XO® SIP Service
Customer Configuration Guide
for Cisco UC500 Series
Table of Contents

1 INTRODUCTION .............................................................................................................................................................4
  1.1 DOCUMENT SCOPE........................................................................................................................................................4
  1.2 TEKVIZION LABS ..........................................................................................................................................................4
  1.3 DEVICES UNDER TEST ..................................................................................................................................................5
  1.4 3RD PARTY COMPONENTS AND THEIR VERSIONS .......................................................................................................5
  1.5 PREREQUISITES.............................................................................................................................................................5
    1.5.1 Test Network Setup for Package-1.......................................................................................................................5

2 SIP TRUNKING AND CISCO UNIFIED COMMUNICATIONS 500 SERIES .................................................................6
  2.1 LIMITATIONS ................................................................................................................................................................7

3 UC520 CONFIGURATION CHECKLIST .............................................................................................................................7
  3.1 INSTALL CISCO CONFIGURATION ASSISTANT ...........................................................................................................8
  3.2 CONNECT ADMIN WORKSTATION TO UC520 .............................................................................................................11
  3.3 CREATE COMMUNITY .................................................................................................................................................12
  3.4 DEVICE SETUP WIZARD ..............................................................................................................................................17
  3.5 NTP SETUP.................................................................................................................................................................26
  3.6 VOICE CONFIGURATION – DEVICE TAB.......................................................................................................................28
  3.7 VOICE CONFIGURATION – SIP TRUNK TAB ..................................................................................................................29
  3.8 VOICE CONFIGURATION – DIAL PLAN TAB ..................................................................................................................30
  3.9 VOICE CONFIGURATION – DID ...................................................................................................................................31
  3.10 VOICE CONFIGURATION – AA AND VOICE MAIL ......................................................................................................32
  3.11 VOICE CONFIGURATION – ANALOG PHONE USERS ...............................................................................................33
  3.12 VOICE CONFIGURATION – IP PHONE USERS ............................................................................................................34
  3.13 T.38 FAX RELAY CONFIGURATION ............................................................................................................................37
  3.14 SAVE CONFIGURATION ...............................................................................................................................................38
  3.15 RESET TO FACTORY DEFAULT ....................................................................................................................................39

4 REFERENCES ................................................................................................................................................................40
**List of Figures**

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Select Installation Directory</td>
<td>9</td>
</tr>
<tr>
<td>2</td>
<td>Installation Progress</td>
<td>10</td>
</tr>
<tr>
<td>3</td>
<td>Installation Complete</td>
<td>11</td>
</tr>
<tr>
<td>4</td>
<td>Administrative Workstation Network Connection</td>
<td>11</td>
</tr>
<tr>
<td>5</td>
<td>Network Interface Configuration</td>
<td>12</td>
</tr>
<tr>
<td>6</td>
<td>CCA First Time Startup</td>
<td>13</td>
</tr>
<tr>
<td>7</td>
<td>Create Community</td>
<td>14</td>
</tr>
<tr>
<td>8</td>
<td>Security Certificate Alert</td>
<td>15</td>
</tr>
<tr>
<td>9</td>
<td>Authentication</td>
<td>15</td>
</tr>
<tr>
<td>10</td>
<td>Create Community Complete</td>
<td>16</td>
</tr>
<tr>
<td>11</td>
<td>Topology View</td>
<td>17</td>
</tr>
<tr>
<td>12</td>
<td>Setup Wizard – Select a Device</td>
<td>18</td>
</tr>
<tr>
<td>13</td>
<td>Setup Wizard – Prepare the Device</td>
<td>19</td>
</tr>
<tr>
<td>14</td>
<td>Setup Wizard – Power up Device</td>
<td>19</td>
</tr>
<tr>
<td>15</td>
<td>Setup Wizard – Connect Device to Your PC/Laptop</td>
<td>20</td>
</tr>
<tr>
<td>16</td>
<td>Setup Wizard – Authentication</td>
<td>20</td>
</tr>
<tr>
<td>17</td>
<td>Setup Wizard – Please Wait</td>
<td>21</td>
</tr>
<tr>
<td>18</td>
<td>Setup Wizard – Connected</td>
<td>21</td>
</tr>
<tr>
<td>19</td>
<td>Setup Wizard – Enter Hostname and User Authentication Information</td>
<td>22</td>
</tr>
<tr>
<td>20</td>
<td>Setup Wizard – Enter Date and Time Information</td>
<td>22</td>
</tr>
<tr>
<td>21</td>
<td>Setup Wizard – Enter IP Address and Other Device Setup Parameters</td>
<td>23</td>
</tr>
<tr>
<td>22</td>
<td>Setup Wizard – Modify Internet Connection</td>
<td>24</td>
</tr>
<tr>
<td>23</td>
<td>Setup Wizard – Enter Other Device Setup Parameters</td>
<td>25</td>
</tr>
<tr>
<td>24</td>
<td>Setup Wizard – Summary</td>
<td>25</td>
</tr>
<tr>
<td>25</td>
<td>Setup Wizard – Finished</td>
<td>26</td>
</tr>
<tr>
<td>26</td>
<td>Select NTP Setup</td>
<td>27</td>
</tr>
<tr>
<td>27</td>
<td>NTP Setup</td>
<td>27</td>
</tr>
<tr>
<td>28</td>
<td>NTP Setup – Confirmation</td>
<td>28</td>
</tr>
<tr>
<td>29</td>
<td>Voice – Configure Device</td>
<td>29</td>
</tr>
<tr>
<td>30</td>
<td>Voice – Configure SIP Trunk</td>
<td>30</td>
</tr>
<tr>
<td>31</td>
<td>Voice – Configure Dial Plan</td>
<td>31</td>
</tr>
<tr>
<td>32</td>
<td>Voice – DID Configuration</td>
<td>32</td>
</tr>
<tr>
<td>33</td>
<td>Voice – AA &amp; Voicemail Configuration</td>
<td>33</td>
</tr>
<tr>
<td>34</td>
<td>Voice – Analog Users Setup</td>
<td>34</td>
</tr>
<tr>
<td>35</td>
<td>Topology After Connecting 2 IP Phones</td>
<td>35</td>
</tr>
<tr>
<td>36</td>
<td>Voice – Users Page After Hitting Refresh On Users Page</td>
<td>36</td>
</tr>
<tr>
<td>37</td>
<td>Voice – Configure New IP Phones</td>
<td>36</td>
</tr>
<tr>
<td>38</td>
<td>Configuration Successfully Sent</td>
<td>38</td>
</tr>
<tr>
<td>39</td>
<td>Save Configuration</td>
<td>39</td>
</tr>
<tr>
<td>40</td>
<td>Reset To Factory Default</td>
<td>40</td>
</tr>
</tbody>
</table>
1 Introduction

SIP trunk interoperability verification testing is performed between the tekVizion Labs Cisco Unified Communications 500 Series (UC520) and XO lab Broadsoft Application Server with Sonus NBS serving as a Session Border Controller. Broadsoft Application Server and Sonus NBS are in XO network and UC520 is in tekVizion Lab (See Figures 1 and 2 for more information on the network setup). The IP-PBX and its version used during this testing are defined in the Section 1.4. Verification testing uses tekVizion Labs’ Standard Test Plan, which is approved by XO Communications.

The verification only applies to the product versions used in the test, and are only classified as interoperable in a configuration matching that under which the test took place, and for the features and functions tested as part of the test plan. For more information regarding the test results please refer to the document labeled “SIP Trunk Verification Test Plan and Report For Cisco UC520”.

1.1 Document Scope

This document describes the configuration of the Cisco Unified Communications 500 Series by tekVizion Labs to perform interoperability between Sonus NBS and the Cisco Unified Communications 500 Series. The document begins with a brief overview of the SIP trunking solution utilizing the UC520. Following that is a section discussing several limitations encountered during the test, and methods for mitigating those limitations. The remainder of the document is devoted to the detailed configuration used during the test. The UC520 supports many possible configurations, including various dialing plans. This document does not attempt to address the various possible combinations of configuration parameters. It presents only the configuration that was tested at tekVizion Labs.

1.2 tekVizion Labs

tekVizion LabsTM is an independent testing and certification facility offered by tekVizion PVS, Inc. (‘‘tekVizion’’). tekVizion Labs offers several types of testing services including:

- Remote Testing – provides secure, remote access to certain products in tekVizion Labs for pre-certification and ad hoc testing
- Certification Testing – certification of interoperability performed on-site at tekVizion Labs between two products or in a multi-vendor configuration (“solution certification”)
- Product Assessment – independent assessment and verification of product functionality, interface usability, assessment of differentiating features as well as suggestions for added functionality, stress and performance testing, etc.

tekVizion is a system integrator specifically dedicated to the telecommunications industry. Our core services include consulting/solution design, interoperability/certification testing, integration, custom software development and solution support services. Our services help service providers achieve a smooth transition to packet-voice networks, speeding delivery of integrated services. While we have expertise covering a wide range of technologies, we have extensive experience surrounding our FastForward>> practice areas which include: IN Evolution, Packet Voice, Service Delivery, and Integrated Services.

The tekVizion team brings together experience from the leading service providers and vendors in telecom. Our unique expertise includes legacy switching services and platforms, and unparalleled product knowledge, interoperability and integration experience on a vast array of VoIP and other next-generation products. We rely on this combined experience to do what we do best: help our clients advance the rollout of services that excite customers and result in new revenues for the bottom line.
tekVizion leverages this real-world, multi-vendor integration and test experience and proven processes to offer services to vendors, network operators, enhanced service providers, large enterprises and other professional services firms. tekVizion’s headquarters, along with a state-of-the-art test lab and Executive Briefing Center, is located in the Telecom Corridor® in Richardson, Texas. (For more information on tekVizion and its practice areas, please visit tekVizion’s web site at www.tekVizion.com.)

### 1.3 Devices Under Test

<table>
<thead>
<tr>
<th>Devices Under Test</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified Communications 500 Series</td>
<td>4.2.5</td>
</tr>
<tr>
<td>UC 520-16U-4FXO-K9</td>
<td>Cisco IOS Software, UC 500 Software (UC 500-ADVIPSERVICEK9-M), Version 12.4(11)XW5, RELEASE SOFTWARE (fc1)</td>
</tr>
<tr>
<td></td>
<td>uc500-advipservicek9-mz.124-11.xw5</td>
</tr>
<tr>
<td>Cisco Configuration Assistant (software)</td>
<td>1.5</td>
</tr>
<tr>
<td>Broadsoft</td>
<td>13.0.362.mp71-42459</td>
</tr>
<tr>
<td>Sonus NBS</td>
<td>V06.04.06 F001</td>
</tr>
</tbody>
</table>

### 1.4 3rd Party Components and their Versions

<table>
<thead>
<tr>
<th>3rd Party Product/Components</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco 7960</td>
<td>P003-08-05-00</td>
</tr>
<tr>
<td>Cisco Access Router (3660)</td>
<td>ROM: 3600 Software (C 3660-J9035-M), Version 12.3(12), RELEASE SOFTWARE (fc3)</td>
</tr>
<tr>
<td>Extreme Alpine Switch (Layer 2 Switch)</td>
<td>6.2.2</td>
</tr>
<tr>
<td>Nortel Meridian</td>
<td>4.5</td>
</tr>
<tr>
<td>Nortel Meridian Phones</td>
<td>A0721949</td>
</tr>
<tr>
<td>Cisco PSTN Gateway (Cisco 5300)</td>
<td>12.3</td>
</tr>
</tbody>
</table>

### 1.5 Prerequisites

A GRE tunnel (VPN) was established between the XO network and the tekVizion Labs network so the network elements can communicate. Through this GRE tunnel, a SIP Trunk was created from Sonus NBS to the UC 520.

#### 1.5.1 Test Network Setup for Package-1
IP and analog phones are directly connected to the UC520. The UC520 version tested has eight 10/100 POE Ethernet ports, one 10/100 Ethernet WAN port, four FXS analog ports, and four FXO analog ports. The FXO ports were not used during testing.

Figure 1 Test network for Cisco CallManager 5.1 Package-1.

2 SIP Trunking and Cisco Unified Communications 500 Series

SIP trunking is a solution for enterprises, whose requisite is to communicate over IP not only within the enterprise but also outside the enterprise. SIP trunks can increase cost savings by eliminating the need for local PSTN gateways, ISDN BRIs (Basic Rate Interfaces) or PRIs (Primary Rate Interfaces).

Call-processing environments use SIP trunks to configure a signaling interface with Cisco UC520 for SIP calls. SIP trunks (or signaling interfaces) connect the UC520 with a SIP proxy server. A SIP signaling interface uses port-based routing, and the UC520 accepts calls from any gateway as long as the SIP messages arrive on the port that is configured as a SIP signaling interface. The SIP signaling interface uses requests and responses to establish, maintain, and terminate calls (or sessions) between two or more endpoints.
2.1 Limitations

SIP trunk interoperability verification testing is performed between the tekVizion Labs UC 520 and XO lab
Broadsoft Application Server with Sonus NBS serving as a Session Border Controller.

During testing, the following limitations were observed:

**T.38 fax relay**

**Issue:** Although the UC520 platform supports T.38 fax relay, the only configuration supported using the Cisco Configuration Assistant is G.711 pass-through. To enable T.38 fax relay on the platform, manual configuration using the IOS CLI is required.

**Mitigation:** The CLI procedure for enabling T.38 fax is described in Section 3.13.

**Incorrect registration with NBS after a device reload**

**Issue:** After a device reload (CCA-invoked reload, power-cycle, etc.), the device registers with
NBS using an invalid Contact address. The Contact URI contains the address of the UC520 internal loopback interface, rather than that of the WAN interface.

**Mitigation:** After a device reload, run the Cisco Configuration Assistant and navigate to SIP Trunk tab in Voice configuration. Delete the Registrar Server and Proxy Server entries, then apply the change. Add the information back and apply the change again. The device will register with the correct Contact information.

**Call Forward All to a SIP Trunk destination**

**Issue:** When an inbound SIP trunk call is forwarded to a destination number that routes back to
the trunk, the SIP Diversion header in the outbound call leg contains the Auto Attendant DID number, rather than the number of the endpoint forwarding the call. This can present a problem if the forward-to number is that of a third party voice mail server. Such a server would depend on the contents of the Diversion header to route the caller to the appropriate voice mailbox.

**Mitigation:** None, although it is noted that Cisco Unity Express voice mail is an integrated feature of the UC520 platform itself.

3 UC520 Configuration Checklist

In this section we present an overview of the steps that are required to configure SIP trunk in Cisco Unified CallManager.

Table 1 – UC520 Configuration Steps

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Install Cisco Configuration Assistant on administrative workstation</td>
<td>Section 3.1, “Install Cisco Configuration Assistant”</td>
</tr>
<tr>
<td>Step 2</td>
<td>Connect administrative workstation to UC 520</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>Create community</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>Configure WAN interface</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>Configure DNS server address</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>Configure time settings</td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td>Configure SIP trunk</td>
<td></td>
</tr>
<tr>
<td>Step 8</td>
<td>Configure dial plan</td>
<td></td>
</tr>
</tbody>
</table>
3.1 Install Cisco Configuration Assistant

Perform the steps below to install the Cisco Configuration Assistant (CSA) on an administrative workstation. The minimum requirements for this workstation are:

- Windows-based PC
- Pentium III or better
- 512Mb RAM (1Gb recommended)
- 1024x768 or better screen resolution
- Windows 2000 Service Pack 3 or later, or Windows XP Service Pack 1 or later


Steps to install:
1. Double-click on the installer file to launch the installation GUI.
2. Click “Yes” to accept the End User License Agreement.
3. Click “Next” to install to the default directory, or click “Browse” and select a different installation directory. Refer to Figure 1.
4. The remainder of the installation occurs automatically. Refer to Figure 2.
5. Click Finish to complete the installation. Refer to Figure 3.
Figure 1 – Select Installation Directory

Click Next to install "Cisco Configuration Assistant" to this directory, or click Browse to install to a different directory.

Directory Name:
C:\Program Files\Cisco Systems\CiscoSMB

Browse
Figure 2 – Installation Progress

Installing Cisco Configuration Assistant. Please wait...

Extracting...

0%
3.2 Connect Admin Workstation to UC520

Perform the following steps to establish network connectivity between the administrative workstation and the UC520.

1. Connect an Ethernet cable from the administrative workstation’s network interface to one of the POE ports on the UC520. Refer to Figure 4.
2. Configure the administrative workstation’s network interface to obtain an IP address automatically. Refer to Figure 5.

Figure 4 – Administrative workstation network connection

Figure 5 – Administrative workstation network connection
3.3 Create Community

Launch the Cisco Configuration Assistant on the administrative workstation by double-clicking on the desktop icon or by going to StartÆAll ProgramsÆCisco Configuration Assistant and clicking on Cisco Configuration Assistant. First create a community by performing the steps below. A community is a collection of Cisco switches and routers managed by the Configuration Assistant. In this case, the only member of the community is the UC520.

1. In the Connect dialog box, select Create Community, then click OK. Refer to Figure 6.
2. On the Create Community page that appears, enter a name for the community and a company name. Refer to Figure 7.
3. Under Discover Devices, select “a single device by IP address” and enter the default IP address of the UC520, 192.168.10.1. Refer to Figure 7.
4. Click Start. Refer to Figure 7.
5. If a Security Certificate Alert appears, select either Yes to accept the certificate for this session, or Always to accept the certificate permanently. “Always” is recommended. Refer to Figure 8.
6. In the Authentication window that appears, enter the default username “cisco” and password “cisco”, then click OK. Refer to Figure 9.
7. Confirm that the UC520 was discovered by locating it in the Devices section of the screen. The Status column should show a green checkmark and the text “Discovered”. Click OK. Refer to Figure 10.

8. Return to the Topology view and confirm that the UC520 appears as the only node. It may be necessary to click the Refresh icon on the toolbar (second icon from the left). Refer to Figure 11.

Figure 6 – CCA First Time Startup
Figure 7 – Create Community

Name: XO
Company Name: tekVizion

Discover devices
Discover: a single device by IP address
IP Address: 192.168.10.1

Start

Devices
Member  IP Address  Hostname  Communic...  Device Type  Status

Total Rows: 0

OK  Cancel  Help
Figure 8 – Security Certificate Alert

The site IOS-Self-Signed-Certificate-2702036782 can’t be identified as a trusted due to the following problem. You should examine the certificate carefully before accepting it.

- The security certificate was issued by a company you have not chosen to trust.
- The security certificate has not expired and is still valid.
- The name of the security certificate doesn’t match the site name.

Are you willing to accept the certificate asserting IOS-Self-Signed-Certificate-2702036782 is a trusted site?

Yes  No  Always  View Certificate

Figure 9 – Authentication

Please enter your username and password for realm "level_15 or view_access" on "192.168.10.1":

Username: cisco
Password: *****

OK  Cancel
Figure 10 – Create Community Complete

Name: XO  
Company Name: tekVizion

Discover devices
Discover: a single device by IP address
IP Address: 192.168.10.1

Status: Discovered

Devices
<table>
<thead>
<tr>
<th>Member</th>
<th>IP Address</th>
<th>Hostname</th>
<th>Communication</th>
<th>Device Type</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>192.168.10.1</td>
<td>UC520</td>
<td>https</td>
<td>UC520-16U-...</td>
<td></td>
</tr>
</tbody>
</table>
3.4 Device Setup Wizard

From the Cisco Configuration Assistant, invoke the Device Setup Wizard (Setup → Device Setup Wizard). Perform the following steps to complete the initial setup of the UC520.

1. On the “Select a device screen” (Figure 12), select UC500 from the drop down list, then click Next.
2. Verify that the only device connected to the UC520 is the administrative workstation, then click Next on the “Prepare the device” screen (Figure 13).
3. If the UC520 is not already powered on, connect the power supply and do so now. Click Next on the “Power up device” screen (Figure 14).
4. The administrative workstation should already be connected to the UC520. If it is not, do so now. Click Next on the “Connect device to your PC/Laptop” screen (Figure 15).
5. Enter the default user name and password (cisco / cisco) in the Authentication dialog box that appears (Figure 16).
6. Connectivity is verified (Figure 17). Once the connection is verified, click Next (Figure 18).
7. Enter a hostname and, if desired, create a new login account by entering a new Username and password in the next screen (Figure 19).
8. Set the current time on the UC520 (Figure 20). You may either synchronize the time with the clock on the administrative workstation by selecting the “Synchronize with PC” checkbox, or you may enter the current date and time manually by clearing that checkbox. (Note: if you wish to synchronize the UC520’s clock with a network time server, that can be configured in a later step.)
9. Configure the SIP trunk (WAN) interface by selecting the appropriate interface and clicking Modify (Figure 21).
10. The trunk interface is typically configured with a static IP address. In the “Modify Internet Connection” window, select Static IP and enter the UC520’s IP address, subnet mask, and default gateway (Figure 22), then click OK, then Next.

11. On the “Enter other device setup properties” screen, select the appropriate region, and phone and voicemail language (Figure 23). For the United States region and US English language, do not edit the default language file location. Click Next.

12. Confirm the information on the Summary screen (Figure 24), then click Finish.

13. The wizard informs you when the settings have been applied (Figure 25).

Figure 12 - Setup Wizard – Select a Device
Figure 13 - Setup Wizard – Prepare the device

Verify that no other network devices are connected to this device. If other devices are connected, disconnect them or power them down.

Figure 14 - Setup Wizard – Power up device

Use the supplied power cable to connect the device to an AC power source.
Figure 15 - Setup Wizard – Connect device to your PC/Laptop

Step 4: Connect device to your PC/Laptop

Use the supplied Category 6 Ethernet cable to connect your PC to the downlink port of the device. Your PC should not be connected to anything else.

Wait a couple of minutes for your PC to receive an IP address from the device.

If you are prompted to enter a username and password, enter the default router credentials. Click Next to begin the connectivity check.

Figure 16 - Setup Wizard – Authentication

Authentication: Device

Please enter your username and password for realm "level_15 or view_access" on "192.168.10.1":

Username: cisco
Password: *****

[OK] [Cancel]
Figure 17 - Setup Wizard – Please wait

The wizard checks whether the device is connected to the PC properly and is ready to receive commands. When the check is complete, the wizard informs you of the results.

Verifying device connectivity...

Figure 18 - Setup Wizard – Connected

The wizard checks whether the device is connected to the PC properly and is ready to receive commands. When the check is complete, the wizard informs you of the results.

Device connectivity status

Success: Connected.
Click Next to continue.
Figure 19 - Setup Wizard – Enter hostname and user authentication information

To configure the hostname and user credentials, follow these steps:

1. In the Hostname field, enter the hostname to be used as the authentication credential. The name must be a single word and cannot contain quotation marks or blank spaces.
2. In the Username field, enter the name to be used as the authentication credential. The name must be a single word and cannot contain quotation marks or blank spaces.
3. In the Password field, enter the password for this hostname. The password must be from 1 to 25 characters long and can contain embedded spaces.
4. In the Confirm Password field, retype the password.

Figure 20 - Setup Wizard – Enter Date and Time information

The wizard takes the date, time, and time zone values from the connected PC and shows them in the drop-down lists. If you want to change any of the values, uncheck Synchronize with PC and select other values from the lists. Daylight Saving Time is supported for these time zones:

- North America
  - (GMT - 09:00) Alaska
  - (GMT - 08:00) Pacific Time (US; Canada; Tijuana)
  - (GMT - 07:00) Mountain Time (US; Canada)
  - (GMT - 06:00) Central Time (US; Canada)
  - (GMT - 05:00) Eastern Time (US; Canada)
  - (GMT - 03:30) Newfoundland (Canada)
- Europe
  - (GMT + 01:00) Azores, Canary
Figure 21 - Setup Wizard – Enter IP Address and other device setup parameters

To enable an internet connection, follow these steps:
1. Choose an interface from the WAN Interfaces list.
2. Click Modify, and use the Modify Internet Connection window.
3. To save your changes and to close the window, click OK.

<table>
<thead>
<tr>
<th>Interface</th>
<th>Type</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>FastEthernet/0</td>
<td>DHCP</td>
<td>FastEthernet</td>
</tr>
</tbody>
</table>
Figure 22 - Setup Wizard – Modify Internet Connection

Please delete NAT/VPN/Firewall to enable this button

- Enable WAN Interface
  - PPPoE

- Static IP
  - DHCP
  - IP Negotiated

Internet IP Address: 205.240.79.253
Subnet Mask: 255.255.255.128
Default Gateway: 205.240.79.129

Original value:
Figure 23 - Setup Wizard – Enter other device setup parameters

To configure the local settings, follow these steps:

1. From the Region list, choose the region for Cisco Unified Communications Manager Express. This sets the tones and cadences of the phones.
2. From the Phone Language list, choose the language that appears on the phones to the user.
3. From the Voicemail Language list, choose the language of the voice mail prompts that voice mail users will hear. To install a language pack, follow these steps:
   a. Download the desired Cisco Unified Communications Manager Express language file.

Local Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Region</td>
<td>United States</td>
</tr>
<tr>
<td>Phone Language</td>
<td>US English</td>
</tr>
<tr>
<td>Voicemail Language</td>
<td>US English</td>
</tr>
</tbody>
</table>

Figure 24 - Setup Wizard – Summary

The parameters listed on this page will be applied to the device.

Summary

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>UC500</td>
</tr>
<tr>
<td>Username</td>
<td>Cisco</td>
</tr>
<tr>
<td>Region</td>
<td>United States</td>
</tr>
<tr>
<td>Phone Language</td>
<td>US English</td>
</tr>
<tr>
<td>Voicemail Language</td>
<td>US English</td>
</tr>
</tbody>
</table>
3.5 NTP Setup

The UC520 can synchronize it's clock to a Network Time Protocol (NTP) server. To configure this perform the following steps.

1. In the task pane to the left, expand the Device Properties tree and select “System Time...” Click on the “NTP” button. Refer to Figure 26.
2. In the “Network Time Server” dialog box that pops up, enter the information required for connecting to your preferred NTP server, then click OK. See Figure 27.
3. Click OK in response to the confirmation prompt (Figure 28).
Figure 26 - Select NTP Setup

Figure 27 - NTP Setup
3.6 Voice Configuration – Device tab

To configure the UC520 for telephony operations, use the task pane on the left, expand Telephony, and select “Voice…” Select the Device tab and confirm that “Configure as a PBX” is selected. Select it if necessary. Refer to Figure 29.

NOTE: While navigating the tabs in Voice setup, the Configuration Assistant may automatically move you to a tab that you haven’t selected. Certain items on the tab being displayed will be outlined in red, indicating that those items are inconsistent with other configuration elements on other tabs. You may safely navigate away from the displayed tab and complete the configuration in the order presented in this document. By the time you complete this configuration all erroneous entries will have been resolved.
3.7 Voice Configuration – SIP Trunk tab

In Voice setup, select the SIP Trunk tab (Figure 30). Select Generic SIP Trunk Provider from the drop down list, and enter the IP addresses of the Registrar Server and the Proxy Server. Then enter the digest authentication user name and password in the appropriate fields. The information required for this tab will have been given to you by your service provider. Do not click the OK button at the bottom of the tab until all of the voice configuration is complete or you will get an error. (You may have to scroll down to expose the OK button.)
3.8 Voice Configuration – Dial Plan tab

In Voice setup, select the Dial Plan tab (Figure 31). On this tab you can configure the number of digits per extension, the type of numbering plan for external calls, the number of digits in a local phone number, the trunk access code, emergency numbers, and the like. Figure 31 shows a sample configuration with four-digit extensions and a North American dialing plan with 10-digit local dialing.
3.9 Voice Configuration – DID

In Voice setup, select the Dial Plan tab if necessary, the click Configure next to Direct Inward Dial. The DID Configuration window appears (Figure 32). In this window you can configure a one-to-one DID numbering pattern or a many-to-one pattern. The example in Figure 32 shows a one-to-one configuration in which the DID numbers 2146355850 through 2146355859 are routed to extensions 5850 through 5859 respectively. With the Caller ID Translation checkbox selected, outbound calls from these extensions will show the full, 10-digit DID number on the called party’s Caller ID. To create this configuration, click Add at the bottom of the One-to-one DID Translation pane and enter the appropriate information.
3.10 Voice Configuration – AA and Voice Mail

Auto Attendant (AA) and Voice Mail configuration is completed on the Voice setup AA and Voicemail tab (Figure 33). Enter the Auto Attendant Extension and PSTN Number and the Voice Mail Access Extension and PSTN Number. A default Auto Attendant script is provided with the system. Customization of this script is beyond the scope of this document.
3.11 Voice Configuration – Analog Phone Users

Analog phones or fax machines may be directly connected to the FXS ports on the UC 520. To configure extension numbers for these devices, go to the Voice setup Users tab (Figure 34). Enter the extension number, and the user’s name, user ID and password for each device to be configured.
3.12 Voice Configuration – IP Phone Users

If you have been performing the system configuration in the order presented in this document, you may now connect IP phones to the Ethernet ports on the device. Figure 35 shows the Configuration Assistant topology view after connecting two IP phones.
Once your IP phones are physically connected to the device, navigate to the Voice setup Users tab. If necessary, click the Refresh toolbar button near the top left to display rows for the newly-added phones. Note in Figure 36 that two IP phones now appear. These phones have automatically been assigned 3-digit extensions. Since this device is configured for 4-digit extensions, the extension numbers are highlighted in red, indicating that they need to be corrected. Figure 37 shows this page after the correct information has been entered.
Figure 36 - Voice – Users page after hitting Refresh on Users page

Figure 37 - Voice – Configure new IP phones
3.13 T.38 Fax Relay Configuration

By default, the UC 520 handles fax calls by embedding the fax modem signals in the audio RTP stream (G.711 pass-through). Fax over IP (FoIP) is implemented using the T.38 protocol, and this is the preferred method for IP trunking solutions. The UC 520 platform supports T.38, but the Cisco Configuration Assistant does not provide any means for configuring it. This configuration must be performed using the Cisco IOS command line interface. This interface is available via a telnet session to the UC 520 platform.

Perform the following steps to configure T.38 fax relay on the UC 520:

1. On the administrative workstation, open a command shell and log into the UC 520 by entering the following commands (user entries are in bold face). In the example below, the default IP address, user name and password are shown. If these have changed in your installation, use the appropriate values.

   C:\Documents and Settings\Administrator>telnet 192.168.10.1
   Trying 192.168.10.1...
   Connected to 192.168.10.1.
   Escape character is '^]'.
   
   User Access Verification
   Username: cisco
   Password: cisco

2. Identify the number of the FXS port to which your analog fax is connected. This will be a value from 0-3 for the basic four-port UC 520. The port numbers are labeled on the faceplate of the UC 520.

3. In your telnet session, enter the following command:

   UC520#sh run

4. In the output that results from the above command, look for a series of lines similar to the example below. There will be one for each FXS port on the UC 520. The last digit in the port line corresponds to the port number. Find the one corresponding to the port you identified in Step 2 above. Note the dial peer number. In the example, the fax device is connected to port 3, and the corresponding dial peer is "dial-peer voice 3 pots".

   dial-peer voice 3 pots
   service stcapp
   port 0/0/3

5. Enter the following commands to configure the port for T.38 fax. Replace the dial peer number in the example with the dial peer number that you identified in the previous step.

   UC520#config t
   Enter configuration commands, one per line.  End with CNTL/Z.
   UC520(config)#dial-peer voice 3 pots
   UC520(config-dial-peer)#no service
   UC520(config-dial-peer)#exit

6. Enter the following commands to enable T.38 fax relay:
3.14 Save Configuration

Additional information unique to your site can be configured on the remaining tabs. In this sample configuration, the default settings on these tabs were used.

Once your configuration is complete, click OK at the bottom of the Voice setup tab (the button appears at the bottom of every tab, although you may have to scroll down to expose it). After a few minutes a popup will appear confirming that the configuration has successfully been sent to the UC520 (Figure 38).

To make sure that your configuration will survive reboots of the UC520, you must save the configuration. In the task pane on the left, select “Save Configuration…” Click Save to write your current configuration to system flash memory. See Figure 39.

Figure 38 – Configuration Successfully Sent
3.15 Reset to Factory Default

At some point it may become necessary to reset the unit to its factory default settings. This can be accomplished from the Configuration Assistant by expanding Maintenance at the bottom of the task pane on the left, then selecting “Reset/Restart”. In the “Reset/Restart” window that appears, select the checkbox under Reset to Factory Default, then click OK. See Figure 40.
4 References


2. Getting Started Guide for the Cisco Unified Communications 500 Series  