



## **Getting Started with Cisco Configuration Assistant 1.8**

**Americas Headquarters**  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

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 TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0807R)

*Getting Started with Cisco Configuration Assistant*

© 2008 Cisco Systems, Inc. All rights reserved.



## CONTENTS

<b>Preface</b>	iii
Audience	iii
Purpose	iii
Obtaining Documentation and Submitting a Service Request	iii

---

### CHAPTER 1

<b>What Is Cisco Configuration Assistant?</b>	1-1
Characteristics of a Community	1-1
Viewing a Community	1-2

---

### CHAPTER 2

<b>GUI Features</b>	2-1
Topology View	2-2
Front Panel View	2-3
Menu Bar, Toolbar, and Feature Bar	2-4
Menu Bar	2-4
Feature Bar	2-4
Toolbar	2-5
Interaction Modes	2-7
Guide Mode	2-7
Expert Mode	2-8
Smartports	2-8
Privilege Levels	2-9
Application Updates	2-9
Online Help	2-9

---

### CHAPTER 3

<b>Installing, Connecting, and Setting Up</b>	3-1
Installation Requirements	3-1
Installing Configuration Assistant	3-1
Connecting Configuration Assistant	3-2
Setting Up Devices	3-2
Event Notification	3-3

---

CHAPTER 4

**Planning and Creating Communities 4-1**

- Planning a Community 4-1
  - Member and Candidate Characteristics 4-1
  - Community Device Limits 4-1
  - Automatic Discovery of Candidates and Members 4-2
  - Community Names 4-2
  - Hostnames 4-2
  - Passwords 4-3
  - Communication Protocols 4-3
  - Community Information 4-3
- Creating a Community 4-3
  - Adding a Group of Devices 4-3
  - Adding Devices One at a Time 4-4
  - Verifying a Community 4-4

---

CHAPTER 5

**UC500 and SR500 Secure Router Setup 5-1**

- Configuring the Cisco UC500 5-2
- Configuring the Cisco SR500 5-8
- Creating a Community 5-13

---

INDEX



## Preface

---

### Audience

This guide is for system administrators and network managers who want use a GUI to manage standalone network devices or groups of devices that are part of the Cisco Smart Business Communication System. The guide presents Cisco Configuration Assistant as a solution.

### Purpose

The purpose of this guide is to help users get started with Configuration Assistant. It consists of these chapters:

Introduction—What Configuration Assistant is and what it does.

GUI Features—How to use Configuration Assistant to manage devices and networks.

Installing, Connecting, and Setting Up—How to install Configuration Assistant on your workstation, connect it to a device or community, and set up devices to be managed.

Planning and Creating Communities—The concepts and procedures for planning and creating communities.

## Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.





# CHAPTER 1

## What Is Cisco Configuration Assistant?

---

Configuration Assistant is an application that manages standalone devices and device groups, called *communities*, from anywhere in your intranet. Using its graphical interface, you can

- Set up Cisco® Smart Business Communications System (SBCS) devices
- Configure port connections quickly
- Configure the IP telephony features of your community
- Manage telephony licenses on IP voice devices
- Set up network address translation, virtual private networks, and firewalls
- Configure the wireless LAN features of your community, including wireless security and wireless guest access
- Manage and audit network security
- View the entire community on a topology map
- View the front panels of community members
- Monitor device status, bandwidth, and links
- See inventory and statistics reports
- Upgrade software on devices

To perform any of these tasks, you select the appropriate feature from the Configuration Assistant feature bar, as shown in the [“Feature Bar” section on page 2-4](#)

## Characteristics of a Community

A community can contain up to 25 connected network devices. Each device must have an assigned IP address. Configuration Assistant uses the automatic discovery capability of Cisco Discovery Protocol (CDP) to find eligible network devices and to add them to a community. If devices do not have CDP enabled, you can still create a community and manually add the devices.

The main reason for creating a community is to manage Cisco devices in the same logical group, regardless of their physical locations and the software installed on the devices. You can create, modify, delete, and manage multiple communities.

With Configuration Assistant, you can communicate securely with every member in a community. If a community member fails, you can continue to manage the other members.

Most types of network devices—routers, switches, wireless LAN controllers—can belong to a community. For a specific list of eligible devices, see the release notes. For information on creating communities, see [Chapter 4, “Planning and Creating Communities.”](#)

## Viewing a Community

Configuration Assistant gives you two graphical views of a community:

- A Topology view, which shows member devices, neighboring devices, device status, device properties, and link information.
- A Front Panel view, from which you can monitor the real-time status of the devices and ports and do many configuration tasks. The devices and port LEDs in the view look like the physical devices and the port LEDs.

To see examples of these views, see the [“Topology View” section on page 2-2](#) and the [“Front Panel View” section on page 2-3](#).

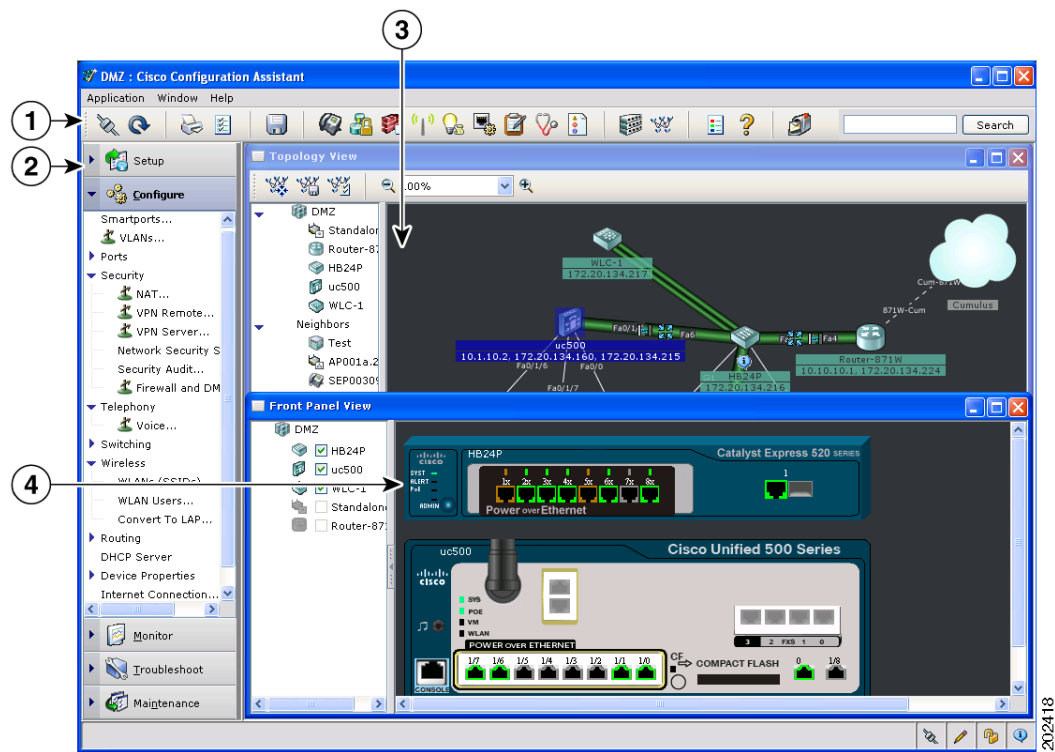


# CHAPTER 2

## GUI Features

Configuration Assistant simplifies the management of a community by offering different views of the community, a menu bar, toolbar, feature bar, two modes for configuring devices, and comprehensive online help. [Figure 2-1](#) shows the main features of the GUI.

**Figure 2-1** Configuration Assistant GUI



1	Toolbar	3	Topology view
2	Feature bar	4	Front Panel view

The following sections describe the Configuration Assistant features.

202418

# Topology View

When Configuration Assistant connects to a standalone device or to a community, the Topology view appears by default. If you change this default, you can see the Topology view by clicking Topology view on the toolbar or by choosing **Monitor > Views > Topology**.



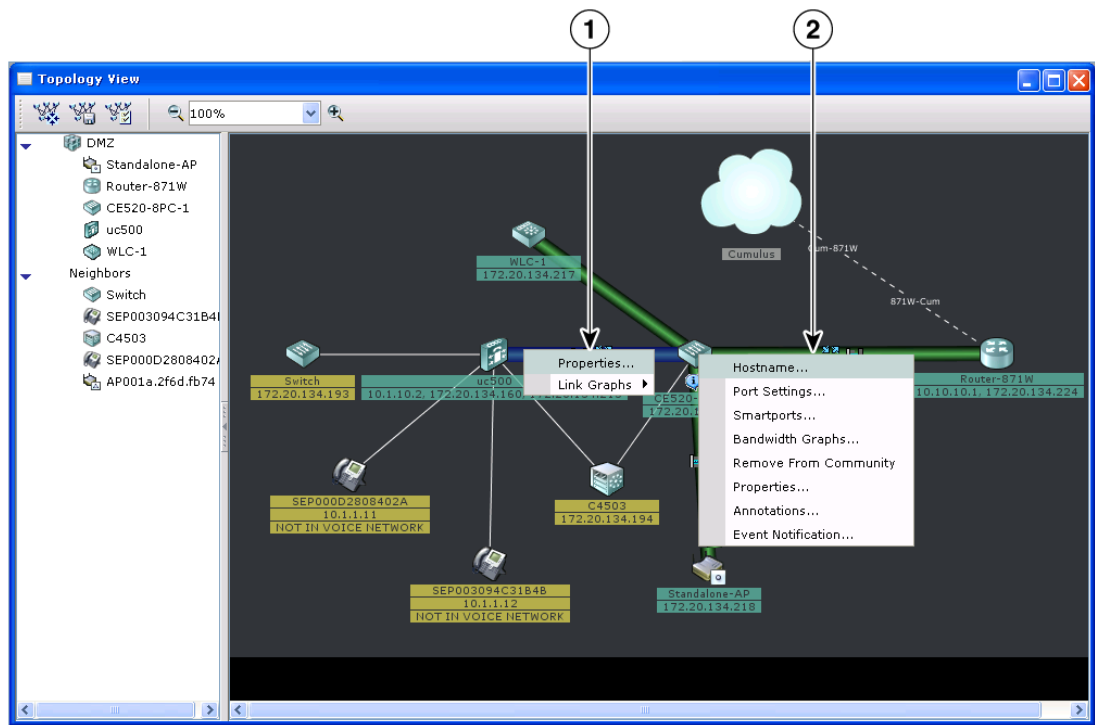
## Note

You can change the preferences in Configuration Assistant to show the Front Panel view by default by choosing **Application > Preferences > Show Front Panel View when connected to network**. If you no longer want Configuration Assistant to show the Topology view by default, deselect **Show Topology View when connected to a network**.

The Topology view shows how the devices within a community are connected. You can see the VLAN links within the community by highlighting them. You can make neighboring devices members of the community, and you can remove members.

The Topology view in [Figure 2-2](#) shows a community, neighboring devices, and the popup windows that appear when you right-click a device or a link icon. (You can open only one popup window at a time.)

**Figure 2-2** Topology View and Popup Windows



1	Link popup window	2	Device popup window
---	-------------------	---	---------------------

# Front Panel View

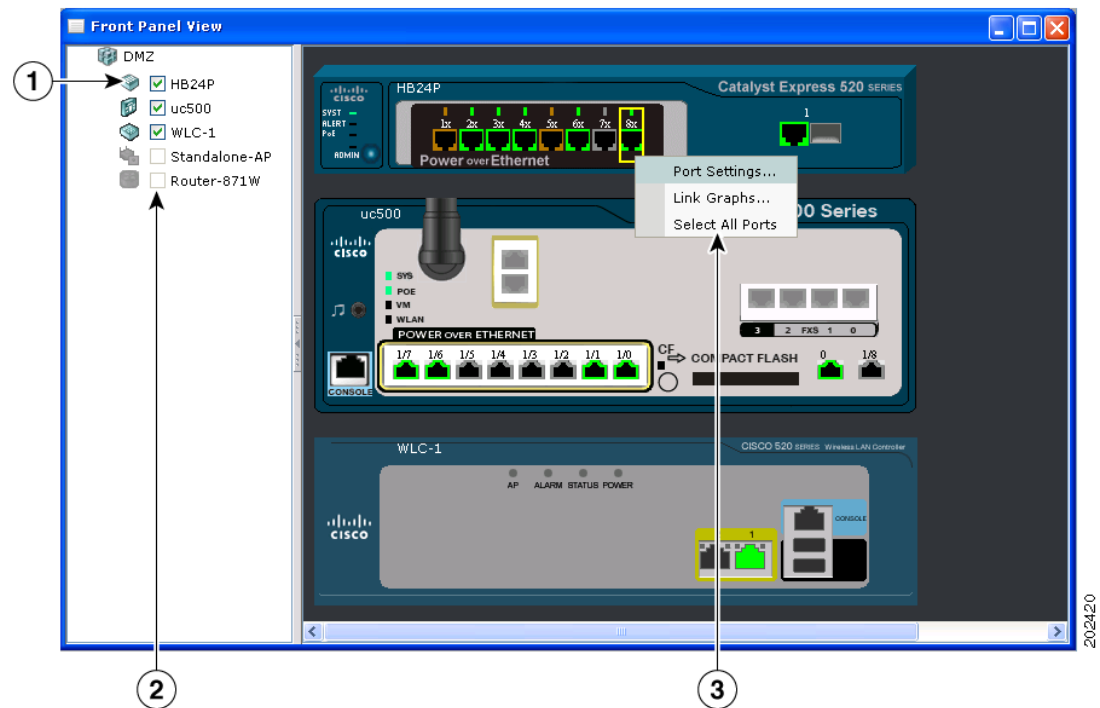
When Configuration Assistant connects to a standalone device or to a community, you can display the Front Panel view by clicking Front Panel on the toolbar or by choosing **Monitor > View > Front Panel** on the feature bar. You see the front-panel image of the standalone device or the community members. The left pane of the view is a tree diagram. In it, you can select the devices that you want to see in the right pane.

By using the Front Panel view, you can

- Drag and re-arrange the devices that appear.
- Select and configure the devices.
- Right-click a port and configure it.
- Select multiple ports, on the same device or on different devices, and configure the ports at the same time.

Figure 2-3 shows a community with these members: a Catalyst Express 520 switch, a Unified Communications 500 Series platform, and a 526 WLAN Controller.

Figure 2-3 Front Panel View and Port Popup Window



1	Member devices	3	Settings popup window
2	Check boxes to show devices		

# Menu Bar, Toolbar, and Feature Bar

The menu bar has features for configuring Configuration Assistant itself. The feature bar has features for configuring, monitoring, troubleshooting, and maintaining a standalone device or a community. The toolbar has a combination of the most often used Configuration Assistant features and Ethernet features.

## Menu Bar

The menu bar provides these options for managing Configuration Assistant, navigating among windows, and accessing online help:

- **Application**—Choose printing options, select interaction modes, set user preferences, search for and install Configuration Assistant updates, show or hide the feature bar, create and modify communities, and request system message notifications.
- **Window**—Navigate to open Configuration Assistant windows.
- **Help**—Open the online help.

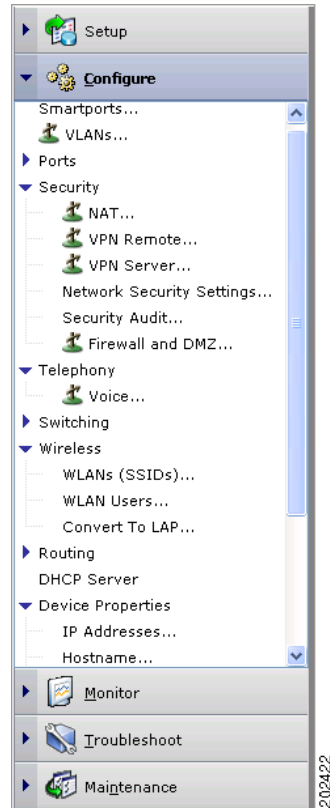
## Feature Bar

The feature bar shows the Ethernet features that are available for the devices that you are managing. By default, the feature bar is in standard mode. In this mode, it is always visible, and you can reduce or increase its width. In autohide mode, the feature bar appears only when you move the cursor to the left edge of the Configuration Assistant workspace.

- To see the feature bar in standard mode, click **Application > Feature Bar**, and select **Standard Mode**.
- To hide the feature bar, click **Application > Feature Bar**, and select **Autohide Mode**.

[Figure 2-4](#) shows a feature bar.

Figure 2-4 Feature Bar



The features are grouped under menus. When you click a menu item, the configuration window for the feature appears.

Access modes affect the availability of features; some are not available in read-only mode. For more information about how access modes affect Configuration Assistant, see the [“Privilege Levels” section on page 2-9](#).

## Toolbar

The toolbar has icons and buttons for commonly used configuration options and for information windows such as the legend and the online help. [Table 2-1](#) lists the toolbar options from left to right on the toolbar.

Table 2-1 *Toolbar Icons and Buttons*







Toolbar Option	Icon	Task
Connect		Connect Configuration Assistant to a standalone device or to a community.
Refresh		Update the views with the latest status.
Print		Print a Configuration Assistant window or a help topic.
Preferences		Set Configuration Assistant display properties, choose the views to open when Configuration Assistant is connected, and choose how often Configuration Assistant searches for an update.
Save Configuration <sup>1</sup>		Save the running configuration of a managed device to its startup configuration.
Voice		Configure options for voice communication.
VPN Server		Configure a VPN server and send security policies to a device.
Firewall and DMZ		Configure a firewall and create a DMZ.
Wireless Networks		Configure security features on a WLAN controller and its associated access points.
Smartports <sup>1</sup>		Quickly configure the essential security, availability, and manageability features of your network port connections.
Port Settings <sup>2</sup>		Display and configure the port parameters on a device.
Inventory		Display the device type, the software version, the IP address, and other information about all the active devices in the community.
Health		Monitor measurements that show the health of your managed devices (excluding WLAN controllers and Aironet autonomous access points).
Event Notification		Display messages about network and device events.
Front Panel		Display the Front Panel view.
Topology		Display the Topology view.

Table 2-1 *Toolbar Icons and Buttons (continued)*

Toolbar Option	Icon	Task
Legend		Display the legend, which describes the icons, labels, and links.
Help for Active Window		Display the help topic for the active, open window. You can also click <b>Help</b> from the active window or press the <b>F1</b> key.
Feedback		Open a web page where you can leave feedback about your experience with Configuration Assistant.
Search		Enter terms in the field at the right of the toolbar, and click the <b>Search</b> button to search the online help.

1. Not available in read-only mode. For more information about the read-only and read-write access modes, see the “[Privilege Levels](#)” section on page 2-9.
2. Some options from this menu option are not available in read-only mode.

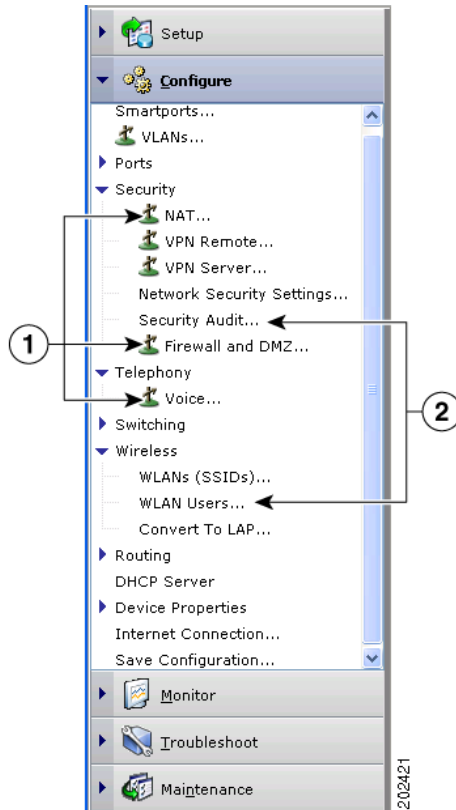
## Interaction Modes

There are two modes for interacting with the Configuration Assistant GUI: guide mode and expert mode. Guide mode presents feature options one step at a time, with accompanying help information. Expert mode presents all the options for configuring a feature in a single window. For help, click **Help** in the window.

### Guide Mode

Configuration Assistant is in expert mode by default. If you choose **Guide** on the **Application** menu and select a feature with a signpost icon (see [Figure 2-5](#)), you see a series of configuration steps—guide mode. If you choose a feature without this icon, you see a configuration window—expert mode.

Figure 2-5 Guide Mode and Expert Mode Examples



<b>1</b>	Examples of features that are available in guide mode and expert mode	<b>2</b>	Examples of features that are available only in expert mode
----------	---	----------	---

Guide mode is not available if your switch access level is read-only. For more information about the read-only access mode, see the “[Privilege Levels](#)” section on page 2-9.

## Expert Mode

If you prefer to see a configuration window for every feature, choose **Expert** in the **Application** menu. Even the features that appear with a signpost on the feature bar appear in expert mode. If you want to see guide mode again, choose **Guide** in the **Application** menu.

To start a guide-mode feature in **Expert** mode, you must choose **Expert** *before* selecting the feature.

## Smartports

Configuration Assistant detects where you have not used Smartports to configure a device connection and provides this information in the Event Notification window. You can configure the connection either manually or based on suggestions provided by Configuration Assistant. Open the Smartports window to either select a role to apply, or use Smartports to suggest a role to apply. See the online help for more information on Smartports.

## Privilege Levels

Configuration Assistant provides two types of access to configuration options: read-write and read-only. Your access type is determined by your privilege level, a number from 1 to 15. Level 15 gives you read-write access. Levels 1 to 14 give you read-only access. At these levels, you cannot modify the configuration shown in Configuration Assistant windows.

By default, Configuration Assistant tries to log you on with privilege level 15. However, this normally requires that you pass the authentication process with a proper username and password. Lower levels do not generally impose this requirement.



Note

---

You must have privilege level 15 to access Configuration Assistant through a TACACS+ or a RADIUS server.

---

## Application Updates

Configuration Assistant can search Cisco.com to see whether updates are available. Use either of these actions to request a search:

- Choose **Application > Preferences**, and use the Preferences window to request an automatic search every week or every month.
- Choose **Application > Application Updates** to request an immediate search for updates.

If an update is found, you can install it through Configuration Assistant.

## Online Help

Configuration Assistant provides comprehensive online help that explains set up, configuration, monitoring, troubleshooting, and maintenance tasks.

Sometimes the information in a help topic differs for different devices. In these cases, the right pane of the Help window contains all the versions of the topic, each labeled with the hostnames of the devices it applies to.

Online help includes these features:

- Conceptual help that gives background information on networking features
- Window help that gives procedures for performing tasks
- An index of online help subjects
- A tab for searching the online help for a subject that you enter
- A glossary of terms used in the online help





## CHAPTER 3

# Installing, Connecting, and Setting Up

---

This chapter describes what is required to install Configuration Assistant, how to install it, how to connect it to a device or to a community, and how to set up devices so that they can be managed.

## Installation Requirements

The PC on which you install Configuration Assistant must meet these minimum requirements:

- Processor speed: 1 GHz
- DRAM: 512 MB minimum, 1024 MB recommended for better performance
- Hard-disk space: 150 MB for the application alone, 300 MB recommended
- Number of colors: 65536
- Resolution: 1024 x 768
- Font size: Small

Configuration Assistant is supported on these operating systems:

- Windows Vista Ultimate
- Windows XP, Service Pack 1 or later

Windows 64-bit versions are not tested or officially supported. You will need write permission to your home directory and to the Configuration Assistant installation directory so that Configuration Assistant can create the necessary log files and preference files.

## Installing Configuration Assistant

To install Configuration Assistant on your PC, follow these steps:

1. Go to this web address: <http://www.cisco.com/go/configassist>.  
You must be a registered Cisco.com user, but you need no other access privileges.
2. Find the Configuration Assistant installer file, `configuration-assistant-windows-k9-installer-1-5-en.exe`.

- Download the Configuration Assistant installer, and run it. (You can run it directly from the web if your browser offers this choice.)

Configuration Assistant is free—there is no charge to download, install, or use it.

When you run the installer, follow the displayed instructions. In the final panel, click **Finish** to complete the Configuration Assistant installation.

After Configuration Assistant is installed, you see its icon on your desktop, a Configuration Assistant shortcut under the **Start** menu, and a Configuration Assistant entry under **Start > Programs**. When you click any of these, you see a partial Configuration Assistant GUI and the Connect window.

In disconnect mode, Configuration Assistant is not connected to a device or a community; it cannot manage a standalone device or a community. Its menu bar and toolbar support only the tasks that customize Configuration Assistant itself. The feature bar, which usually lists device features, is empty.

## Connecting Configuration Assistant

You can connect Configuration Assistant to a standalone device, to an existing community, or to a new community. For all of these connections, you use the Connect window, shown in [Figure 3-1](#). The **Connect To** button and its pulldown menu are for connections to devices and existing communities. For instructions on creating a community, see the [“Creating a Community”](#) section on page 4-3.

*Figure 3-1 Connect Window*



When the connection occurs, the Configuration Assistant window is in *connect* mode. The toolbar adds icons that represent device features. Similarly, the feature bar fills with menus that list the Ethernet features that Configuration Assistant offers.

## Setting Up Devices

Devices that are new or that have been reset to their factory defaults must be set up. Use the Device Setup Wizard for this task. It makes devices ready for Configuration Assistant to manage. To start the wizard, select **Setup** on the feature bar, and click **Device Setup Wizard**.

The wizard is available on the feature bar even if you are in disconnect mode.

## Event Notification

Configuration Assistant informs you of events that it detects by putting an event icon on the status bar and under devices in the Topology view. Clicking an event icon opens the Event Notification window. It describes the event and, whenever possible, connects you to windows where you can take the needed actions.

If you are informed of an event while in disconnect mode, you can open the Event Notification window by selecting **Monitor** on the feature bar and clicking **Event Notification**.





## CHAPTER 4

# Planning and Creating Communities

---

This chapter provides the concepts and procedures for planning and creating communities by using Configuration Assistant. For information on using it to configure communities, refer to the online help.

## Planning a Community

This section describes the guidelines, requirements, and caveats that you should understand before you create a community.

## Member and Candidate Characteristics

Members are network devices that belong to a community. *Candidates* are network devices that do not. To join a community, a candidate must

- Be supported by Configuration Assistant
- Have an IP address
- Have HTTP or HTTPS enabled on the default ports.

## Community Device Limits

The combined number of these device types cannot exceed 25:

- Catalyst Express switches.
- Cisco 800 Series routers.
- Unified Communications 500 Series platforms.
- Cisco SR520 Series Routers
- Cisco 526 Wireless Express Controllers.
- Cisco 521 Wireless Express autonomous access points. These are fully featured standalone access points that do not require a Cisco 526 Mobility Controller.
- HWIC access points. These are high-speed WAN interface cards with an integrated access point for Unified Communications 500 Series platforms.

There is no limit on the number of IP phones or lightweight access points—access points managed by a WLAN controller—in a community, nor is there a limit on the number of communities that Configuration Assistant can manage.

Besides the overall limit of 25 devices, there are these device-type limits:

- Catalyst Express switches—no more than 15
- Cisco 800 Series routers plus Unified Communications 500 Series platforms—no more than 5
- Cisco 526 Wireless Express Controllers—no more than 2
- Cisco 521 autonomous access points plus HWIC access points—no more than 3

If the overall limit or a device-type limit is exceeded, you cannot manage the community. You must remove devices until the limit is no longer exceeded.

## Automatic Discovery of Candidates and Members

Beginning with the IP address for a starting device and the port numbers for HTTPS and HTTP, Configuration Assistant uses CDP to compile a list of community candidates that are within four CDP hops of the starting device. Configuration Assistant can discover candidate and member devices across multiple networks and VLANs if they have valid IP addresses. See the [“Member and Candidate Characteristics” section on page 4-1](#) for a list of requirements that network devices must meet in order to be discovered.



### Note

---

Do not disable CDP on candidates, members, or any network devices that you might want Configuration Assistant to discover.

---

You can edit the list of discovered devices to fit your needs and to add them to the community. If Configuration Assistant does not discover a network device, you can manually add the device.

For instructions on adding discovered devices to a community or manually adding devices to a community, see the [“Adding Devices One at a Time” section on page 4-4](#).

## Community Names

When you create a community, Configuration Assistant requires that you assign a name to it. The name can contain up to 64 alphanumeric characters and is not case sensitive.

## Hostnames

You do not need to assign a hostname to a community member, and Configuration Assistant does not assign one by default. However, Cisco IOS assigns the hostname *Switch* to switches without a hostname. Therefore, you might want to assign hostnames to switches to avoid confusing them.

## Passwords

When connecting to a community, Configuration Assistant prompts you for each unique password that has already been assigned for members of the community. Configuration Assistant attempts to use these passwords to connect to other devices. You are prompted for a password only if the previously entered password does not work for a device.

For example, if a community has ten members, and five members share one password and the other five share a different password, Configuration Assistant prompts you twice, once for each password. Configuration Assistant does not save the passwords to your PC, so it prompts you for the passwords each time that you attempt to connect to a community.

## Communication Protocols

Configuration Assistant uses HTTPS, HTTP, Telnet, and SSH to communicate with devices. It tries to use HTTPS when discover neighboring devices and when devices are manually added to a community. If HTTPS fails, it tries HTTP.

The HTTPS port is fixed at 443; the HTTP port defaults to 80. You can specify a different HTTP port when you create a community. Afterward, you use the HTTP Port window to change the HTTP port. The port settings for both HTTPS and HTTP must be the same for all the members of a community.

## Community Information

Configuration Assistant saves all individual device information, such as the IP address, the hostname, and the communication protocol, to your local PC. When Configuration Assistant connects to a community, it uses the locally saved data to rediscover the member devices.

If you try to use a different PC to manage an existing community, none of the member device information is available. You need to create the community again and add the same member devices.

## Creating a Community

You can create a community in these ways:

- Add a group of devices to a community
- Add devices one at a time

You should verify that the community contains the devices that you think it contains. This section tells you how to perform these tasks.

## Adding a Group of Devices

Follow these steps to build a list of candidate devices and to add them to a community:

1. Start Configuration Assistant, and select **Create community** in the Connect window. Click **Connect**.
2. In the Create Community window, enter a name for the community.

3. Click the **Advanced** button if you want to set an HTTP port other than 80, the default port. Enter the HTTP port number that you want to use. Click **OK**.
4. Enter a *seed* IP address, the beginning and ending IP addresses of an address range, or the IP address of a subnet. (A *seed* IP address implicitly requests the discovery of the device with that address and the discovery of connected devices.)
5. Start the discovery process.
6. In the Devices list, deselect the candidate devices that you want to remove, and click **Remove**.

## Adding Devices One at a Time

Use either of these ways to add devices one at a time:

- In the Create Community window, enter the IP address for a single device, and start the discovery process.
- In the Topology view, right-click a candidate icon, and select **Add to Community**.

## Verifying a Community

Follow these steps to verify the community:

1. Choose **Monitor > View > Topology** to display the Topology view.
2. Choose **Monitor > Reports > Inventory** to display an inventory of the devices in the community. This summary includes device model numbers, serial numbers, software versions, IP information, and location.
3. Choose **Monitor > View > Front Panel** to display the Front Panel view.



# CHAPTER 5

## UC500 and SR500 Secure Router Setup

The Cisco SR500 provided asymmetric digital subscriber line (ADSL) or FastEthernet WAN termination and advanced security features for a Cisco Smart Business Communications System (SBCS) network. This document describes how to connect a Cisco UC500 behind a Cisco SR500 in secure router mode. It includes the following sections:

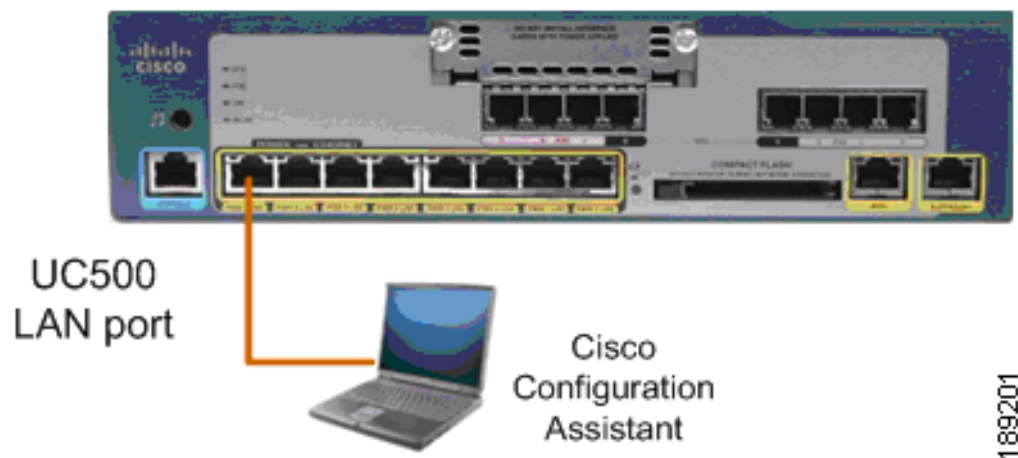
- [Configuring the Cisco UC500](#)
- [Configuring the Cisco SR500](#)
- [Creating a Community](#)

### Prerequisites:

- UC500 Series Router
- SR500 Series Router
- A PC with an operating system that supports Cisco Configuration Assistant: Windows Vista Ultimate, or Windows XP, Service Pack 1 or later
- Cisco Configuration Assistant with version 1.8 or higher installed

Connect your Cisco UC500 to a Windows PC, as shown in [Figure 5-1](#).

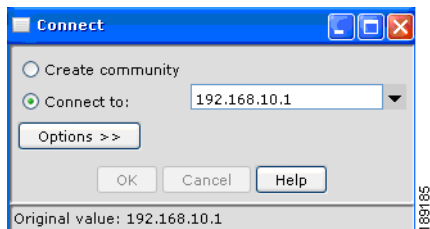
*Figure 5-1 Cisco UC500 Connection*



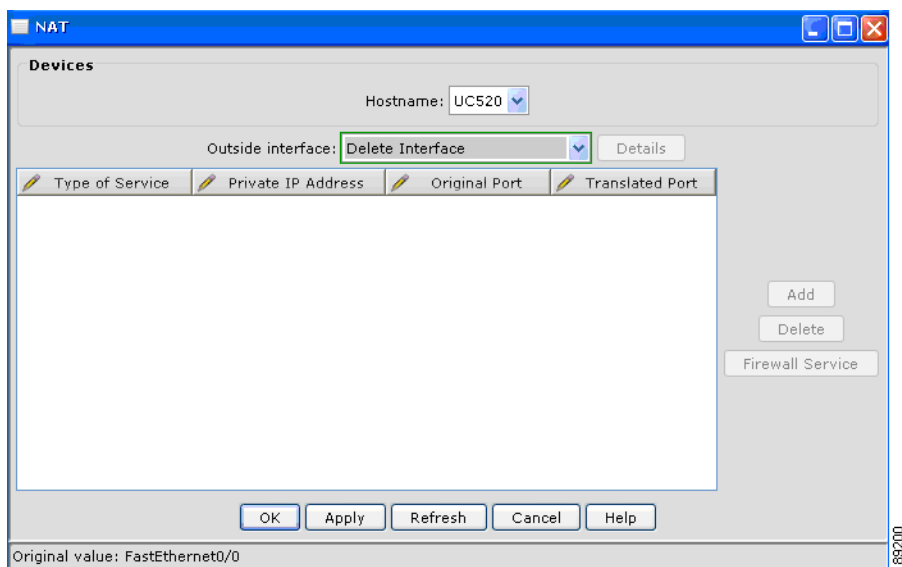
## Configuring the Cisco UC500

Network address translation (NAT) is not required on the UC500 in this configuration, because the SR500 manages NAT for the network. To configure the Cisco UC500 using CCA, do the following:

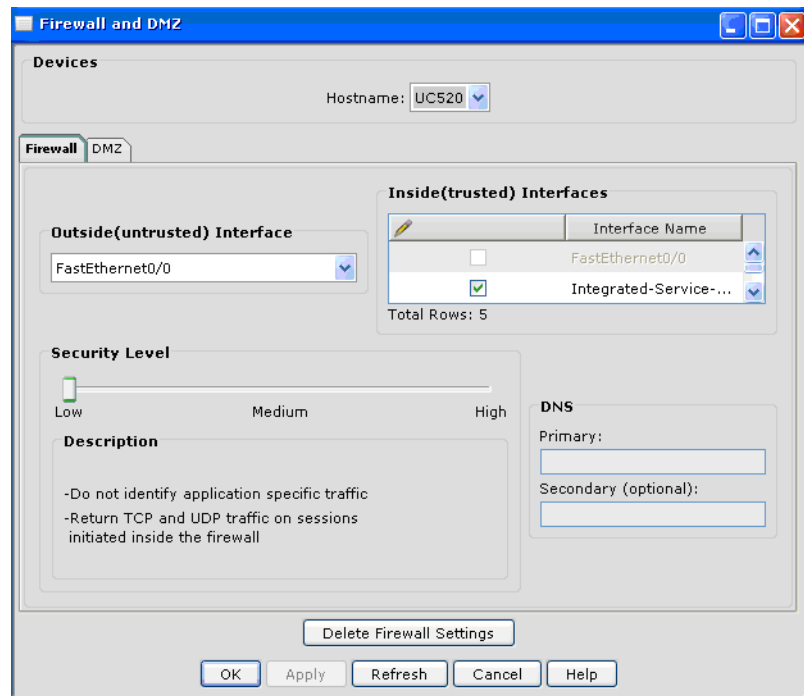
- Step 1** Enter the Cisco UC500 LAN IP address in the Connect to field on the **Connect** window.



- Step 2** Enter your Cisco UC500 administrator username and password.
- Step 3** Go to **Configure > Security > NAT**.
- Step 4** From the **Outside Interface** menu on the NAT window, select **Delete Interface**.
- Step 5** Click **Apply** to disable NAT on the UC500. (The Cisco SR500 will NAT incoming and outgoing Internet traffic; the Cisco UC500 does not require that NAT is enabled.)



- Step 6** Go to **Configure > Security > Firewall and DMZ**.



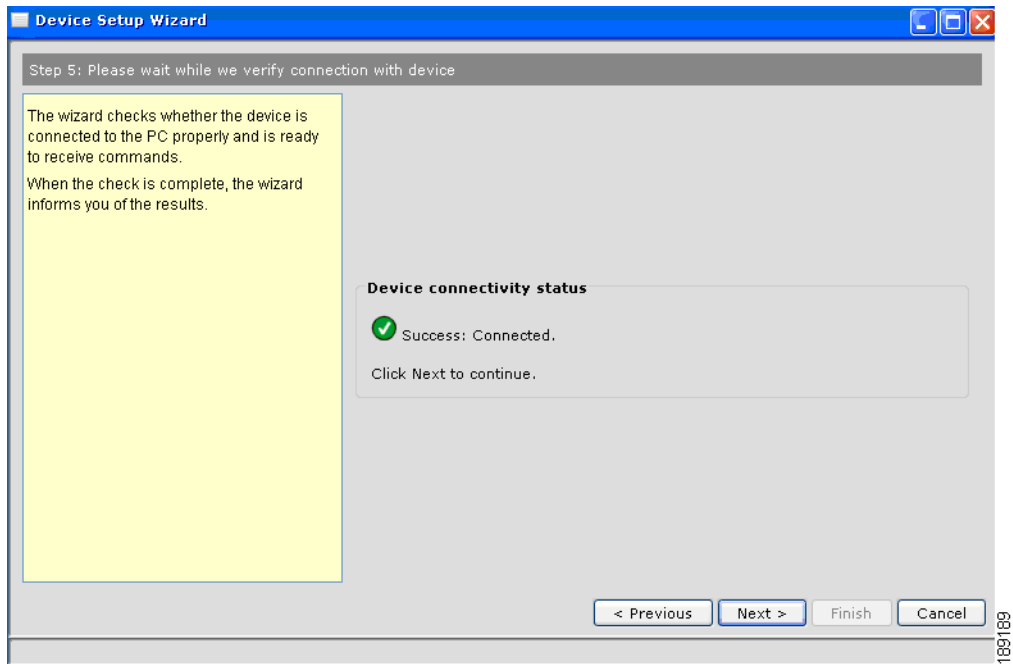
**Step 7** Click **Delete Firewall Settings**.

**Step 8** Click **Yes** to clear the warning message. This deletes the firewall settings from Cisco UC500. A firewall is not required on Cisco UC500, because the Cisco SR500 provides a firewall for the network.

**Step 9** Go to **Setup > Device Setup Wizard**.

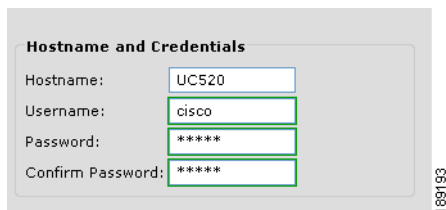
**Step 10** Select **UC500** from the menu and click **Next**.

**Step 11** Click **Next** until device connectivity is verified. It might take 2-3 minutes to verify the device connectivity.

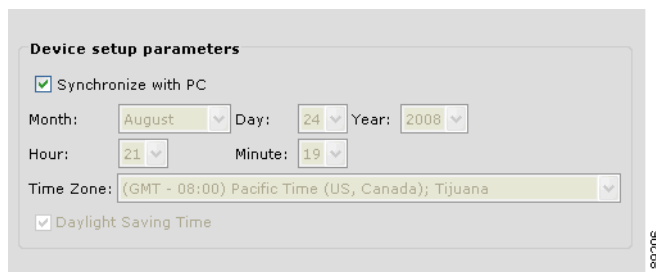


**Step 12** Click Next.

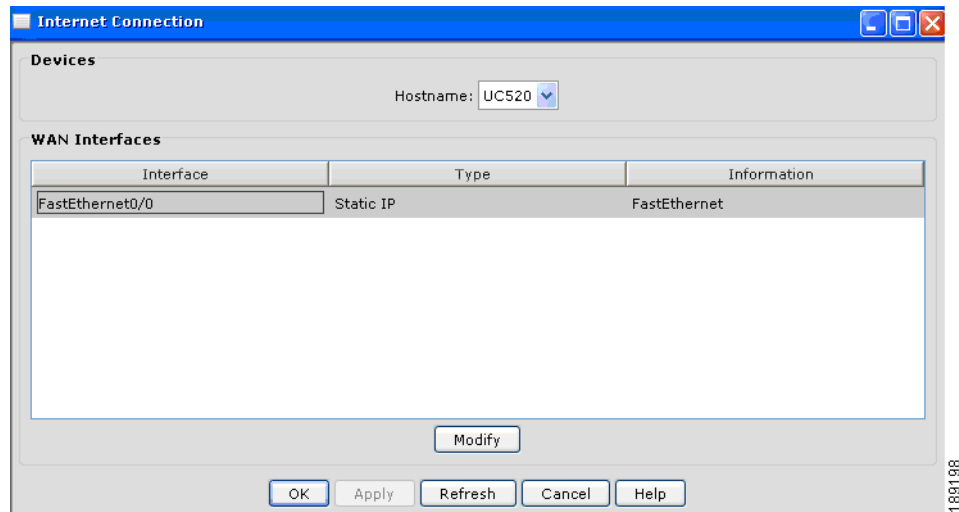
**Step 13** Enter your UC500 administrator username and password. The default username is **cisco**. The default password is **cisco**.



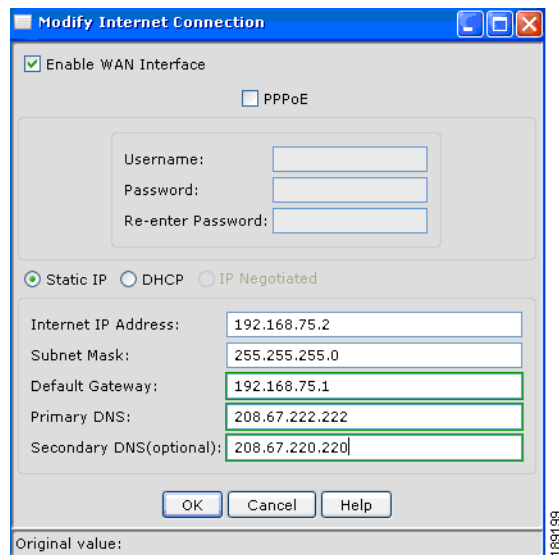
**Step 14** Click Next.



**Step 15** Verify that the **Synchronize with PC** checkbox is checked. This synchronizes the time and date settings on the UC500 with your PC and click **Next**.



**Step 16** Select **Fastethernet0/0** and click **Modify**.



**Step 17** In the Internet IP Address field, enter **192.168.75.2**.

**Step 18** Choose **Static IP**.

**Step 19** Enter the **Primary DNS** IP address and the **Secondary DNS** IP address that match the DNS server IP addresses used in your network and click **OK**.

**VLAN1 IP address assignment**

IP Address: 192.168.10.1  
Subnet Mask: 255.255.255.0

**DHCP Pool**

Network: 192.168.10.1  
Subnet Mask: 255.255.255.0  
Primary DNS: 208.67.222.222  
Secondary DNS(optional): 208.67.220.220  
Default Gateway: 192.168.10.1

**DHCP Exclusions**

Start IP Address: 192.168.10.1  
End IP Address: 192.168.10.10

< Previous   Next >   Finish   Cancel

189208

**Step 20** Click **Next**.

**Local Settings**

Region: United States  
Phone Language: US English  
Voicemail Language: US English  
Location of Language Files: isco Configuration Assistant\appdata\phoneloads\

189197

**Step 21** Select your language from the **Phone Language** menu. and voicemail language.

**Step 22** Select your language **Voicemail Language** menu.

**Step 23** Click **Next**.

**Summary**

Hostname: UC520  
 Username: cisco  
 Region: United States  
 Phone Language: US English  
 Voicemail Language: US English

**VLAN1 Summary**

**IP Address**

IP Address: 192.168.10.1  
 Subnet Mask: 255.255.255.0

**DHCP Server**

Network: 192.168.10.1  
 Subnet Mask: 255.255.255.0  
 Primary DNS: 208.67.222.222  
 Secondary DNS(optional): 208.67.220.220  
 Default Gateway: 192.168.10.1

**DHCP Exclusions**

Start IP Address: 192.168.10.1  
 End IP Address: 192.168.10.10

**Warning**

The setup process may take up to 10 minutes

< Previous    Next >    Finish    Cancel

**Step 24** Verify your settings. To make any changes, click **Previous**; otherwise, click **Finish**.

**Step 25** Click **Yes** when the warning displays.



**Note** If you retained the VLAN 1 IP address of 192.168.10.1, Cisco Configuration Assistant does not lose connectivity to the Cisco UC500 and applies the configuration settings to the Cisco UC500. This process can take 8-10 minutes

Once the process is complete, you should see the following message.

**Finish status**

✓ Success: The settings have been applied to the device.  
 Press Close to exit.

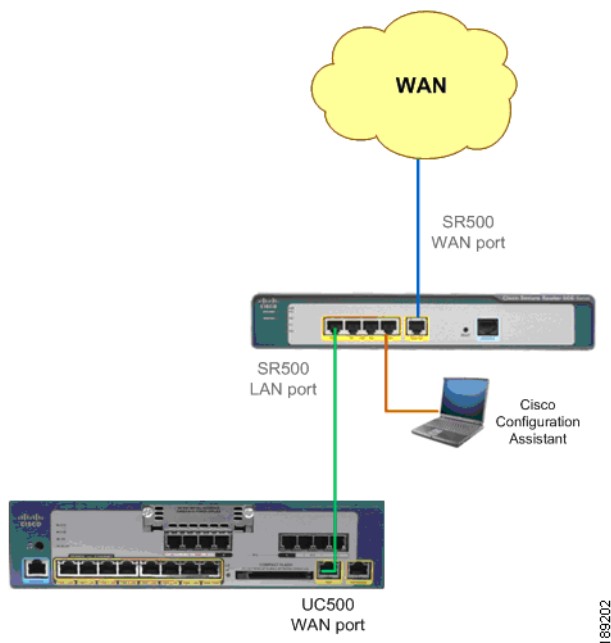
**Step 26** Click **Close** to exit the setup wizard.

**Step 27** Go to **Configure > Save Configuration** and click **Save**.

## Configuring the Cisco SR500

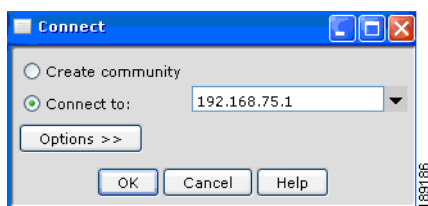
Connect your Cisco UC500, Cisco SR500, and Windows PC as shown in [Figure 5-2](#).

*Figure 5-2 Cisco UC500, Cisco SR500, and Windows PC Connection*



Your Internet/WAN connection might be an ADSL or an Ethernet connection, depending on the Cisco SR500 chassis type.

**Step 1** Enter the SR500 LAN IP address in the **Connect to** field in Cisco Configuration Assistant.



If your connection is rejected, it might be necessary to manually release and renew your DHCP lease to obtain an IP address from the Cisco SR500, by doing the following:

1. To open a **Run** window, select **Start > Run**.
2. Enter **CMD** in the Open field to launch a Windows Command window.
3. Enter **ipconfig /release** at the Windows command prompt.

- Enter **ipconfig /renew** at the Windows command prompt. You should get an IP address that is in the 192.168.75.xxx network. For example:

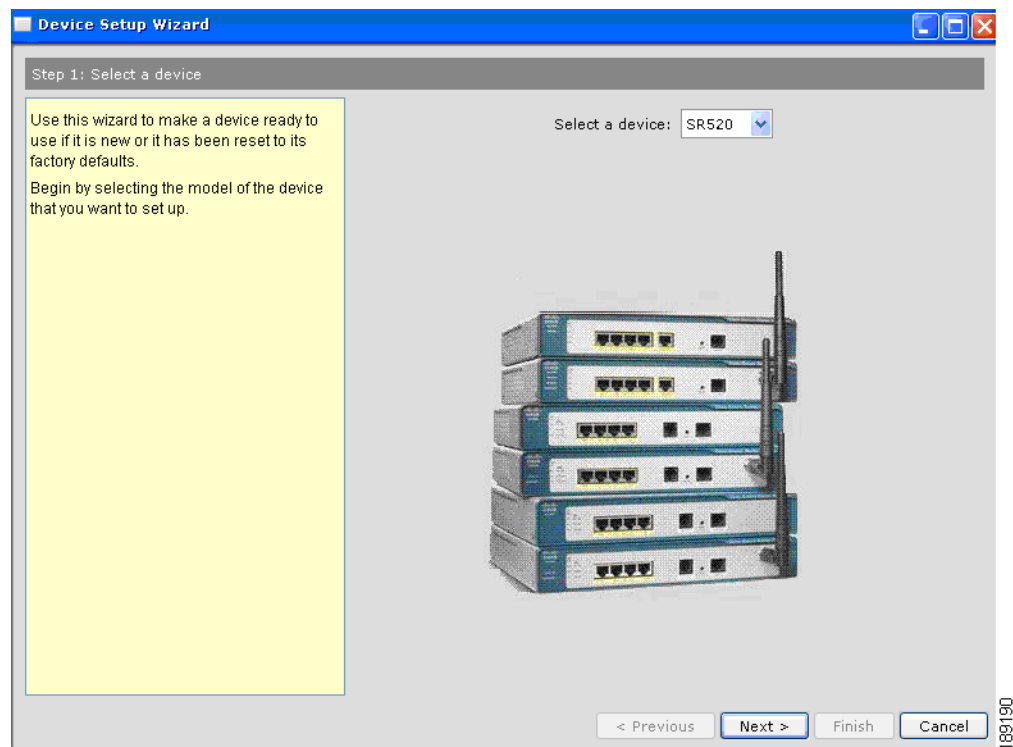
```
C:\temp>ipconfig /renew
```

```
Windows IP Configuration
```

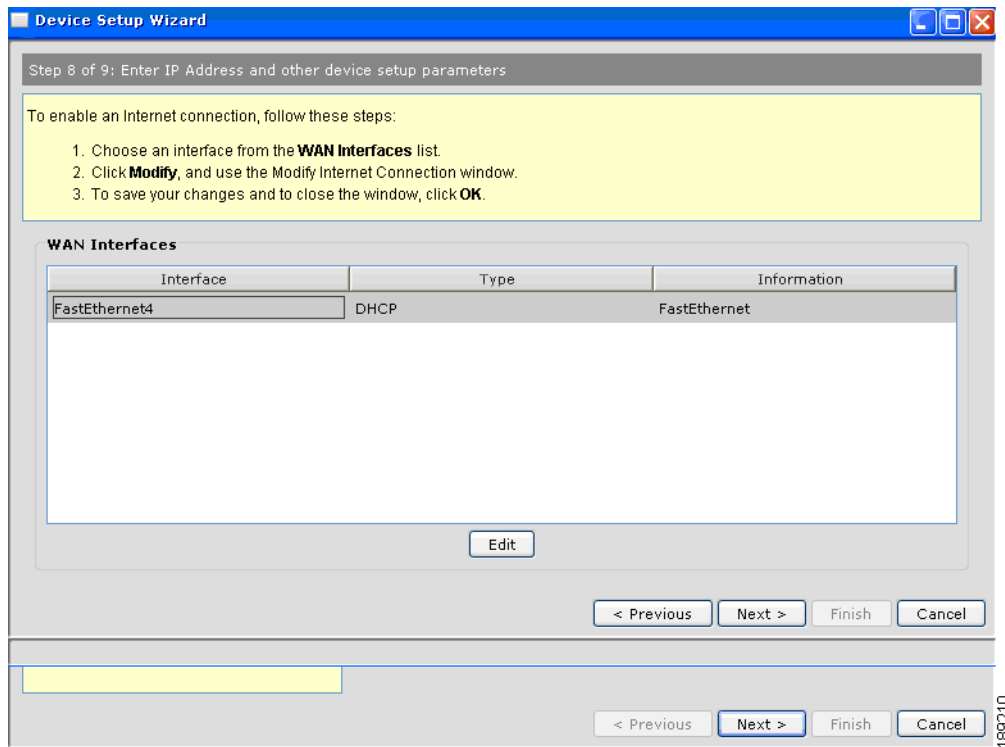
```
Ethernet adapter Local Area Connection:
```

```
Connection-specific DNS Suffix . : cisco.com
IP Address. . . . . : 192.168.75.11
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.75.1
```

- Go to **Setup > Device Setup Wizard**.

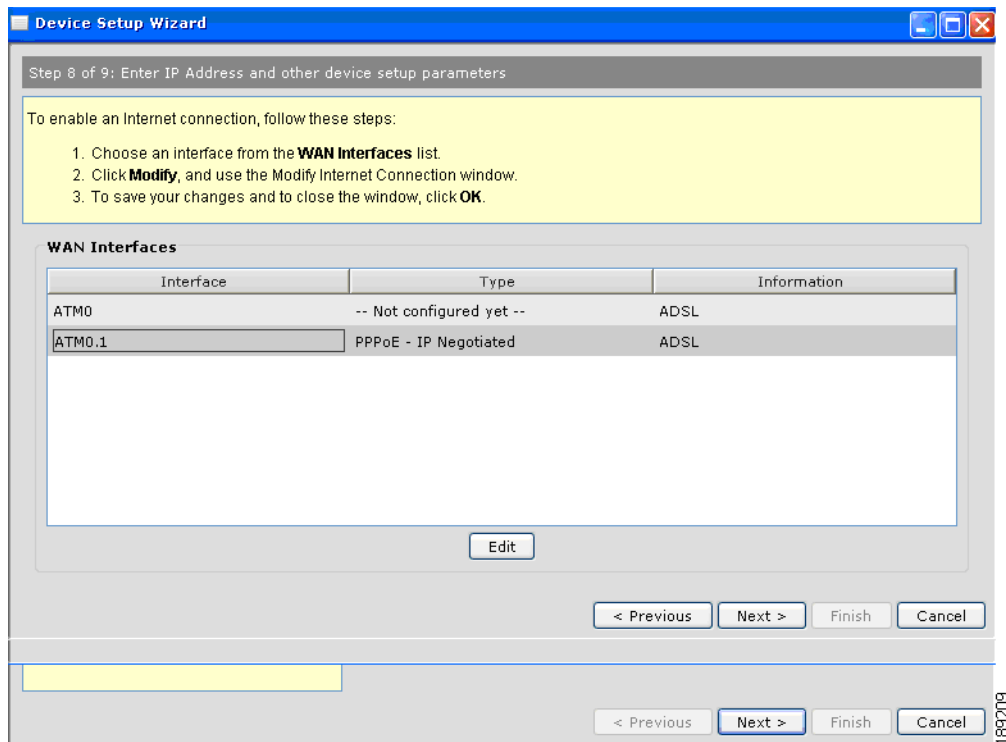


- From the **Select a device** menu, select **SR500** and click **Next**.
- Click **Next** until device connectivity is verified. It might take 2-3 minutes to verify the device connectivity.
- Enter your Cisco SR500 administrator username and password. The default username is **admin**. The default password is **admin**.
- Verify that the **Synchronize with PC** checkbox is checked. This synchronizes the time and date settings on the UC500 with your PC and click **Next**.
- If you are using WAN FastEthernet, the following window displays:



Select **Fastethernet4** and click **Edit**.

If you are using ADSL, the following window displays:



Select **ATM0.1** and click **Edit**.

- Step 8** Specify your Cisco SR500 Internet connection settings and click **OK**. These settings vary depending on which provider and what WAN type you are using to connect to the Internet. For example:

#### DHCP with FastEthernet

The screenshot shows the 'Modify Internet Connection' dialog box. At the top, it says 'Please delete NAT/VPN/Firewal to enable this button'. Below that, there is a checked checkbox for 'Enable WAN Interface' and an unchecked checkbox for 'PPPoE'. Underneath, there are three text input fields for 'Username:', 'Password:', and 'Re-enter Password:'. Below these fields are three radio buttons: 'Static IP', 'DHCP' (which is selected), and 'IP Negotiated'. At the bottom, there are three text input fields for 'Internet IP Address:', 'Subnet Mask:', and 'Default Gateway:'. At the very bottom are three buttons: 'OK', 'Cancel', and 'Help'. A small vertical number '188194' is visible on the right side of the dialog box.

#### PPPoE with FastEthernet.

The username and password should match the account information provided by your Internet service provider.

The screenshot shows the 'Modify Internet Connection' dialog box with different settings. The 'Enable WAN Interface' checkbox is checked, and the 'PPPoE' checkbox is also checked. The 'Username:' field contains the text 'adslmodemuser'. The 'Password:' and 'Re-enter Password:' fields contain six asterisks '\*\*\*\*\*'. The radio buttons are 'Static IP', 'DHCP', and 'IP Negotiated' (which is selected). The 'Internet IP Address:', 'Subnet Mask:', and 'Default Gateway:' fields are empty. At the bottom are 'OK', 'Cancel', and 'Help' buttons. A small vertical number '188195' is visible on the right side of the dialog box.

#### PPPoE with ADSL.

The username and password should match the account information provided by your Internet service provider.

**Step 9** Click **Next**. Verify your settings. To make any changes, click **Previous**; otherwise click **Finish**. After 1-2 minutes, the Summary message displays.

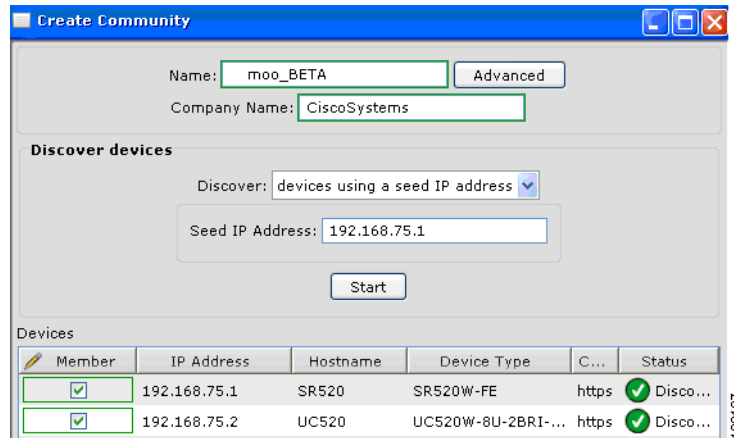
**Step 10** Click **Close**.

The configuration of the Cisco SR500 is complete.

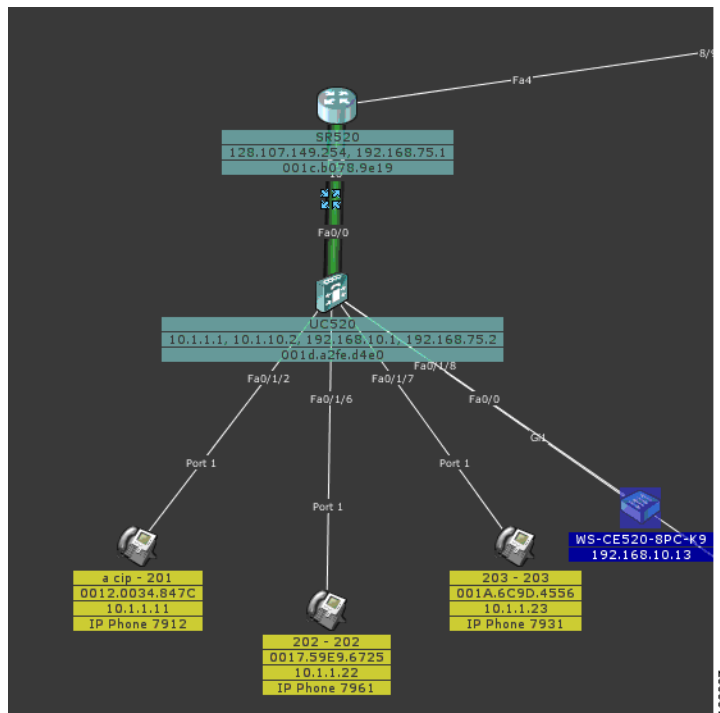
# Creating a Community

To create a community that includes both the Cisco UC500 and the Cisco SR500, do the following:

- Step 1** Start Configuration Assistant, and select **Create community** in the Connect window. Click **Connect**.
- Step 2** In the **Create Community** window, enter a name for the community.



- Step 3** Enter the Cisco SR500 IP address in the Seed IP Address field. Click **Start**.
- Step 4** When prompted, enter the Cisco UC500 and the Cisco SR500 administrator usernames and passwords. Click **OK**.
- Step 5** In Topology view, verify that the Cisco UC500 is connected behind the Cisco SR500.



- Step 6** Go to **Configure > Save Configuration**.
- Step 7** Select **All Devices** in the **Hostname** menu. Click **Save**.



The configuration is complete.

---

You can now connect your Cisco Configuration Assistant PC to any LAN port on the Cisco UC500 or Cisco SR500 to access the community you created, allowing you to monitor the network and modify the device configurations.

You should connect all LAN devices, such as PCs, IP phones, printers, switches, and access points, to the Cisco UC500 LAN ports to access the WAN or the Internet from the LAN devices. LAN devices connected to the UC500 have secure access to the WAN and the Internet, because they are protected by the security features you enabled on the Cisco SR500.

You might choose to connect DMZ devices, such as Web servers or email servers, to the Cisco SR500.



## INDEX

---

### A

- accessing communities [4-2](#)
- asymmetric digital subscriber line (ADSL) [5-1, 5-8](#)
- automatic discovery
  - adding members [4-3](#)
  - considerations
    - connectivity [4-2](#)
    - non-CDP-capable devices [4-4](#)
  - in communities [4-2](#)
- See also CDP

---

### C

- CDP, use of in communities [4-2](#)
- Cisco Discovery Protocol
  - See CDP
- communities
  - accessing [4-2](#)
  - adding members [4-3](#)
  - advantages of [1-1](#)
  - automatic discovery [4-2 to 4-3](#)
  - candidates
    - adding [4-3](#)
    - automatic discovery of members [4-2 to 4-3](#)
    - defined [4-1](#)
    - discovering [4-3](#)
    - requirements [4-1](#)
  - See also community member
  - characteristics [1-1](#)
  - communication protocols [4-3](#)
  - community information [4-3](#)
  - community names [4-2](#)

- composition [4-1](#)
- creating [4-3](#)
- limits [4-1](#)
- management, local PC [4-3](#)
- members
  - adding [4-4](#)
  - automatic discovery [4-2 to 4-3](#)
  - hostnames [4-2](#)
  - requirements [4-1](#)
- planning considerations
  - hostnames [4-2](#)
  - identifying information [4-3](#)
  - passwords [4-3](#)
  - saving identification information [4-3](#)
  - verifying [4-4](#)

- Configuration Assistant
  - connecting [3-2](#)
  - GUI [2-1](#)
  - installing
    - procedure [3-1](#)
    - requirements [3-1](#)
  - introduced [1-1](#)
  - starting [3-2](#)
- connecting Configuration Assistant [3-2](#)

---

### D

- device limits in a community [4-1](#)
- devices, setting up [3-2](#)
- DHCP lease [5-8](#)
- discovery, communities
  - See automatic discovery

DMZ [5-2](#), [5-14](#)

DNS server [5-5](#)

---

## E

events, notice of [3-3](#)

expert mode [2-8](#)

---

## F

FastEthernet [5-11](#)

feature bar [2-4](#)

features

    expert mode [2-8](#)

    feature bar [2-4](#)

    Front Panel view [2-3](#)

    guide mode [2-7](#)

    menu bar [2-4](#)

    online help [2-9](#)

    privilege levels [2-9](#)

    toolbar [2-5](#)

    Topology view [2-2](#)

firewall [5-3](#)

---

## G

guide mode [2-7](#)

---

## H

hostnames, reason for assigning [4-2](#)

---

## I

installing Configuration Assistant

    procedure [3-1](#)

    requirements [3-1](#)

interaction modes [2-7](#)

IP address

    seed [5-13](#)

IP address requirement [4-1](#)

---

## L

language [5-6](#)

limitations for communities [4-1](#)

---

## M

member devices, adding [4-3](#)

menu bar [2-4](#)

---

## N

network address translation (NAT) [5-2](#)

network events, notification [3-3](#)

---

## O

online help [2-9](#)

---

## P

passwords, prompts for [4-3](#)

phone, language [5-6](#)

ports, configuring device connections [2-8](#)

PPPoE [5-11](#)

privilege levels [2-9](#)

---

## S

seed IP address [5-13](#)

setting up devices [3-2](#)

SR500 5-1

- administrator default username 5-9
- community 5-13
- default password 5-9

starting Configuration Assistant 3-2

---

## T

toolbar 2-5

Topology view 2-2, 5-13

---

## U

UC500 5-1

- administrator default username 5-4
- community 5-13
- default password 5-4

---

## V

VLAN 1 IP address 5-7

voicemail

- language 5-6

---

## W

WAN type 5-11

