



Integrating the UC500 into an existing Network

This lab exercise provides general guidelines for inserting an UC500 into an existing network.

The following document illustrates the process that needs to be followed if the UC500 is being installed in an existing network.

The information in this document applies to CCA Version 1.9 and Cisco SBCS software package version 1.4.

Network with Existing Firewalls

Deployment Scenario #1 - UC500 behind ALG Capable Firewall

In this Deployment Scenario, the Firewall or ASA provides Internet connectivity and provides the Application Layer Gateway capabilities (ALG) for protocol fix-up and application-aware Network Address Translation (NAT). It is up to this device to maintain state and create the appropriate pinholes for the traffic coming from the UC500 (data and voice).

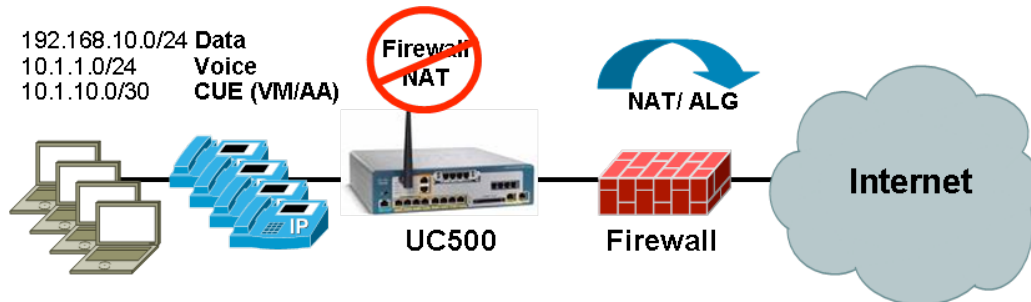
You need to ensure the following policies are applied to the firewall:

- If IPsec is used (for a multi-site data VPN and the Data LAN resides behind the UC500), make sure that the firewall allows access to the following ports and protocols:
 - ✓ IP Protocol ID 50, for both inbound and outbound filters. It should be set to allow Encapsulating Security Protocol (ESP) traffic to be forwarded.
 - ✓ UDP Port 500, for both inbound and outbound filters. It should be set to allow ISAKMP traffic to be forwarded.
- SIP and/or H.323 protocols must be allowed if doing IP trunks or multisite voice:
 - ✓ UDP Port 5060 for SIP.
 - ✓ TCP port 1720 for H.225 and 11000-65535 for H.245.
- The UDP range from 16384-32767 (inbound and outbound) must be open in order for VoIP Real Time Protocol (RTP) traffic to be transmitted correctly. Notice this port range is the one used by Cisco voice gateways. Other vendors may require different port numbers.
- Additional Services that may need to be allowed:
 - ✓ DNS, UDP port 53.
 - ✓ NTP, UDP port 123.
 - ✓ SNMP, UDP ports 161 (messages) and 162 (traps).
 - ✓ Applications and protocols used by LAN Clients (such as HTTP and HTTPS)

Depending on the application, additional ports would need to be allowed. A list of ports is shown in the **Commonly Used Protocols by the UC500** section, later in this document.

The embedded firewall on the UC500 needs to be turned off. Additionally, NAT must be turned off. Make sure your network routing configuration has knowledge of the IP subnet on the LAN side of the UC500 after disabling NAT.

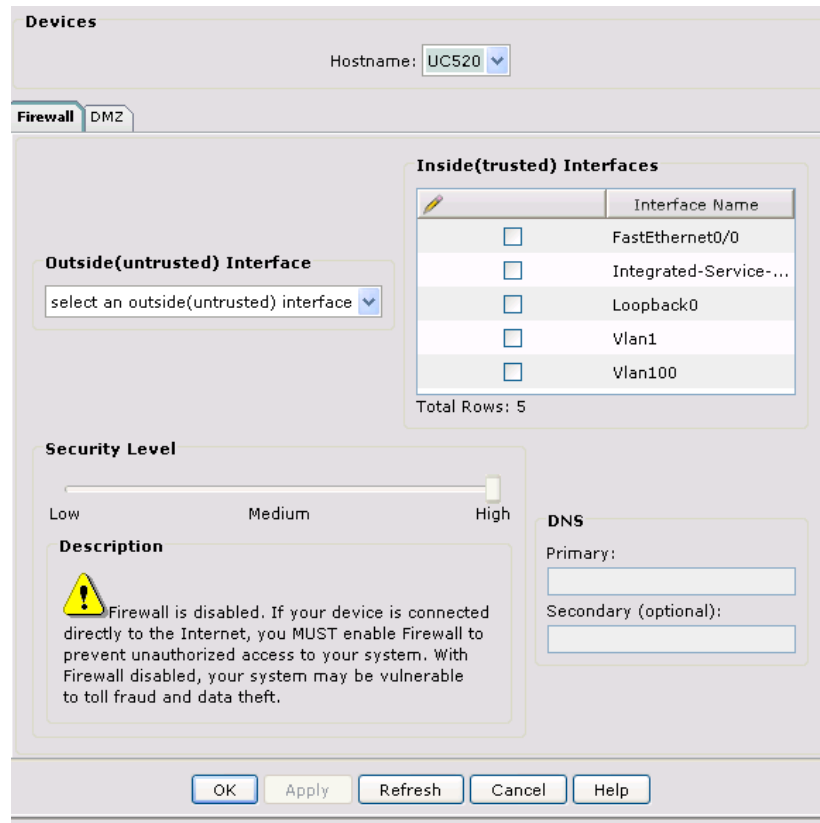
It is recommended that a static IP is assigned to the WAN interface of the UC500, for ease of administration and better control of the security policies.



To disable the UC500 embedded firewall on the UC500, follow these steps:

- Step 1. Open the Cisco Configuration Assistant (CCA) and connect to the UC500
- Step 2. Navigate to **Configure >> Security >> Firewall and DMZ**
- Step 3. Click **Delete Firewall Settings**.
- Step 4. Click **Yes** to clear the warning message. This deletes the firewall settings from Cisco UC500.

You will see the following screen:



To disable NAT on the UC500, follow these steps:

- Step 5. Open the Cisco Configuration Assistant (CCA) and connect to the UC500
- Step 6. Navigate to **Configure >> Security >> NAT**
- Step 7. Click on **Delete NAT Settings** menu on the NAT window, and click **OK**.

You will see the following screen:

The screenshot shows the 'Devices' configuration window in Cisco Configuration Assistant (CCA). The window title is 'Devices'. At the top, there is a 'Hostname' dropdown menu set to 'UC520'. Below that is an 'Outside interface' dropdown menu set to 'Choose Interface', with a 'Details' button to its right. A table with four columns is visible: 'Application', 'Internal Address', 'Internal Port', and 'External Port'. Each column has a pencil icon to its left. The table is currently empty. To the right of the table are three buttons: 'Add', 'Delete', and 'Firewall Service'. At the bottom of the window, there is a status bar that says 'NAT Disabled' and a row of five buttons: 'OK', 'Apply', 'Refresh', 'Cancel', and 'Help'.

The UC500 can be integrated with the Secure Router 520, which is an SBCS product that can be configured using CCA. The following document offers more information about this integration:

http://www.cisco.com/en/US/docs/net_mgmt/cisco_configuration_assistant/version1_8/quick/guide/English/UC500SR500.html

Deployment Scenario #2 - UC500 behind Firewall, no ALG Support

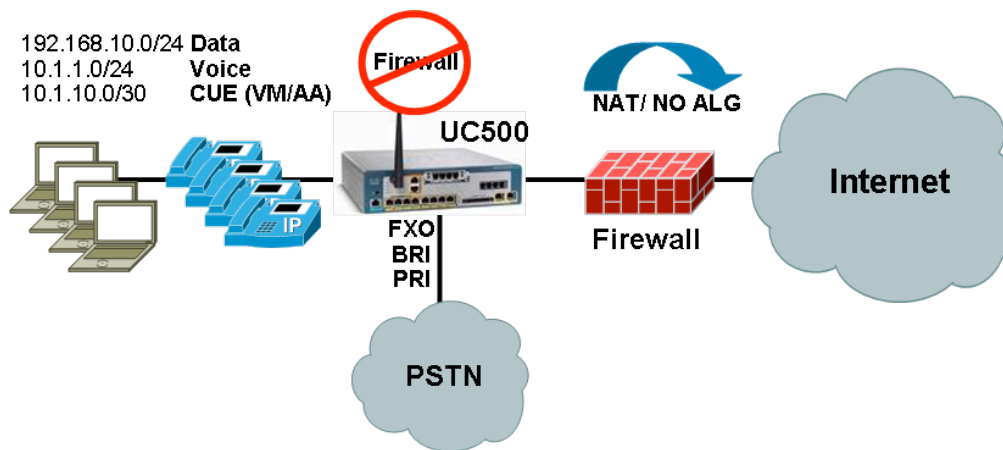
The UC500 can sit behind a firewall that has no ALG and only provides basic NAT functions. NAT could be disabled on the UC500.
Note: If you decide to disable NAT on the UC500, make sure your network routing configuration has knowledge of the IP subnet on the LAN side of the UC500.

A 3rd party Firewall may serve the Data LAN but it is shown behind the UC500 in this example.

No ALG support on the firewall means that VoIP protocols will not work over the Internet. This deployment is used when the UC500 is only doing POTS for voice (using locally connected voice ports).

The UC500 firewall needs to be disabled in this scenario. To disable the UC500 embedded firewall on the UC500, follow these steps:

- Step 1. Open the Cisco Configuration Assistant (CCA) and connect to the UC500
- Step 2. Navigate to **Configure >> Security >> Firewall and DMZ**
- Step 3. Click **Delete Firewall Settings**.
- Step 4. Click **Yes** to clear the warning message. This deletes the firewall settings from Cisco UC500.



When deploying this scenario, please consider the following:

- If IPsec is used (for a multi-site data VPN and the Data LAN resides behind the UC500), make sure that the firewall allows access to the following ports and protocols:
 - ✓ IP Protocol ID 50, for both inbound and outbound filters. It should be set to allow Encapsulating Security Protocol (ESP) traffic to be forwarded.
 - ✓ UDP Port 500, for both inbound and outbound filters. It should be set to allow ISAKMP traffic to be forwarded.
- Additional Services that may need to be allowed:
 - ✓ DNS, UDP port 53.
 - ✓ NTP, UDP port 123.

- ✓ SNMP, UDP ports 161 (messages) and 162 (traps).
- ✓ Applications and protocols used by LAN Clients (such as HTTP and HTTPS)

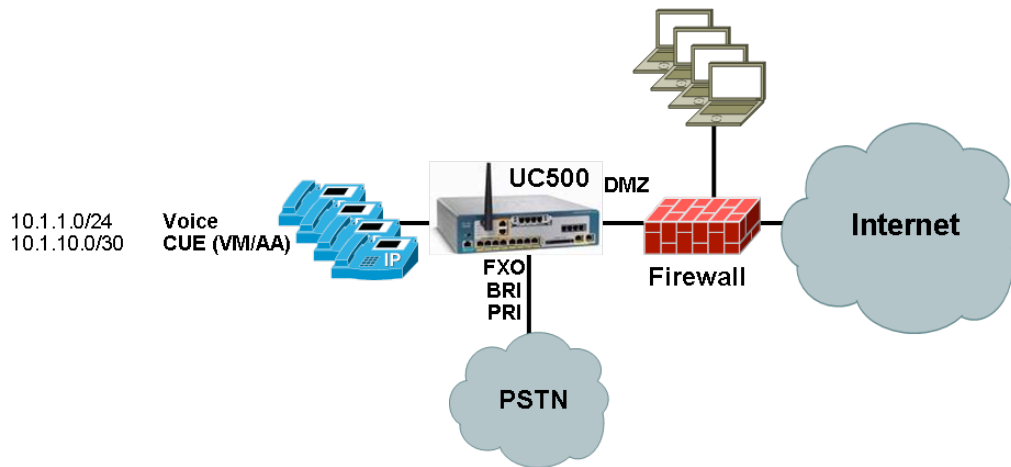
Depending on the application, additional ports would need to be allowed. A list of ports is shown in the **Commonly Used Protocols by the UC500** section, later in this document.

Deployment Scenario #3 - UC500 located in the Firewall's DMZ

The UC500 can also sit on the firewall's Demilitarize Zone (DMZ), so all protocols are allowed. This advanced port forwarding may not offer ALG capabilities, so it is a common deployment when the UC500 is only doing POTS for voice (using locally connected voice ports), so no SIP/H.323 is in the picture.

The UC500 will likely need a static IP address assigned to its WAN interface, for ease of administration and better control of the security policies. This IP may be public or private.

The diagram below shows the data subnet being served by the Firewall directly. No special configuration is needed on the UC500. Please refer to the 3rd party firewall documentation for instructions on how to create and administer a DMZ.

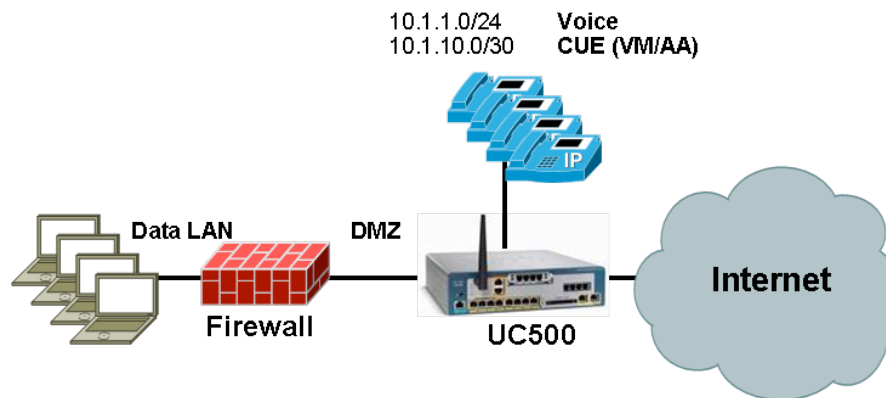


Deployment Scenario #4 - Firewall deployed on the UC500's DMZ

The UC500 system can also be integrated with an existing network where a firewall already exists and serves the Data LAN. The UC500 becomes the then Internet access device. The Firewall is placed in the UC500's Demilitarized Zone (DMZ) and is given a static IP. This IP may be public or private.

This model can also be used to integrate with Microsoft Small Business Server (SBS). Microsoft SBS has some requirements that are unique. It must run a DHCP server and it acts like a gateway for data devices on the network. It can also run VPN, Firewall, Email, and Web Hosting Services.

The following diagram depicts the proposed deployment topology:



Please note that additional static routing may be needed on the UC500 to reach the Data LAN, in the case where the firewall is not doing NAT.

To configure the above scenario, follow these steps:

- Step 1. Open the Cisco Configuration Assistant (CCA) and connect to the UC500
- Step 2. Navigate to **Configure >> VLANs**.
- Step 3. Create a new VLAN and give it the name "DMZ". Apply your changes.
- Step 4. Navigate to **Configure >> Smartports** and select the physical port that will connect to your DMZ. Click **Modify** and map it to the newly created VLAN. Make sure you select "Desktop" as the smartport Role. Apply your changes.
- Step 5. Navigate to **Configure >> Device Properties >> IP Addresses**. Assign an IP address to the new VLAN interface and apply your changes.
- Step 6. Navigate to **Configure >> Security >> Firewall and DMZ**. Click on the **DMZ** tab.
- Step 7. Select the VLAN interface as your DMZ interface and apply the changes.
- Step 8. (Optional) Navigate to **Configure >> Routing >> Static Routing**, and add routes pointing to the Data LAN if needed.

If the data LAN physically connects to the UC500 switch ports, or to the IP phones, you may need to disable the UC500's DHCP server. To do this:

- Step 9. Open the Cisco Configuration Assistant (CCA) and connect to the UC500
- Step 10. Navigate to **Configure >> DHCP Server**.
- Step 11. Delete the Data DHCP Server and apply your changes.

Commonly Used Protocols by the UC500

The following tables illustrate some commonly used voice and data ports by the UC500 Cisco Unified Communications Manager (CUCME) application, as well as the protocols used by Cisco Unity Express (CUE):

CUCME Voice:

Protocol	Port	Usage
SCCP	TCP 2000	Call control for SCCP phones
SIP	TCP 5060	Call control for SIP endpoints
RTP	UDP 16384-32767	Media from Cisco Unified CME to H.323/SIP endpoint, including Cisco Unity Express
RTP	UDP 2000	Media from Cisco Unified CME to SCCP phone
H.225	TCP 1720	H.323 Call Setup
H.245	TCP 11000-65535	H.323 Call control, port assignment random
H.323 RAS	UDP 1718	GK Discovery
H.323 RAS	UDP 1719	GK Call Control
H.323 RAS	UDP 223.0.1.4	GK Multicast discovery
TLS	TCP 3804	CAPF Authentication Request
TLS	TCP 2443	Secure Call control for SCCP phones

CUCME Data:

Protocol	Port	Usage
DHCP	UDP 67	IP addressing for IP phones
HTTP	TCP 80	Cisco Unified CME GUI access, IP phone local directory access
HTTPS/SSL	TCP 443	Secure Cisco Unified CME GUI access
NTP	UDP 123	Time sync for Cisco Unity Express, IP Phones
Radius	UDP 1645	Authentication for Cisco Unified CME CLI/GUI users
Radius	UDP 1646	CDR accounting
SNMP	UDP 161	Traps for Cisco Unified CME monitoring
SSH	TCP 22	Secure Cisco Unified CME CLI access
Syslog	UDP 514	System monitoring, CDR accounting
Telnet	TCP 23	Cisco Unified CME CLI access

Cisco Unity Express:

Protocol	Remote Source Port	Cisco Unity Express Destination Port	Cisco Unity Express Source Port	Remote Device Destination Port	Remote Device	Notes
SSH					Secure Shell Client	Not supported on Cisco Unity Express. Use SSH to the host router.
Telnet					Telnet Client	Not supported on Cisco Unity Express. Use Telnet to the host router.
DNS			TCP/UDP 53		DNS Servers	
TFTP			UDP 69		TFTP Server	Used for loading RAM kernel

FTP			TCP 20 (data), TCP 21 (control)		FTP Server	Used for software install; backup and restore
HTTP		TCP 80			Administrator/User Web browsers	Cisco Unity Express and Cisco CallManager Express Admin and User access
NTP		UDP 123			NTP server	Usually the Cisco CallManager Express host router
SNMP					Network Management station	SNMP hardware inventory for Cisco Unity Express is supported out of the host router. Cisco Unity Express itself does not support SNMP
Syslog		TCP 514			Syslog service	
SIP		UDP 5060			Cisco CallManager Express host router	No SIP trunking supported in Cisco Unity Express R1
RTP	UDP 16384-32767	UDP 16384-32767	UDP 16384-32767	UDP 16384-32767	Voice Media	IP Phone and GW ports

Changing the default IP subnets for Voice and Data

Sometimes, the UC500's default subnets for Voice and Data are in conflict with existing networks at the customer premise. Changing the default values is very simple:

- Step 1. Navigate to **Configure >> Device Properties >> IP Addresses**. Assign an IP address to the new VLAN interface and apply your changes.

Devices

Hostname: UC520

Interface Configuration | Device Configuration

Interface Name	IP Address	Subnet Mask
Vlan1	192.168.10.1	255.255.255.0
Vlan100	10.1.1.1	255.255.255.0

OK Apply Refresh Cancel Help

Deleting the DHCP Server

If the UC500 is integrated in a scenario where a DHCP Server already exists for the data devices, you need to disable the UC500's DHCP server. To do this:

- Step 1. Open the Cisco Configuration Assistant (CCA) and connect to the UC500
- Step 2. Navigate to **Configure >> DHCP Server**.
- Step 3. Delete the Data DHCP Server and apply your changes.

Devices

Hostname: UC520

DHCP Pools | DHCP Bindings | DHCP Exclusions

Pool Name	Interface
phone	Vlan100
data	Vlan1

Total Rows: 2

Create Delete Modify

Property	Value
Network	192.168.10.0
Netmask	255.255.255.0
Start IP Address	192.168.10.11
End IP Address	192.168.10.254
Default Router	192.168.10.1

Total Rows: 5

OK Apply Refresh Cancel Help

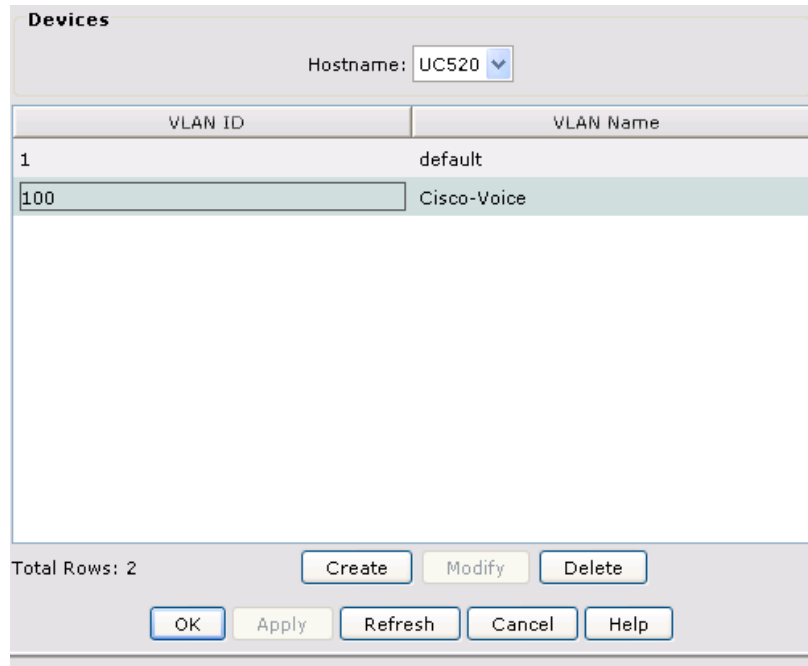
- Step 4. Change the static IP of the Voice and Data VLANs if necessary. See next section for instructions on how to do this.

Note: Make sure that you renew your DHCP lease and pull an IP from the new DHCP server.

Changing the default VLANs

Sometimes, the UC500's default VLAN's for Voice and Data are in conflict with existing Layer 2 topologies at the customer premise. Changing the default values is very simple:

Step 1. Navigate to **Configure >> VLANs**. Delete and recreate the VLAN's accordingly.



Devices

Hostname: UC520

VLAN ID	VLAN Name
1	default
100	Cisco-Voice

Total Rows: 2

Create Modify Delete

OK Apply Refresh Cancel Help

Note: You may lose connectivity to the device after applying the changes.

For More Information

For more information on Cisco SBCS solutions, visit the SBCS Support Community at the following URL:

www.myciscocommunity/community/smallbizsupport