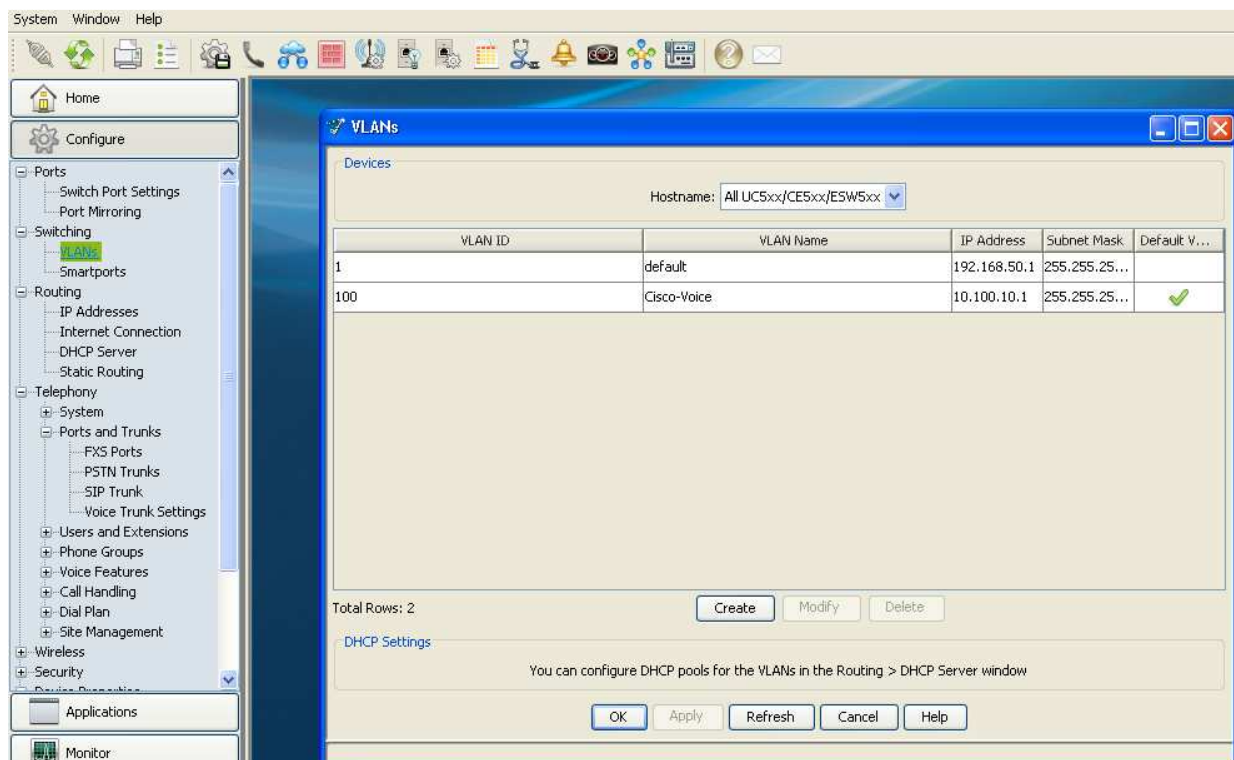


Cisco Small Business Pro

Smart Business Communication System

Technical Enablement Labs



LAB

UC 540/560 Adding a new VLAN

Overview 3

Information Required 4

Links for more info 4

Configuration 5-13

 Intital Setup

 Creating the VLAN

 DHCP Pool creation

 DHCP exculsions

Switch Configuration 14-15

 CCA changes

 Web GUI change

Topology options 18

AP541N 19

General Help 20 - 23

Overview

The UC540/560 platform allows a partner to add a new VLAN outside of the two that come preconfigured on the system. This functionality will allow separating of video or guest VLAN traffic from the voice and data traffic. This makes better use of the box by separating the video stream or guest access of the internal data/voice traffic, therefore allowing you to control the access to your network. By separating the video traffic off the data network, you can have the camera's broadcasting the max frame rate and size to the internal storage (NSS) or to the SPA525 phones.

The lab will focus on the use of the PVC2300 camera's that are supported by CCA 3.0 at this time and will establish a feed that will be recorded on a NSS2000 that is on the data VLAN (1). I will have two PVC2300 camera's using the VLAN25, with the IP address of 192.168.25.X network. The existing data VLAN1 use's the IP address of 192.168.50.X and is set to give out DHCP to the network. The gateway for the system is 192.168.50.1 with a class subnet of 255.255.255.0. The UC560/540 is configured using CCA3.0 on software pack 8.1.0. At this time the PVC2300/WVC2300 cameras are supported, but it can be configured to use any cameras in the SMB Line.

I will be using the ESW500 series switches for the connection to the camera's, as they have the ability to do smartport roles. This allows me to control what IP address the camera will receive when connected to the ports.

The screenshot shows a 'VLANs' configuration window. At the top, there's a 'Devices' section with a 'Hostname' dropdown set to 'All UC5xx/CE5xx/ESW5xx'. Below this is a table of existing VLANs:

VLAN ID	VLAN Name	IP Address	Subnet Mask	Default V...
1	default	192.168.50.1	255.255.25...	
100	Cisco-Voice	10.100.10.1	255.255.25...	✓

Below the table, there's a 'Create VLAN' dialog box with the following fields:

- VLAN ID:[2 - 1000]:
- VLAN Name:
- ☐ Make Default Voice VLAN
- IP Address:
- Subnet Mask:

At the bottom of the dialog are 'OK', 'Cancel', and 'Help' buttons. Below the dialog, the main window shows 'Total Rows: 2' and a 'DHCP Settings' section with a message: 'You can configure DHCP pools for the VLANs in the Routing > DHCP Server window'. At the bottom of the main window are 'OK', 'Apply', 'Refresh', 'Cancel', and 'Help' buttons.

Information Required

You will need the following information to add a new VLAN to your UC560/540

1. CCA 3.0
2. Software pack 8.1.0
3. VLAN # and a naming plan
4. IP scheme for the different VLAN's
5. Updated firmware on the camera
6. Updated firmware on the switch's involved
7. Be sure to add all the devices to you community in CCA3.0
8. Good attitude and just a little patience

Here are the links to find useful information or pull the latest firmwares for the equipment in your network. Valid CCOID is required for some of the software. Most of the SMB cameras, switched and access point's software can be downloaded without the need to login.

Download site

<http://www.cisco.com/cisco/web/support/index.html>

Support Forum

<https://supportforums.cisco.com/community/netpro/small-business>

Software packs

<https://upload.cisco.com/cgi-bin/swc/fileexg/main.cgi?CONTYPES=UC500>

Smart Designs

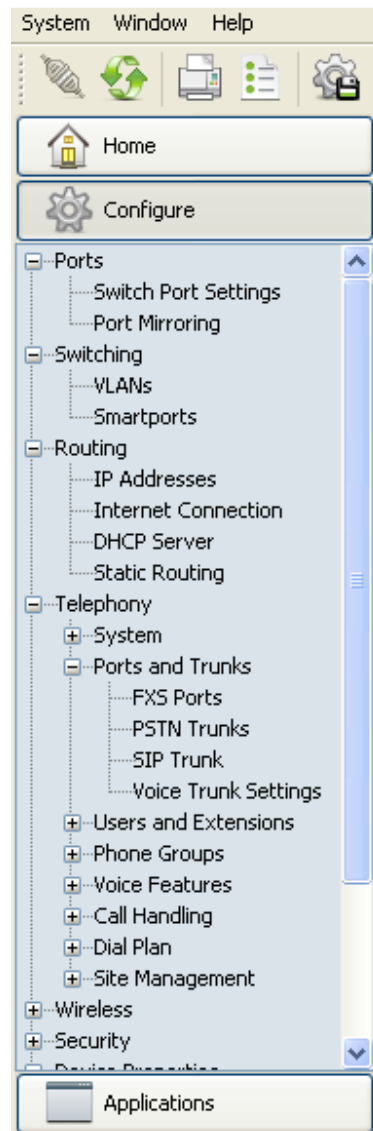
http://www.cisco.com/web/partners/sell/smb/tools_and_resources/validated_commercial_solutions.html

Support Phone #'s

http://www.cisco.com/en/US/support/tsd_cisco_small_business_support_center_contacts.html

INITIAL SETUP

After logging into CCA 3.0 and establishing the proper credentials, you will need to navigate to the configure section of the screen. You will then see the following information displayed on your screen.



Choose the following section. Switching -> VLANs and click on the button

This will bring up the box to set the VLAN's up and push the config out to the ESW switches. Yes the ESW switch line will automatically see the new VLAN's by default and allow you to pass them along to devices in the network.

VLANs

Devices

Hostname: All UC5xx/CE5xx/ESW5xx

VLAN ID	VLAN Name	IP Address	Subnet Mask	Default V...
1	default	192.168.50.1	255.255.25...	
100	Cisco-Voice	10.100.10.1	255.255.25...	✓

Total Rows: 2

Create Modify Delete

DHCP Settings

You can configure DHCP pools for the VLANs in the Routing > DHCP Server window

OK Apply Refresh Cancel Help

Click on the create button

VLANs

Devices

Hostname: All UC5xx/CE5xx/ESW5xx

VLAN ID	VLAN Name	IP Address	Subnet Mask	Default V...
1	default	192.168.50.1	255.255.25...	
100	Cisco-Voice	10.100.10.1	255.255.25...	✓

Create VLAN

VLAN ID:[2 - 1000]:

VLAN Name:

☐ Make Default Voice VLAN

IP Address:

Subnet Mask:

OK Cancel Help

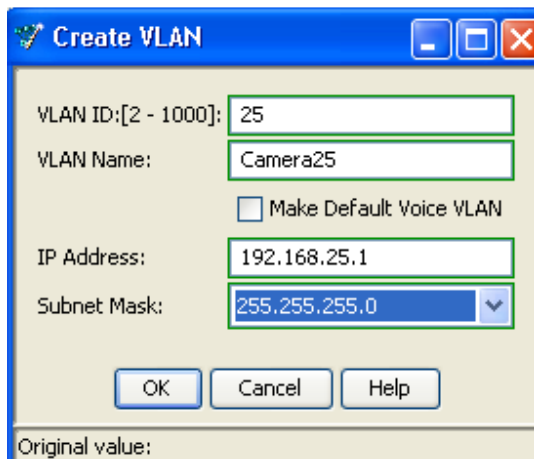
Create Modify Delete

DHCP Settings

You can configure DHCP pools for the VLANs in the Routing > DHCP Server window

OK Apply Refresh Cancel Help

Add the VLAN ID (# that you want for the VLAN) I chose VLAN25 for the camera and 75 for the GUEST VLAN. Name the VLAN and give it an IP address. The IP will be 192.168.25.1 with a class C subnet of 255.255.255.0 for the Camera VLAN25 and 192.168.75.1 /24 for the GUEST VLAN75.



Create VLAN

VLAN ID:[2 - 1000]: 25

VLAN Name: Camera25

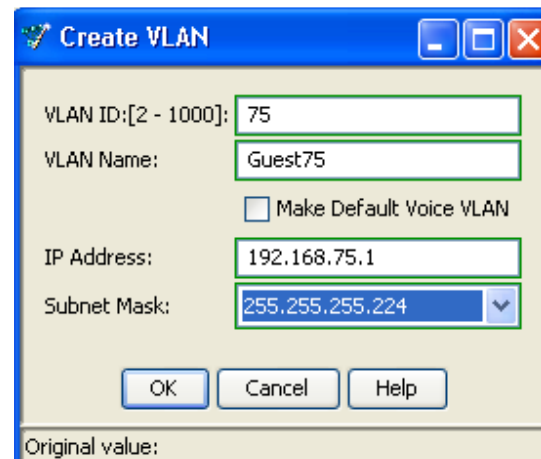
☐ Make Default Voice VLAN

IP Address: 192.168.25.1

Subnet Mask: 255.255.255.0

OK Cancel Help

Original value:



Create VLAN

VLAN ID:[2 - 1000]: 75

VLAN Name: Guest75

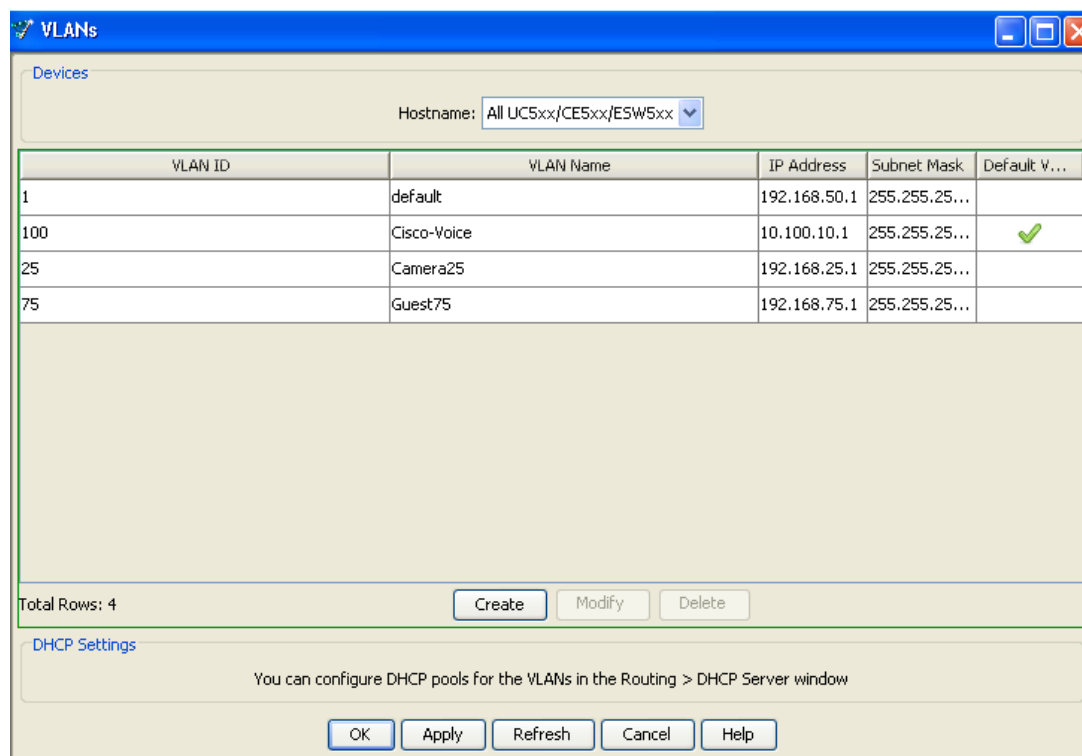
☐ Make Default Voice VLAN

IP Address: 192.168.75.1

Subnet Mask: 255.255.255.224

OK Cancel Help

Original value:



VLANs

Devices

Hostname: All UC5xx/CE5xx/ESW5xx

VLAN ID	VLAN Name	IP Address	Subnet Mask	Default V...
1	default	192.168.50.1	255.255.25...	
100	Cisco-Voice	10.100.10.1	255.255.25...	✓
25	Camera25	192.168.25.1	255.255.25...	
75	Guest75	192.168.75.1	255.255.25...	

Total Rows: 4

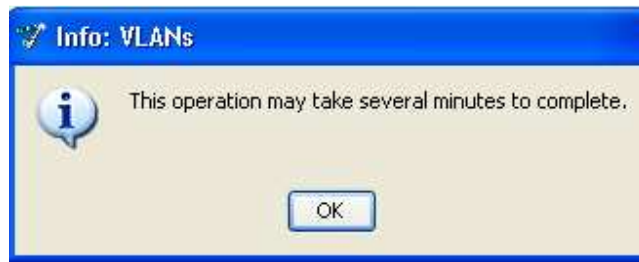
Create Modify Delete

DHCP Settings

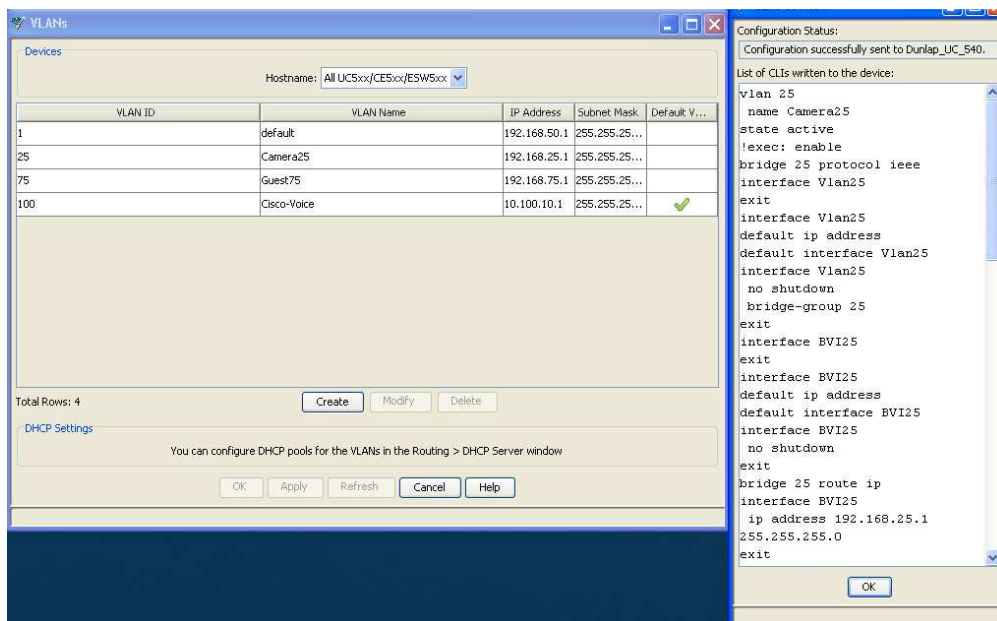
You can configure DHCP pools for the VLANs in the Routing > DHCP Server window

OK Apply Refresh Cancel Help

You then click on apply to add the VLAN's to all the devices in the discovered network.

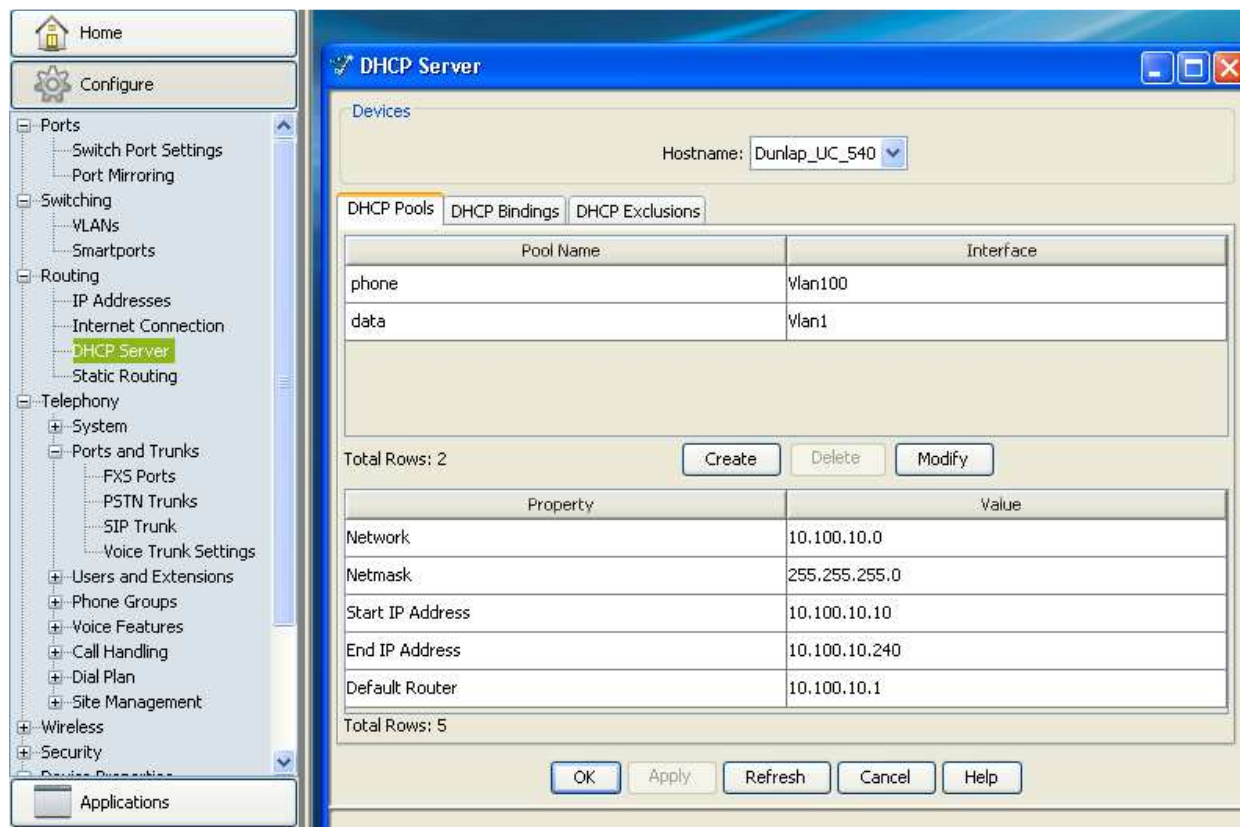


You will then see the CLI output of the action of adding the VLAN's to your network.

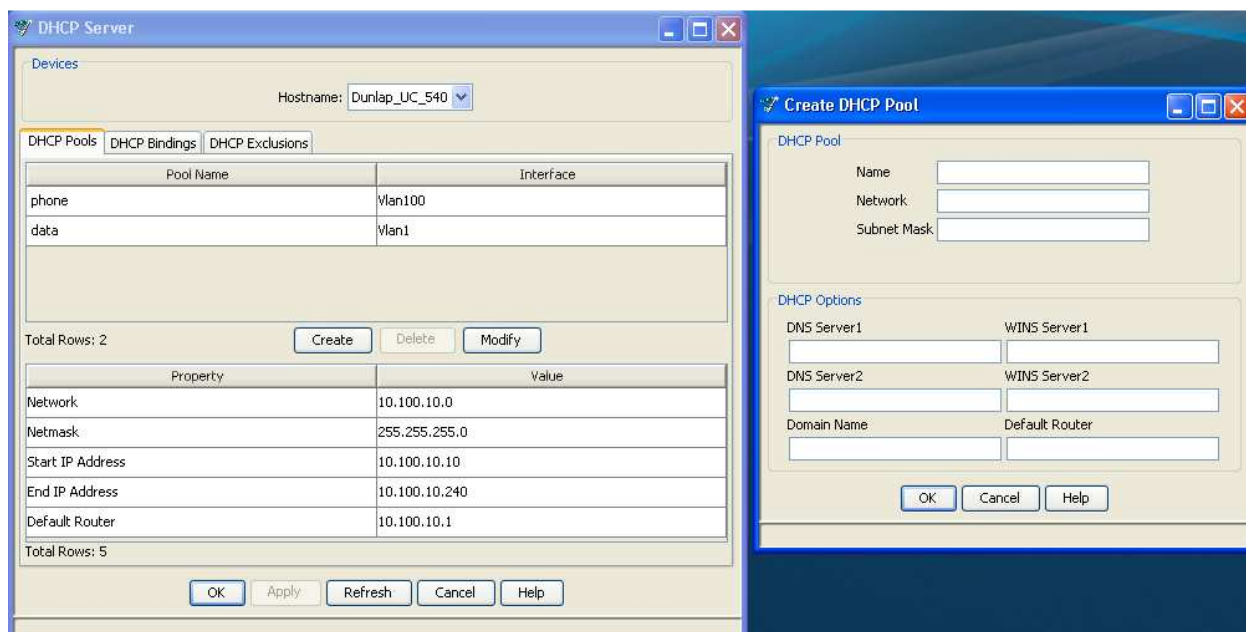


Close down the screens and then go to the next step in the process.

Click on the following section to add the DHCP pool to the different VLAN's that you just setup.



Click on the create button to establish what IP address will be available for the attached devices to use. You will notice that you can set the pool to 1 IP address, but add the exception list to block out static IP's that you will assign the camera's when staging the unit.



Create DHCP Pool

DHCP Pool

Name:

Network:

Subnet Mask:

DHCP Options

DNS Server1: WINS Server1:

DNS Server2: WINS Server2:

Domain Name: Default Router:

Original value:

Create DHCP Pool

DHCP Pool

Name:

Network:

Subnet Mask:

DHCP Options

DNS Server1: WINS Server1:

DNS Server2: WINS Server2:

Domain Name: Default Router:

Original value:

DHCP Server

Devices

Hostname:

DHCP Pools | DHCP Bindings | DHCP Exclusions

Pool Name	Interface
phone	Vlan100
data	Vlan1
Cameras	Vlan25
Guest	Vlan75

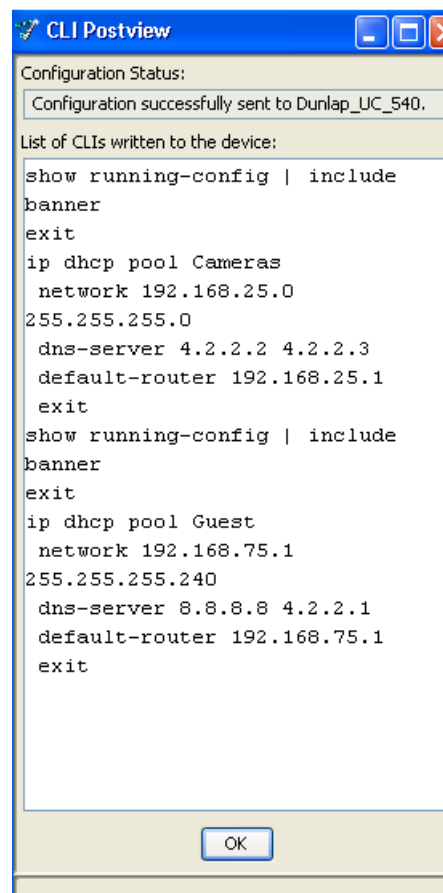
Total Rows: 4

Property	Value
Network	192.168.25.0
Netmask	255.255.255.0
Default Router	192.168.25.1
DNS Server1	4.2.2.2
DNS Server2	4.2.2.3

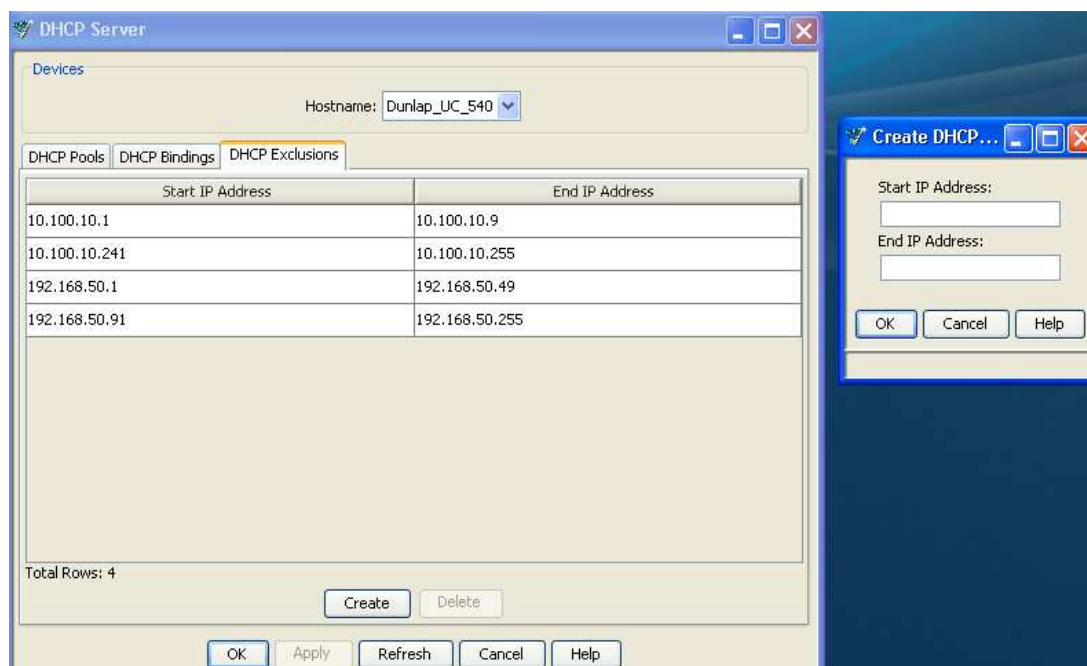
Total Rows: 5

Original value:

Once you set them up, save your config and then add the exceptions to your planned network



After getting the successful config applied message click back to the DHCP Exclusions section, seen below



DHCP Pools		DHCP Bindings		DHCP Exclusions	
Start IP Address			End IP Address		
10.100.10.1			10.100.10.9		
10.100.10.241			10.100.10.255		
192.168.50.1			192.168.50.49		
192.168.50.91			192.168.50.255		
192.168.25.1			192.168.25.50		
192.168.75.1			192.168.75.20		

Total Rows: 6

Create Delete

Then click on apply to set the exclusions up for the different VLAN's

CLI Postview

Configuration Status:

Configuration successfully sent to Dunlap_UC_540.

List of CLIs written to the device:

```

show running-config | include
banner
exit
ip dhcp excluded-address
192.168.25.1 192.168.25.50
ip dhcp excluded-address
192.168.75.1 192.168.75.20

```

OK

You will be able to click back on the screen and look at the information on both of the new VLAN's and see the following info

DHCP Server

Devices

Hostname: Dunlap_UC_540

DHCP Pools

DHCP Bindings

DHCP Exclusions

Pool Name	Interface
phone	Vlan100
Cameras	Vlan25
Guest	Vlan75
data	Vlan1

Total Rows: 4

Create

Delete

Modify

Property	Value
Network	192.168.25.0
Netmask	255.255.255.0
Start IP Address	192.168.25.51
End IP Address	192.168.25.254
Default Router	192.168.25.1
DNS Server1	Default Router 4.2.2.2
DNS Server2	4.2.2.3

Total Rows: 7

OK

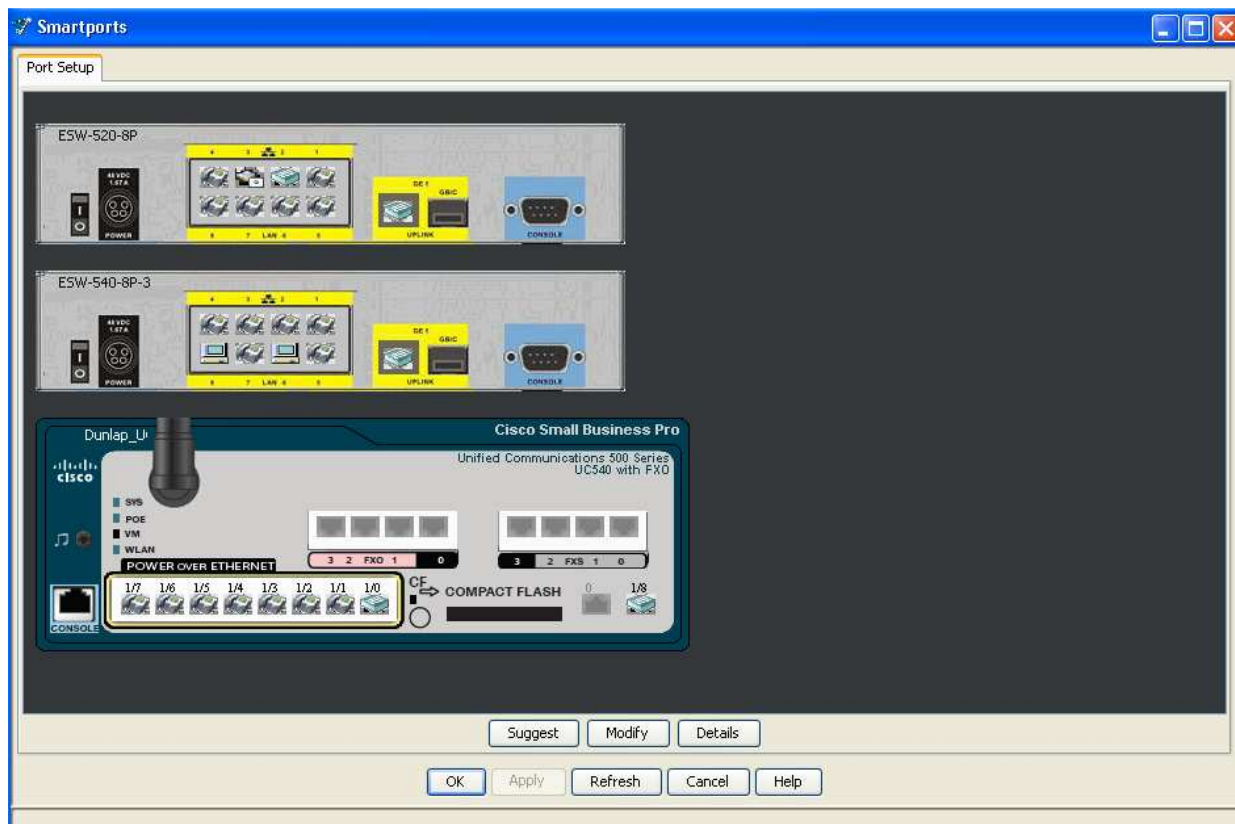
Apply

Refresh

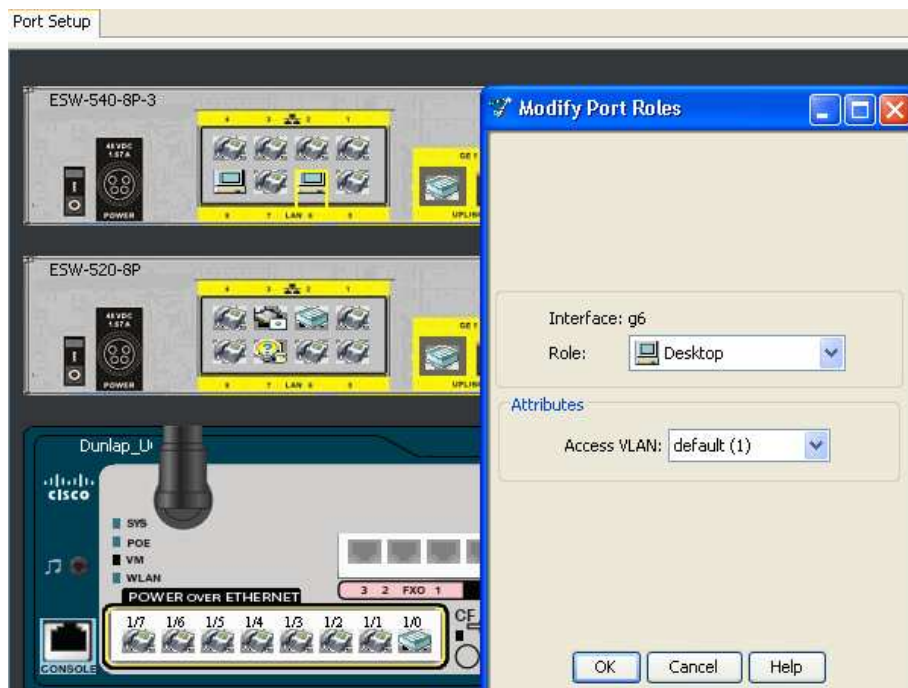
Cancel

Help

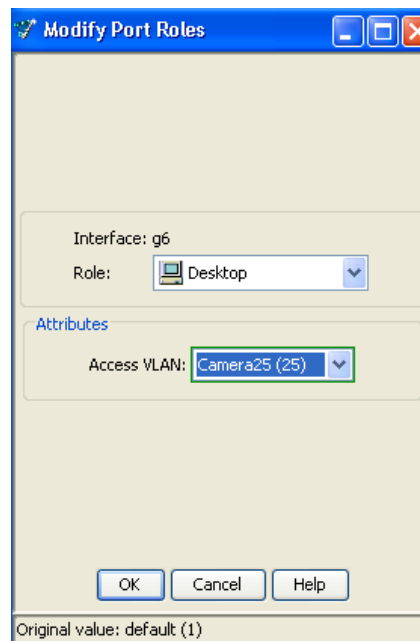
At this point will need to log into the switch, this can be done from two different points, the smart ports wizard in CCA 3.0 or the web GUI for the switch itself. NOTE, be sure to have the camera's staged at this point to use DHCP off the ports that they will plug into or stage them to use a static IP within the range that you have setup during the last steps.



When you highlight and click modify the port role you will see the following information in a pop up screen.



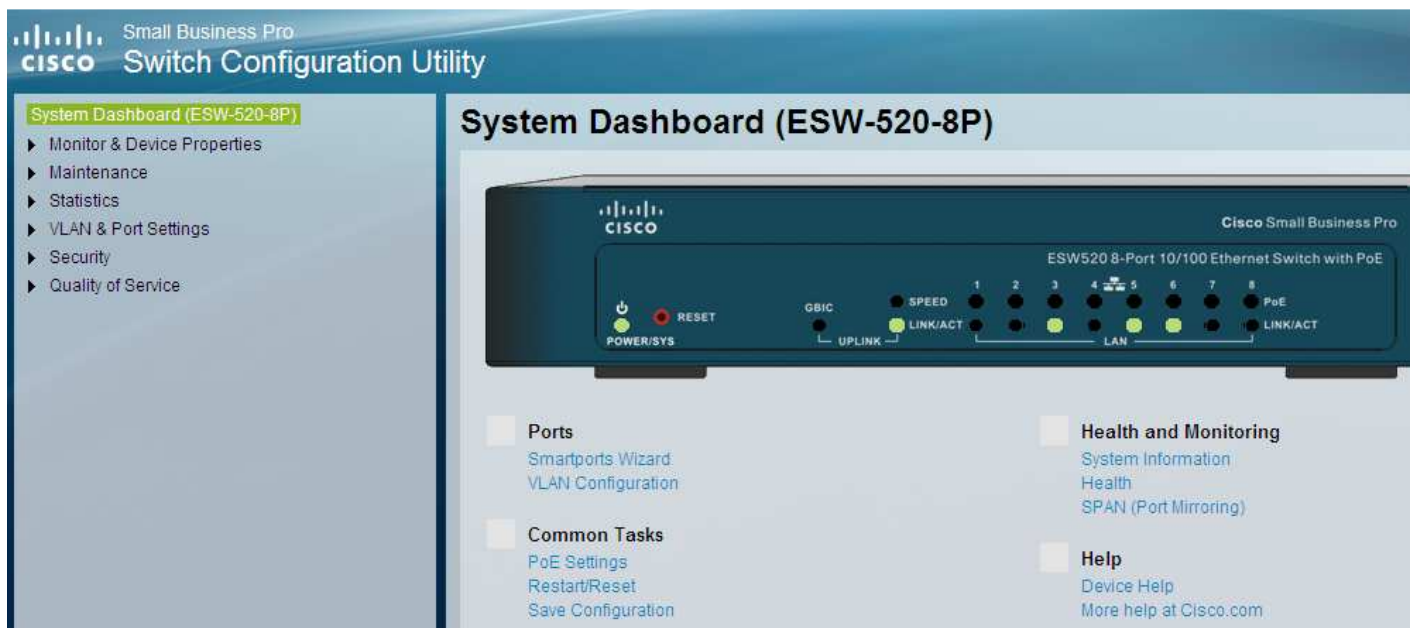
Change the role of the port to show the following information



And then click OK to set the port to use the VLAN25 (192.168.25.x) as its access VLAN

Click on apply to change the role and you are done. Then you can plug the camera into the port and it should be visible using the IP that you set on the camera or that was assigned using DHCP.

Or the WEB GUI for the switch itself (IP Address in a web browser) 192.168.50.2 in my lab



Smart Ports Setting

Select Port/s for Profile:



[Select All](#) [Clear All](#)

Assign Profile:

[Next](#)

Select the appropriate port role for the port on the switch

Smart Ports Setting

Select Port/s for Profile:



[Select All](#) [Clear All](#)

Assign Profile:

Desktop

IP Phone + Desktop

Access Point

Switch

Router

Guest

Server

Printer

VS Camera

Other

Change the default VLAN to reflect the role of the port (Which VLAN do you want the port to see). In my example we have chosen VLAN25.

VS Camera ➤

Ports	e7
VLAN Port Mode	Access
VLAN ID	25 ▼
Port Security Mode	Dynamic Lock
Max MAC Addresses	1
Port Security Action	Discard
Violation Trap Every	60 Sec
Broadcast Storm Control	10%
Spanning Tree Port Fast	Enabled
Spanning Tree BPDU Guard	Enabled
QoS Policy	video-surveillance-map
Macro Description	VSCamera

Back

Apply

Then click on the apply button, this will allow any device that is plugged into that port to pull on the VLAN25 or IP address of 192.168.25.X off it.

VS Camera Setting Status ➤

Successful ports: e7

Port	All Selected
VLAN Port Mode	✓
VLAN Membership	✓
Port Security	✓
Broadcast Storm Control	✓
Spanning Tree	✓
Quality of Service	✓

OK

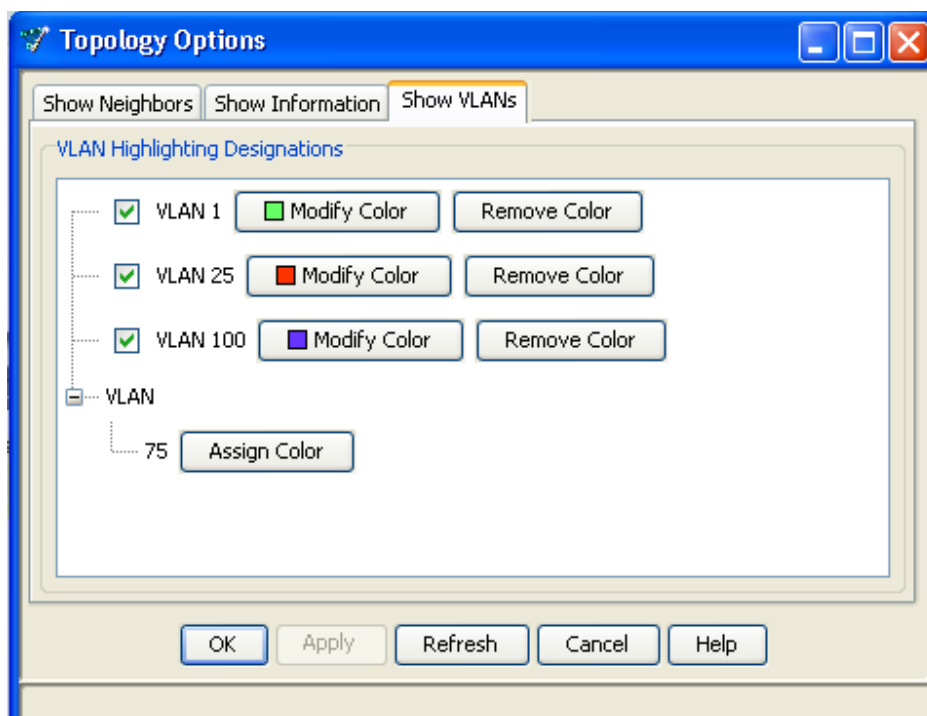
The role of the port has successfully been changed to a video port using VLAN25 on it. You will notice the symbol look's different on port 7 of the switch.

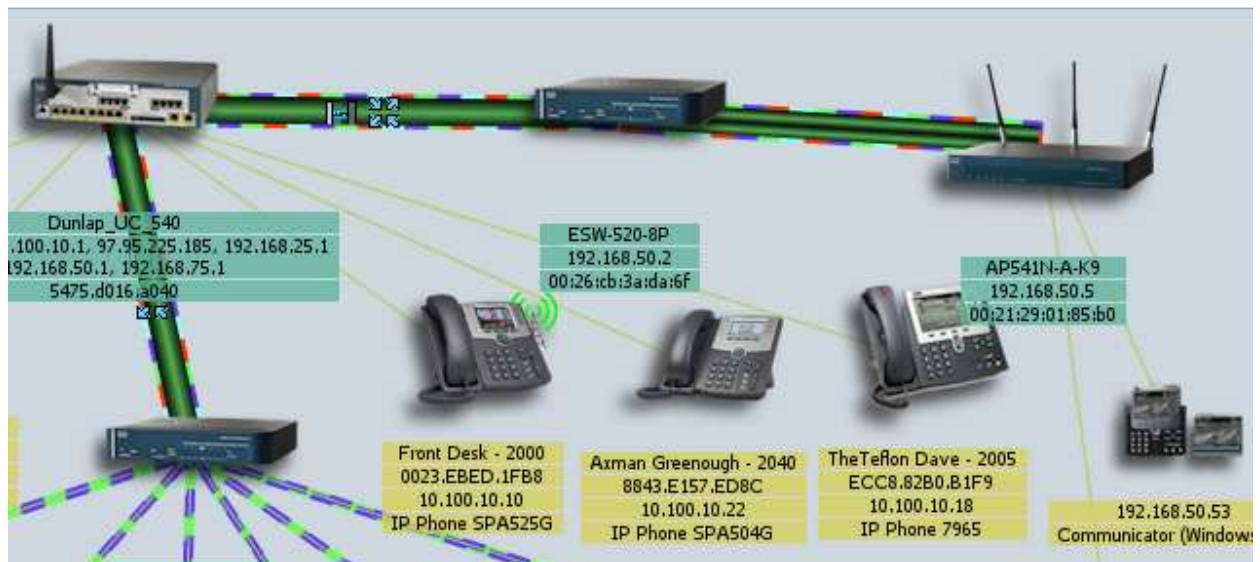
Select Port/s for Profile:



This should allow the video cameras on the network to use VLAN25 (192.168.25.X), while the data network will use VLAN1 (192.168.50.X). The same for the guest network will apply; note that the guest VLAN will be able to see the data network at this time. The CCA team has proposed the ability to block this in future versions of CCA. This change will allow you to configure the ACCESS-LIST to block that traffic from everything internal, but allow you to access the internet. This block can only be done in CLI at this time.

The following section will give you screenshots of the AP541N and the topology view once you have configured the UC540/560 with the new VLAN's. Notice that you can change the view on the topology view to show the VLAN's leaving the UC500 to the other devices.





AP541N

Wireless Network Setup (VAPs)

► Global RADIUS server settings

▼ Configure Virtual Access Points (SSIDs)

VAP	Enabled	VLAN ID	SSID	Broadcast SSID	Security	MAC Filtering	Station Isolation	HTTP Redirect	Redirect URL	Delete
0	<input checked="" type="checkbox"/>	1	dunlap-data	<input checked="" type="checkbox"/>	WPA Personal	Disabled	Disabled	Disable		
					Show details					
1	<input checked="" type="checkbox"/>	100	dunlap-voice	<input type="checkbox"/>	None	Disabled	Disabled	Disable		<input checked="" type="checkbox"/>
2	<input checked="" type="checkbox"/>	25	dunlap-camera	<input type="checkbox"/>	WPA Personal	Local	Enabled	Disable		<input checked="" type="checkbox"/>
					Show details					
3	<input checked="" type="checkbox"/>	75	dunlap-guest	<input checked="" type="checkbox"/>	None	Disabled	Disabled	Enable	http://www.cisco.com	<input checked="" type="checkbox"/>

Click "Apply" to save the new settings.

Apply

Add Another

General Help for VLAN Config

VLANs

This window appears when you choose **Configure > Switching > VLANs** on the feature bar.

When you select a device from the **Hostname** list, you see the following information for each VLAN:

- VLAN ID
- VLAN name
- IP address, subnet, and subnet mask
- Default Voice VLAN (indicated by a Green checkmark)

If VLAN-synchronized devices such as a UC500, ESW500 Series switches, and Catalyst Express CE520 switches are part of the customer site, the **Hostname** device selector displays the value **All UC5xx/CE/ESW**.

See the following sections for more information about VLANs and VLAN settings:

- [Overview](#)
- [Notes](#)
- [Procedures](#)

Overview ▼

You can create VLANs for the following devices:

- All UC500 devices
- All SR500 devices
- All C8xx devices

A VLAN (Virtual LAN) is a switched network that is logically segmented by function, project team, or application, without regard to the physical locations of the users. VLANs have the same attributes as physical LANs, but you can group end stations even if they are not physically located on the same LAN segment. Any switch port can belong to a VLAN, and uncast, broadcast, and multicast packets are forwarded and flooded only to the end stations in the VLAN.

VLANs define broadcast domains in a Layer 2 network. A broadcast domain is the set of all devices that receive broadcast frames originating from any device within the set. Broadcast domains are typically bounded by routers because routers do not forward broadcast frames. Layer 2 switches create broadcast domains based on the configuration of the switch. Switches are multiport bridges that allow you to create multiple broadcast domains. Each broadcast domain is like a distinct virtual bridge within a switch.

You can define one or many virtual bridges within a switch. Each virtual bridge that you create in the switch defines a new broadcast domain (VLAN). Traffic cannot pass directly to another VLAN (between broadcast domains) within the switch or between two switches. To interconnect two different VLANs, you must use routers or Layer 3 switches.

By default, switches are configured with a single VLAN, VLAN 1. If you want to create additional VLANs, you can do this from the VLAN window. You can also use this window to change the name of a VLAN or to remove it.

When you create, modify, or delete a VLAN on a switch or a Unified Communications 500 Series platform, your action is automatically duplicated on all the devices of these types in your customer site. The duplication preserves VLAN consistency among the devices. If you add a device to the site that already has a VLAN associated with it, a VLAN conflict occurs with the devices that do not have this VLAN association. When this happens, you are prompted to use the VLAN Synchronization Window to restore VLAN consistency. See [VLAN Synchronization](#).

Notes ▼

The following notes apply to VLAN creation and modification:

- Up to 15 VLANs can be associated with a device. All devices are associated by default with VLAN 1.
- Only the VLAN Name and VLAN ID are synchronized to ESW500 and CE520 switches.
- In a multisite deployment, VLANs can only be configured on the local UC500. VLAN changes made on the local UC500 are not applied to other UC500s in the multisite deployment, and only local devices are synchronized.

Procedures ▼

To create a VLAN, select a **Hostname**, click **Create**, and complete the settings in the Create VLAN window. See [Create VLAN](#).

To change the name, IP address, subnet, or subnet mask of a VLAN, select the VLAN in this window, and click **Modify**. See [VLAN Synchronization](#). VLAN 1 is reserved by CCA, so you cannot modify its name or VLAN ID.

To remove a VLAN, select it, and click **Delete**.

When you are finished making changes, click **OK** or **Apply**.

For more information, see these topics:

- [Create VLAN](#)
- [VLAN Synchronization](#)

Help with DHCP Config

DHCP Server

To configure DHCP Server settings, choose **Configure > Routing > DHCP Server** from the feature bar.

Overview ▼

A DHCP (Dynamic Host Configuration Protocol) IP address pool is a range of IP addresses that a DHCP server can dynamically issue to client devices. Because not all clients are connected all the time, providing IP addresses as needed reduces the number of IP addresses required to serve a group of clients by reusing the same IP address for different clients at different times.

To manage the DHCP IP address pool, you can:

- Create a DHCP IP address pool that identifies the range of IP addresses in the pool.
- Bind a specific IP address in the pool to a specific MAC address, creating a static IP address for that client device. (Some clients require static IP addresses to maintain connectivity to support running applications.)
- Exclude specific IP address from the pool so that they will not be assigned to a client by the DHCP server. (A few IP addresses in the range might have been assigned through other processes. To avoid conflicts, you can exclude those addresses from the pool.)

The range of the pool is calculated from the network number and subnet mask. All available node-level IP addresses are included in the pool and made available to the server unless they are specifically bound to a MAC address or excluded from the pool; the server ignores manual address bindings and exclusions.

The DHCP Server window has these tabs:

- **DHCP Pools:** Display, create, modify, or delete a DHCP pool of IP addresses.
- **DHCP Bindings:** Manually assign IP addresses in the DHCP pool to the MAC addresses of clients.
- **DHCP Exclusions:** Specify the IP address that the DHCP server should not assign to (exclude from) clients.

DHCP Pools ▼

A DHCP (Dynamic Host Configuration Protocol) IP address pool is a range of IP addresses that a DHCP server can dynamically issue to client devices.

Two default DHCP pools are created for the UC500: **phone** and **default**. These default DHCP pools can be modified, but these default pool names are reserved and cannot be modified.

- The **phone** pool is associated with the Voice VLAN (VLAN 100) on the UC500. IP addresses from the phone DHCP pool are assigned to IP phones during auto-registration.
- The **data** pool is associated with the Data VLAN (VLAN1) on the UC500. IP addresses from this pool are assigned to devices on the data VLAN that request an IP address from the DHCP server.

To display the properties configured for a DHCP pool, click on the DHCP pool name.

To create a new DHCP pool, click **Create**, and use the Create DHCP Pool window. See [Create DHCP Pool](#).

To modify an existing DHCP pool, choose the DHCP pool, click **Modify**, and use the Modify DHCP Pool window. See [Modify DHCP Pool](#).

To delete a DHCP pool, choose the DHCP pool name, and then click **Delete**. A window appears, warning you that if you proceed, you will delete the DHCP pool.

To close the window, click **OK**.

DHCP Bindings ▼

After you create a DHCP pool, you can manually assign IP addresses from that pool to specific devices based on their MAC address.

To create a new DHCP binding, click **Create**, and use the Create DHCP Binding window. See [Create DHCP Binding](#).

To modify an existing DHCP binding, choose the pool name, click **Modify**, and use the Modify DHCP Binding window. See [Modify DHCP Binding](#).

To delete a DHCP binding, choose the DHCP binding name, and then click **Delete**. A window appears, warning you that if you proceed, you will delete the DHCP binding.

To close the window, click **OK**.

DHCP Exclusions ▼

From this tab, you specify individual IP addresses or ranges of IP address to be excluded from the DHCP address pool. These addresses cannot be assigned to DHCP clients.

To create a new DHCP exclusion, click **Create**, and use the Create DHCP Exclusion window. See [Create DHCP Exclusion](#).

To delete DHCP exclusion, choose the IP address, and click **Delete**.

By default, these IP addresses are excluded from DHCP pools:

- 10.1.1.1 through 10.1.1.10 (reserved for Cisco IOS and CUE)
- 192.168.10.1 through 192.168.10.10 (reserved for the UC500)
- 10.1.1.255 and 192.168.10.255 broadcast addresses

DHCP Pool Bindings ▼

Two types of DHCP pool bindings can be used:

- Automatic binding — The DHCP server will create the binding. After the lease time expires, the device may get a new IP address.
- Manual binding — Use a manual binding if you want this device to use this IP address. The lease does not expire.

For more information or issues please contact the SBSC (STAC) at 1-866-606-1866 or open a TAC online to troubleshoot the issue.