shell (SSH) and HTTPS Secure Sockets Layer (SSL) access to the Cisco Unified 500 Series management interfaces. Administrative access to the management interfaces may also be configured through the use of local usernames and passwords, privilege levels, and the use of authentication, authorization, and accounting (AAA) servers such as Cisco's Secure Access Control Server (ACS), which provides RADIUS and TACACS+ services. This configuration can be performed by the VAR or end customer with the Cisco Configuration Assistant.

The Cisco Unified 500 Series templates also include Class of Restrictions (COR) to enable access control for different classes of users. International calling, for example, may be restricted to specific phones.

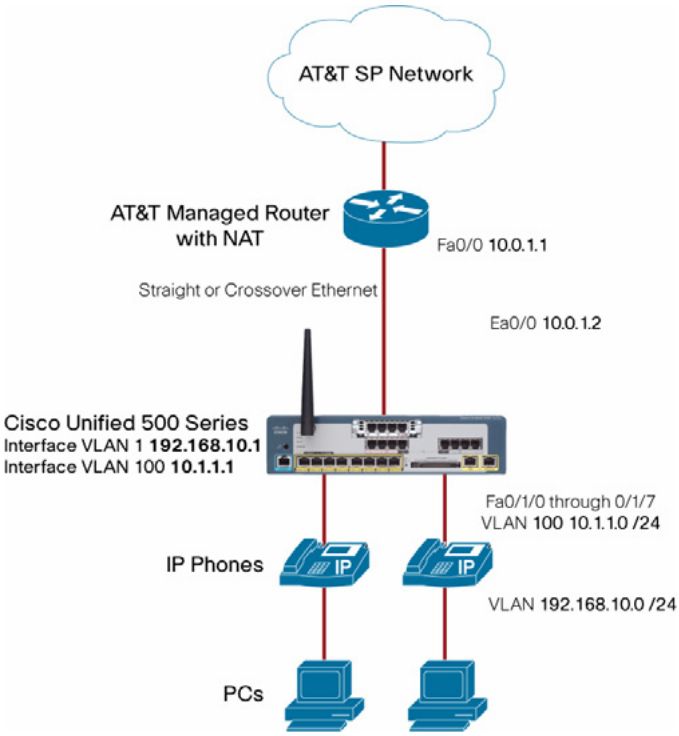
Care should be taken to avoid disabling call control, voicemail, and phone features when enabling security features manually. As an example, many security administrators will limit access to the HTTP server in Cisco IOS Software through the use of access control lists (ACLs). If those ACLs, however, inadvertently prevent IP phones from reaching the HTTP server embedded in the Cisco Unified 500 Series, features such as user directories and IP phone services will be disabled.

2.6 Topology for a Cisco Unified 500 Series Installation

There are several ways in which a Cisco Unified 500 Series system can be integrated into a LAN. AT&T provides a managed access router that is not modified for customer premises equipment (CPE) scenarios. This router provides a SIP NAT ALG and NAT router for local private network addressing, but it does not participate in local routing decisions for subnets and VLANs defined by the end customer or VAR. This enables AT&T to provide a reliable, consistent, and supportable configuration for the router that works across a wide customer base.

Figure 1 depicts the topology used in this guide.

Figure 1. Topology Used in This Guide



In this topology, the Cisco Unified 500 Series is placed inline between the managed access router and CPE devices, including IP phones and personal computers. The Cisco Unified 500 Series becomes the default gateway, Trivial File Transfer Protocol (TFTP), and Dynamic Host Configuration Protocol (DHCP) server for the phones and PCs. Requirements for this configuration include:

- A Layer 2 Ethernet switch, a straight-through cable, or a crossover cable between the managed access router and the Cisco Unified 500 Series
- Cisco Unified 500 Series appliance
- Cisco Unified IP Phones
- Analog phones or other devices such as fax machines

This template for a LAN topology also supports running the Cisco IOS Firewall feature set on the Cisco Unified 500 Series platform. See the example in step 8 of section 4.2.

Considerations for this topology example include the following:

- The WAN segment between the managed access router and the Cisco Unified 500 Series is assumed to be in the 10.100.101.0/24 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 Cisco Unified 500 Series WAN interface and routing configuration.
- 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.
- Inline power support for the IP phones is provided by the Cisco Unified 500 Series.
- The Cisco Unified 500 Series 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.

3. Requirements

3.1 Hardware Requirements

Required hardware consists of the Cisco Unified 500 Series appliance, Unified 500 Series companion switches, supported Cisco IP phones, and the AT&T IP Flexible Reach Service managed access router.

An uninterruptible power supply (UPS) is strongly recommended for the Cisco Unified 500 Series, which runs a Linux OS in the embedded Cisco Unity Express module. The Cisco Unity Express appliance is fairly robust but nevertheless involves a spinning hard disk drive that is subject to errors in the event of sudden power loss.

3.2 Software Requirements for Compatibility with the AT&T IP Flexible Reach Service

Table 1 lists the **supported** software releases and versions for the various components of the Cisco Unified 500 Series and the Cisco Smart Business Communication System (SBCS):

Table 1. Supported Software Releases

SBCS Release	Cisco Unified 500 Series Software Package	Cisco Configuration Assistant version	Cisco Unity Express release	Unified 500 Series Cisco IOS Software release	Comments
1.0	4.2.5	1.5	2.3.4	124-11.XW5	Minimum
1.1	4.2.6	1.5(1)	2.3.4	124-11.XW6	
1.2	4.2.7	1.6(0)	3.0.3	124-11.XW7	
1.2	4.2.8	1.7(0)	3.0.3	124-11.XW8	
1.3	4.2.9	1.8(0)	3.2.1	124-11.XW9	

Note: Other combinations may work but have not been tested and certified. This document will be updated as new Cisco SBCS releases are supported for AT&T IP Flexible Reach.

For a list of supported software, firmware, locales, and languages for the Cisco Unified Communications 500 Series UC520-4.2(0), visit http://supportwiki.cisco.com/sbcs/.

4. Configuring the Cisco Unified 500 Series with Cisco Configuration Assistant

Use the Cisco Configuration Assistant to configure the Cisco Unified 500 Series for use with the AT&T IP Flexible Reach Service. Configuration Assistant release 1.5 or later creates the required Cisco IOS Software configuration to support this integration.

This guide documents the configuration tasks in the Configuration Assistant for AT&T IP Flexible Reach Service. The command-line interface (CLI) is used only to customize the template to address required configurations not supported in the current Configuration Assistant release.

4.1 Installation

Please refer to the “Getting Started Guide” located at http://www.cisco.com/en/US/products/ps7293/products_getting_started_guide09186a00808c2b57.html for instructions for physically connecting the Cisco Unified 500 Series ports. Briefly, the procedure is as follows:

- Connect the WAN port to the same Ethernet segment as the inside interface of the managed access router. This can be accomplished either with a crossover cable, straight through, or with a LAN switch.

- Connect IP phones to the Fast Ethernet ports on the front of the Cisco Unified 500 Series.
- PCs should generally be connected to the switch port on the phones.
- Any analog devices (such as fax machines) may be connected to the FXS ports on the Cisco Unified 500 Series.

* Cisco Unified 500 Series software (Cisco IOS Software), phone loads, and Cisco Unity Express releases are at http://www.cisco.com/cgi-bin/tablebuild.pl/UC500.
* For the Cisco Configuration Assistant, go to: http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=281010085.

Install the Configuration Assistant on a PC connected to one of the Fast Ethernet ports on the front of the Cisco Unified 500 Series. Make sure this PC is configured for DHCP to receive an IP address from the Cisco Unified 500 Series.

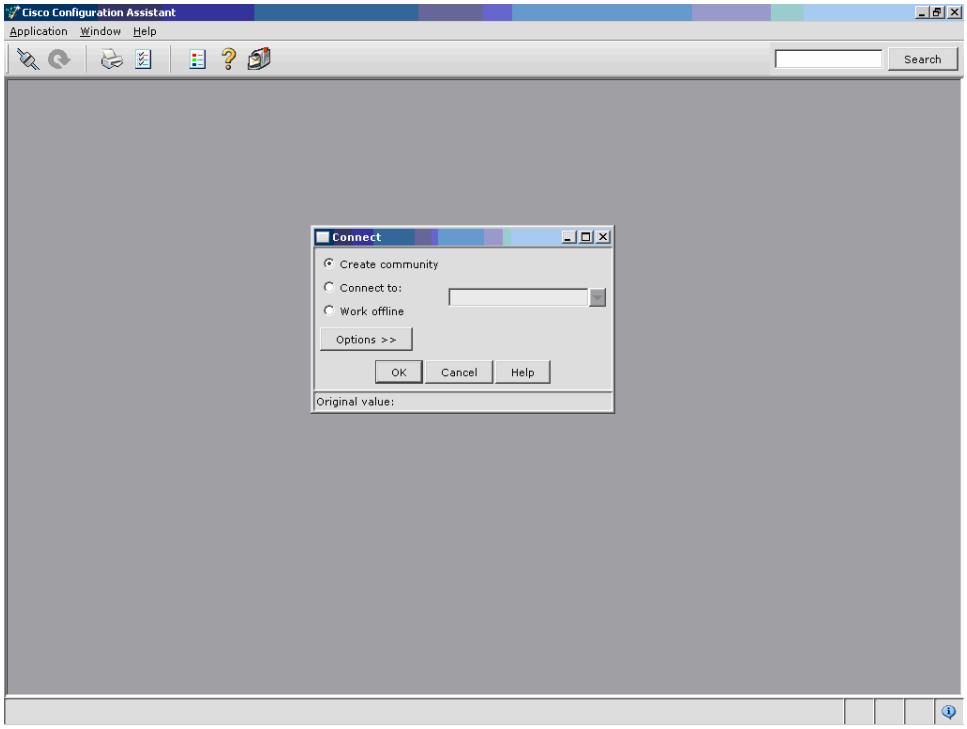
* These require a Cisco.com login.

4.2 Using the Configuration Assistant to Connect the Cisco Unified 500 Series with the AT&T IP Flexible Reach Service

These examples act as a guide for new Cisco Unified 500 Series installations. Proceed to step 7 if the Cisco Unified 500 Series is currently managed by Cisco Configuration Assistant release 1.5.

Step 1. Install and launch the Configuration Assistant on the workstation attached to a Cisco Unified 500 Series Fast Ethernet port. The Configuration Assistant displays a prompt to connect. Select **Create Community** and click **OK** to add this Cisco Unified 500 Series to a new community (Figure 2).

Figure 2. Configuration Assistant Connect Prompt



Step 2. A new window will appear (Figure 3). Enter the following:

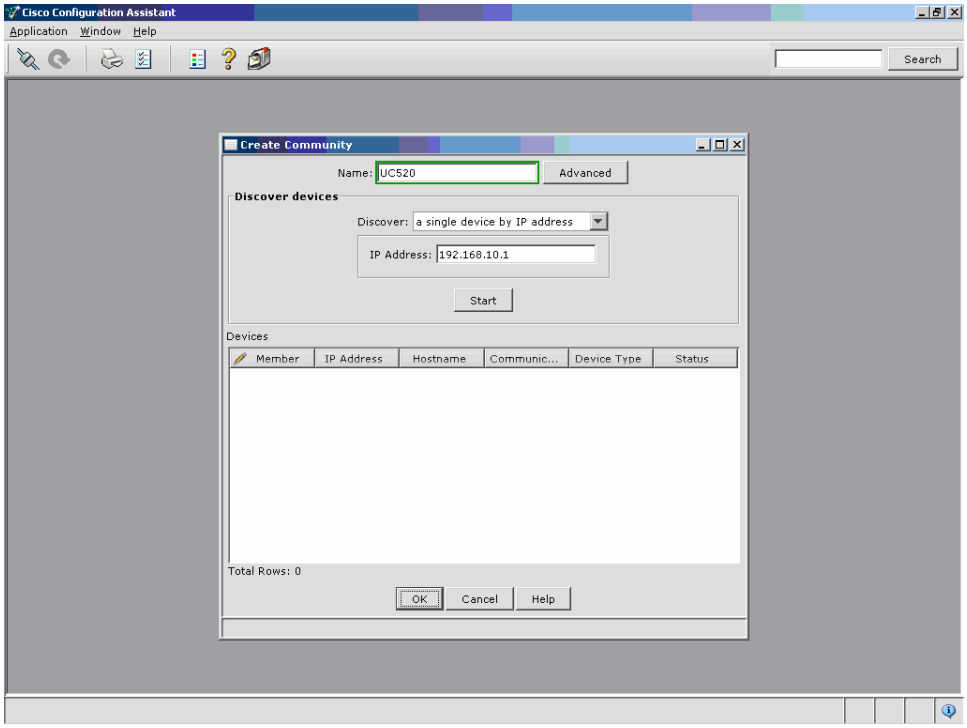
Name: Create the name you need for the community (usually the customer name).

Discover: Choose “a single device by IP address” from the drop-down menu.

IP address: Enter 192.168.10.1 (the default) or the current Cisco Unified 500 Series IP address.

Click **Start**.

Figure 3. Community Setup Dialog Box

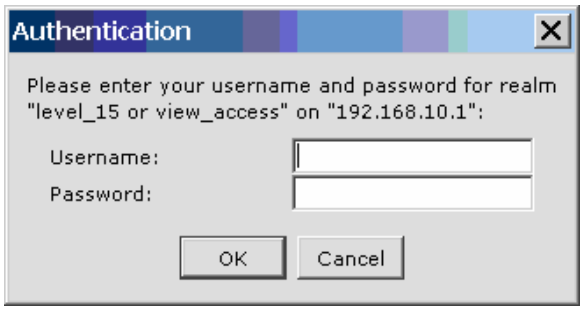


Step 3. An SSH certificate warning will appear (Figure 4).

Figure 4. SSH Certificate Warning

Select **Yes** or **Always** to continue to a login prompt (Figure 5).

Figure 5. Login Prompt



Enter the Cisco Unified 500 Series defaults or customer-specific entries.

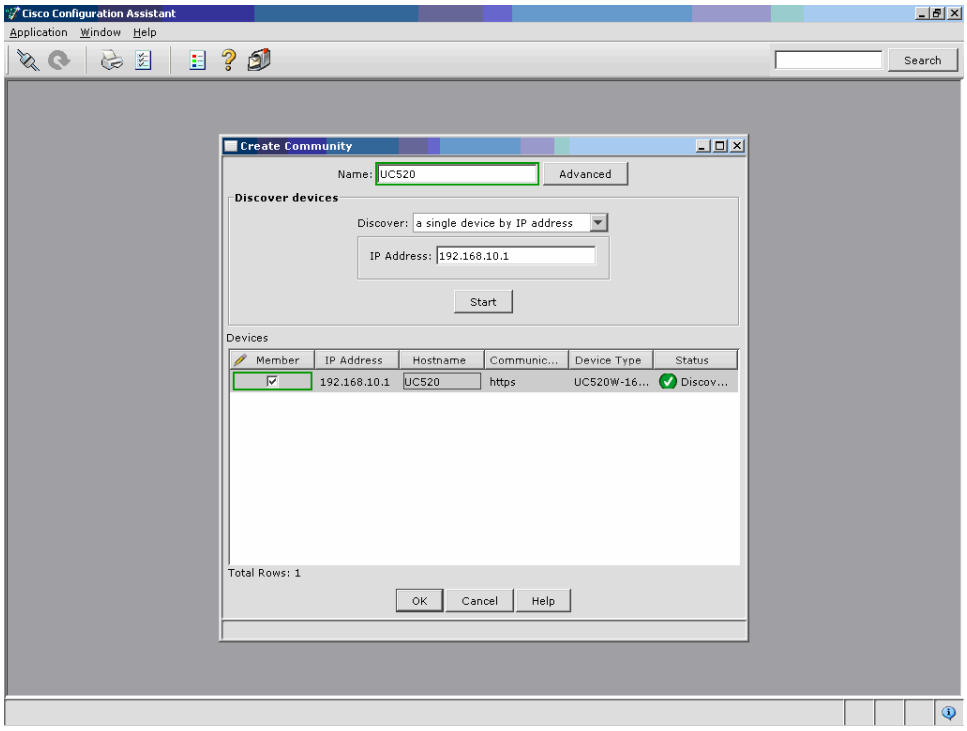
Username: cisco (default)

Password: cisco (default)

Click **OK**.

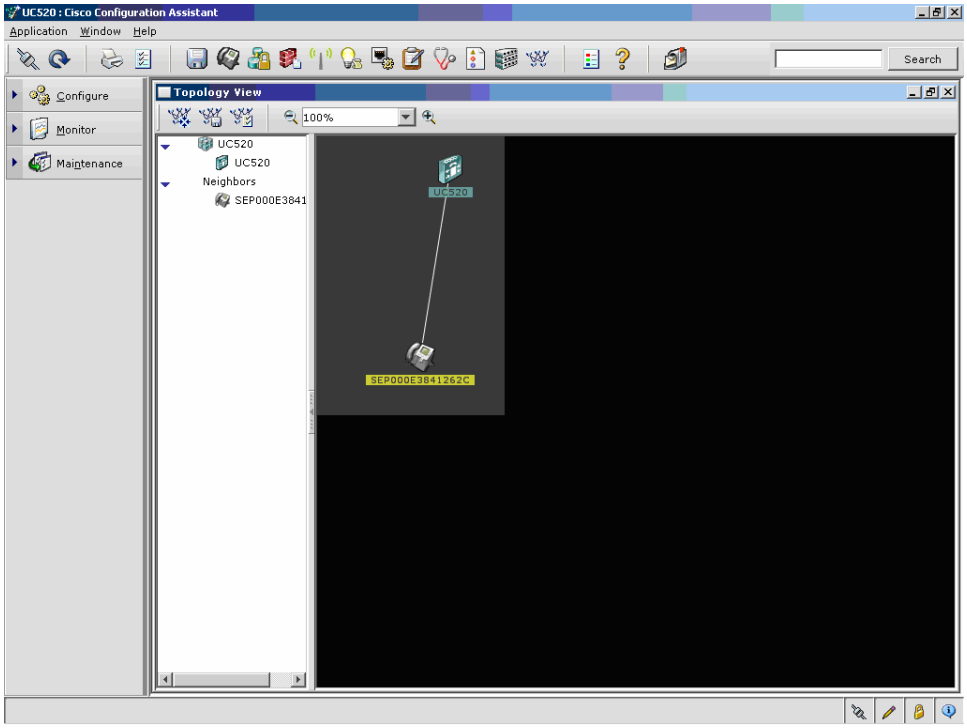
Step 4. An updated screen will now show the Cisco Unified 500 Series that was discovered. Select it and click **OK** (Figure 6).

Figure 6. Selecting the Cisco Unified 500 Series



Step 5. The Configuration Assistant will go through a network discovery process. This may take several minutes. It will then display a topology view showing all the connected devices, as shown in Figure 7.

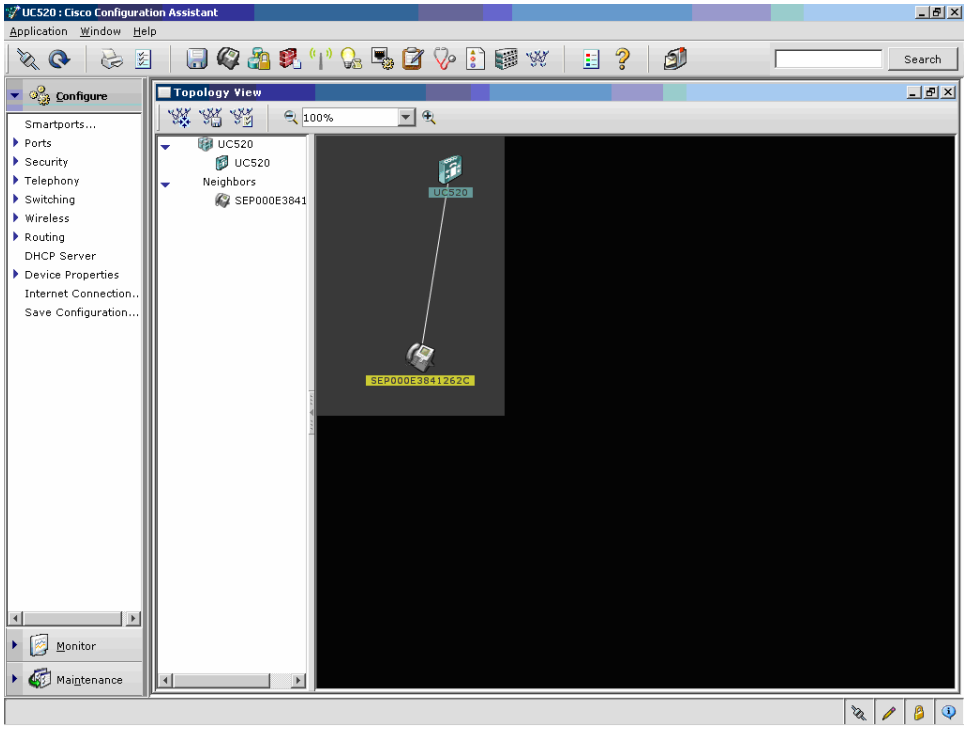
Figure 7. Topology View



In the example topology, a single phone is connected to the Cisco Unified 500 Series.

Step 6. To configure the Cisco Unified 500 Series, click Configure in the left pane. The Configuration Assistant screen will update to expand the configuration options available (Figure 8).

Figure 8. Left Pane Showing the Configure Options



These configuration elements may be modified or kept at their default values.

- **Smartports** configuration options allow you to change the data and voice VLAN assignments from the recommended defaults.
- **Ports** allows the assignment of static duplex and speed settings, power management, and enablement.
- **Security** allows the creation or modification of NAT, VPN server, and firewall options. This document will not address these options; they are discussed in the Cisco Unified 500 Series product documentation.
- **Telephony** is where the majority of the AT&T IP Flexible Reach configuration takes place. These options are addressed in the next section of this document.

Cisco recommends that VARs leave the Switching, Routing, Smartports, and Ports options at their default settings unless customer requirements dictate the addition of IP interfaces, VLANs, static routing decisions, or other changes.

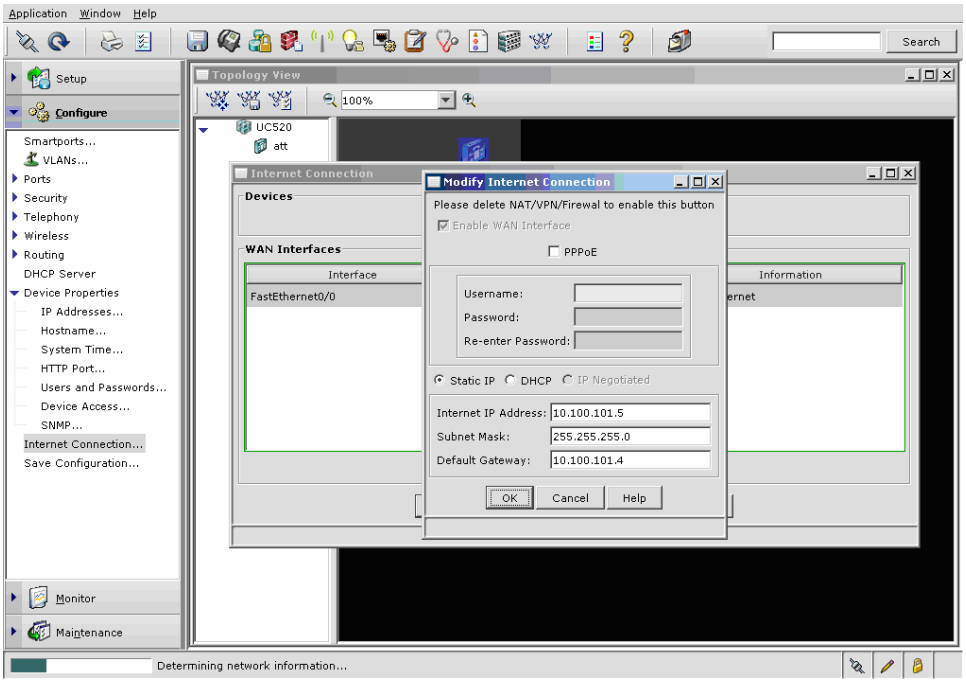
Step 7. The **Internet Connection** setting is a required configuration component for connecting to the AT&T IP Flexible Reach managed router. This is a ***mandatory*** step when using the Configuration Assistant to configure the Cisco Unified 500 Series for the AT&T IP Flexible Reach Service.

Click **Internet Connection** in the left pane to configure the WAN interface with the appropriate IP address option. The **Fast Ethernet 0/0** interface is used to connect the Cisco Unified 500 Series to the AT&T managed router.

Click the **Fast Ethernet 0/0** interface to highlight it in green, and then click the Modify button.

In this example (Figure 9), a **Static IP** is being used (10.100.101.5).

Figure 9. Internet Connection



Select **Static IP**.

Enter the required **Internet IP Address, Subnet Mask, and Default Gateway**.

Click **OK** in the **Modify Internet Connection** window to continue.

Click **OK** in the **Internet Connection** window.

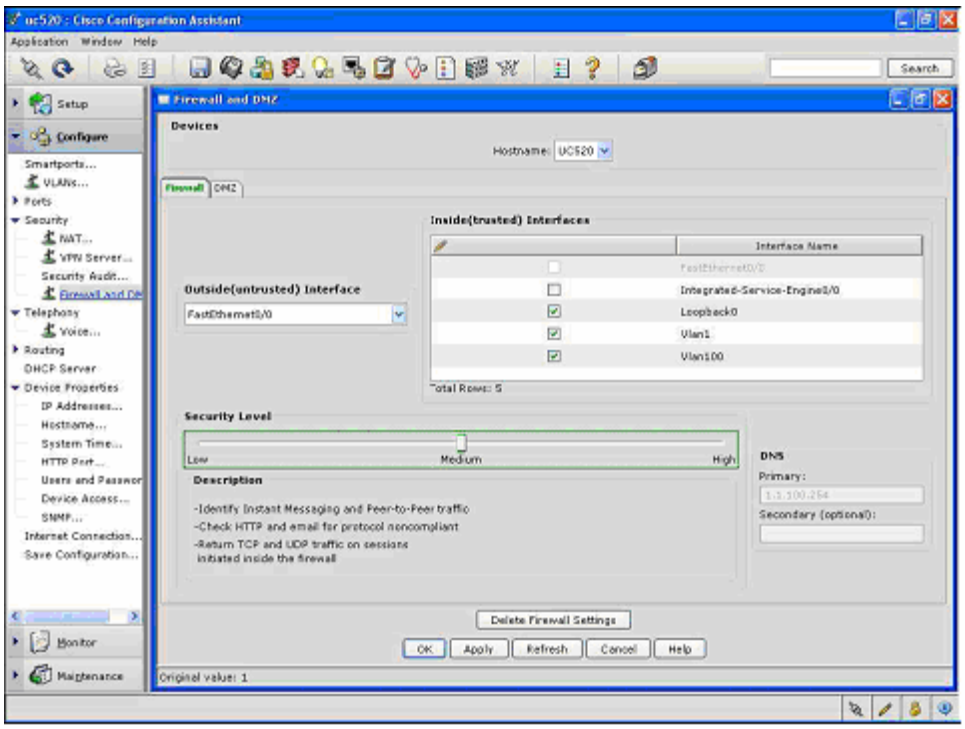
Step 8. The Cisco Unified 500 Series Firewall setting is not a requirement for connecting to the AT&T IP Flexible Reach Service. The Cisco Unified 500 Series Firewall is a tested component used to build this configuration template and can be set to customer preference.

If you do not plan to update the firewall settings, proceed to the next step.

Click **Security** in the left pane and select **Firewall and DMZ**. On the Firewall tab, the security level can be set to High, Medium, or Low (the default level) based on customer/VAR requirements.

In Figure 10, the firewall is set to the **Medium** security level.

Figure 10. Firewall Settings



Click **Apply** to apply the selected settings.

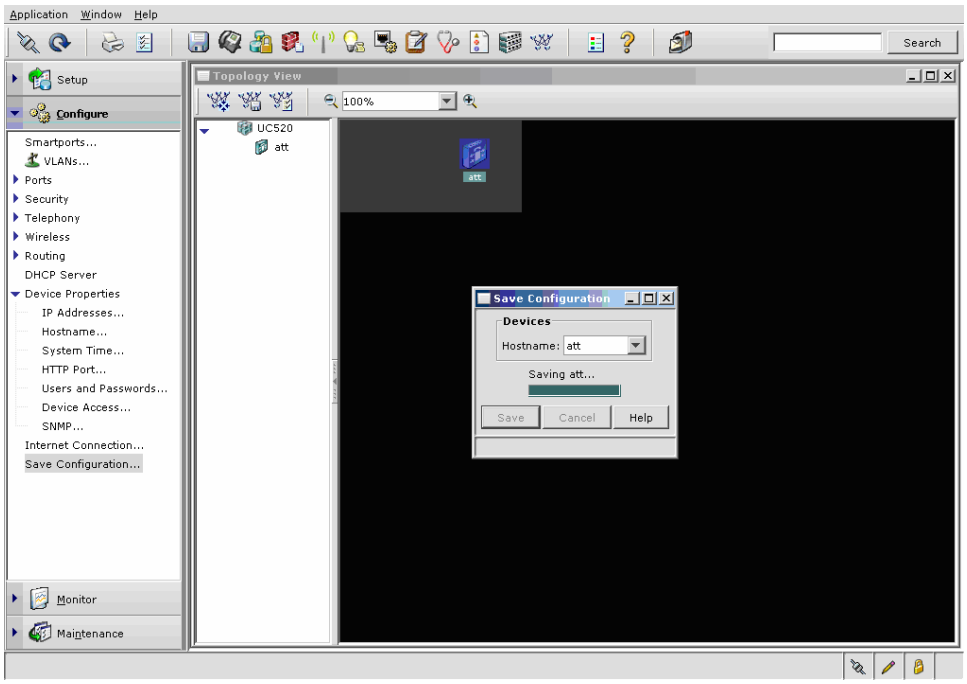
Click **OK**.

Step 9. At this point, saving the configuration of the Cisco Unified 500 Series is strongly recommended:

In the left pane, click **Save Configuration**. A **Devices** window pops up.

Select the correct **Hostname** from the drop-down menu and click **Save** (Figure 11).

Figure 11. Saving the Configuration



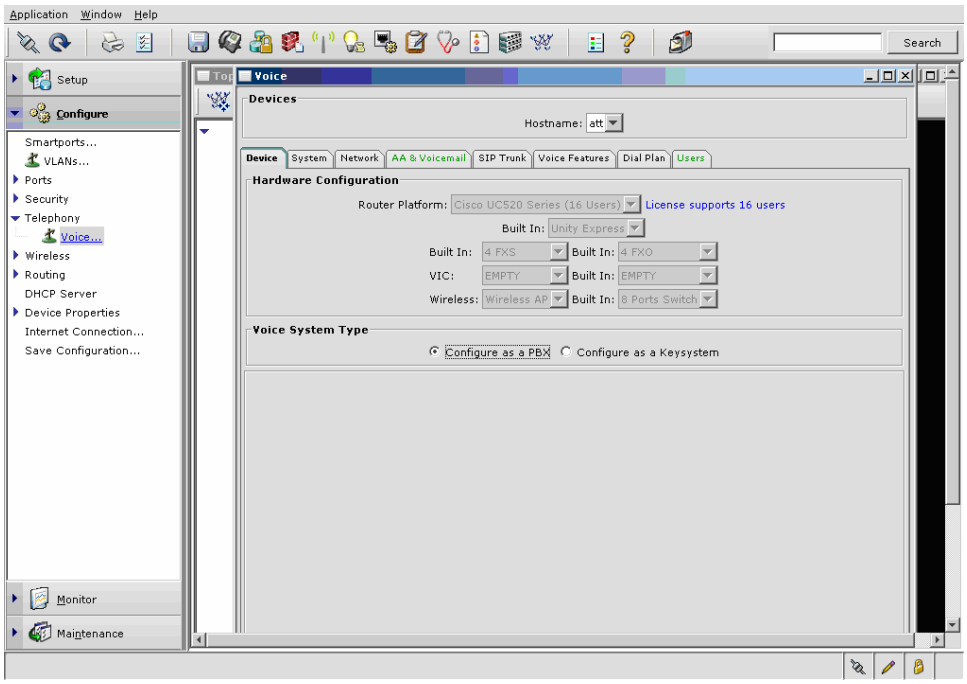
Step 10. Telephony Configuration for the AT&T IP Flexible Reach Service

Select **Telephony -> Voice** in the left pane of the Configuration Assistant screen. A **Voice** window appears, displaying the Device tab.

The **Device** tab provides Cisco Unified 500 Series platform and license information, the hardware installed, and the hostname (Figure 12).

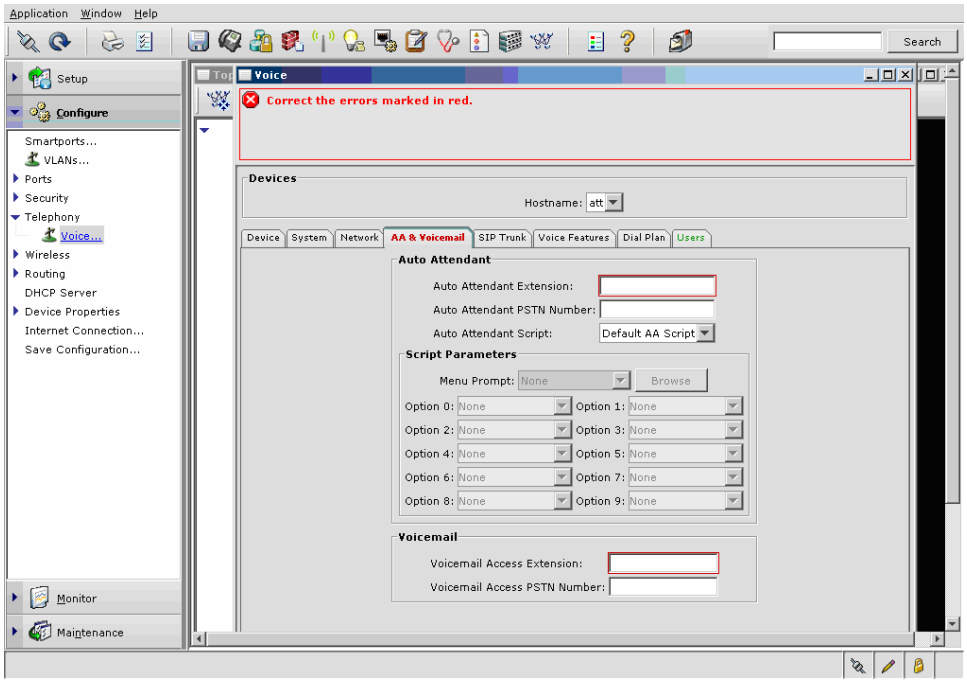
Make sure **Configure as a PBX** (the default) is selected as your Voice System Type for SIP trunking.

Figure 12. Device Parameters



Step 11. Select the **AA & Voicemail** tab on the right. The fields highlighted in red indicate mandatory entries (Figure 13).

Figure 13. AA & Voicemail Tab



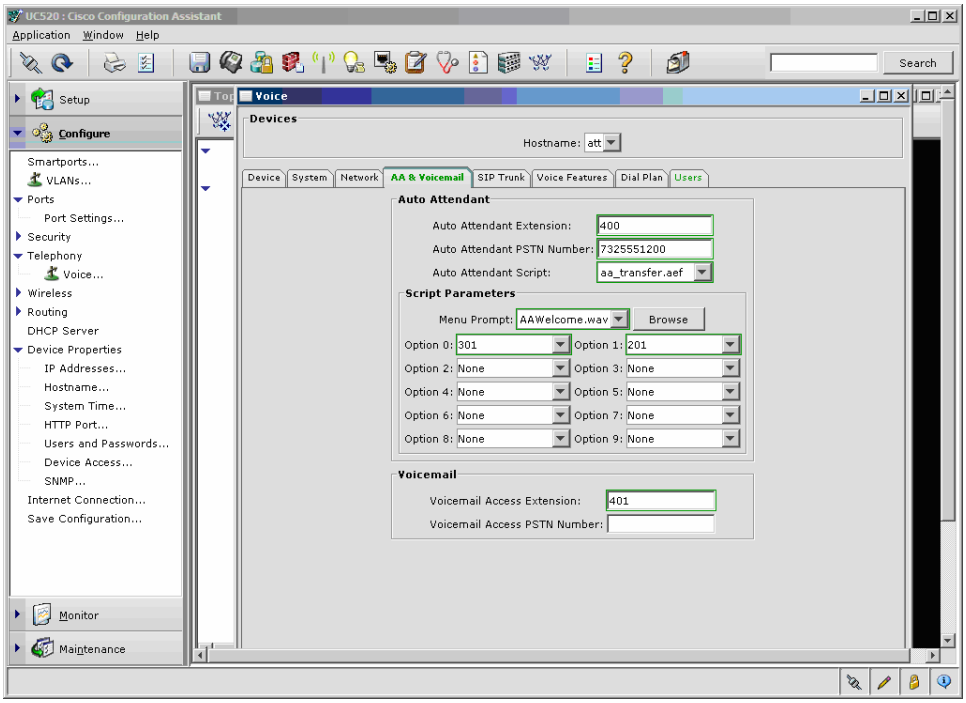
Complete the fields in the AA & Voicemail tab as required. Note that the number of digits in an extension must be the same as in all the other tabs to ensure consistent extension numbering.

The following settings have been used in this example (Figure 14):

- **Auto Attendant Extension:** 400
- **Auto Attendant PSTN number:** 7325551200
- **Auto Attendant Script:** Choose aa_transfer.aef.
- **Menu Prompt:** Choose AAWelcome.wav (or a customer-recorded prompt to upload).
- **Script Parameters:** These are not required for the AT&T IP Flexible Reach Service and can be adjusted by the customer or VAR.
- **Voicemail Access Extension:** 401
- **Voicemail Access Extension PSTN Number:** Left blank for this example.

The AA & Voicemail parameters can be changed to meet the requirements of the VAR/customer network.

Figure 14. Updated AA & Voicemail Tab



Do not click **OK** (scroll down to see this) until the entire Voice configuration is complete.

Step 12. Click the **SIP Trunk** tab and enter the required parameters.

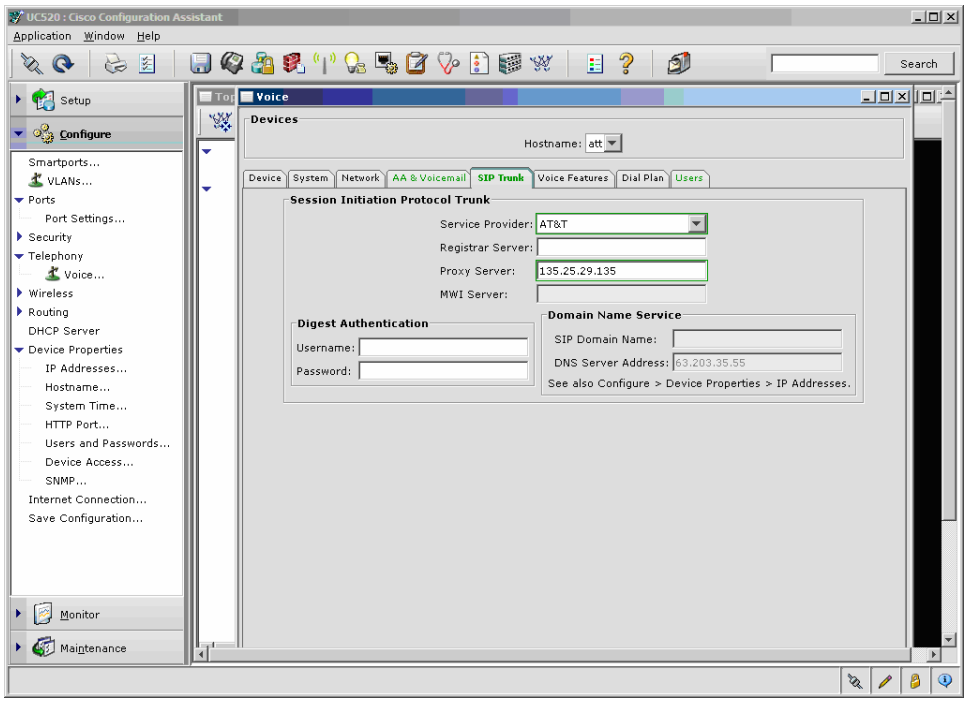
This tab relates specifically to the AT&T border element addresses used for call signaling.

The following settings have been used in this example (Figure 15):

- **Service Provider:** Choose AT&T from the drop-down menu.
- **Registrar Server:** Leave this field blank.

- **Proxy Server:** Enter the IP address of one of the border elements provided. AT&T provides two border element addresses. Section 4.3 of this guide describes how to configure the second border element address, via the command-line interface.
- **Digest Authentication:** Leave these fields blank.

Figure 15. SIP Trunk Tab



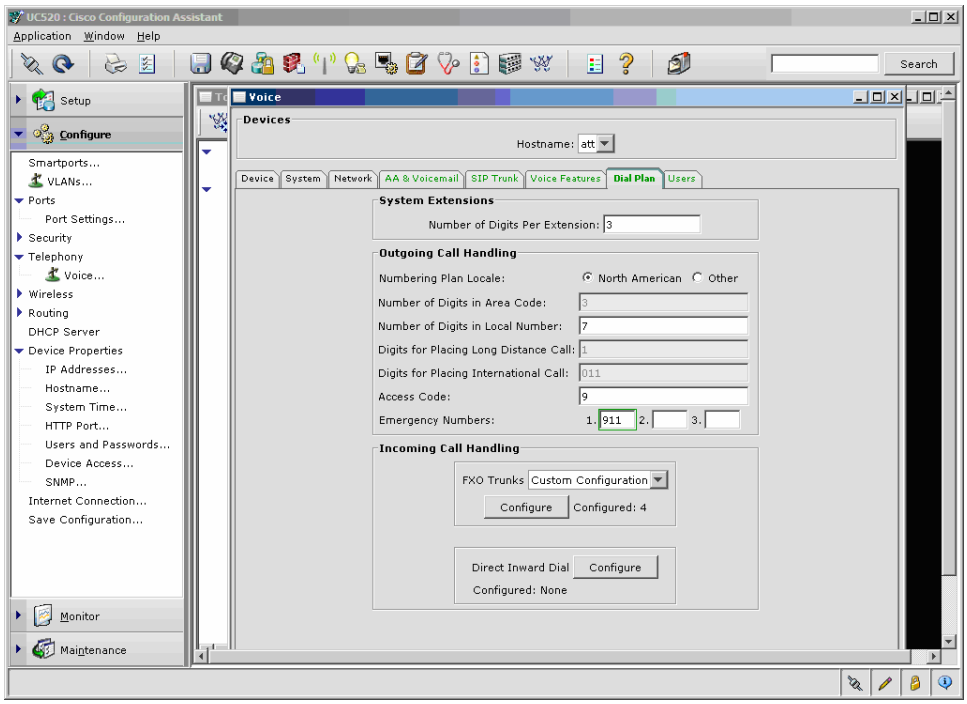
Do not click **OK** (scroll down to see this) until the entire Voice configuration is complete.

Step 13. Click on the **Dial Plan** tab to continue. This tab addresses systemwide features, such as the access code to dial outside, digits per extension, and incoming and outgoing call handling features. Parameters on this tab should be configured according to customer requirements.

The following settings have been used in this example (Figure 16):

- **Number of Digits per Extension:** 3
- **Numbering Plan Locale:** North American
- **Emergency Numbers:** 911

Figure 16. Dial Plan Tab



The FXO Trunks configuration is not required for AT&T IP Flexible Reach.

Do not click **OK** (scroll down to see this) until the entire Voice configuration is complete.

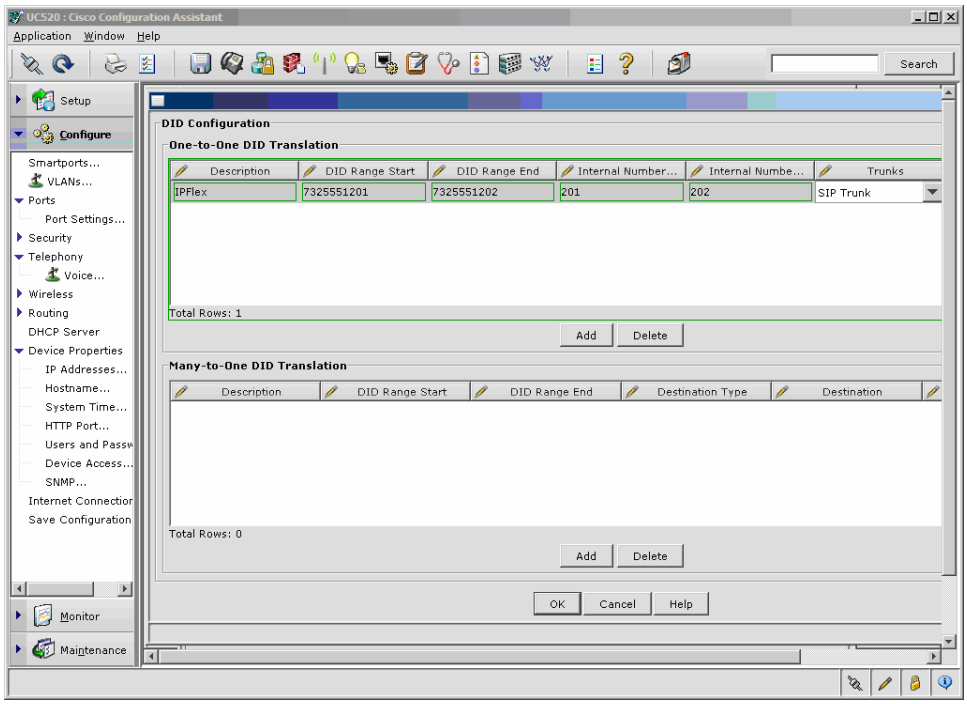
Step 14. Configure Direct Inward Dial as follows:

On the **Dial Plan** tab, select the **Direct Inward Dial Configure** button. A new **DID Configuration** pane opens. Select **Add** to create a new entry in the **One-to-One DID Translation** section. Click on the **New Entry** in **gray** to highlight it in **green**. Select each of the DID fields and fill them in as required.

In the example, we are configuring the DIDs for two extensions (Figure 17):

- **Description:** IPFlex
- **DID Range Start:** 732551201
- **DID Range End:** 732551202
- **Internal Number Extension Start:** 201 and End: 202
- **Trunks:** SIP Trunk selected from the pull-down menu.
- **Caller ID:** Leave unchecked; this implies that the caller ID for all outbound calls will be the automated attendant PSTN number. If a unique caller ID for every DID is a requirement, check this box. Consult **Appendix A** for caller ID guidelines.

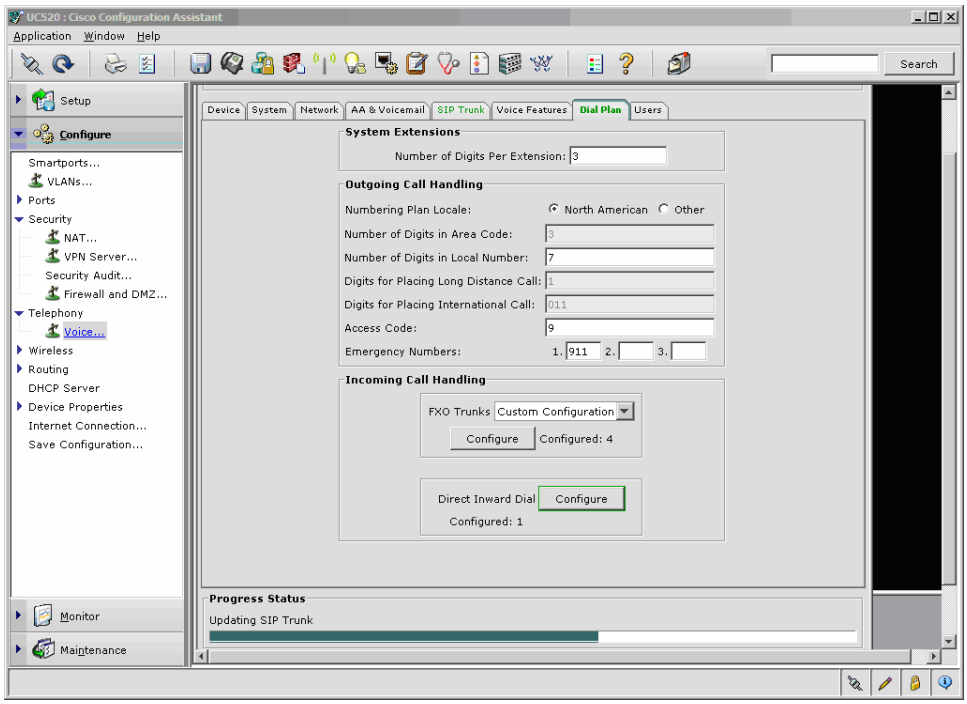
Figure 17. Direct Inward Dial



Select **OK** in the DID Configuration pane. You will return the Dial Plan tab.

Step 15. Click **Apply** at the bottom of the **Dial Plan** tab. A **Progress Status** bar appears at the bottom of the right pane, showing the various stages of the configuration as it is being loaded (Figure 18). (Scroll down if you cannot see this bar.)

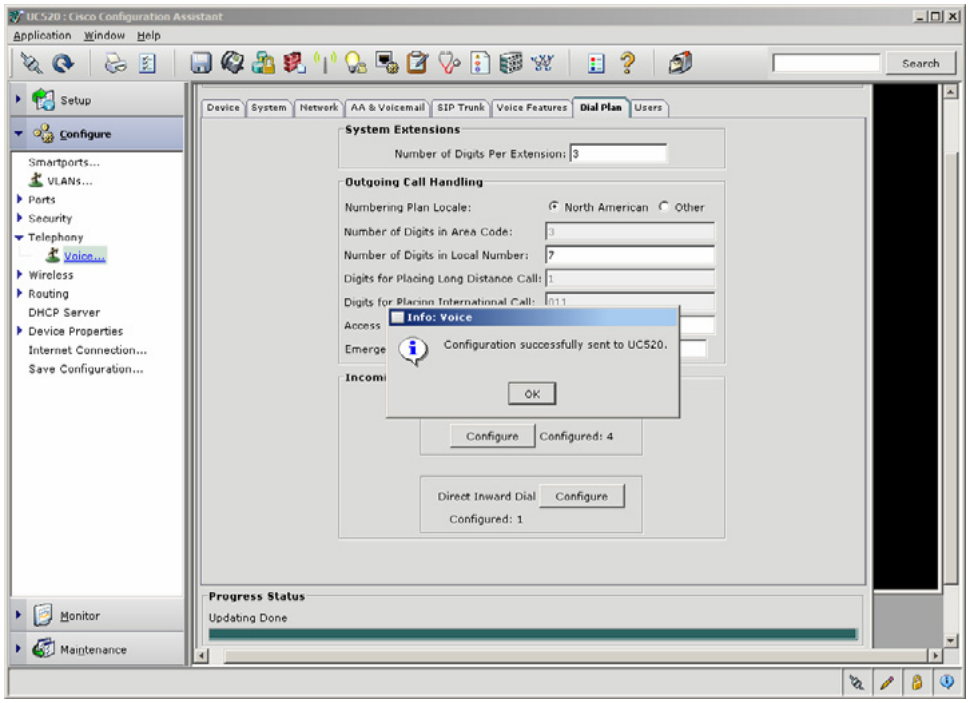
Figure 18. Applying the Configuration



The settings on the User tab are not required for connecting to the AT&T IP Flexible Reach Service.

A **Configuration Successfully Sent** message will appear, indicating that the Configuration Assistant has built the configuration and downloaded it to the Cisco Unified 500 Series (Figure 19).

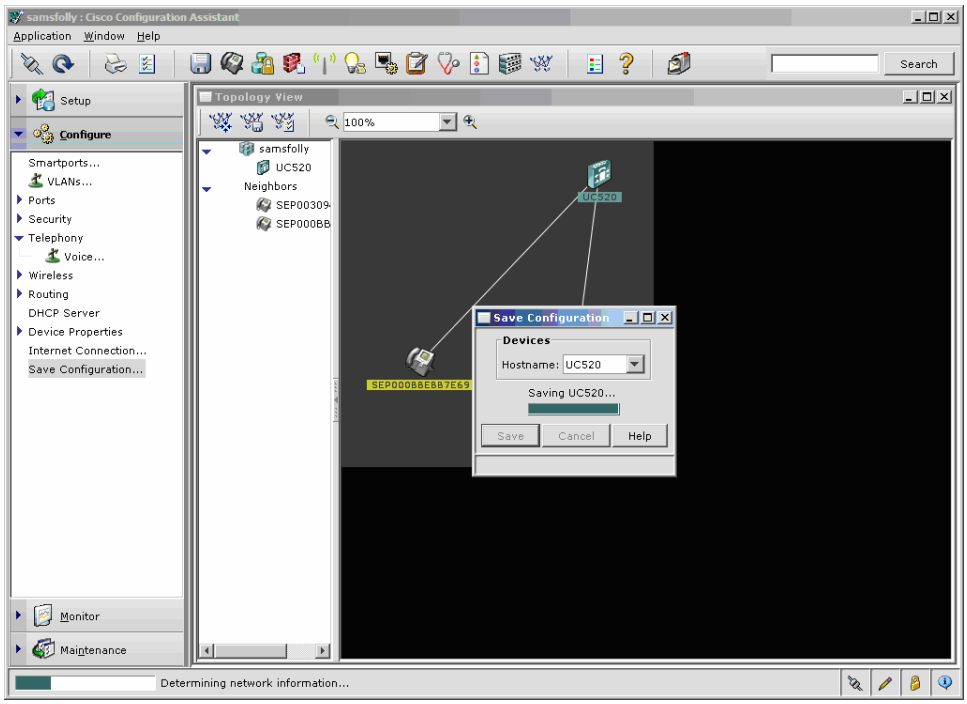
Figure 19. Configuration Successfully Sent Message



Click **OK**.

Step 16. Although the configuration has been applied and is running, it will not survive a reload. To ensure that the configuration is saved to NVRAM, click **Save Configuration** on the left, then select the **Hostname** and click **Save**, as shown previously in step 9 (Figure 20).

Figure 20. Saving the Configuration



This completes the Configuration Assistant release 1.5 configuration of the Cisco Unified 500 Series SIP trunking portion. Proceed to section 4.3 for the appropriate command-line changes.

4.3 Adding a Secondary AT&T Border Element Address

This section covers the commands used to add the secondary AT&T border element address to the Cisco Unified 500 Series configuration for the AT&T IP Flexible Reach Service. The administrator should be familiar with console access, the Cisco IOS Software command-line interface (CLI), and the required passwords. Consult the AT&T VTQ for the secondary border element address needed in this step.

Step 1. Access the Cisco Unified 500 Series via the CLI:

Open a console, SSH, or Telnet session to 192.168.10.1 or the required IP address (using an application such as Putty from the same PC that the Configuration Assistant was launched from). The username and password are the same as those configured earlier. Once you are logged in, follow the standard Cisco IOS Software CLI configuration command procedure.

Step 2. The following example creates redundant dial peers, as required to signal the secondary AT&T border element address. The dial peers referenced are renamed copies created during the configuration of the Cisco Unified 500 Series using the Configuration Assistant. Dial peers 1001 through 1007 and 1050 (fax) are used for this example, with **preference 1** added. This example does not cover all implementations; other dial-peer configurations may be necessary.

Highlight the dial peers 10001 through 10007 and 10050 (fax), and copy and paste to a document editor.

Maintain or edit the **dial-peer tags (10001-10007, 10050)** as required by the customer or VAR.

Edit the **session-target ipv4:x.x.x.x,** using the secondary AT&T border element address.

Highlight the **updated** dial peers, and cut and paste them to the Cisco Unified 500 Series Telnet session in config mode.

Verify the dial-peer configuration changes with the **sh dial-peer voice sum** command.

Step 3. Issue the **write mem** command to save the updated configuration.

```
dial-peer voice 10001 voip
 corlist outgoing call-local
 description ** Outgoing call to SIP trunk (AT&T) – BE 2 **
 translation-profile outgoing PSTN_Outgoing
 preference 1
 destination-pattern 9[2-9].....
 rtp payload-type cisco-codec-fax-ind 98
 voice-class codec 1
 session protocol sipv2
 session target ipv4:x.x.x.x
 dtmf-relay rtp-nte
 ip qos dscp cs5 media
 ip qos dscp cs4 signaling
 no vad
 !
dial-peer voice 10002 voip
 corlist outgoing call-domestic
 description ** Outgoing call to SIP trunk (AT&T) – BE 2 **
 translation-profile outgoing PSTN_Outgoing
 preference 1
 destination-pattern 91[2-9]..[2-9].....
 rtp payload-type cisco-codec-fax-ind 98
 voice-class codec 1
 session protocol sipv2
 session target ipv4:x.x.x.x
 dtmf-relay rtp-nte
 ip qos dscp cs5 media
 ip qos dscp cs4 signaling
 no vad
!
dial-peer voice 10003 voip
 corlist outgoing call-international
 description ** Outgoing call to SIP trunk (AT&T) – BE 2 **
 translation-profile outgoing PSTN_Outgoing
 preference 1
 destination-pattern 9011T
 rtp payload-type cisco-codec-fax-ind 98
```

```
 voice-class codec 1
 session protocol sipv2
 session target ipv4: x.x.x.x
 dtmf-relay rtp-nte
 ip qos dscp cs5 media
 ip qos dscp cs4 signaling
 no vad
!
dial-peer voice 10004 voip
 corlist outgoing call-local
 description ** 911/411 call to SIP trunk (AT&T) – BE 2 **
 translation-profile outgoing PSTN_Outgoing
 preference 1
 destination-pattern 9[2-9]11
 rtp payload-type cisco-codec-fax-ind 98
 voice-class codec 1
 session protocol sipv2
 session target ipv4: x.x.x.x
 dtmf-relay rtp-nte
 ip qos dscp cs5 media
 ip qos dscp cs4 signaling
 no vad
!
dial-peer voice 10005 voip
 corlist outgoing call-local
 description ** star code to SIP trunk – BE 2**
 preference 1
 destination-pattern *..
 rtp payload-type cisco-codec-fax-ind 98
 voice-class codec 1
 session protocol sipv2
 session target ipv4: x.x.x.x
 dtmf-relay rtp-nte
 ip qos dscp cs5 media
 ip qos dscp cs4 signaling
 no vad
!
dial-peer voice 10006 voip
 description ** Emergency outgoing call to SIP trunk– BE 2 **
 preference 1
 translation-profile outgoing CALLER_ID_TRANSLATION_PROFILE
 destination-pattern 911
 rtp payload-type cisco-codec-fax-ind 98
 voice-class codec 1
 session protocol sipv2
 session target ipv4: x.x.x.x
 dtmf-relay rtp-nte
```

```
 ip qos dscp cs5 media
 ip qos dscp cs4 signaling
 no vad
!
dial-peer voice 10007 voip
 corlist outgoing call-local
 description ** star code to SIP trunk– BE 2 **
 preference 1
 destination-pattern *..
 rtp payload-type cisco-codec-fax-ind 98
 voice-class codec 1
 session protocol sipv2
 session target ipv4: x.x.x.x
 dtmf-relay rtp-nte
 ip qos dscp cs5 media
 ip qos dscp cs4 signaling
 no vad
!
dial-peer voice 10050 voip
 corlist outgoing call-fax
 description ** Outgoing fax call to SIP trunk– BE 2 **
 preference 1
 translation-profile outgoing PSTN_Outgoing
 answer-address 301
 destination-pattern 9T
 rtp payload-type cisco-codec-fax-ind 98
 session protocol sipv2
 session target ipv4: x.x.x.x
 dtmf-relay rtp-nte
 codec g711ulaw
 ip qos dscp cs5 media
 ip qos dscp cs4 signaling
 no vad
```

4.4 Editing the CLI Translation Rule for 4- to 10-Digit Mapping

Edit voice translation rule 1111 to match the following example, using the customer telephone number (TN). The example assumes that a 4-digit TN is 2754 and a 10-digit DID is 7325552754.

```
voice translation-rule 1111
 rule 15 /.*/ /7325552754/
```

CLI configuration of the Cisco Unified 500 Series for AT&T IP Flexible Reach is now complete.

5. Troubleshooting

The most common issues with SIP trunking on the Cisco Unified 500 Series are configuration errors. Some common issues are listed here, along with the best practices for troubleshooting these issues.

5.1 Best Practices When Troubleshooting the Cisco Unified 500 Series

There are essentially three ways in which to gather information. Most times you will need a combination of all three methods to get to the root of the issue.

- Use **show** commands in the CLI to check the configuration and status. These are nonintrusive commands. Common examples would be:

  `show run` ← **`configuration on the Cisco Unified 500 Series`**
  `show version` ← **`Cisco IOS Software version on the Cisco Unified 500 Series`**

- Use debug commands in the CLI to check message exchanges for active calls. These commands can be intrusive, and care must be taken that they are run during a low number of calls in testing. A common example would be:

  `debug ccsip messages` ← **`to look at SIP messages sent and received by the Cisco Unified 500 Series`**

To ensure that the debug commands do not adversely affect the performance of the Cisco Unified 500 Series, the following set of commands is commonly added:

```
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 debug commands you need and clear the log:

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

To view debug commands once the call has completed, use the following commands:

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

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

5.2 Troubleshooting SIP Inbound or Outbound calls on the Cisco Unified 500 Series

If calls cannot be placed to or from the Cisco Unified 500 Series to the SIP, the following are useful:

- Show commands:

  `show ephone registered` ← `Ensure that the SCCP phones are registered`

  `show voip rtp connection` ← `Check the RTP streams and IP address and port numbers`

  `show sip-ua call` ← `Check whether the active SIP calls are up`

  `show call active voice brief` ← `Check whether there are SIP and SCCP call legs up`

- Debug commands:

  `debug ccsip message` ← `For SIP messages in and out`

  `debug voip ccapi inout` ← `For generic Cisco IOS voice stack – dial peers, etc.`

  `debug voice translation` ← `For Cisco 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`

- Areas to check:
  - If no inbound or outbound calls are successful, DNS resolution may not be working or registration may have failed.

    From the CLI, attempt to ping the DNS.

    Check **ip nameserver** addresses.

    Make sure that **no ip domain-lookup** is not configured.

6. 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.

Appendix A

Cisco Configuration Assistant Release 1.5 Direct Inward Dial Rules and Guidelines

- One-to-one DID translation involves direct mapping between an external PSTN number and the internal extension.
- Many-to-one DID translation involves mapping multiple external PSTN numbers to a single internal extension (such as an operator).

The following are the rules for implementing caller ID in Cisco Configuration Assistant release 1.5:

1. If the caller ID box is checked and the last digits of the extension match those of the DID, the outbound number would be the DID.
2. If the caller ID box is checked and the last digits of the extension do not match those of the DID, an error is shown.
3. If the caller ID box is not checked, the outbound number would be the automated attendant.
4. For any internal extension without DID, the outbound number would be the automated attendant.

AT&T Virtual TNs and Nonvirtual TNs

A customer may receive one of two types of DIDs from AT&T: virtual TNs and nonvirtual TNs.

- A virtual TN is one that has a numbering plan area (NPA) that is different from the NPA at the customer site to which it is being routed. For a virtual TN, AT&T will pass 10 digits to the Cisco Unified 500 Series. For example, if a Cisco Unified 500 Series telephone is associated with a virtual TN, the number received from AT&T would be 10 digits (such as 732-216-2700).
- A nonvirtual TN has an NPA that is the same as that for the customer site. For a nonvirtual TN, AT&T will pass the phone extension plus some prefix if needed (typically a four-digit extension without a prefix). For example, if a Cisco Unified 500 Series telephone is associated with a nonvirtual TN, the number received from AT&T would be four digits (such as 2701 for the TN 908-216-2701).

However, when originating calls to AT&T, the calling party number must be a 10-digit number regardless of the type of TN associated with the phone that is originating the call. On the Cisco Unified 500 Series, a specific 10-digit AT&T TN will always be used as the calling number for calls made from the Cisco Unified 500 Series to AT&T.

Analog Fax Interfaces

FXS interfaces configured as anl(fax) are set to G.711 using Configuration Assistant release 1.5 and the AT&T SIP trunk.

Cisco Unified 500 Series Digital Signal Processor Support

Table 2. Using G.729 as the codec on the SIP Trunk

Cisco Unified 500 Series Model	Music on Hold Port	Voice (G.729)	T.38 Fax	Transcoding	HW Conferencing
8/16 user (PVDM2-32)	1	15	15	15	2 sessions (16 conferees)
32/48 user (PVDM2-64)	1	30	30	30	2 sessions (16 conferees)

Note: All values listed are the maximum for each function. You must mix and match to get the optimum number of calls that can be supported over the SIP trunk.

CLI Configuration Example

ftp://ftpeng.cisco.com/sbcs/doc/ATT-UC520-SIPTrunkcfg-Jun08.txt

This configuration guide is offered as a convenience only; 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.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C07-487479-00 08/08