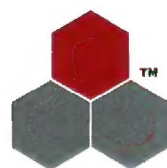"When will you be an IPexpert?"

IPexpert's Student Handbook

for the Cisco® CCIE™ Voice Laboratory Exam

Version 1.0

ipexpert

powered by **PROCTOR** LABS

For technical support peer groups, subscribe for free to

CertificationTalk
http://www.certificationtalk.com

ONLINE study list
http://www.onlinestudylist.com

IPexpert

CCIE Voice

Student Handbook

ipexpert

ipexpert

Blueprint

Basic Campus Design
- DHCP, TFTP
- Catalyst voice and data VLAN configuration
- Catalyst VTP configuration

Call Manager and Call Manager Express Configuration
- Phone registration
- Phone configuration

Voice Gateway and Signaling
- Analog and digital voice protocols: analog FXS, FXO-M1, T1, E1, PRI, CAS, R2
- VoIP protocols: H323, MGCP, SCCP, SIP, RAS

Call Routing
- CCM route patterns (@ wildcard not tested)
- CCM route preference and redundancy
- IOS dial peers
- Digit manipulation and translation

Voice CODEC
- G711ulaw, G711alaw, G729, G723

Call Admission Control
- Location-based
- RAS-based

High Availability Features
- SRST
- AAR

Media Resource Management
- Conference bridge software and hardware
- Transcoder
- MTP
- MOH

QoS Considerations
- L2/L3 classifications and policing
- Queuing mechanisms
- LFI
- Catalyst switch QoS

Unified Messaging
- Unity voicemail integration
- Unity administration

ipexpert

CRS/IPCC Express Application
- Default script configuration and integration
- Custom script configuration and integration

Call Manager Voice Applications
- Any native applications to Call Manager, examples are extension mobility, attendant console, IPMA

Supplementary Services

Directory Services and Integration

Fax
- Fax pass-through
- Fax relay

ipexpert

Infrastructure

6500 (CatOS)

Data or native vlan is configured using:

```
set vlan {vlans} mod/ports
```

Voice vlan is known as auxiliary vlan on 6500. Configure using:

```
set port auxiliaryvlan mod/port {vlan}
```

Default and method to remove auxiliary VLAN is:

```
set port auxiliaryvlan mod/port none
```

If VLAN does not exist, create VLAN using:

```
set vlan {vlans} name {name}
```

The HQ-RTR must be configured as a trunk if not already done. Use the following command:

```
set trunk mod/ports on dot1q 1-4094
```

> [keyword 'on': Keyword to force the port to become a trunk port and persuade the neighboring port to become a trunk port. The port becomes a trunk port even if the neighboring port does not agree to become a trunk.]

Use the clear trunk command to restore a trunk port to its default trunk type and mode or to clear specific VLANs from the allowed VLAN list for a trunk port.

```
clear trunk mod/port [vlans]
```

Use the set spantree portfast command to allow a port that is connected to a single workstation or PC to start faster when it is connected.

```
set spantree portfast mod/port {enable | disable}
```

Other useful commands include:

```
set port disable mod/port
```

ipexpert

3550

Configure a port or range of ports for Voice and Data VLAN using the following commands:

```
interface range FastEthernet 0/1 - 3
 switchport voice vlan 3
 switchport access vlan 2
 spantree portfast
```

OR

```
interface range FastE 0/1 - 3
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switch trunk native vlan 2
 switchport voice vlan 3
 spantree portfast
```

3725 Etherswitch

Configure VLAN using VLAN database.

```
vlan database
vlan 1
vlan 2
vlan 3
exit
conf t
interface vlan 1
 ip address 10.203.1.1 255.255.255.0
interface vlan 2
 ip address 10.203.2.1 255.255.255.0
interface vlan 3
 ip address 10.203.2.1 255.255.255.0

interface range FastE 0/1 - 3
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switch trunk native vlan 2
 switchport voice vlan 3
 spantree portfast
```

ipexpert

NTP Configuration

Configure NTP on an IOS router as shown below.

```
Ntp server <ip address of NTP server>
clock timezone GMT 0
```

Verify using sh ntp status and check the clock is synchronized.

Configure DHCP

DHCP can be configured either on the Call Manager Server or an IOS router.

Checklist for Windows DHCP Server Configuration.

- Start DHCP service on the designated server
- Add DHCP server in the MMC
- Set predefined option 150 for TFTP and give address of PUB or designated TFTP server
- Create scopes with Default Gateway, exclusion range and TFTP server
- Repeat for any other scopes that need to be defined
- Restart the DHCP service

IOS DHCP

Configure either an ip address to exclude or a range of ip addresses to exclude. The router will assign ip addresses which are not configured in this list.

```
ip dhcp excluded-address <First IP Address of range> <Last ip>
```

Define one or more scope. The TFTP server is either the Call Manager ip address or the CME Source Address.

```
ip dhcp pool <SCOPE NAME>
   network <NETWORK> <MASK>
   default-router <IP ADDRESS DFLT GW>
   option 150 ip <IP ADDRESS TFTP Server>
```

If the DHCP Server is on a different network to the phones then the following command is required on the router interface on the phone network. In the case of the 37X5 Etherswitch then this would be inside the Vlan interface.

```
ip helper-address <DHCP SERVER IP ADDR>
```

ipexpert

Call Manager Basics

Configure the basic parameters required by all Endpoints from the CCMADMIN Web interface.

Call Manager System configuration

From *System-Server:* Configure IP address

From *System-Cisco Call Manager:* Add Call Manager servers (PUB and SUB)

From *System-Cisco Call Manager Group:* Add Call Manager Groups. Highest Call Manager in the order it appears is the higher priority.

From *System-Date/Time Group:* Configure relevant time settings

From *System-Region:* Configure Region settings based on required Codec. This is perhaps the most important setting in Call Manager and must be configured correctly.

Typically the codec being used within a region is G711 and between Regions is G729 (79xx phones support both codecs). It is important to note that configuring a inter-region setting with G711 is not restricting the codec to G711 only- it is in fact allowing all codecs that require less than or equal to the bandwidth per call G711 requires. So a 79XX phone configured in a Device Pool with Region set to G711 can also use G729 if the other endpoint involved in the call cannot support G711 for whatever reason.

Rename the 'Default' region to HQ and create another region call BR1

ipexpert

From *System-Enterprise parameters:* Change URLs to use the IP Address of Call Manager rather than the hostname (DNS is not supported in the CCIE Voice Lab).

From *System-Location:* Configure Locations required.

Call Admission Control (CAC) within Call Manager (Centralized model) is typically done using 'Locations' settings in Call Manager. It is less confusing to provision Locations for Remote sites only and NOT to provision a location for the HQ site (assuming the CCM is located on the HQ LAN) since CAC is not necessary inside the LAN. If an HQ location is created then the amount of bandwidth provisioned should be 0Kbps (unlimited).

To allow 1 G729 call between HQ and BR1 provion 24kbps inside the BR1 location.
To allow 1 G711 call between HQ and BR1 provion 80kbps inside the BR1 location.

Locations are assigned to Devices and NOT Device Pools.

From *System-Enterprise Parameters:* Replace dns name w/ ip address

From *System-Device Pool:* Rename Default to HQ and create another Device Pool. At this stage assign appropriate Call Manager Group, Date Time Group, Region.

ipexpert

Calling Search Space and Partition

From *Route-Partition:* Add list of *partitions*
*From Route-*Calling Search Space: Create CSS

A **granular** approach is recommended since troubleshooting and re-use within applications will be easier. It is also recommended to use intuitive PT/CSS names. It is recommended you put Route Patterns in Partitions and for devices (phones, gateways, CTI Route Points, Voicemail Ports, etc...) leave in the default or Null partition (<None>) or place them in an 'Internal' partition.

A *partition* is a group of devices with similar accessibility, and a *calling search space* defines which partitions are accessible to a particular device. A device can call only those devices located in the partitions that are part of its calling search space.

Devices in the Null partition are accessible from all other devices in the Call Manager since the Null partition is the last partition in every CSS (hidden). Devices without any CSS configured are assigned the Null CSS (<None>) which contains the Null PT.

If it is required to apply COR between phones registered to CCM then the Null Partition cannot be used.

Note: Two devices in the same partition cannot necessarily call each other- the partition will still need to be added to the partition list inside the Devices CSS. The reason Devices in the Null PT are accessible to all devices is because the Null PT is in the NULL CSS and all other configured CSS.

Phone Registration

From *Enable Services* from Control Centre: Either add MAC addresses of devices into the Call Manager database or From *Call Manager* enable Auto-Registration define the Auto-Registration number range.

Phones should TFTP .cnf files and register with Call Manager within 2 minutes.

From *Device-Phone:* Set the Description name, CSS and Location in 'Device'. Set the DN, Partition [Name and Line Text Label] from the Line.

It is recommended you set the CSS on the Device and not the LINE.

If you configure a calling search space both on an IP phone line and on the device (phone) itself, Cisco CallManager concatenates the two calling search spaces and places the line's calling search space in front of the device's calling search space. If the same route pattern appears in two partitions, one contained in the line's calling search space and one contained in the device's calling search space, then Cisco CallManager selects

ipexpert

the route pattern listed first in the concatenated list of partitions (in this case, the route pattern associated with the line's calling search space).

ipexpert

CME Basics

CME files

Locate the CME file that has been downloaded from CCO.

A Cisco IOS command allows you to uncompress the tar files and copy them to router Flash at the same time.

```
archive tar /xtract source-url flash:/file-url
```

For example, to extract contents of cme-basic-3.0.1.tar from TFTP server 192.168.1.1 to router Flash memory, use this command:

```
archive tar /xtract tftp://192.168.1.1/cme-basic-3.0.1.tar flash:
```

Basic concepts

An ephone, or "Ethernet phone," is a single instance of the software configuration of the physical instrument with which a phone user makes and receives calls in a Cisco CME system. The physical ephone is either a Cisco IP phone or an analog phone equipped with an analog telephone adaptor (ATA) device.

An ephone-dn, or "Ethernet phone directory number," is a software construct that represents the line that connects a voice channel to a phone instrument on which a user can receive and make calls.

An ephone-dn is created by the **ephone-dn** command, which builds one virtual voice port and one or more dial peers for the ephone-dn.

There are 6 different types of ephone-dn in a CCME system

- Single-Line Ephone-dn
- Dual-Line Ephone-dn
- Two Ephone-dns with one number
- Dual-Number Ephone-dn
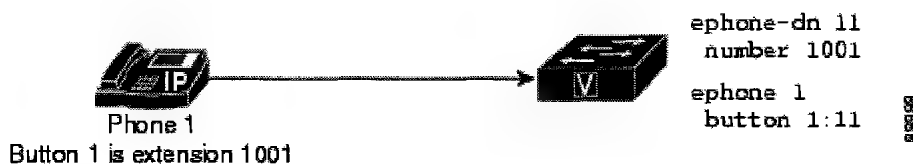- Shared Ephone-dn
- Overlay Ephone-dn

Single-Line Ephone-dn

A single-line ephone-dn has the following characteristics:

- Makes one call connection at a time using one phone line button. A single-line ephone-dn has one telephone number associated with it.
- Should be used when phone buttons have a one-to-one correspondence to the PSTN lines that come into a Cisco CME system.
- Should be used for lines that are dedicated to intercom, paging, message-waiting indicator (MWI), loopback, and music-on-hold (MOH) feed sources.
- When used with multiple-line features like call waiting, call transfer, and conferencing, there must be more than one single-line ephone-dn on a phone.
- Can be combined with dual-line ephone-dns on the same phone.

Note that you must make the choice to configure each ephone-dn in your system as either dual-line or single-line when you initially create ephone-dn configuration entries. If you need to change from single-line to dual-line later, you must delete the ephone-dn and then recreate it.

The figure below shows a single-line ephone-dn.


```
                                            ephone-dn 11
                                             number 1001

                                            ephone 1
          Phone 1                            button 1:11
Button 1 is extension 1001
```

Dual-Line Ephone-dn

- A dual-line ephone-dn has the following characteristics:
- Can make two call connections at the same time using one phone line button. A dual-line ephone-dn has two channels for separate call connections.
- Can have one number or two numbers (primary and secondary) associated with it.
- Should be used for an ephone-dn that needs to use just a single button for features like call waiting, call transfer, or conferencing.
- Cannot be used for lines that are dedicated to intercom, paging, message-waiting indicator (MWI), loopback, and music-on-hold (MOH) feed sources.
- Can be combined with single-line ephone-dns on the same phone.

Note that you must make the choice to configure each ephone-dn in your system as either dual-line or single-line when you initially create ephone-dn configuration entries. If you need to change from single-line to dual-line later, you must delete the ephone-dn and then recreate it.
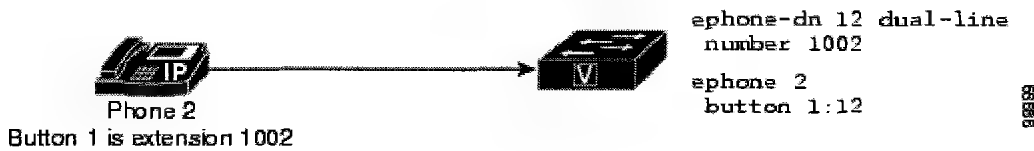
The figure below shows a dual-line ephone-dn.

```
ephone-dn 12 dual-line
  number 1002

ephone 2
  button 1:12
```

Phone 2
Button 1 is extension 1002

Two Ephone-dns with One Number

Two ephone-dns with one number have the following characteristics:
Have the same telephone number but two separate virtual voice ports, and therefore can have two separate call connections.

- Can be single-line or dual-line ephone-dns.
- Can appear on the same phone on different buttons or on different phones.
- Should be used when you want the ability to make more call connections while using fewer numbers.

The Figure below shows a phone with two buttons that have the same number, extension 1003. Each button has a different ephone-dn (button 1 is ephone-dn 13 and button 2 is ephone-dn 14), so each button can make one independent call connection if the ephone-dns are single-line and two call connections (for a total of four) if the ephone-dns are dual-line.

```
ephone-dn 13
  number 1003
  no huntstop

ephone-dn 14
  number 1003
  preference 1

ephone 3
  button 1:13 2:14
```

Phone 3
Button 1 is extension 1003
Button 2 is also extension 1003
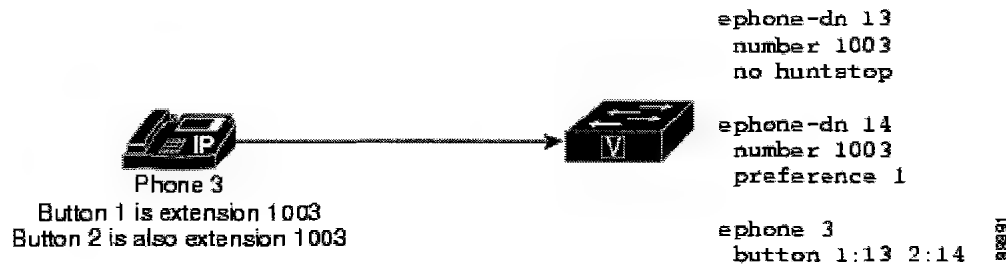
The Figure shows two phones that each have a button with the same number. Because the buttons have different ephone-dns, the calls that are connected on these buttons are independent of one another. The phone user at phone 4 can make a call on extension 1004, and the phone user on phone 5 can receive a different call on extension 1004 at the same time.

ipexpert

```
Phone 4                              ephone-dn 13
Button 1 is extension 1003             number 1003
                                       no huntstop

                                     ephone-dn 14
                                       number 1003
                                       preference 1

Phone 5                              ephone 4
Button 1 is extension 1003             button 1:13

                                     ephone 5
                                       button 1:14
```
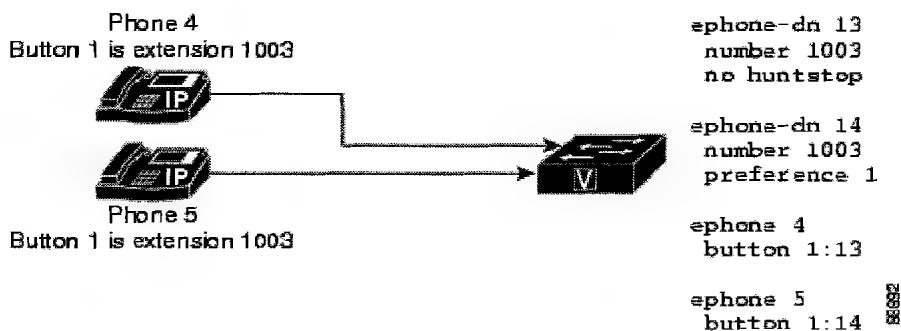
The two ephone-dns-with-one-number situation is different than a shared line, which also has two buttons with one number but has only one ephone-dn for both of them. A shared ephone-dn will have the same call connection at all the buttons on which the shared ephone-dn appears. If a call on a shared ephone-dn is answered on one phone and then placed on hold, the call can be retrieved from the second phone on which the shared ephone-dn appears. But when there are two ephone-dns with one number, a call connection appears only on the phone and button at which the call is made or received.

The two examples above show how two ephone-dns with one number are used to provide a small hunt group capability. If the ephone-dn on button 1 is busy or does not answer, an incoming call to extension 1003 rolls over to the ephone-dn associated with button 2 because the **preference** and **no huntstop** commands have been used. Values assigned in the **preference** command are passed to the dial peers created by the two ephone-dns. Both dial peers for the ephone-dns are matched when this extension number is dialed. The call is connected to the ephone-dn with the highest preference. The default preference value is 0 (the highest value), so ephone-dn 13 on button 1 gets the first call. The **no huntstop** command tells the dial peers not to stop hunting for another match, so the second call to extension 1003 is sent to ephone-dn 14.

Dual-Number Ephone-dn

A dual-number ephone-dn has the following characteristics:

- Has two telephone numbers, a primary number and a secondary number.
- Can make one call connection if it is a single-line ephone-dn.
- Can make two call connections at a time if it is a dual-line ephone-dn.
- Should be used when you want to have two different numbers for the same button without using more than one ephone-dn.

ipexpert

The Figure below shows an ephone-dn that has two numbers, extension 1006 and extension 1007.


```
ephone-dn 15
 number 1006 secondary 1007

ephone 6
 button 1:15
```

Phone 6
Button 1 is extension 1006
Button 1 is also extension 1007
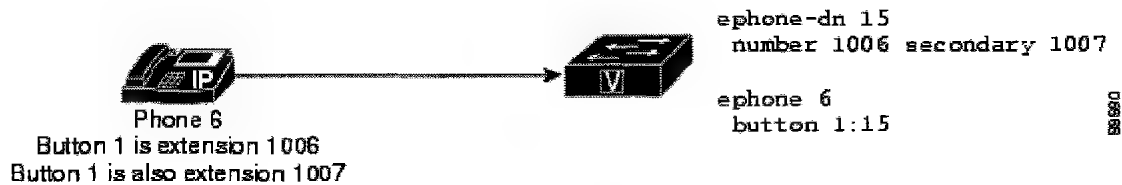
Shared Ephone-dn

A shared ephone-dn has the following characteristics:

- Appears on two different phones but uses the same ephone-dn and number.
- Can make one call at a time between the two phones, and that call appears on both phones.
- Should be used when you want the capability to answer or pick up a call at more than one phone.

Because these phones share the same ephone-dn, if the ephone-dn is connected to a call on one phone, that ephone-dn is unavailable for other calls on the second phone. If a call is placed on hold on one phone, it can be retrieved on the second phone. This is like having a single-line phone in your house with multiple extensions. You can answer the call from any phone on which the number appears, and you can pick it up from hold on any phone on which the number appears.

The Figure below shows a shared ephone-dn. Extension 1008 appears on both phone 7 and phone 8.

Phone 7
Button 1 is extension 1008


```
ephone-dn 16
 number 1008

ephone 7
 button 1:16

ephone 8
 button 1:16
```

Phone 8
Button 1 is extension 1008
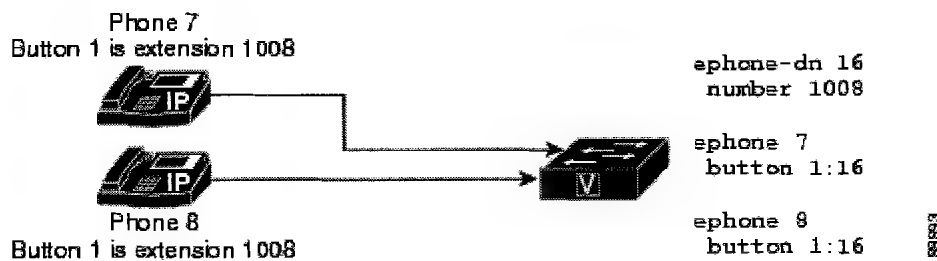
Overlay Ephone-dn

An overlay ephone-dn has the following characteristics:

- Is a member of an overlay set, which includes all the ephone-dns that have been assigned together to a particular phone button.
- Can have the same telephone or extension number as other members of the overlay set or different numbers.

ipexpert

- Can be single-line or dual-line, but cannot be mixed single-line and dual-line in the same overlay set.
- Can be shared on more than one phone.

Overlay ephone-dns provide call coverage similar to shared ephone-dns because the same number can appear on more than one phone. The advantage of using two ephone-dns in an overlay arrangement rather than as simple shared ephone-dns is that a call to the number on one phone does not block the use of the same number on the other phone as would happen if this was a shared ephone-dn.

You can overlay up to ten lines on a single button and create a "10x10" shared line with ten lines in an overlay set shared by ten phones, resulting in the possibility of ten simultaneous calls to the same number.

The Figure shows an overlay set with two ephone-dns and one number that is shared on two phones. Ephone-dn 17 has the default preference value of 0, so it will receive the first call to extension 1001. The phone user at phone 9 answers the call, and a second incoming call to extension 1001 can be answered on phone 10 using ephone-dn 18.
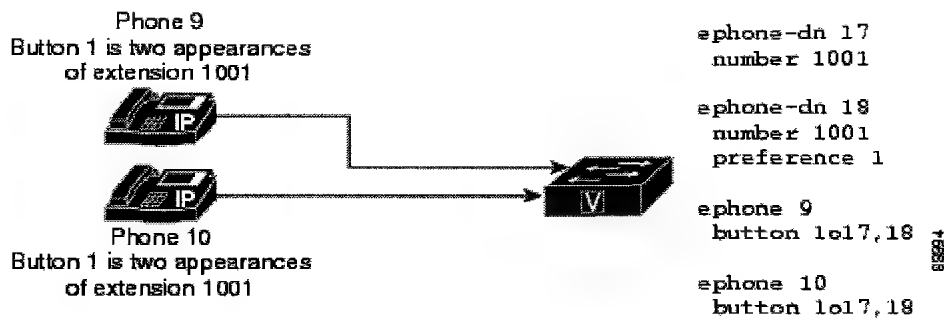
A more complex ephone-dn configuration mixes overlay ephone-dns with shared ephone-dns and plain dual-line ephone-dns on the same phones. The next diagram illustrates the following example of a manager with two assistants. On the manager's phone the same number, 2001, appears on button 1 and button 2. The two line appearances of extension 2001 use two single-line ephone-dns, so the manager can have two active calls on this number simultaneously, one on each button. The ephone-dns are set up so that button 1 will ring first, and if a second call comes in, button 2 will ring. Each assistant has a personal ephone-dn and also shares the manager's ephone-dns. Assistant 1 has all three ephone-dns in an overlay set on one button, whereas assistant 2 has one button for the private line and a second button with both of the manager's lines in an overlay set. A sequence of calls might be as follows.

1. An incoming call is answered by the manager on extension 2001 on button 1 (ephone-dn 20).
2. A second call rings on 2001 and rolls over to the second button on the manager's phone (ephone-dn 21). It also rings on both assistants' phones (also ephone-dn 21, a shared ephone-dn).

ipexpert

3. Assistant 2 answers the call. This is a shared overlay line (one ephone-dn, 21, is shared among three phones, and on two of them this ephone-dn is part of an overlay set). Because it is shared with button 2 on the manager's phone, the manager can see when assistant 2 answers the call.
4. Assistant 1 makes an outgoing call on ephone-dn 22. The button is available because of the additional ephone-dns in the overlay set on the assistant 1 phone.

At this point, the manager is in conversation on ephone-dn 20, assistant 1 is in conversation on ephone-dn 22, and assistant 2 is in conversation on ephone-dn 21.


```
Manager phone
Button 1 is extension 2001
Button 2 is extension 2001

Assistant 1 phone
Button 1 is extension 2001
  and extension 2002

Assistant 2 phone
Button 1 is extension 2003
Button 2 is extension 2001
```

```
ephone-dn 20
 number 2001
 no huntstop
 ! Manager number

ephone-dn 21
 number 2001
 preference 1
 ! Manager number

ephone-dn 22
 number 2002
 ! Assistant 1 personal number

ephone-dn 23
 number 2003
 ! Assistant 2 personal number

ephone 8
 button 1:20 2:21
 ! Manager phone

ephone 9
 button 1o22,20,21
 ! Assistant 1 phone

ephone 10
 button 1:23 2o20,21
 ! Assistant 2 phone
```

System Setup

In a Cisco CME system, the IP phones receive their initial configuration information and phone firmware from the TFTP server associated with the Cisco CME router. In most cases, the phones obtain the IP address of their TFTP server using the Dynamic Host Configuration Protocol (DHCP) **option 150** command. For Cisco CME operation, the TFTP server address obtained by the Cisco IP phones should point to the Cisco CME router IP address. The Cisco IP phones attempt to transfer a configuration file called XmlDefault.cnf.xml. This file is automatically generated by the Cisco CME router through the **ip source-address** command and placed in router memory. The XmlDefault.cnf.xml file contains the IP address that the phones use to register for service, using the Skinny Client Control Protocol (SCCP). This IP address should correspond to a valid Cisco CME router IP address (and may be the same as the router TFTP server address).

ipexpert

IOS DHCP server can be created using the following commands.

```
ip dhcp exclude-address 10.1.202.1
!
ip dhcp pool CME
 network 10.1.200.0 255.255.255.0
 option 150 ip 10.1.202.1
 default-router 10.1.202.1
```

Network Time Protocol (NTP) allows you to synchronize your Cisco CME router to a single clock on the network, which is known as the clock master. NTP is disabled on all interfaces by default, but it is essential for Cisco CME.

```
clock timezone India 5
clock summer-time India recurring
ntp server 64.104.222.16
```

There are some mandatory parameters that need to be defined in CME- these are configured under the '**telephony-service**' command in global configuration. If this command is not available then the router is running a version of IOS that does not support CME.

There are two ways of defining service parameters- use the "telephony-service setup" wizard or through manually defining the parameters. For speed use the wizard wherever possible- this will automatically configure all mandatory steps with the exception of configuring NTP server.

CME configuration setup	Done by wizard?
DHCP server	Yes
NTP	No
Source-Address for CME	Yes
Create cnf files	Yes
Max-ephone	Yes
Max-dn	Yes
Auto-assign	Yes
Dialplan-pattern	Yes

ipexpert

Running the CME Wizard

Initiate the CME wizard and create DHCP server.

```
P4-BR2-RTR(config)#telephony-service setup

— Cisco IOS Telephony Services Setup —


Do you want to setup DHCP service for your IP Phones? [yes/no]: yes
Configuring DHCP Pool for Cisco IOS Telephony Services:

   IP network for telephony-service DHCP Pool: 10.4.202.0
   Subnet mask for DHCP network: 255.255.255.0
   TFTP Server IP address (Option 150): 10.4.202.1
   Default Router for DHCP Pool: 10.4.202.1
```

Confirm that you want to start the service and define source address/port that CME will use. Also choose language.

```
Do you want to start telephony-service setup? [yes/no]: yes
Configuring Cisco IOS Telephony Services:

   Enter the IP source address for Cisco IOS Telephony Services: 10.4.202
   Enter the Skinny Port for Cisco IOS Telephony Services: [2000]:
   How many IP phones do you want to configure: [0]: 7
   Do you want dual-line extensions assigned to phones? [yes/no]: yes
   What Language do you want on IP phones:
      0 English
      1 French
      2 German
      3 Russian
      4 Spanish
      5 Italian
      6 Dutch
      7 Norwegian
      8 Portuguese
      9 Danish
     10 Swedish
     11 Japanese
   [0]:
   Which Call Progress tone set do you want on IP phones:
      0 United States
      1 France
```

ipexpert

```
     2  Germany
     3  Russia
     4  Spain
     5  Italy
     6  Netherlands
     7  Norway
     8  Portugal
     9  UK
    10  Denmark
    11  Switzerland
    12  Sweden
    13  Austria
    14  Canada
    15  Japan
[0]:
```

Define the phone extension in the range you want to auto-register. Also if DID is being used then enter the full digit-string that the PSTN is sending. If you know the DN of your Unity ports then you can also enter that information at this stage.

```
What is the first extension number you want to configure: 3001

Do you have Direct-Inward-Dial service for all your phones? [yes/no]: yes
  Enter the full E.164 number for the first phone: 33132430001

Do you want to forward calls to a voice message service? [yes/no]: no
```

Finally you will be prompted to confirm that you do no wish to change any information and that the wizard configuration is complete. Notice in this example NTP was not configured and on creating the configuration files (cnf files) a warning is displayed. If this message is seen it is recommended that you remove all CME configuration (from configuration type 'no telephony-service'), configure NTP and run the wizard again.

```
Do you wish to change any of the above information? [yes/no]: no
CNF-FILES: Clock is not set or synchronized,
           retaining old versionStamps

--- Setup completed config ---
```

Verify configuration once the wizard has completed adding the configuration.

```
P4-BR2-RTR#sh run | b telephony-service
telephony-service
 max-ephones 2
 max-dn 2
 ip source-address 10.4.202.1 port 2000
```

ipexpert

```
auto assign 1 to 2
create cnf-files version-stamp Jan 01 2002 00:00:00
dialplan-pattern 1 3313243.. extension-length 4
transfer-system full-consult
!
```

Under telephony-service you will notice several commands have already been entered and also the ephone-dn's and ephone's have been created. It is recommended that you DO NOT auto-assign any more ephone-dn's since this could cause major problem if Unity Integration with CME is required.

Max-ephone < *max-phones*>	Sets the maximum number of Cisco IP phones to be supported by this router. The maximum number of phones is platform- and version-dependent.
Max-dn < *max-directory-numbers*>	Sets the maximum number of extensions (ephone-dns) to be supported by this router. The maximum number of extensions is platform- and version-dependent.
ip source-address *ip-address* [**port** *port*] [**any-match** | **strict-match**]	Identifies the IP address and port number that the Cisco CME router uses for IP phone registration. The default port is 2000. • **any-match**—(Optional) Disables strict IP address checking for registration. This is the default. • **strict-match**—(Optional) Instructs the router to reject IP phone registration attempts if the IP server address used by the phone does not exactly match the source address
create cnf-files	Builds the XML configuration files that are required for Cisco CME phones.
auto assign *dn-tag* **to** *dn-tag*	Automatically assigns ephone-dn tags from the specified range to newly discovered IP phones. • *dn-tag* **to** *dn-tag*—Range of ephone-dn tags (unique sequence numbers) to be automatically assigned to IP phones. The value of the *dn-tag* argument ranges from 1 to 288.

ipexpert

dialplan-pattern *tag pattern* extension-length *length* [extension-pattern *epattern*] [no-reg]	Maps a digit pattern for an abbreviated extension-number prefix to the full E.164 telephone number pattern. • *tag*—Dial-plan string tag used before a ten-digit telephone number. Range is from 1 to 5. • *pattern*—Dial-plan pattern for full E.164 number. • extension-length *length*—Number of digits in the *epattern* argument that is associated with the extension-pattern keyword.
transfer-pattern *transfer-pattern*	Allows transfer of telephone calls by Cisco IP phones to specified phone number patterns. If no transfer pattern is set, the default is that transfers are permitted only to other local IP phones. • *transfer-pattern*—String of digits for permitted call transfers. Wildcards are allowed.

In addition to the commands under telephony-service, two ephone-dn and ephones are created by the system automatically.

```
ephone-dn 1 dual-line
 number 3001


ephone-dn 2 dual-line
 number 3002


ephone 1
 mac-address 0030.94C4.22D6
 type 7960
 button 1:1    // line number on device : ephone-dn tag



ephone 2
 mac-address 0011.BBE1.ADDF
 type 7940
 button 1:2
```

ipexpert

The dual-line command is explained in the section titled 'Basic Concepts'. Inside the ephone-dn a number is provision and the ephone-dn is assigned to a device or ephone via the 'button' command.

CME Auto-Attendant

CCME ships with a basic configurable automated attendant that can be deployed on your router, without additional hardware. The CCME AA software is a customizable TCL script that is located in the main CCME package. It is a tar file that is extracted via TFTP to your router's flash memory. The AA asks the caller where to forward an extension when an incoming call arrives and then sends the call off, or can forward the call to an operator to be directed. The premade audio files can be modified to suit your purposes, i.e. "Hello, you've reached Pat's Auto. Your call is very important to us. If you know your parties extension, please dial it now otherwise press 0 or hold for an operator."

Once extracted to your router, you then setup a custom voice application and add it to your incoming voice ports. Keep in mind, the AA software is built to handle incoming calls from your voice ports only. You will not be able to dial to it directly from your IP phone sets.

Using the following commands, you can download and install the CCME AA to your router. You will need to obtain the CCME AA package from CCO. (link on the Quick Links bar)

```
archive tar /xtract tftp://192.168.1.100/cme-aa-2.0.1.0.tar flash:
```

You may want to replace the listed IP above and filename as appropriate. Once the tar has been installed, you will need to configure the automated attendant using the following commands:

```
call application voice ccmeaa flash:its-Cisco.2.0.1.0.tcl
call application voice ccmeaa language 1 en
call application voice ccmeaa aa-pilot <a pilot number used to reach the AA -
should be a number not used elsewhere>
call application voice ccmeaa operator <your operator/receptionist number>
call application voice ccmeaa set-location en.0 flash:
```

Once you have set your pilot number and where the AA should send calls to the operator, you can then apply your automated attendant to the voice ports you would like it to answer. The example below is for analog FXO ports:

ipexpert

```
dial-peer voice 1 pots
 application ccmeaa
 port 1/0
dial-peer voice 2 pots
 application ccmeaa
 port 1/1
```

Alternately, for an ISDN PRI here is an example:

```
dial-peer voice 1 pots
 application ccmeaa
 incoming called-number 1000 (for 555-1000 to ring to the AA)
```

Music on Hold

A music file must be in stored in the router's Flash memory. This file should be in G.711 format. The file can be in .au or .wav file format, but the file format must contain 8-bit 8-kHz data; for example, Consultative Committee for International Telegraph and Telephone (CCITT) a-law or mu-law data format.

MOH is supplied only to PSTN and VoIP G.711 calls. Local IP phone callers hear a repeating tone on hold for reassurance that they are still connected.

IP phones do not support multicast at 224.x.x.x addresses.

Configuration

```
telephony-service
 moh filename
 multicast moh ip-address port port-number [route ip-address-list]
 exit
```

Troubleshooting

Most of the troubleshooting will be done during the dialplan section, however some verification of the system can be done at this stage.

```
P4-BR2-RTR#sh ephone-dn summ
PORT    CH DN STATE   MWI STATE   CODEC   VAD VTSP STATE      VPM STATE

50/0/1  1  IDLE       NONE        -       -   EFXS ONHOOK
50/0/1  2  IDLE       NONE        -       -   EFXS ONHOOK
50/0/2  1  IDLE       NONE        -       -   EFXS ONHOOK
50/0/2  2  IDLE       NONE        -       -   EFXS ONHOOK
```

ipexpert

```
P4-BR2-RTR#sh ephone summ

ephone-1 Mac:0030.94C4.22D6 TCP socket:[1] activeLine:0 REGISTERED
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 debug:0
IP:10.4.202.100 Telecaster 7960 keepalive 3286 1:1

ephone-2 Mac:0011.BBF1.ADDF TCP socket:[2] activeLine:0 REGISTERED
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 debug:0
IP:10.4.202.101 Telecaster 7940 keepalive 3286 1:2

Max 2, Registered 2, Unregistered 0, Deceased 0, Sockets 2
ephone_send_packet process switched 0


Max Conferences 8 with 0 active (8 allowed)
Skinny Music On Hold Status
Active MOH clients 0 (max 96), Media Clients 0
No MOH file loaded

P4-BR2-RTR#sh telephony-service
CONFIG (Version=3.2)
========================

Version 3.2
Cisco CallManager Express
For on-line documentation please see:
www.cisco.com/univercd/cc/td/doc/product/access/ip_ph/ip_ks/index.htm

ip source-address 10.4.202.1 port 2000
max-ephones 2
max-dn 2
max-conferences 8
dspfarm units 0
dspfarm transcode sessions 0
hunt-group report delay 1 hours
max-redirect 5
dialplan-pattern 1 3313243. extension-length 4
moh moh_file.wav
time-format 12
date-format mm-dd-yy
timezone 0 Greenwich Standard Time
keepalive 30
timeout interdigit 10
timeout busy 10
timeout ringing 180
caller-id name-only: enable
edit DN through Web: disabled.
```

ipexpert

```
edit TIME through web:  disabled.
Log (table parameters):
    max-size: 150
    retain-timer: 15
create cnf-files version-stamp Jan 01 2002 00:00:00
transfer-system full-consult
auto assign 1 to 2
local directory service: enabled.
```

Miscellaneous

Other Sections that cover CME configuration are SRST COR, Unity Integration, Dialplan. For further information consult the following on-line resources:

http://ciscogroups.anvi.com/cme/index.html

http://www.cisco.com/univercd/cc/td/doc/product/access/ip_ph/ip_ks/itscdc/itsph.htm

ipexpert

Gateways

Gateway control protocols provide communication and control between CiscoCallManager and the voice gateway.

The amount and type of information that you configure in CiscoCallManager Administration versus what is configured on the gateway vary, depending on whether gateway control protocol is MGCP or H.323.

- Media Gateway Control Protocol (MGCP) —When MGCP is used, Call Manager controls routing and tones and provides supplementary services to the gateway. MGCP provides call preservation (calls are maintained during failover and fallback), redundancy, dial plan simplification (no dial peer configuration is required on the gateway), hookflash transfer, and tone on hold. MGCP-controlled gateways do not require a media termination point (MTP) to enable supplementary services such as hold, transfer, call pickup, and call park.
- H.323 Protocol —The Cisco IOS integrated router gateways use the H.323 protocol to communicate with CallManager.

Compared to MGCP, H.323 requires more configuration on the gateway, because the gateway must maintain the dial plan and route patterns.

IOS MGCP Gatways

Up to two signaling channels are involved in an IOS MGCP gateway that communicated with Call Manager, depending on the POTS interface in use.

- The UDP-based MGCP signaling (UDP 2427)
- A signaling channel for PRI gateways (TCP 2428)

The signaling channel is required for PRI gateways since the MGCP gateway backhauls the Q931 messages back to Call Manager. Q921 terminates on the gateway.

The first step in configuring a MGCP gateway is to enable the physical interface and Layer 2 Q921.

```
P4-BR1-RTR(config)# isdn switch-type primary-ni

P4-BR1-RTR(config-controller)# pri-group timeslots 1-3 service mgcp
*Jun 22 15:31:08.906: %LINK-3-UPDOWN: Interface 2/0/0:23(1), changed state
to up
*Jun 22 15:31:08.906: %LINK-3-UPDOWN: Interface 2/0/0:23(2), changed state
to up
*Jun 22 15:31:08.906: %LINK-3-UPDOWN: Interface 2/0/0:23(3), changed state
to u
```

ipexpert

```
*Jun 22 15:31:09.894: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial2/0/0:0, changed state to down
*Jun 22 15:31:09.894: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial2/0/0:1, changed state to down
*Jun 22 15:31:09.898: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial2/0/0:2, changed state to down
*Jun 22 15:31:09.898: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial2/0/0:23, changed state to up
*Jun 22 15:31:10.898: %LINK-3-UPDOWN: Interface Serial2/0/0:23, changed
state to up
```

```
P4-BRI-RTR(config-controller)# int Serial2/0/0:23
P4-BRI-RTR(config-if)# isdn bind-l3 ccm-manager
```

Verify the timeslots of the T1 PRI. In the example below the first 3 Bearer Channels are idle.

```
P4-BRI-RTR(config-if)# do sh isdn serv
PRI Channel Statistics:

%Q.931 is backhauled to CCM MANAGER 0x0003 on DSL 0, Layer 3 output
may not apply

ISDN Se2/0/0:23, Channel [1-24]
  Configured Isdn Interface (dsl) 0
   Channel State (0=Idle 1=Proposed 2=Busy 3=Reserved 4=Restart
5=Maint_Pend)
    Channel : 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4
    State   : 0 0 0 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3
    Service State (0=Inservice 1=Maint 2=Outofservice 8=MaintPend 9=OOSPend)
    Channel : 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4
    State   : 0 0 0 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2
```

Assign a **unique** name to the VG200 so that the Cisco CallManager server can identify it.

```
router(config)# hostname P4-BRI-RTR
```

Configure the router to run MGCP as a signaling protocol.

```
P4-BRI-RTR(config)# mgcp
```

Configure the IP address (or DNS name) for the Cisco CallManager server.

```
P4-BRI-RTR(config)# mgcp call-agent 10.4.200.21
```

ipexpert

Note: To configure redundant Cisco CallManagers in the CallManager cluster, issue the following commands:

```
P4-BR1-RTR(config)# ccm-manager redundant-host [ip-address |
   dns-name] [ip-address | dns-name]
P4-BR1-RTR(config)# ccm-manager switchback {graceful | immediate
   |schedule-time hh:mm | uptime-delay minutes}
```

Select the **codec** type and the DTMF relay function.

```
P4-BR1-RTR(config)# mgcp dtmf-relay codec all mode out-of-band
```

To enable support for Cisco CallManager within MGCP, issue the following command:

```
P4-BR1-RTR(config)# ccm-manager mgcp
```

Bind the MGCP application to the voice ports.

```
P4-BR1-RTR(config)# dial-peer voice 1 pots
P4-BR1-RTR(config)# application MGCPAPP
P4-BR1-RTR(config)# port 2/0/0:23
```

Before adding the gateway to Call Manager, the hardware type, module and card type must be derived. This is done using the following method:

```
P4-BR1-RTR#sh diag
Slot 0:       C3825 Mother board 1GE(TX-SFP),1GE(TX), integrated VPN unit
4W Port adapter, 3 ports

Slot 2:
      High Density Voice NM-HDV2-2T1/E1 Port adapter




      WIC Slot 0:
      T1 (1 Port) Multi-Flex Trunk WAN Daughter Card

P4-BR1-RTR#sh run | b controller
controller T1 2/0/0
 framing esf
 linecode b8zs
 pri-group timeslots 1-3,24 service mgcp
```
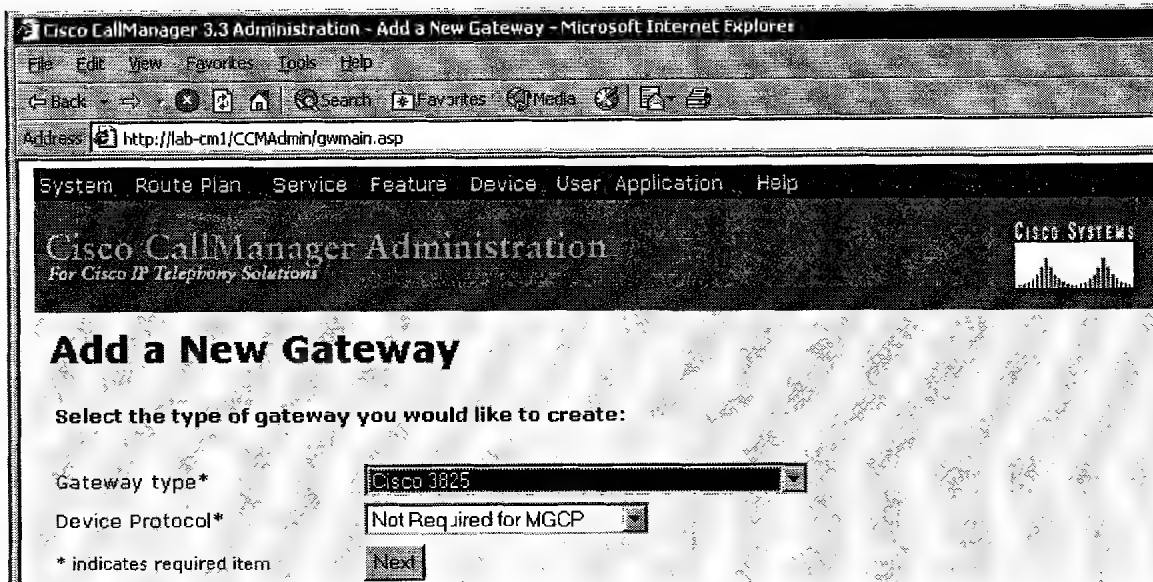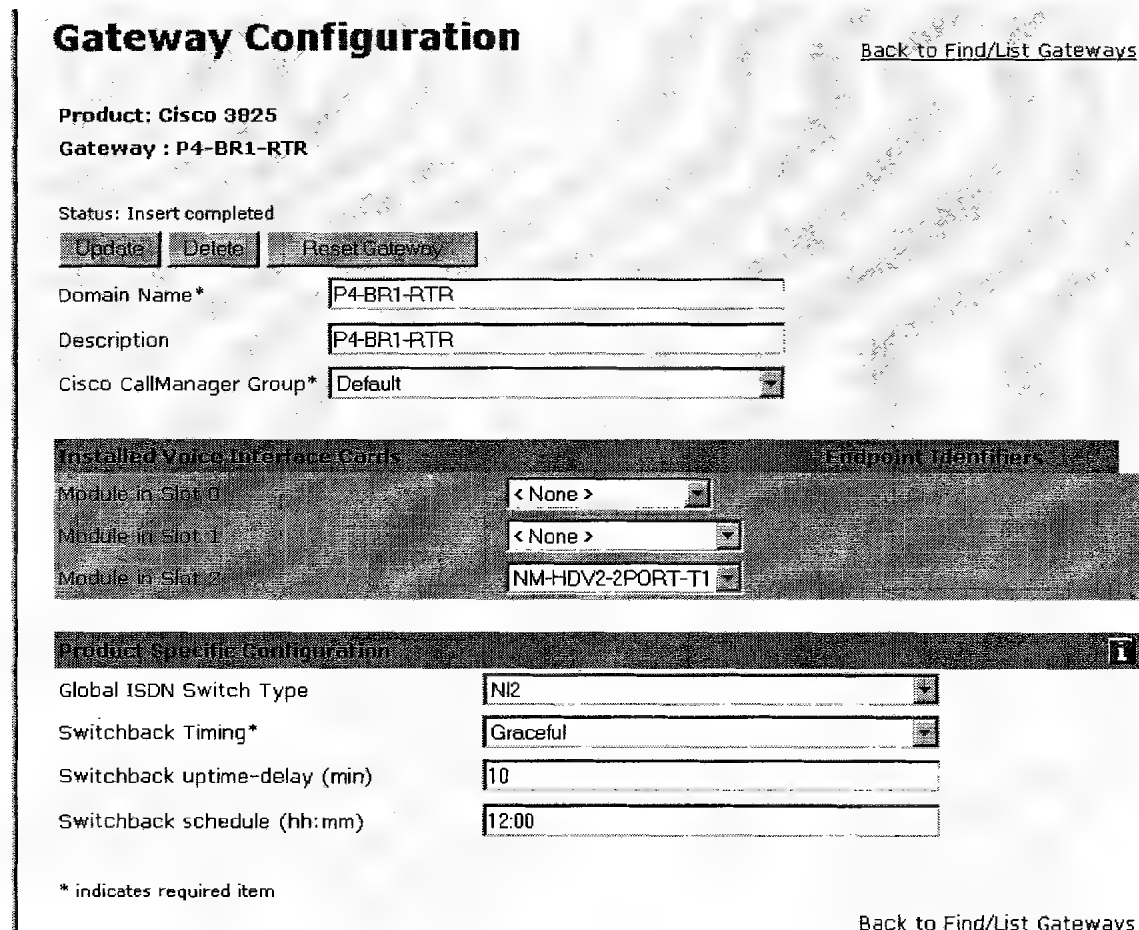
The module is NM-HDV2-2T1/E1 and the card is VWIC1-MFT-1T1 which resides in port 2/0/0.

Now we are ready to add the gateway to the Call Manager using the information above.

Add the MGCP gateway using the unique Hostname of the router. It is also vital you choose the correct module and slot! Also set the ISDN switch type.

Select the correct card based on earlier information.

ipexpert

Gateway Configuration

Back to Find/List Gateways

Product: Cisco 3825
Gateway : P4-BR1-RTR

Status: Update completed

Update   Delete   Reset Gateway

Domain Name*   P4-BR1-RTR
Description   P4-BR1-RTR
Cisco CallManager Group* Default

Installed Voice Interface Cards   **Endpoint Identifiers**

Module in Slot 0   < None >
Module in Slot 1   < None >
Module in Slot 2   NM-HDV2-2PORT-T1

Subunit 0   VWIC-1MFT-T1   Begin Port 0
Subunit 1   < None >   Begin Port 0

In this case the T1 is configured as a PRI.

Gateway Configuration

Back to MGCP Configuration
Back to Find/List Gateways

Select protocol for this gateway

Device Protocol*   – Not Selected –

                        – Not Selected –
                        T1 - CAS
                        T1 - PRI

Under **Device Information** select the relevant Device Pool, Location and PRI Protocol Type.

Configure **Interface Information** with the correct Switch Type and Channel Selection- 'Top Down' is Ascending and 'Bottom up' is Descending- to avoid glare configure with the opposite setting as the Telco.

ipexpert

Call Routing Information must have the correct Significant Digits set- assuming the Devices registered to Call Manager are using 4 digit extension this is set to '4'. Also the gateway needs to be configured with a Calling Search Space that can see the Phone Partitions.

Device Information

End-Point Name*	S2/SU0/DS1-0@P4-BR1-RTR
Description	S2/SU0/DS1-0@P4-BR1-RTR
Device Pool*	RS1
Network Locale	< None >
Media Resource Group List	< None >
Location	RS1
AAR Group	< None >
Load Information	

Interface Information

PRI Protocol Type*	PRI NI2
Protocol Side*	User
Channel Selection Order*	Bottom Up
Channel IE Type*	Use Number when 1B
Delay for first restart (1/8 sec ticks)	32
Delay between restarts (1/8 sec ticks)	4

☑ Inhibit restarts at PRI initialization

☐ Enable status poll

Call Routing Information
Inbound Calls

Significant Digits*	4
Calling Search Space	< None >
AAR Calling Search Space	< None >
Prefix DN	

Outbound Calls

Calling Party Presentation*	Allowed
Calling Party Selection*	Originator
Called party IE number type unknown*	Cisco CallManager
Calling party IE number type unknown*	Cisco CallManager
Called Numbering Plan*	Cisco CallManager
Calling Numbering Plan*	Cisco CallManager
Number of digits to strip*	0
Caller ID DN	
SMDI Base Port*	0

Check Framing, LineCoding and clock parameters are correct.

Once you have configured the gateway '**Update**' and '**Reset**'. You should see the gateway's registration status change to '**Registered**',

Verify from the gateway itself.

```
P4-BR1-RTR#sh ccm-manager
MGCP Domain Name: P4-BR1-RTR
Priority      Status            Host

Primary       Registered        10.4.200.21
First Backup  Down              10.4.200.20
Second Backup None
```

Check the Layer 1/2/3 status of the T1 PRI. Layer 2 status should be "Multiple Frame Established".

ipexpert

```
P2-BRI-RTR(config-controller)#do sh isdn stat
Global ISDN Switchtype = primary-ni

%Q.931 is backhauled to CCM MANAGER 0x0003 on DSL 0 Layer 3 output may not
apply

ISDN Serial2/0/0:23 interface
      dsl 0, interface ISDN Switchtype = primary-ni
      L2 Protocol    Q.921 0x0000 L3 Protocol(s) = CCM MANAGER 0x0003
   Layer 1 Status:
      ACTIVE
   Layer 2 Status:
      TEI = 0, Ces = 1, SAPI = 0, State
MULTIPLE_FRAME_ESTABLISHED
   Layer 3 Status:
      0 Active Layer 3 Call(s)
   Active dsl 0 CCBs = 0
   The Free Channel Mask: 0x80000007
   Number of L2 Discards = 0, L2 Session ID = 0
   Total Allocated ISDN CCBs = 0
```

6608 T1 PRI

The WS-6608 also registers to Call Manager- however configuration is much easier. On the 6608 itself put the port into the correct VLAN and enable DHCP. Verify the settings- if DHCP is set up correctly you should see the port assigned an IP Address and TFTP Server.

```
Console> (enable) set port voice int 4/4 dhcp enable vlan 240
Port 4/4 DHCP enabled.
Console> (enable) sh port 4/4
* = Configured MAC Address

# = 802.1X Authenticated Port Name.

Port  Name            Status   Vlan   Duplex Speed   Type
---- ------------- -------- ----- ----------- -------
4/4                  enabled   240     full    - unknown

Port  DHCP   MAC-Address     IP-Address    Subnet-Mask
---- ------- ------------- ------------- ---------------
4/4   enable 00-02-7e-38-e7-97 10.4.200.104  255.255.255.0

Port  Call-Manager(s) DHCP-Server  TFTP-Server  Gateway
---- --------------- ----------- ------------ ---------
4/4             10.4.200.21  10.4.200 21  10.4.200.1
```

```
Port    DNS-Server(s)    Domain

4/4

Port    CallManagerState DSP-Type

4/4     notregistered   C549
```

From the Call Manager Admin interface add a gateway.

Once again, ensure the settings are correct as discussed in the previous section.

ipexpert

Device Information

MAC Address*	00027E38C797
Description	
Device Pool*	Main
Network Locale	< None >
Media Resource Group List	< None >
Location	Main
AAR Group	< None >
Load Information	

Interface Information

PRI Protoco Type*	PRI NI2
Protocol Side*	User
Channel Selection Order*	Bottom Up
Channel IE Type*	Use Number when 1B
PCM Type*	μ-law
Delay for first restart (1/8 sec ticks)	32
Delay between restarts (1/8 sec ticks)	4

☑ Inhibit restarts at PRI initialization

☐ Enable status poll

After updating and resetting verify the registration status.

System   Route Plan   Service   Feature   Device   User   Application   Help

Cisco CallManager Administration
For Cisco IP Telephony Solutions

CISCO SYSTEMS

Gateway Configuration   Cisco CallManager 3.3 Administration

Back to Find/List Gateways
Dependency Records
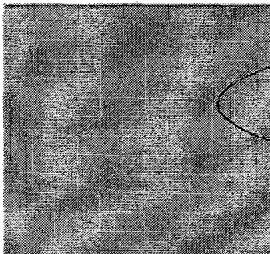
Product : Cisco Catalyst 6000 T1 VoIP Gateway
Gateway : S0/DS1-0@SDA00027E38C797
Device Protocol: Digital Access PRI
Registration: Registered with Cisco CallManager 10.4.200.21
IP Address: 10.4.200.104

Status: Insert completed.

[Update] [Delete] [Reset Gateway]

Also verify from the Catalyst- you should see the Call Manager field set to the correct IP Address.

```
Console> (enable) sh port 4/4
* = Configured MAC Address

# = 802.1X Authenticated Port Name.

Port  Name          Status    Vlan    Duplex Speed    Type

4/4                 connected 240      full 1.544 T1

Port   DHCP   MAC-Address      IP-Address     Subnet-Mask

4/4    enable 00-02-7e-38-c7-97 10.4.200.104   255.255.255.0

Port   Call-Manager(s)  DHCP-Server    TFTP-Server    Gateway

4/4    10.4.200.21      10.4.200.21    10.4.200.21    10.4.200.1
```

Channel Selection

When configuring a partial PRI you may find that the gateway set with Channel Selection 'Bottom-Up' for all outgoing calls will not work- you will receive Reorder Tone on making a call. The reason is the Call Manager is attempting to use timeslot 23 for the bearer channel but only timeslots 1-3 are lit (using the above example).

The quickest way to test if you are running into this issue is to use '**Top-Down**' and reset the gateway. The first timeslot will be selected as the bearer channel and the call should proceed.

To configure Call Manager correctly using Channel Selection='Bottom-Up' with a partial PRI you will have the Call Manager Service parameter.

Let's just take another look at the PRI on the IOS MGCP gateway.

```
P2-BR1-RTR(config-controller)#do sh isdn serv
PRI Channel Statistics:

%Q.931 is backhauled to CCM MANAGER 0x0003 on DSL 0. Layer 3 output
may not apply

ISDN Se2/0/0:23, Channel [1-24]
  Configured Isdn Interface (dsl) 0
   Channel State (0=Idle 1=Proposed 2=Busy 3=Reserved 4=Restart
5=Maint_Pend)
    Channel : 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4
```

ipexpert

```
State  : 0 0 0 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3
Service State (0=Inservice 1=Maint 2=Outofservice 8=MaintPend 9=OOSPend)
  Channel : 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4
  State  : 0 0 0 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2
```

The first three timeslots are in the idle status indicated by the '0'. However Call Manager
is unaware of this and when channel selection is set to 'Bottom-Up' or descending
channel 23 will be used.

Go to the gateway page in CCMAdmin and copy the complete gateway name shown
below.

Gateway Configuration

Product : Cisco 3825
Gateway : S2/SU0/DS1-0@P2-BR1-RTR
Device Protocol: Digital Access PRI
Registration: Registered with Cisco CallManager 10.2.200.21
IP Address: 162.2.101.2

Status: Ready

Update   Delete   Reset Gateway

Check the 'Enable Status Poll' checkbox under the Gateway page.

Interface Information

PRI Protocol Type*	PRI NI2
Protocol Side*	User
Channel Selection Order*	Bottom Up
Channel IE Type*	Use Number when 1B
Delay for first restart (1/8 sec ticks)	32
Delay between restarts (1/8 sec ticks)	4

☑ Inhibit restarts at PRI initialization

☑ Enable status poll

ipexpert

Go to CCM Service Parameters, click the 'Advanced' tab and changed the B-channel Maintenance Status parameter. You will notice that you are allowed a maximum of 5 partial PRIs in a Call Manager cluster. In this example the service parameter is set to:

S2/SU0/DS1-0@P2-BR1-RTR=0001 1111 1111 1111 1111 1110

The '0' indicates an active bearer channel. The last '0' is to indicate that the signaling channel is active.

Caller ID	
Calling Name Not Available Timeout (msec)*	2000
Calling Party Number Screening Indicator*	CallManager sets the screening indicator value ▼
Change B-Channel Maintenance Status 1	S2/SU0/DS1-0@P2-BR1-RTR=0001 1111
Change B-Channel Maintenance Status 2	

Finally, restart the Call Manager Service.

E1 R2

Theory

R2 signaling is a channel associated signaling (CAS) system developed in the 1960s that is still in use today in Europe, Latin America, Australia, and Asia. The specification is defined in (ITU-T) Recommendations Q.400 through Q.490.

There are two elements to R2 signaling: line signaling (supervisory signals) and interregister signaling (call setup control signals). Most country variations in R2 signaling are with the interregister signaling configuration.

Line signaling is defined with these types:

R2-Digital—R2 line signaling type ITU-U Q.421, typically used for PCM systems (where A and B bits are used).

R2-Analog—R2 line signaling type ITU-U Q.411, typically used for carrier systems (where a Tone/A bit is used).
R2-Pulse—R2 line signaling type ITU-U Supplement 7, typically used for systems that employ satellite links (where a Tone/A bit is pulsed).

Note: R2-Pulse reflects the same states as the analog signaling, but the analog signal is a steady state (continuous signal), while the pulsed signal stays on for only a short duration. Pulsed is just a single pulse to reflect the state change.

There are three types of interregister signaling:

R2-Compelled—When a tone-pair is sent from the switch (forward signal), the tones stay on until the remote end responds (sends an ACK) with a pair of tones that signals the switch to turn off the tones. The tones are compelled to stay on until they are turned off.
R2-Non-Compelled—The tone-pairs are sent (forward signal) as pulses so they stay on for a short duration. Responses (backward signals) to the switch (Group B) are sent as pulses. There are no Group A signals in non-compelled interregister signaling.
Note: Most installations use the non-compelled type of interregister signaling.
R2-Semi-Compelled—Forward tone-pairs are sent as compelled. Responses (backward signals) to the switch are sent as pulses. It is the same as compelled, except that the backward signals are pulsed instead of continuous.

E1 R2 is not supported with MGCP signaling therefore it must be configured as an H323 gateway and hence the dial plan must be defined in the H323 dial-peers on the router.

Configuration

The command **ds0-group** (or **cas-group**, depending on the Cisco IOS® version) needs to be defined on the E1 controllers.

The command **cas-custom** is used to customize the E1 R2 variants for different countries or regions.

Set up the controller E1 that connects to the PSTN.

- Ensure that the framing of the E1 is properly set- for E1 framing, choose either **CRC** or **non-CRC**.
- Ensure that the linecoding of the E1 is properly set- for E1 linecoding, choose either **HDB3** or **AMI**.
- For the E1 clock source, choose either **internal** or **line**.

Create DS0 group, define how many timeslots are lit and choose line signaling type- this must match the other side's configuration.

```
P2-BR2-RTR(config-controller)#ds0-group 0 timeslot 1-3 type ?
  e&m-delay-dial      E & M Delay Dial
  e&m-fgd             E & M Type II FGD
  e&m-immediate-start E & M Immediate Start
  e&m-melcas-delay    MEL CAS (CEPT) E & M Delay Start
  e&m-melcas-immed    MEL CAS (CEPT) E & M Immediate Start
  e&m-melcas-wink     MEL CAS (CEPT) E & M Wink Start
  e&m-wink-start      E & M Wink Start
  ext-sig             External Signaling
  fxo-ground-start    FXO Ground Start
  fxo-loop-start      FXO Loop Start
  fxo-melcas          MEL CAS (Mercury) FXO
  fxs-ground-start    FXS Ground Start
  fxs-loop-start      FXS Loop Start
  fxs-melcas          MEL CAS (Mercury) FXS
  none                Null Signalling for External Call Control
  r2-analog           R2 ITU Q411
  r2-digital          R2 ITU Q421
  r2-pulse            R2 ITU Supplement 7
```

Next configure Interregister Signaling, again this must match the PSTN side's configuration.

```
P2-BR2-RTR(config-controller)#ds0-group 0 timeslots 1-3 type r2-digital ?
  dtmf              DTMF tone signalling
  r2-compelled      R2 Compelled Register Signalling
  r2-non-compelled  R2 Non Compelled Register Signalling
  r2-semi-compelled R2 Semi Compelled Register Signalling
```

The Cisco implementation of R2 signaling has Dialed Number Identification Service (DNIS) support enabled by default. If you enable the Automatic Number Identification (ANI) option, the collection of DNIS information is still performed. Specification of the ANI option does not disable DNIS collection.

```
P2-BR2-RTR(config-controller)#$ 1-3 type r2-digital r2-semi-compelled ani
```

The **cas-custom** command under the controller E1 is used to customize the E1 R2 country variants and channel associated signaling (CAS) parameters. An example is the 'dnis-digits' command- If the router does not know the number of DNIS digits beforehand, it has to rely on a timeout mechanism (three seconds) in order to detect the end of DNIS. The configuration of max speeds up the call setup time by three seconds.

```
controller E1 0/0/0
  ds0-group 0 timeslots 1-3 type r2-digital r2-semi-compelled ani
  cas-custom 0
   dnis-digits min 3 max 11
```

Verify.

```
P2-BR2-RTR#sh voice port summ
                      IN    OUT
PORT    CH  SIG-TYPE  ADMIN OPER STATUS  STATUS  EC

0/0/0:0  01  r2-digital  up    dorm idle    idle    y
0/0/0:0  02  r2-digital  up    dorm idle    idle    y
0/0/0:0  03  r2-digital  up    dorm idle    idle    y
```

Debug and troubleshoot using the following command:

```
P2-BR2-RTR#deb vpm signal
Voice Port Module signaling debugging is enabled
```

H323 Dial-Peers

Each leg of a call has two dial-peers associated with it- an incoming leg and an outgoing leg (from the perspective of the router). An inbound call leg originates when an incoming call comes *to* the router. An outbound call leg originates when an outgoing call is placed *from* the router.

T
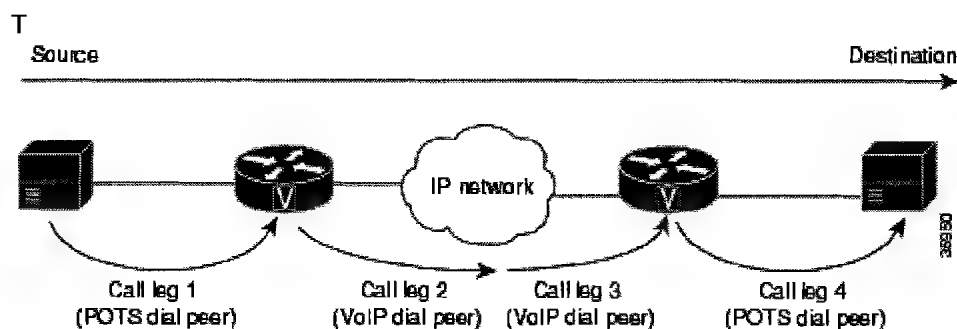
Depending on the call leg, a call is routed using one of the two types of dial peers:

- **POTS Dial peer:** that defines the characteristics of a traditional telephony network connection. POTS dial peers map a dialed string to a specific voice port on the local router, normally the voice port connecting the router to the local PSTN.

- **VoIP Dial-Peer**: Dial peer that defines the characteristics of a packet network connection and map a dialed string to a remote network device, such as the destination Call Manager. Can also be MMoIP or VoFR dial-peers as well.

Incoming POTS Leg
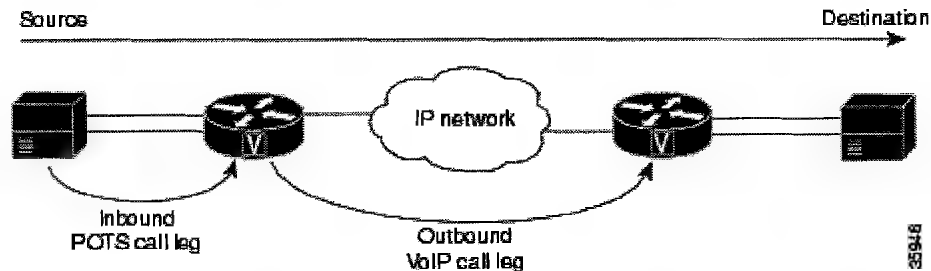
In the example above the incoming dial-peer will be a POTS dial-peer and the outgoing dial-peer will be a VoIP dial-peer.

To match inbound call legs to dial peers, the router uses three information elements in the call setup message and four configurable dial peer attributes. The three call setup elements are:

- Called number or dialed number identification service (DNIS)—A set of numbers representing the destination, which is derived from the ISDN setup message or CAS DNIS.
- Calling number or automatic number identification (ANI)—A set of numbers representing the origin, which is derived from the ISDN setup message or CAS ANI.
- Voice port—The voice port carrying the call.

The four configurable dial peer attributes are:

- Incoming called-number—A string representing the called number or DNIS. It is configured by using the incoming called-number dial-peer configuration command in POTS or MMoIP dial peers.
- Answer address—A string representing the calling number or ANI. It is configured by using the answer-address dial-peer configuration command in POTS or VoIP dial peers and is used only for inbound calls from the IP network.
- Destination pattern—A string representing the calling number or ANI. It is configured by using the destination-pattern dial-peer configuration command in POTS or voice-network dial peers.
- Port—The voice port through which calls to this dial peer are placed.

The router selects an inbound dial peer by matching the information elements in the setup message with the dial peer attributes. The router attempts to match these items in the following order:

ipexpert

1. Called number with incoming called-number
2. Calling number with answer-address
3. Calling number with destination-pattern
4. Incoming voice port with configured voice port

The router must match only one of these conditions. It is not necessary for all the attributes to be configured in the dial peer or that every attribute match the call setup information; only one condition must be met for the router to select a dial peer. The router stops searching as soon as one dial peer is matched and the call is routed according to the configured dial peer attributes. Even if there are other dial peers that would match, only the first match is used.

We recommend the following as the incoming POTS dial-peer

```
dial-peer voice 1 pots
incoming called-number
port 0/0/0:0
```

Note that '.' is the only wildcard for incoming called-number. Add the '**direct-inward-dial**' line into the incoming POTS dial-peer if DID is supported.

Outgoing VOIP Leg

Outgoing dial-peers are responsible for routing the call to the appropriate Call Manager or far-end router.

Destination-pattern is used for call routing- a text string follows the destination-pattern parameter and can contain a digit or any of the wildcard characters shown below.

Wildcard Symbols Used in Destination Patterns	
Symbol	Description
.	Indicates a single-digit placeholder. For example, 555.... matches any dialed string beginning with 555, plus at least four additional digits.
[ ]	Indicates a range of digits. A consecutive range is indicated with a hyphen (-); for example, [5-7]. A nonconsecutive range is indicated with a comma (,); for example, [5,8]. Hyphens and commas can be used in combination; for example, [5-7,9]. **Note** Only single-digit ranges are supported. For example, [98-102] is invalid.
( )	Indicates a pattern; for example, 408(555). It is used in conjunction with the symbol ?, %, or +.
?	Indicates that the preceding digit occurred zero or one time. Enter ctrl-v before entering ? from your keyboard.
%	Indicates that the preceding digit occurred zero or more times. This

ipexpert

	functions the same as the "*" used in regular expression.
+	Indicates that the preceding digit occurred one or more times.
T	Indicates the interdigit timeout. The router pauses to collect additional dialed digits.

For example destination-pattern 9T matches the digit 9 followed by zero or more digits- it will route the call only after the expiry of the inter-digit timeout.

It is also possible that there may be more than one matching dial-peer, for example **destination-pattern 3...** and **destination-pattern 30..** will both be matched when the outgoing digit string is '3001'. In this case IOS uses longest-match routing. However if the call to that peer fails the gateway attempts to use the other peer that matches.

When there is an equal match (i.e. two identical destination-pattern statements in different dial-peers) then the **preference** command is the tie-breaker- the higher the preference the lower the priority of the dial-peer.

Once the dial-peer has been matched using the destination-pattern command, you must tell the gateway what IP Address to send the call to. You do this using the **session-target ipv4:***ip address* command.

An example of two outgoing VoIP dial-peers is shown below:

```
dial-peer voice 3000 voip
 destination-pattern 3...
 session target ipv4:10.2.200.21
!
dial-peer voice 3001 voip
 preference 1
 destination-pattern 3...
 session target ipv4:10.2.200.20
```

The second dial-peer will only be used if dial-peer 3000 fails since it has higher preference.

You can configure a variety of commands on the VoIP dial-peer to set various characterisitics of a call that is routed via that dial-peer. On a VoIP dial-peer some of these include codec, DTMF relay and VAD. The default settings are G729, DTMF disabled and VAD (Voice Activity Detection) enabled.
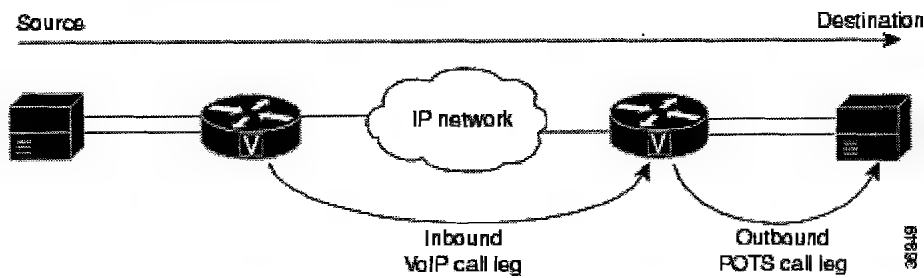
A VoIP dial-peer that supports G711 and G729, VAD disabled and DTMF relay set appropriately is shown below:

```
voice class codec 1
 codec preference 1 g711ulaw
 codec preference 2 g729r8
```

```
dial-peer voice 3000 voip
 destination-pattern 3...
 voice-class codec 1
 session target ipv4:10.2.200.21
 dtmf-relay h245-alphanumeric
 no vad
```

Outgoing POTS dial-peer

The concepts are the same as for outgoing VOIP dial-peer in that destination-pattern must be used- the only difference is that we specify where the call shall be routed based on POTS settings as opposed to IP settings. Instead of using the session target command we shall use the **port** command.

```
dial-peer voice 911 pots
 destination-pattern 9..
 port 0/0/0:0
```

When a call is routed to a POTS dial-peer, the default behavior is to strip any digits that were explicitly matched and pass the rest. In the above example the leading '9' is stripped and the next two digits are passed. To override the default behavior use the **no digit-strip** or **forward-digits all** commands. You can also use the **prefix** command to insert the digits that were stripped.

You can also use the same wildcard characters specified in the previous section.

Incoming VOIP dial-peer

The same routing matches as for incoming POTS dial-peer (with the exception that direct-inward-dial cannot be used). If there are no matches with incoming called-number, answer-address and destination-pattern (matching on a dial-peer with port is not an option for voip dial-peers) then the default dial-peer is used- this is peer ID 0 or dial-peer 0 (not visible). This dial-peer has the following characteristics:

- Any support codec
- No DTMF relay
- IP Precedence 0
- VAD-enabled
- Fax rate voice

ipexpert

We recommend always using a dial-peer with the incoming called-number command to ensure you always have a match.

Debug and Troubleshooting

Use the show call active voice brief command to verify which dial-peers are matched for an active call.

```
Router# show call active voice brief
...
pkts>/<t120 bytes> rx:<audio pkts>/<audio bytes>,<video pkts>/<video bytes>,<t120
pkts>/<t120 bytes>
Total call-legs:2
1269 :7587246hs.1 +260 pid:0 Answer active
 dur 00:07:14 tx:590/11550 rx:21721/434420
 IP 172.29.248.111:17394 rtt:3ms pl:431850/0ms lost:0/0/0 delay:69/69/70ms g729r8
1269 :7587246hs.2 +259 pid:133001 Originate 133001 active
 dur 00:07:14 tx:21717/434340 rx:590/11550
 Tele 1/0:1 (2):tx:434350/11640/0ms g729r8 noise:-44 acom:-19 i/0:-45/-45 dBm
```

ipexpert

Gatekeeper

The basic idea of gatekeeper CAC is that each Call Manager cluster (and possibly ATA with H323 firmware and CME) registers with the gatekeeper and uses it to determine whether it is allowed to make a call and to help make a routing decision (E164 number resolution).

Gatekeeper Configuration

Gatekeeper can be configured in IOS software with appropriate licenses. All gatekeeper commands can be found under the *"gatekeeper"* command from global configuration.

The first step is to define the local zone using the *"zone local"* command.

```
zone local gatekeeper-name domain-name [ras IP-address]
```

Note that the zone name is case sensitive. A domain name is mandatory even if DNS resolution is not being used. The RAS IP Address is optional but it is recommended that one is defined to avoid gatekeeper registration problems.

Remote zones can be defined in using the same command except the keyword *"...local..."* is replaced with *"remote"*.

When registering to the gatekeeper, unlike IOS gateways including CME and terminals such as ATA 186, Call Manager does not register its E164 numbers and therefore to route calls TO the Call Manager from gatekeeper the default tech-prefix must be used.

```
gw-type-prefix 1# default-technology
```

Call Manager must register to the gatekeeper with whatever you have defined as the tech-prefix, in the example 1#.

Gatekeeper is not involved with codec selection- codec negotiation takes place between the two endpoints for example Call Manager and an IOS gateway or ATA. The Region setting on Call Manager will determine what codec calls through the gatekeeper. Call Admission control for calls passing through the gatekeeper should not be dependent on Locations CAC- instead gatekeeper CAC should be configured using the *"bandwidth"* command.

```
bandwidth total zone PSTN-WAN 16
```

One G729 call should be provisioned with 16Kbps and a single G711 call should be provisioned with 128Kbps.

Note: In a scenario where Gatekeeper controls several zones, we recommend you make use of the "*bandwidth interzone*" command. The "*bandwidth total*" command can cause issues in some configurations.

To route calls within or between zones use the "*zone prefix*" command

A sample configuration is displayed below.

```
gatekeeper
zone local HQ-RTR ipexpert.com 172.5.100.1
zone remote PSTN-WAN ipexpert.com 10.5.200.2 1719
zone prefix PSTN-WAN 011*
gw-type-prefix 1#* default-technology
no use-proxy HQ-RTR remote-zone PSTN-WAN outbound-from gateway
bandwidth remote 16
no shutdown
```

ipexpert

CCM Registration

Configure a Gatekeeper and H225 trunk. CCM registers to gatekeeper as a gateway- zone name and tech prefix is required in the trunk configuration on Call Manager.

From Device-Trunk add a H225 Trunk (Gatekeeper Controlled) and give it a unique name. Also don't forget to set Device Pool and Location information. The Location should be the unrestricted location and the Device Pool should contain the relevant region setting.

Product: H.225 Trunk (Gatekeeper Controlled)
Device Protocol: H.225

Status: Ready

[Insert]

Device Information

Device Name*	ccm_trunk
Description	ccm_trunk
Device Pool*	HQ
Media Resource Group List	< None >
Location	< None >
AAR Group	< None >

☐ Media Termination Point Required

Be careful not to forget the parameters at the bottom of the trunk page.

Gatekeeper Information

Gatekeeper Name*	172.2.100.1
Terminal Type*	Gateway
Technology Prefix	1#
Zone	HQ-RTR

* indicates required item

Verify using the following command:

```
P2-HQ-RTR# sh gatek end
              GATEKEEPER ENDPOINT REGISTRATION

CallSignalAddr   Port  RASSignalAddr   Port  Zone Name      Type    Flags

10.2.200.21   54029 10.2.200.21   52991 HQ-RTR        VOIP-GW
   H323-ID: GK-TRUNK_1
   Voice Capacity Max.= Avail.= Current.= 0
Total number of active registrations = 1
```

ipexpert

Proxy Configuration

The proxy terminates the RTP streams of the devices that are configured to use it. The proxy itself can be co-resident on the gatekeeper or configured on a different IOS router supporting the proxy or MCM feature.

```
proxy h323
!
!
interface Loopback
 ip address 172.5.100.1 255.255.255.0
 h323 interface
 h323 h323-id proxy
 h323 gatekeeper id HQ-RTR ipaddr 172.3.100.1
```

Tell the gatekeeper which calls to use the proxy. Note- only one Proxy is allowed per gatekeeper.

```
gatekeeper
 ...
 use-proxy HQ-RTR remote-zone PSTN-WAN outbound-from gateway
```

ipexpert

Gatekeeper Call Routing

The Default Technology prefix is required to route calls to Call Manager since Call Manager does not register its E164 number.
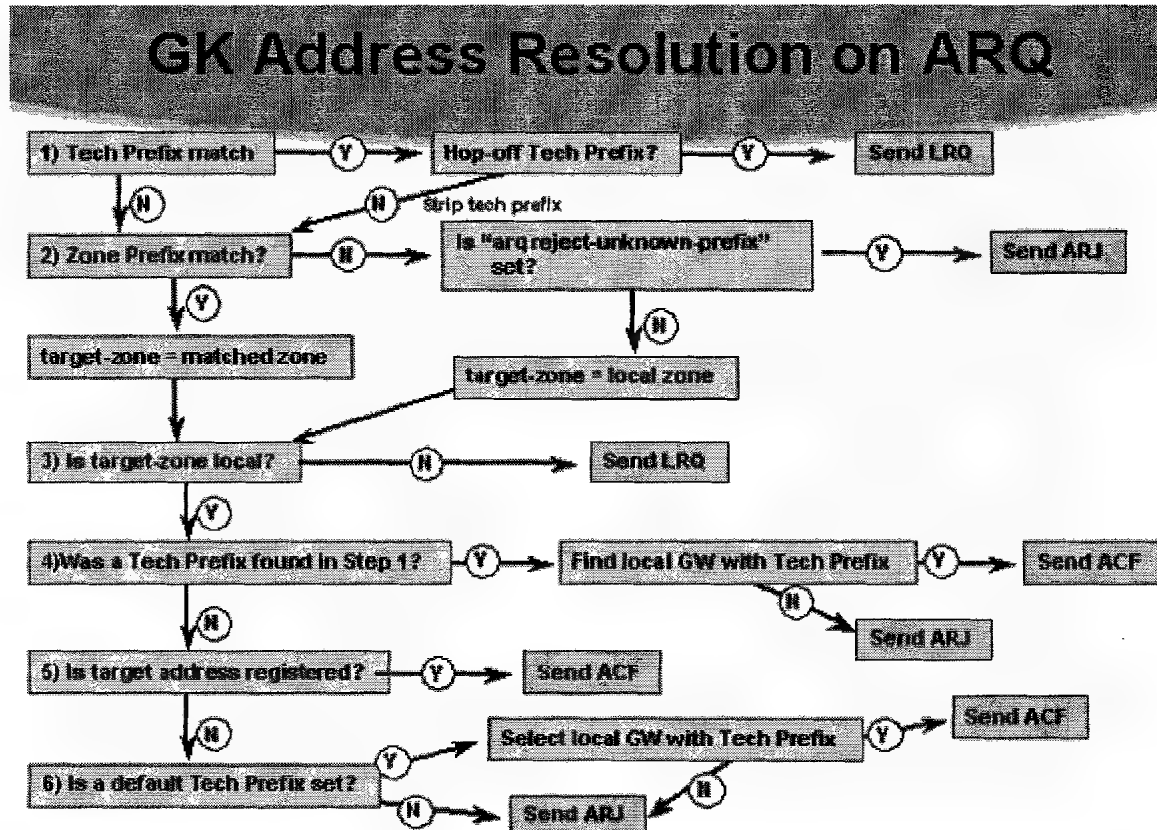
Call Routing no Tech Prfefix

The Default Tech Prefix allows calls to be routed TO Call Manager- see above diagram!

IOS gateways and Terminals register their respective E164 numbers and therefore do not require the default Tech Prefix.
To route calls to Call Manager without the default technology use the following command:

```
Gatekeeper

gw-type-prefix 1#* gw ipaddr <CCM-IP-ADDRESS>
```

ATA and CCME routing to CCM will need to prefix the tech prefix CCM registered to gatekeeper with.

ipexpert

To route calls to Call Manager without any Tech Prefix use the "*alias static*" command.

IOS Gateway Registration and Call Routing

Enter gateway configuration mode.

```
configure terminal
Router(config)# gateway
```

Configure the gateway H.323 interface.

```
Router(config)# interface fastethernet 0/0
Router (config-if)# h323-gateway voip interface
Router (config-if)# h323-gateway voip h323-id gateway-id
Router (config-if)# h323-gateway voip id gatekeeper-id {ipaddr ip-address
[port-number] | multicast}
```

Configure the gateway to register to the gatekeeper with a technology prefix, if you use a technology prefix.

```
Router (config-if)# h323-gateway voip tech-prefix prefix
```

The *prefix* defines the numbers that serve as the technology prefixes. Although not strictly
necessary, a pound (#) symbol frequently serves as the last digit in a technology prefix.

Configure VoIP dial peers.with the session target as RAS.
Note: If the gateway sends a prefix in the call setup, be sure to configure the prefix in the
VoIP dial-peer that corresponds.

```
Router (config-dial-peer)# session target ras
Router (config-dial-peer)# tech-prefix number
```

Debug and Troubleshooting

To debug gatekeeper registration use **sh gatekeeper status**

To debug Proxy use **sh proxy h323 status**

To debug call routing use **Debug gatekeeper main 10**

Media

IP Media Streaming Application

The Cisco IP Voice Media Streaming Application provides voice media streaming functionality for Cisco Call Manager for use with MTP, conferencing, and music on hold (MOH). The Cisco IP Voice Media Streaming Application relays messages from Cisco Call Manager to the IP voice media streaming driver. The driver handles the RTP streaming. The MTP and conference bridge components of the Cisco IP Voice Media Streaming Application support G.711 mu-law and a-law codecs. The MOH component supports G.711 mu-law/a-law, G.729a, and wideband codecs.

When you activate the Cisco IP Voice Media Streaming Application, Cisco Call Manager automatically adds the MTP, MOH, and conference devices to the database. By default, the installation program places the executable in the C:\Program Files\Cisco\bin directory.

Conference Bridge and Transcoder

A Conferencing Bridge in Call Manager is either a software or hardware device that caters for both Ad Hoc and Meet-Me voice conferencing.

The software conference bridge supports G711 only whereas the hardware conference bridge (NM-HDV module or WS-6608 DSP card) supports transcoding between the G.711, G.729, G.723, G711 GSM Full Rate (FR), and G711 GSM Enhanced Full Rate (EFR) codecs. We recommend you disable use of the software conference bridge unless instructed otherwise.

Transcoder allows devices with incompatible codecs to communicate with each other. A transcoder connects a full-duplex RTP stream using one codec (such as G711) to another full-duplex RTP stream using a different codec (such as G729) in real time. Transcoding resources must reside on dedicated hardware because of the DSP resources required to convert from one codec to another.

A common example where a transcoder is required is if a remote site calls into IPCC Express over the WAN- typically the Transcoder will be placed in the HQ Region and Device Pool and the Branch phones will be in the BR1 Region and Device Pool. Codec within regions is G711 and between regions is G729. IPCC Express version 3.0 does NOT support playing back recorded messages using the G729 codec hence a transcoder is required.

ipexpert

BR1 Region/Device Pool   HQ Region/Device Pool
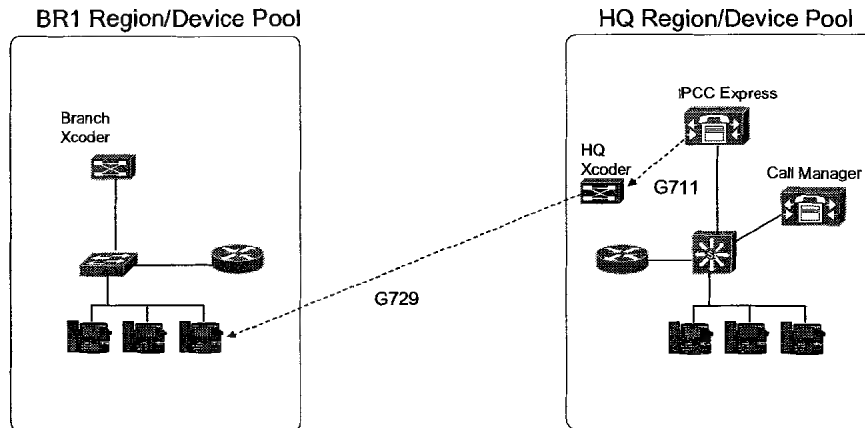
A transcoder can also function as a media termination point (MTP) which allows for supplementary serives such as hold and transfer to H323 devices that otherwise would not support this functionality due to a lack of support for the null capabilities set H323 feature. All IOS gateways DO support the null capabilities set so the MTP functionality is generally only required when dealing with non-cisco H323 ays.

MTP resources can also be provided in software, however unlike a transcoder will only support G711.
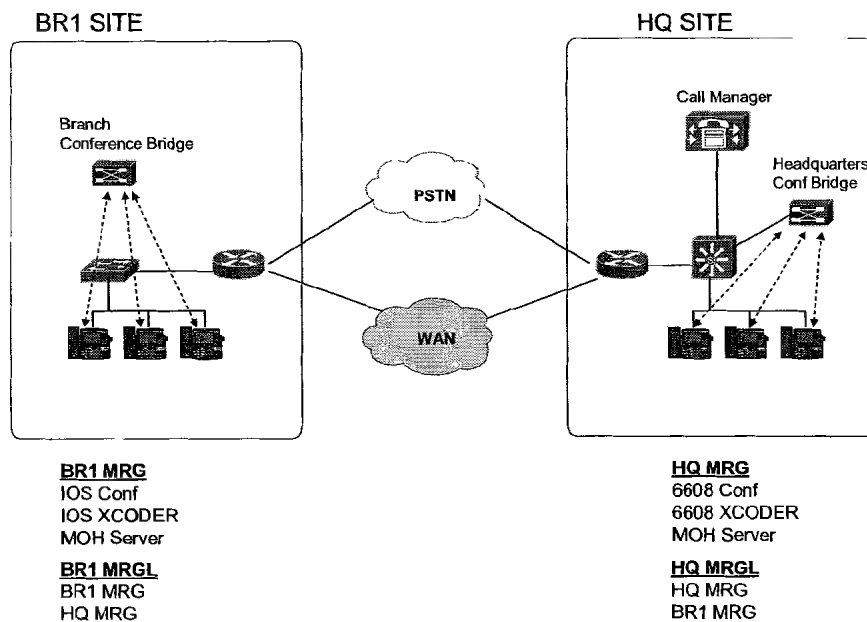
Media Resource Management

Call Manager supports Media Resource Groups (MRG) and Media Resouce Group Lists (MRGL).

MRGs are logical groupings of media resources and can contain hardware conference resources, software conference resources, transcoder resources, MOH servers and software MTPs.

MRGLs are just ordered lists of MRGs.

The most common use of MRGs and MRGLs is to restrict media resource usage on a geographic basis. For example HQ phones can use the HQ media resources and BR1 phones can use the BR1 media resources in the example below.

Another use is to provide resiliency- for example if the HQ conference bridge is out of service then the HQ can also access the BR1 media resources.

BR1 SITE

Branch
Conference Bridge

PSTN

WAN

HQ SITE

Call Manager

Headquarters
Conf Bridge

BR1 MRG
IOS Conf
IOS XCODER
MOH Server

BR1 MRGL
BR1 MRG
HQ MRG

HQ MRG
6608 Conf
6608 XCODER
MOH Server

HQ MRGL
HQ MRG
BR1 MRG

All media resources in a MRG are load balanced therefore the order the media resources appear in a MRG is irrelevant.

The order in which MRGs appear in a MRGL is however relevant- the resources in the second MRG will only ever be used if the media resources in the first MRG are exhausted.

MRGLs are assigned to Devices or Device Pools. If a device has a MRGL assigned on a per-device level and also to its Device Pool, then the MRGL for the device is searched first followed by the MRGL assigned to the Device Pool.

The last place where a device can gain access to media resources is through the default MRGL. Any media resource that is not assigned to a MRG is automatically assigned to the default MRGL. As soon as a media resource is in an MRG, it is no longer available to devices via the default list. The default list is always searched last when looking for media resources.

Configuring IOS Conference Bridge

Enable Voice Card Services

Perform these tasks in order to configure DSP Farm services for a particular digital T1/E1 packet voice trunk network module (NM-HDV) or high-density voice (HDV) Transcoding/Conferencing DSP Farm (NM-HDV-FARM).

```
Gateway#configure terminal
Gateway(config)#voice-card 1

Gateway(config-voicecard)#dsp services dspfarm
```

Enable the DSPFARM

Perform these tasks in order to add a specified voice card to those that participate in a DSP resource pool and in order to configure Transcoding and Conference Bridge maximum sessions.

Note: This example is for two SIMMS with three DSPs each for a total of six DSPs. The three Conference Bridges use one DSP each and the twelve Transcoding sessions require three DSPs for a total of six.

```
Gateway#configure terminal
Gateway(config)#dspfarm transcoder maximum sessions 12

Gateway(config)#dspfarm confbridge maximum sessions 3

Gateway(config)#dspfarm
Gateway(config)#dspfarm rtp timeout 60

Gateway(config)#dspfarm connection interval 60

If you want to disable G.729 VAD, use these commands:
Gateway#configure terminal
Gateway(config)#dspfarm codec g729 vad disable
```

Enable SCCP Gateway Mode

Perform these tasks in order to enable the Skinny Client Control Protocol (SCCP) protocol and its related applications (transcoding and conferencing).

```
Gateway#configure terminal
Gateway(config)#sccp
Gateway(config)#sccp local FastEthernet 0/0

Gateway(config)#sccp ccm 10.82.84.144 priority 1
Issue these commands in order to configure a connection to a second Cisco CallManager:
Gateway(config)#sccp ccm 10.82.84.145 priority 2
Gateway(config)#sccp switchback timeout guard 180
```

ipexpert

Cisco IOS Conference Bridge Configuration Settings

From the Call Manager web page add a conference bridge based on the settings below.

Field	Description
Conference Bridge Type	Choose **Cisco IOS Conference Bridge**.
Conference Bridge Name	Enter CFB*xxxxxxxxxxxx* where *xxxxxxxxxxxx* is the MAC address of interface used in the **sccp local** *interface* command.. **Tip:** Obtain the MAC address of the SCCP local interface with the use of the **show interface** *interface* **name** command. Verify that you use the correct interface by making sure the interface IP address matches the Gateway IP address from the **show sccp** command. Use the **show ip interface brief** command for a list of interface names and IP addresses.
Description	Enter any description for the Conference Bridge.
Device Pool	Choose a device pool that has the highest priority within the Cisco CallManager group that you use or choose **Default**.

In this example the interface is FastEthernet 0/0. Obtain the MAC address of FastEthernet 0/0 by the use of the **show interface** *FastEthernet 0/0* command.

```
Gateway#show interface FastEthernet 0/0

FastEthernet0/0 is up, line protocol is up
  Hardware is AmdFE, address is 0009.43b8.5660 (bia 0009.43b8.5660)
  Internet address is 10.82.84.54/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not set
  Full-duplex, 100Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 1/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
```

ipexpert

```
Output queue: 0/40 (size/max)
5 minute input rate 7000 bits/sec, 10 packets/sec
5 minute output rate 3000 bits/sec, 4 packets/sec
```

The figure below shows a successfully registered Conference Bridge resource in Cisco CallManager.

Verify the SCCP Configuration

Issue the **show sccp** command in order to verify the SCCP configuration.

```
Gateway#show sccp
SCCP Admin State: UP
Gateway IP Address: 10.82.84.54
Switchover Method: IMMEDIATE, Switchback Method: GUARD_TIMER
Switchback Guard Timer: 1200 sec, IP Precedence: 5
Max Supported MTP sessions: 0
User Masked Codec list: None
Call Manager: 10.82.84.144, Port Number: 2000
          Priority: 1, Version: 3.1 or Higher
```

Verify the DSP Farm Configuration

Issue the **show dspfarm** command in order to verify the DSP Farm configuration.

ipexpert

```
Gateway#show dspfarm
DSPFARM Configuration Information:
Admin State: UP, Oper Status: ACTIVE - Cause code: NONE
Transcoding Sessions: 12(Avail: 12), Conferencing Sessions: 3 (Avail: 3)
Trans sessions for mixed-mode conf: 0 (Avail: 0), RTP Timeout: 600
Connection check interval 600 Codec G729 VAD: ENABLED
```

Verify DSP Farm Resource Registration on the Gateway

Issue the **show sccp** command in order to verify the Transcoder and Conference Bridge registration from the gateway.

```
Gateway#show sccp
SCCP Admin State: UP
Gateway IP Address: 10.82.84.54
Switchover Method: IMMEDIATE, Switchback Method: GUARD_TIMER
Switchback Guard Timer: 1200 sec, IP Precedence: 5
Max Supported MTP sessions: 0
User Masked Codec list: None
Transcoding Oper State: ACTIVE - Cause Code: NONE
Active Call Manager: 10.82.84.144, Port Number: 2000
TCP Link Status: CONNECTED
Conferencing Oper State: ACTIVE - Cause Code: NONE
Active Call Manager: 10.82.84.144, Port Number: 2000
TCP Link Status: CONNECTED
Call Manager: 10.82.84.144, Port Number: 2000
         Priority: 1, Version: 3.1 or Higher
```

ipexpert

Configuring IOS Transcoder

This figure shows a successfully registered Transcoder resource in Cisco CallManager.

Add a Transcoder based on the following Cisco IOS MTP Configuration Settings

Field	Description
Media Termination Point Type	Choose **Cisco IOS Media Termination Point**.
Description	Enter any description for the MTP.
Device Name	Enter MTP*xxxxxxxxxxx* where *xxxxxxxxxxx* is the MAC address of interface used in the **sccp local** *interface* command. **Tip:** Obtain the MAC address of the **sccp local interface** with the use of the **show interface** *interface* **name** command. Verify that you use the correct interface by making sure the interface IP address matches the Gateway IP address from the **show sccp** command. Use the **show ip**

ipexpert

	interface brief command for a list of interface names and IP addresses.
Device Pool	Choose a device pool that has the highest priority within the Cisco CallManager group that you use or choose **Default**.

Confguring WS-6608 Conference Bridge

The way that the WS-X6608 is configured as a device in Cisco CallManager determines whether the ports act as WAN interfaces (T1/E1 hardware-specific) or support transcoding and conferencing. Each of the eight ports on the blade has a separate MAC address that you can define for transcoder or conference functionality. Once the choice is made, the port is exclusive to that function and is not available for use with the other function. Any attempt made to double-assign the MAC address of a port is rejected with the error MAC address already in use.

Most of the configuration parameters are entered on the Cisco CallManager server. The WS-X6608 Blade in the Catalyst 6000/6500 Switch receives its configuration from the Cisco CallManager server via TFTP.

Note: If you do not configure or disable all of the ports on a WS-X6608 Blade, this system message continually appears on your console screen and in your system logs (if you have them configured):

```
%SYS-4-MODHPRESET:Host process (860) mod_num/port_num got reset
asynchronously
```

This is the expected behavior for this blade. It does not affect system performance. Issue the **set port voice interface 5/1 dhcp enable vlan <aux-vlan>** command in order to enable DHCP on a port and place it in the correct VLAN.

Issue the **reset** *module-number* command in order to reset the module after you set up the new IP parameters.

```
AV-6509-1 (enable) reset 5

This command will reset module 5 and may disconnect your telnet session.
Do you want to continue (y/n) [n]? y

2001 May 29 05:33:23 %SYS-5-MOD_RESET:
        Module 5 reset from telnet/10.21.8.172/

!--- This timestamped line appears on one line.

Resetting module 5...
```

ipexpert

The WS-X6608 port cannot register with Cisco CallManager until it has been configured on the CallManager server and has been reset from the server. The next procedure explains how to add the new conference bridge.

In order to configure one of the ports of the WS-X6608 Blade as conference bridge resources, choose **Service > Conference Bridge** from the Cisco CallManager Administration menu.
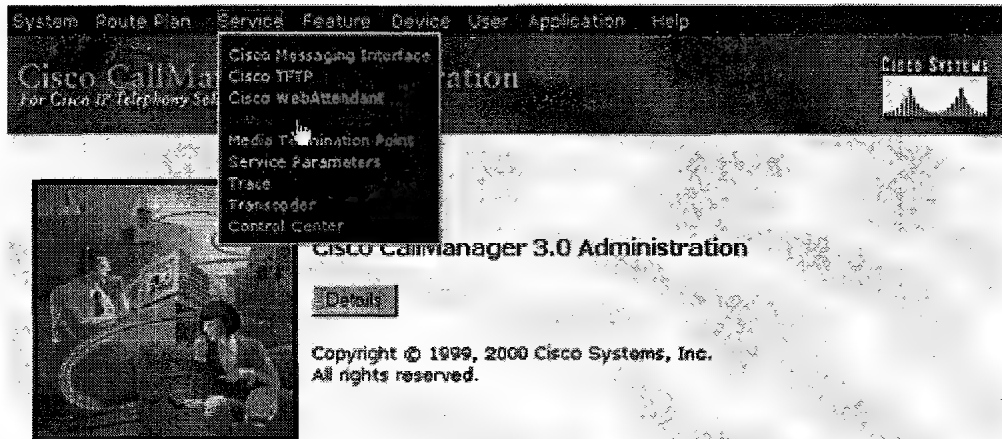
A screen similar to this appears:
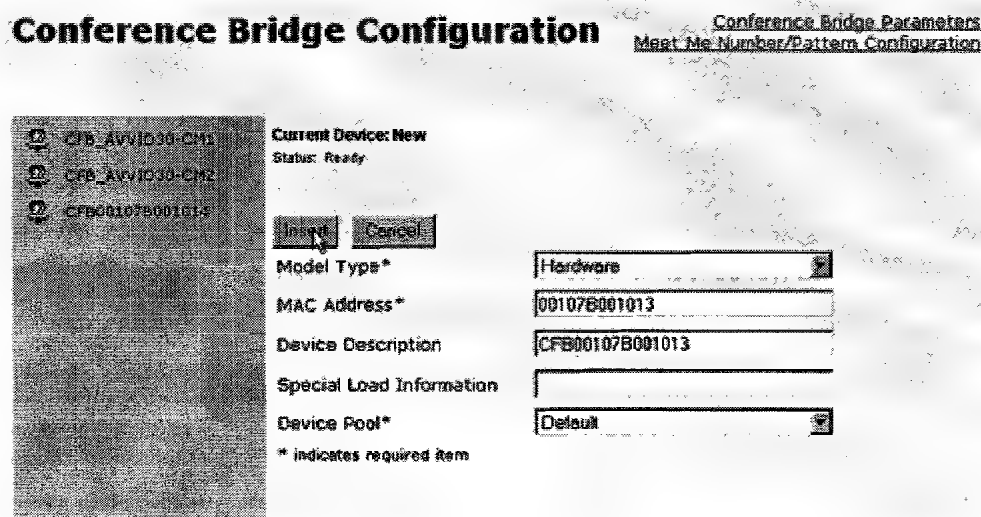
Set the Model Type field to **Hardware**.

Enter the MAC address of the WS-X6608 port that you want to be configured as a conference bridge.

The MAC address in this example is from port 5/4 of the WS-6608-T1 Blade on the Catalyst 6000/6500 Switch. This information can be discovered by issuing the **show port** command.

```
AV-6509-1 (enable) show port 5

!    Output is suppressed.

Port   DHCP    MAC-Address       IP-Address      Subnet-Mask
----------------------------------------------------------------------
5/1    enable  00-10-7b-00-10-10 172.16.14.97   255.255.255.224
5/2    disable 00-10-7b-00-10-11 172.16.14.71   255.255.255.224
5/3    disable 00-10-7b-00-10-12 172.16.14.73   255.255.255.224
5/4    enable  00-10-7b-00-10-13 172.16.14.72   255.255.255.224
5/5    disable 00-10-7b-00-10-14 172.16.14.25   255.255.255.224
5/6    disable 00-10-7b-00-10-15 172.16.14.26   255.255.255.224
5/7    disable 00-10-7b-00-10-16 172.16.14.81   255.255.255.224
5/8    disable 00-10-7b-00-10-17 172.16.14.80   255.255.255.224
```

Click **Insert** when you complete this screen.

You can possibly be notified that the device needs to be reset before it becomes active. A screen similar to this then appears:

Click **Reset Device**.

A screen similar to this appears:

Click **Reset**.

Once the Cisco CallManager server has finished resetting the device, it is registered on the switch.

You can verify that the port is configured for conferencing and display any active conference sessions with the **show port voice active** *module-number/port-number* **conference** command.

```
AV-6509-1 (enable) show port voice active 5/4 conference

Total: 0 conferencing session
```

You can also verify that the port is properly configured with the **show port** *module-number/port-number* command. In this case, the port type is listed as Conf Bridge.

```
AV-6509-1 (enable) show port 5/4

Port  Name      Status    Vlan    Duplex Speed Type
----- --------- --------- ------- ------ ----- ----------
5/4             enabled   64          full  -   Conf Bridg
```

Configuring 6608 Transcoder

The Catalyst configuration is the same as the conference bridge. The Call Manager configuration is as follows.

Choose **Service** > **Media Resource** > **Transcoder**.

Cisco CallManager 4.0 Administration

Copyright © 1999 – 2003 Cisco Systems, Inc.
All rights reserved.
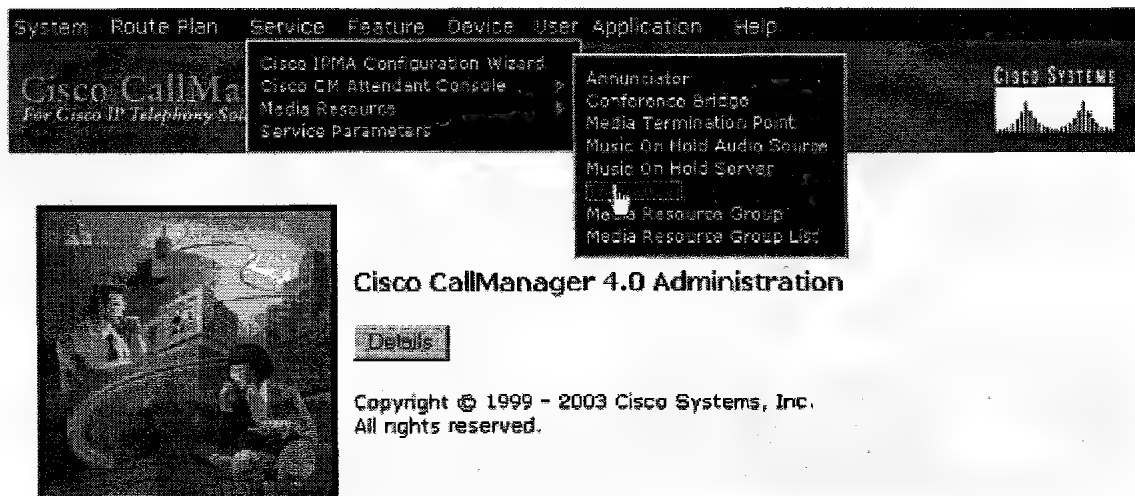
Click on **Add a New Transcoder** and fill in the MAC address of the ports on the WS-X6608 blade.

The MAC address in this example is from port 5/2 of the WS-6608-T1 blade on the Catalyst 6000 switch. You can discover this information when you use the **show port** command.

```
AV-6509-1 (enable) show port 5


(Text Deleted)


Port    DHCP    MAC-Address      IP-Address      Subnet-Mask
----    -----   --------------   ------------    ---------------
5/1     enable  00-10-7b-00-10-10 172.16.14.97   255.255.255.224
5/2     disable 00-10-7b-00-10-11 172.16.14.71   255.255.255.224
5/3     disable 00-10-7b-00-10-12 172.16.14.73   255.255.255.224
5/4     enable  00-10-7b-00-10-13 0.0.0.0        0.0.0.0
5/5     disable 00-10-7b-00-10-14 172.16.14.25   255.255.255.224
5/6     disable 00-10-7b-00-10-15 172.16.14.26   255.255.255.224
5/7     disable 00-10-7b-00-10-16 172.16.14.81   255.255.255.224
5/8     disable 00-10-7b-00-10-17 172.16.14.80   255.255.255.224
```

Enter the MAC addresses in the Transcoder Configuration window.

The Description is created automatically. You can change it in order to suit your requirements. If you have a special load file, enter the file name in the text area. This load file must be located on the TFTP server in order for the port to become active. Otherwise, leave it blank for the default load file.

System   Route Plan   Service   Feature   Device   User   Application   Help

Cisco CallManager Administration
For Cisco IP Telephony Solutions

CISCO SYSTEMS

Transcoder Configuration

Add a New Transcoder
Back to Find/List Transcoders

Transcoder: New
Status: Ready

[Insert]

Transcoder Type   [Cisco Media Termination Point Hardware ▼]

MAC Address*   [00107B001011]

Description   [MTP00107B001011]

Device Pool*   [Default ▼] (View details)

Special Load Information [   ] (Leave blank to use default)

* indicates required item

Click **Insert**.

ipexpert

A window similar to this appears.

Note: In the Transcoder Configuration window the Registration status is Unknown. The Registration status needs to read Ready. You need to troubleshoot this.

Click the **Reset** button in order to ensure that the Transcoder is reset.

Once the Cisco CallManager server has finished resetting the device, it is registered on the switch.

Verify

Verify that the port is configured for transcoding and display any active transcoding sessions with the **show port voice active** *<mod_num/port_num>* **transcode** command.

```
AV-6509-1 (enable) show port voice active 5/2 transcode
Total: 0 transcoding session
AV-6509-1 (enable)
```

Another method of verification that the port is properly configured is by using the **show port** *<mod_num/port_num>* command.

In this case the port type is listed as MTP. It can also perform transcoding.

```
AV-6509-1 (enable) show port 5/2
Port  Name        Status   Vlan   Duplex Speed Type

5/2               enabled  64       full   - MTP
```

ipexpert

You can now make calls between phones that use different codecs. You are also able to use additional phone services that require an MTP from the WS-X6608 such as call holding, call transfer, and call park.

Music On-Hold

The integrated Music On Hold (MOH) feature allows users to place on-net and off-net users on hold with music that is streamed from a streaming source. The Music On Hold feature allows two types of hold:

- End-user hold
- Network hold, which includes transfer hold, conference hold, and call park hold

Cisco CallManager supports two types of MoH transport mechanisms:

- Unicast
- Multicast

Unicast MoH consists of streams sent directly from the MoH server to the endpoint requesting an MoH audio stream. A unicast MoH stream is a point-to-point one-way audio Real-Time Transport Protocol (RTP) stream between the server and the endpoint device. Unicast music on hold uses a separate source stream for each user or connection. As more endpoint devices go on hold via a user or network event, the number of MoH streams increases. Thus, if twenty devices are on hold, then twenty streams of RTP traffic are generated over the network between the server and these endpoint devices.

Multicast MoH consists of streams sent from the MoH server to a multicast group IP address that endpoints requesting an MoH audio stream can join as needed. A multicast MoH stream is a point-to-multipoint one-way audio RTP stream between the MoH server and the multicast group IP address. Multicast music on hold conserves system resources and bandwidth because it enables multiple users to use the same audio source stream to provide music on hold. Thus, if twenty devices are on hold, then potentially only a single stream of RTP traffic is generated over the network.

The MoH feature requires the use of a server that is part of a Cisco CallManager cluster. You can configure the MoH server in either of the following ways:

Coresident deployment

In a coresident deployment, the MoH feature runs on any server (either publisher or subscriber) in the cluster that is also running the Cisco CallManager software. Because MoH shares server resources with Cisco CallManager in a coresident configuration, this type of configuration drastically reduces the number of simultaneous streams that an MoH server can send.

ipexpert

Standalone deployment

A standalone deployment places the MoH feature on a dedicated server within the Cisco CallManager cluster. The sole function of this dedicated server is to send MoH streams to devices within the network. A standalone deployment allows for the maximum number of streams from a single MoH server.

You can set up the source for MoH in any of the following ways:
- MoH from an audio file on the Cisco CallManager or MoH server
- Unicast MoH from an audio file
- Multicast MoH from an audio file
- MoH from a fixed music source (via sound card)
- Unicast MoH from a fixed source
- Multicast MoH from a fixed source

MoH can be generated from an audio file stored on the MoH server. Audio files must be in one of the following formats:

- G.711 A-law or mu-law (recorded at a sampling rate of 8 KHz)
- G.729 Annex A
- Wideband

You can create these files with the **Cisco MoH Audio Translator** service, which transcodes and formats audio source files (such as .wav or .mp3 files) into the appropriate MoH source file for the specified codec type(s). The MoH server requests these files based on the audio sources configured and loads them into memory during initialization or when the audio sources are requested. When an MoH event occurs, the configured audio source file is streamed to the requesting device on hold.

Basic MoH

The basic operation of MoH in a Cisco IP Telephony environment consists of a holder and holdee. The *holder* is the endpoint user or network application placing a call on hold, and the *holdee* is the endpoint user or device placed on hold.

The MoH stream that an endpoint receives is determined by a combination of the User Hold MoH Audio Source of the device placing the endpoint on hold (holder) and the configured media resource group list (MRGL) of the endpoint placed on hold (holdee). The User Hold MoH Audio Source configured for the holder determines the audio file that will be streamed when the holder puts a call on hold, and the holdee's configured MRGL indicates the resource or server from which the holdee will receive the MoH stream.

Basic MoH and MoH Call Flows

In simplest terms, the holder's configuration determines which audio file to play, and the holdee's configuration determines which resource or server will play that file. As

illustrated by the example below, if phones A and B are on a call and phone B (holder) places phone A (holdee) on hold, phone A will hear the MoH audio source configured for phone B (Audio-source2). However, phone A will receive this MoH audio stream from the MRGL (resource or server) configured for phone A (MRGL A).

BR1 SITE   HQ SITE

BR1 MRG   **HQ MRG**
IOS Conf   6608 Conf
IOS XCODER   6608 XCODER
MOH Server   MOH Server

BR1 MRGL   **HQ MRGL**
BR1 MRG   HQ MRG
HQ MRG   BR1 MRG
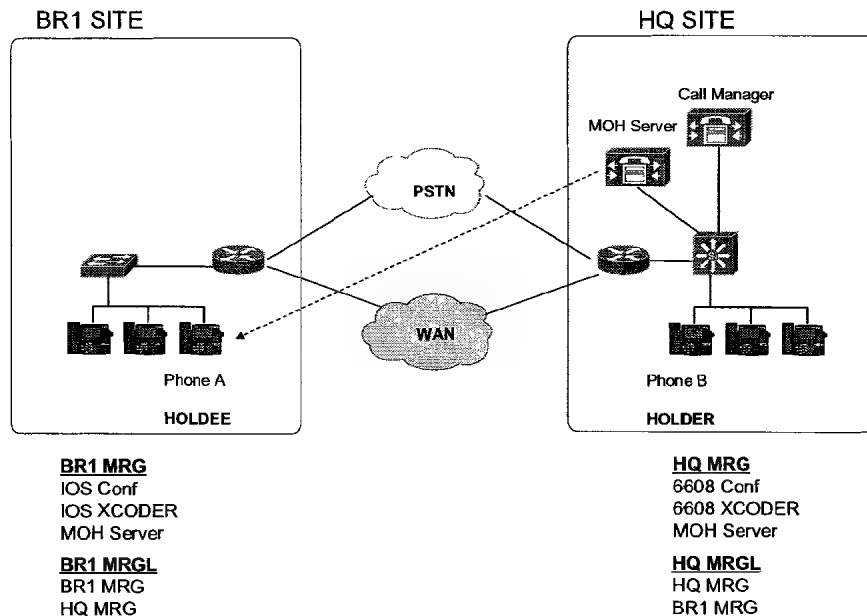
Because the configured MRGL determines the server from which a unicast-only device will receive the MoH stream, you must configure unicast-only devices with an MRGL that points to a unicast MoH resource or media resource group (MRG). Likewise, a device capable of multicast should be configured with an MRGL that points to a multicast MRG.

MoH Configuration Settings

You can configure the settings for MRGLs and User and Network Hold Audio Sources in several places within Cisco CallManager Administration, and you can configure different (and potentially conflicting) settings in each place. To determine which User and Network Audio Source configuration setting to apply in a particular case, Cisco CallManager interprets these settings for the *holder* device in the following priority order:

- Directory or line setting (Devices with no line definition, such as gateways, do not have this level.)
- Device setting
- Device pool setting
- Cluster-wide default setting

When attempting to determine the audio source for a particular holder, Cisco CallManager first looks at the User Audio Source configured at the directory or line level. If this level is not defined, then Cisco CallManager looks at the User Audio Source

configured on the holder device. If this level is not defined, then Cisco CallManager looks at the User Audio Source configured for the device pool of the holder device. If this level is not defined, then Cisco CallManager looks at the cluster-wide default audio source ID configured under the Cisco CallManager system parameters. (By default, this audio source ID is set to 1, which is the SampleAudioSource.) Cisco CallManager also interprets the MRGL configuration settings of the *holdee* device in the following priority order:

- Device setting
- Device pool setting
- System default MoH resources

When attempting to determine the MRGL for a particular holdee, Cisco CallManager looks at the MRGL configured at the device level. If this level is not defined, then Cisco CallManager looks at the MRGL configured for the device pool of the holdee device. If this level is not defined, then Cisco CallManager uses the system default MoH resources. System default MoH resources are those resources not assigned to any MRG, and they are always unicast.

Codec Selection

If you need multiple codecs for MoH deployment (based on the Device Pool and Region of the MOH Server and remote site phones), configure them in the **IP Voice Streaming Media App** service parameter under Cisco CallManager Service Parameters Configuration. Select the desired codec types from the Supported MoH Codecs list under the Clusterwide Parameters section. By default, only G.711 mu-law is selected. To select another codec type, click on it in the scrollable list. For multiple selections, hold down the CTRL key and use the mouse to select multiple codecs from the scrollable list. After making your selection, click the Update button and restart the IP Media Streaming App service.

Conference Bridge (CFB) Parameters

Parameter Name	Parameter Value	Suggested Value
Call Count*	48	48
Run Flag*	True	True

Media Termination Point (MTP) Parameters

Parameter Name	Parameter Value	Suggested Value
Call Count*	48	48
Run Flag*	True	True

Clusterwide Parameters (Parameters that apply to all servers)

Parameter Name	Parameter Value	Suggested Value
Supported MOH Codecs*	711 mulaw / 711 alaw / 729 Annex A	711 mulaw
Default TFTP MOH IP Address*	10.2.200.21	
Ip Type-of-Service to Cisco CallManager*	0x68	0x68

ipexpert

Configuring Multicast MOH

Multicast MOH is configured on the Call Manager in three places- MOH Server, MOH
Source and MRGs containing the Multicast MOH server.

Dependency Record

Music On Hold Server: MOH_10.2.200.21 (MOH_10.2.200.21)
Registration: Registered with Cisco CallManager 10.2.200.21
IP Address: 10.2.200.21

Status: Ready

Copy   Update   Delete   Reset

Device Information

Host Server	10.2.200.21
Music On Hold Server Name*	MOH_10.2.200.21
Description	MOH_10.2.200.21
Device Pool*	HQ
Location	< None >
Maximum Half Duplex Streams*	250
Maximum Multicast Connections*	30
Fixed Audio Source Device	
Run Flag*	Yes

Multicast Audio Source Information

☑ Enable Multicast Audio Sources on this MOH Server

Base Multicast IP Address	239.1.1.1
Base Multicast Port Number	16384 (Even numbers only)
Increment Multicast on	○ Port Number ⊙ IP Address

Selected Multicast Audio Sources

There are no Music On Hold Audio Sources selected for Multicasting. Click Configure Audio Sources in the
top right corner of the page to select Multicast Audio Sources.

We strongly recommend incrementing multicast on IP address instead of port number to
avoid network saturation in firewall situations. This results in each multicast audio source
having a unique IP address and helps to avoid network saturation.

The Max Hops field in the Music On Hold (MOH) Server Configuration window
indicates the maximum number of routers that an audio source is allowed to cross. If max
hops is set to zero, the audio source must remain in its own subnet. If max hops is set to
one, the audio source can cross up to one router to the next subnet.

ipexpert

Configure a multicast source.

Configuration

MOH Audio Sources
\<Add new MOH Audio Source\>
1 **SampleAudioSource**
51 Fixed Audio Source (Disabled)

MOH Audio Source: SampleAudioSource (1)

Source File Last Updated: 06/11/2001 17:39:22

Status: Multicast MOH Server Reset completed

[Copy] [Update] [Delete]

MOH Audio Source Information

MOH Audio Source File*   [SampleAudioSource ▼]

MOH Audio Source Name*   [SampleAudioSource]

Play continuously (repeat)   ☑

Allow Multicasting   ☑

* indicates required item

MOH Audio Source File Status

Input File Name: SampleAudioSource.wav
Error Code: 0
Error Text: Translation Complete
Low Date Time: -90446076
High Date Time: 29422270
Output File List:
    SampleAudioSource.ULAW.wav (status: OK)
    SampleAudioSource.ALAW.wav (status: OK)
    SampleAudioSource.G729.wav (status: OK)
    SampleAudioSource.WB.wav (status: OK)
MOH Audio Translation completed at 06/11/2001 17:39:22

MOH Server Reset Information

Click the button below to reset all MOH Servers. Music On Hold will not be available while the servers are resetting.

[Reset MOH Servers]

ipexpert

Go back to the server and increase Max Hops.

| Copy | Update | Delete | Reset |

Device Information

Host Server	10.2.200.21
Music On Hold Server Name*	MOH_10.2.200.21
Description	MOH_10.2.200.21
Device Pool*	HQ
Location	< None >
Maximum Half Duplex Streams*	250
Maximum Multicast Connections*	30
Fixed Audio Source Device	
Run Flag*	Yes

Multicast Audio Source Information

☑ Enable Multicast Audio Sources on this MOH Server

Base Multicast IP Address	239.1.1.1
Base Multicast Port Number	16384 (Even numbers only)
Increment Multicast on	○ Port Number ● IP Address

Selected Multicast Audio Sources

No.	Audio Source Name	Max Hops
1	SampleAudioSource	5

* indicates required item

ipexpert

Allow Multicasting for the appropriate MRGs.

Media Resource Group Configuration

Media Resource Group: HQ-MRG (used by 0 devices)

Status: Insert completed

[Copy] [Update] [Delete] [Reset Devices]

Media Resource Group Information

Media Resource Group Name*	HQ-MRG
Description	HQ-MRG

Devices for this Group

Available Media Resources
Includes Conference Bridges (CFB),
Media Termination Points (MTP),
Music On Hold Servers (MOH),
and Transcoders (XCODE)

```
CFB_10.2.200.21 (CFB)
MTP_10.2.200.21 (MTP)
```

▼ ▲

Selected Media Resources*

```
MOH_10.2.200.21 (MOH)[Multicast]
```

☑ Use Multicast for MOH Audio (requires at least one multicast MOH resource)

* indicates required item

The only remaining step is to configure multicast on the routers and switches.

Multicast Routing needs to be enabled on all routers and pim dense-mode (or sparse-dense-mode) needs to be configured on all interfaces between the MOH server and the phones.

```
P2-HQ-RTR(config)#
P2-HQ-RTR(config)#ip multicast-routing
P2-HQ-RTR(config)#int FastEthernet0/0.2
P2-HQ-RTR(config-subif)#ip pim dense-mode
```
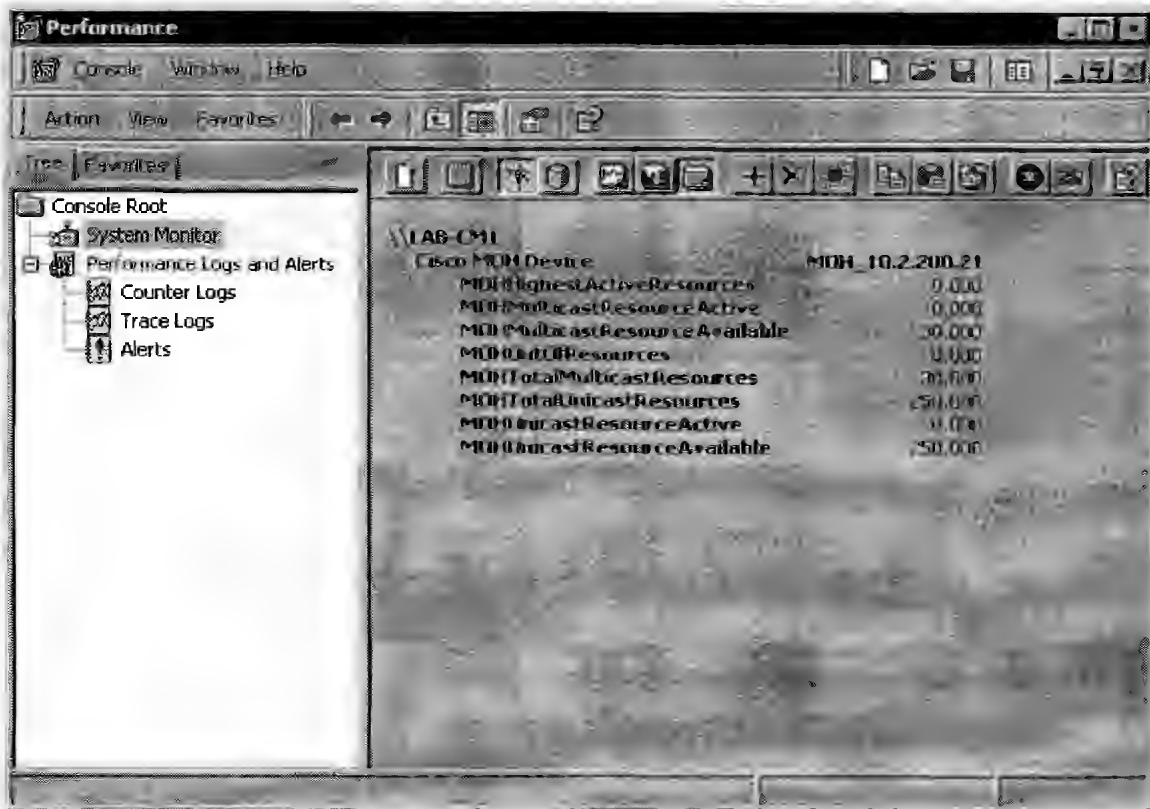
On the 6500:

```
Console> (enable) set igmp enable
IGMP feature for IP multicast enabled
```

ipexpert

On the 3550:

BR2-3550(config)#ip igmp snooping vlan 220

This is on by default.

Verify

When the Call Manager has one active multicast stream, the MOHMulticastResourcesActive counter in PerfMon will increment.

Unicast and Multicast in the Same Cisco CallManager Cluster

In some cases, administrators might want to configure a single Cisco CallManager cluster to handle both unicast and multicast MoH streams. This configuration might be necessary because the telephony network contains devices or endpoint that do not support multicast or because some portions of the network are not enabled for multicast.
Use one of the following methods to enable a cluster to support both unicast and multicast MoH audio streams:

- Deploy separate MoH servers, with one server configured as a unicast MoH server and the second server configured as a multicast MoH server.
- Configure separate media resource groups (MRGs) for the same MoH server, with one MRG configured to use multicast for audio streams and the second MRG configured to use unicast.

ipexpert

In either case, you must configure at least two MRGs and at least two media resource group lists (MRGLs). Configure one unicast MRG and one unicast MRGL for those endpoints requiring unicast MoH. Likewise, configure one multicast MRG and one multicast MRGL for those endpoints requiring multicast MoH.

When deploying separate MoH servers, configure one server without multicast enabled (unicast-only) and configure a second MoH server with multicast enabled. Assign the unicast audio resource of the unicast-only MoH server and the multicast audio resource of the multicast MoH server to the unicast and multicast MRGs, respectively. Ensure that the **Use Multicast for MoH Audio** box is checked for the multicast MRG but not for the unicast MRG. Also assign these unicast and multicast MRGs to their respective MRGLs. In this case, an MoH stream is unicast or multicast based on the server from which it is served and on whether the MRG is configured to use multicast.

When configuring separate MRGs for the same MoH server, configure the server and its audio source for multicast. Assign this same audio source to both the unicast MRG and the multicast MRG, and check the **Use Multicast for MoH Audio** box for the multicast MRG. In this case, an MoH stream is unicast or multicast based solely on whether the MRG is configured to use multicast. **Note:** Configuring the unicast MRG can be confusing because the audio resource you are adding to this MRG has [Multicast] appended to the end of the resource name even though you are adding it to the unicast MRG. This label is simply an indication that the resource is capable of being multicast, but the Use Multicast for MoH Audio box determines whether the resource will be sent as unicast or multicast.

In addition, you must configure individual devices or device pools to use the appropriate MRGL. You can place all unicast devices in a device pool or pools and configure those device pools to use the unicast MRGL. Likewise, you can place all multicast devices in a device pool or pools and configure those device pools to use the multicast MRGL. Optionally, you can configure individual devices to use the appropriate unicast or multicast MRGL. Also configure a User Hold Audio Source and Network Hold Audio Source for each device pool, individual device, or (in the case of phone devices) individual lines or directory numbers to determine the appropriate audio source to stream.

Call Manager Features

Attendant Console

Understanding Pilot Points and Hunt Groups

A pilot point, a virtual directory number that is never busy, alerts the Cisco Telephony Call Dispatcher (TCD) to receive and direct calls to hunt group members. A hunt group comprises a list of destinations that determine the call redirection order.

For Cisco TCD to function properly, make sure that the pilot point number is unique throughout the system (it cannot be a shared line appearance).

When configuring the pilot point, you must choose one of the following options from the Pilot Point Configuration window in Cisco CallManager Administration:

- First Available Hunt Group Member—Cisco TCD goes through the members in the hunt group in order until it finds the first available destination for routing the call.
- Longest Idle Hunt Group Member—This feature arranges the members of a hunt group in order from longest to shortest idle time. Cisco TCD finds the member with the longest idle time and, if available, routes the call. If not, Cisco TCD continues to search through the group. This feature evenly distributes the incoming call load among the members of the hunt group.

You can also configure pilot points to use circular hunting in which Cisco TCD maintains a record of the last hunt group member to receive a call. When a new call arrives, Cisco TCD routes the call to the next hunt group member in the hunt group.

When a call comes into a pilot point, Cisco TCD uses the hunt group list and the selected call- routing method for that pilot point to determine the call destination. During hunt group configuration, you must specify one of the following options for each hunt group member:

- Directory number (device member): If a directory number is specified, Cisco TCD only checks whether the line is available (not busy) before routing the call.
- Attendant console user plus a line number (user member): The number of lines that are configured for the attendant phone determines the number of available lines that display in the attendant console graphical user interface.

If a user and line number are specified, Cisco TCD confirms the following details before routing the call:

- That the user is logged in to the attendant console
- That the user is online
- That the line is available

ipexpert

When you specify a user and line number, the user can log in to and receive calls on any Cisco IP Phone in the cluster the attendant console controls.

Example 1: Pilot Points and Hunt Groups Working Together

Assume a pilot point named Support exists at directory number 4000. The hunt group for the Support pilot point contains the following members:

- Support Admin, Line 1 and Support Admin, Line 2 (Support Admin represents the attendant console login for the administrative assistant for Support.)
- Three directory numbers for support staff, i.e., 1024, 1025, and 1026, listed in the hunt group in that order
- A voice-mail number, 5060, which is the final member of the hunt group
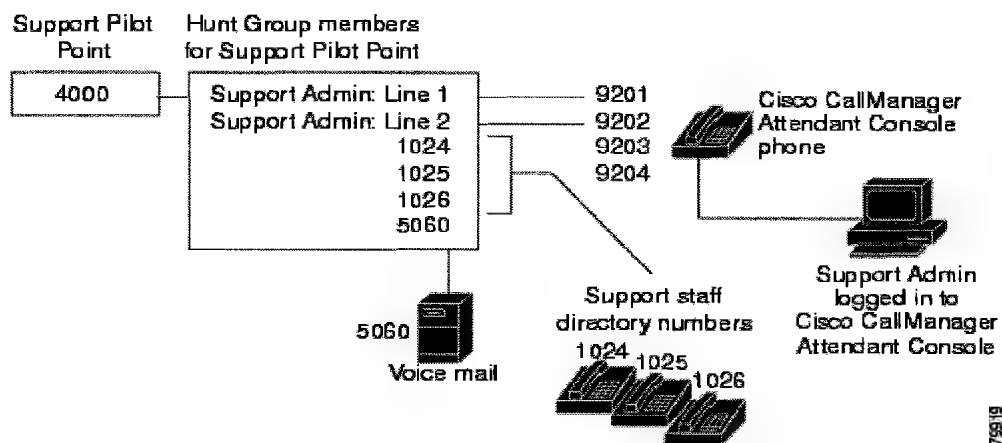
The above example describes a simple call-routing scenario where the user chose First Available Hunt Member during the configuration of the pilot point:

1. The attendant console receives a call and directs it to the Support Pilot Point, directory number 4000.
2. Because 4000 is a pilot point and First Available Hunt Group Member is chosen as the call-routing option, the Cisco Telephony Call Dispatcher (TCD) that is associated with the pilot point checks the members of the hunt group in order, beginning with Support Admin, Line 1. Cisco TCD determines that the Support Admin user is not online, directory number 1024 is busy, directory number 1025 is busy, and directory number 1026 is available.
3. Cisco TCD routes the call to the first available directory number, which is 1026. Because 1026 is available, the Cisco TCD never checks the 5060 number.

Understanding Circular Hunt Groups

Circular hunt groups enable Cisco TCD to route calls on the basis of last hunt group member to receive a call. Each hunt group maintains a record of which hunt group member receives a call. When a new call arrives, Cisco TCD dispatches the call to the next hunt group member in the hunt group. In other words, Cisco TCD routes the first

call to a hunt group to the first hunt group member, the second call to the second hunt group member, and so on. When the last hunt group member receives a call, Cisco TCD routes calls beginning with the first hunt group member again.

To set up circular hunt groups, add the pilot points of those hunt groups to the CIRCULAR_HUNTING_PILOT variable in the ACServer.properties file that is located in ..\Program Files\Cisco\CallManager Attendant Console\etc on the Cisco CallManager Attendant Console server. If you want to use circular hunting for linked hunt groups, include each of the pilot points of the linked hunt groups.

Example 2 Circular Hunting

Assume a pilot point that is named Circular exists at directory number 4000 and that the circular hunting pilot variable in the ACServer.properties file contains the Circular pilot point (CIRCULAR_HUNTING_PILOT=Circular.) The hunt group for this pilot point contains the three directory numbers; i.e., 1024, 1025, and 1026, that are listed in the hunt group in that order. Because the Always Route check box is not checked for any of the hunt group members, Cisco TCD does not determine whether the directory number is busy before routing the call.

Circular Pilot

4000

Hunt Group members
1024
1025
1026

Call routing method   91197
Circular Hunting
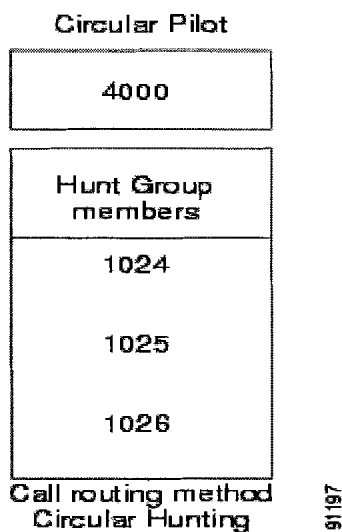
As shown in Figure 3, the following example describes a simple call-routing scenario where the user configured a Circular pilot point:

1. The attendant console receives a call and directs it to the Circular pilot point, directory number 4000.
2. Because 4000 is a pilot point and Circular Hunting is chosen as the call-routing option, the Cisco TCD routes the call to the first hunt group member, which is directory number 1024.
3. The attendant console receives another call and directs it to the Circular pilot point, directory number 4000.

4. Because Circular Hunting is chosen as the call-routing option and directory number 1024 received the last call, Cisco TCD attempts to route the call to the next hunt group member, which is directory number 1025.
5. Cisco TCD determines that directory number 1025 is busy and routes the call to the next hunt group member, directory number 1026.
6. The attendant console receives another call and directs it to the Circular pilot point, directory number 4000.
7. Because Circular Hunting is chosen as the call-routing option and directory number 1026 received the last call, Cisco TCD attempts to route the call to the next hunt group member, which is directory number 1024.

Creating Huntgroups and Pilot

From Service > Cisco CM Attendant Console > Pilot Point enter the Pilot configuration based on the table below.

Pilot Point Configuration Settings	
Field	Description
Pilot Name	Enter up to 50 alphanumeric characters, including spaces, to specify a descriptive name for the pilot point.
Device Pool	Same as HQ phones
Partition	Same as phones
Calling Search Space	The Pilot will need to see the Phone Partitions
Pilot Number (DirN)	Enter a directory number into this field to designate a directory number for this pilot point. Make sure that this number is unique throughout the system (that is, it cannot be a shared line appearance).
Route Calls To	From the drop-down list, choose the First Available Hunt Group Member option to route incoming calls to the first available member of a hunt group. From the drop-down list, choose the Longest Idle Hunt Group Member option to order members based on the time that each directory number or line remains idle. If the voice-mail number is the longest idle member of the group, Cisco TCD will route the call to voice mail without first checking the other members of the group.

ipexpert

Address http://10.2.200.21/CCMAdmin/pilotconfig.asp

System Route Plan Service Feature Device User Application Help

Cisco CallMa
For Cisco IP Telephony Sol

Cisco IPMA Configuration Wizard
Cisco CM Attendant Console
Media Resource
Service Parameters

Hunt Group
Cisco CM Attendant Console User
Cisco CM Attendant Console Server

Cisco Systems

Pilot Point Configuration

Add a New Pilot Point
Back to Find/List Pilot Points

Pilot Point: New
Pilot Number: Not Assigned

Status: Ready

Insert

Pilot Name*	ACPILOT
Device Pool*	Default
Partition	< None >
Calling Search Space	< None >
Pilot Number *	1550
Route Calls to	First Available Hunt Group Member

To create a huntgroup: From **Service > Cisco CM Attendant Console > Hunt Group** click **'Add Member'**. The Hunt Group Members list initially displays the text <<Not Configured>>.

Decide whether the hunt group member that you want to add will be a directory number (device member) or a user and line number (user member):

- If you specify a directory number, Cisco TCD always attempts to route the call to that number.
- If you specify an attendant console user and line number, Cisco TCD first checks whether the attendant console user is logged in to an attendant console and online before attempting to route the call. When you specify a user and line number, the user can log in to and receive calls on any Cisco IP Phone in the cluster that the attendant console controls.

If the hunt group member is a directory number, fill in only the Partition and Directory Number fields in the **Device Member Information** section. The optional Always Route Member check box only applies to directory numbers.

If the hunt group member is a user and line number, fill in only the User Name and Line Number fields in the **User Member Information** section.

ipexpert

Note: The User Name that you specify designates an attendant console User ID. This user name does not duplicate a User ID that is added through the Cisco CallManager User area of Cisco CallManager Administration.

As you make selections, the Hunt Group Members list box reflects the information that you choose. The Hunt Group Members list displays either the device directory number or the attendant console user name and line number.

To add more hunt group members to the pilot point, repeat the previous steps.

Hunt Group Configuration

Pilot Points

ACPILOT   1550

Pilot Point: ACPILOT
Pilot Number (DirN): 1550

Status: Ready

| Add Member | Update | Delete Member |

Hunt Group Members

```
#1: Direct call to < None >, line 0
#2: Call directory number 1002
```

▲
▼

Device Member Information

Partition	< None >
Directory Number	1002
Always Route Member	☐

User Member Information

User Name	< None >
Line Number	< None >

Configuring the ac User in the User Information Window

You must configure one user named "ac" in Cisco CallManager Administration and associate the attendant phones and the pilot points with the user. If you do not configure this user, the attendant console cannot interact with CTIManager.

ipexpert

User Configuration

Application Profiles of Attendant
- Device Association
- Cisco IPMA
- Extension Mobility
- SoftPhone

User : Attendantr Console

Status: Ready

[Update]

First Name — Attendantr

Last Name* — Console

User ID — ac

User Password* — [Change]

PIN * — [Change]

Telephone Number — [ ]

Manager User ID — [ ]

Department — [ ]

User Locale — < None >

Enable CTI Application Use — ☑

Call Park Retrieval Allowed — ☑

79748

The only fields that have relevant are UserID and password- this MUST be set to **ac / 12345** respectively. Also the **Enable CTI Application Use** and **Call Park Retrieval Allowed** check boxes must be checked. Finally, the Attendant Console Phones and the Pilot Points must be associated with the ac user.

Activating Services

Attendant Console requires that the TCD and CTI Manager Services are running- go to Call Manager Serviceability-Tools-Service Activiation and ensure that these services are running.

The attendant console application registers with and receives call dispatching services from the Cisco Telephony Call Dispatcher (TCD). The Cisco TCD, a Cisco CallManager service, provides communication among Cisco CallManager servers, attendant consoles, and the Cisco IP Phones that are used with the attendant consoles.

If you use the attendant console in a cluster environment, make sure that you install and run the Cisco TCD service on all servers that run the Cisco CallManager service. Attendant console redundancy requires this setup to work properly; however, not all Cisco TCDs are required to have a pilot point.

ipexpert

Cisco TCD handles requests for the following items:

- Call dispatching from pilot point to the appropriate hunt group destination
- Line status (unknown, available, on hook, or off hook)
- User directory information (Cisco TCD stores and periodically updates directory information for fast lookup by the attendant console.)

Cisco TCD also provides the mechanism for automated recovery for the attendant console if a Cisco CallManager fails. If a Cisco CallManager fails, the following events occur:

- Another Cisco TCD service that is running on a Cisco CallManager server within the cluster takes over servicing of the route points that are associated with the failed Cisco CallManager.
- The attendant console that is attached to the failed Cisco TCD service attempts to locate and connect to the Cisco TCD service on the Cisco CallManager server where it's associated Cisco IP Phone registered after failover.
- When the Cisco CallManager comes back up, its Cisco TCD will resume servicing its route points and attendant consoles.

Attendant Console System Files

Change AC User password

It is common that administrators wish to change the password of the ac user from '12345' to a user-defined setting.

As well as making changes for the ac user in the Directory (via the 'User' page), the ACServer.properties files located in
Program Files\Cisco\CallManager Attendant Console\etc directory on the
Cisco CallManager Attendant Console server must be edited.

Before the password can be changed in this text file, the encrypted password must be generated using the acenc.exe tool. Below is the output from the command prompt when changing the ac user password to 'cisco'.

```
C:\Program Files\Cisco\CallManagerAttendant>dir
 Volume in drive C is W2K
 Volume Serial Number is 70BE-674B

 Directory of C:\Program Files\Cisco\CallManagerAttendant

06/23/2005  05:40p    <DIR>
06/23/2005  05:40p    <DIR>          ..
05/26/2005  12:05a    <DIR>          bin
06/23/2005  05:39p    <DIR>          data
05/26/2005  12:05a    <DIR>          etc
```

```
06/23/2005  05:39p    <DIR>        lib
06/23/2005  05:39p    <DIR>        logs
06/23/2005  05:40p    <DIR>        UserLists
            0 File(s)          0 bytes
            8 Dir(s)  24,778,563,072 bytes free


C:\Program Files\Cisco\CallManagerAttendant>cd bin

C:\Program Files\Cisco\CallManagerAttendant\bin>dir
Volume in drive C is W2K
Volume Serial Number is 70BB-674B

Directory of C:\Program Files\Cisco\CallManagerAttendant\bin

05/26/2005  12:05a    <DIR>        .
05/26/2005  12:05a    <DIR>        ..
10/07/2004  06:57p           932 accollectlogs.bat
10/07/2004  06:57p        32,768 acenc.exe         // tool to generate password
10/07/2004  06:57p        40,960 ACNative.dll
10/07/2004  06:57p         1,117 builddir.bat
10/07/2004  06:57p        53,248 RegistryCtl.dll
10/07/2004  06:57p        86,016 tcdsrv.exe
            6 File(s)    215,041 bytes
            2 Dir(s)  24,778,538,496 bytes free

C:\Program Files\Cisco\CallManagerAttendant\bin>acenc cisco    // cisco is new
passwd
0c0a000a2c                                            // encrypted passwd

C:\Program Files\Cisco\CallManagerAttendant\bin>cd ../etc

C:\Program Files\Cisco\CallManagerAttendant>notepad AcServer.Properties
```

Open the ACServer.properties in notepad and paste the encrypted password into the JTAPI_PASSWORD setting. Use the '#' key to comment out the original line. This change must be made on all servers that have TCD running.

Notice at the foot of this file is the 'CIRCULAR_HUNTING_PILOT' setting- in order to enable circular hunting add the name of the PILOT of the Attendant Console.

```
#Jtapi Password
#JTAPI_PASSWORD=5e51405d76
JTAPI_PASSWORD=0c0a000a2c
```

ipexpert

```
# Specify comma seperated pilot point device names for which
# circular hunting algorithm is used. This will override
# what is configured in the admin pages.
CIRCULAR_HUNTING_PILOT=
```

Once the changes to ACServer.properties are complete the TCD service on all servers
that have TCD running should be restarted.

Note: don't forget to make the corresponding changes to the password of the ac user in
the directory as well!

To access **voice mail** from Cisco CallManager Attendant Console, you must include
information about each voice-mail system in the appropriate system file on the
Cisco CallManager Attendant Console server. To configure the system file, perform the
following procedure:

- On the Cisco CallManager Attendant Console server, open the
  VoiceMailProfilesExample.xml file that is located in the
  ..\Program Files\Cisco\CallManagerAttendant\etc directory.
- Copy the contents of this file into the VoiceMailProfiles.xml file that is located in
  the same directory. You will need to provide the following information: Voice-
  mail profile name & Voice-mail pilot number
- Save and close the VoiceMailProfiles.xml file.

Extension Mobility

Cisco CallManager Extension Mobility (an XML-based authentication feature) is
comprised of the Cisco CallManager Extension Mobility application and the
Cisco CallManager Extension Mobility service. The feature, along with other
Cisco CallManager services such as Cisco IP Manager Assistant (IPMA) and CDR
Analysis and Reporting (CAR), uses the Cisco Tomcat Service.

Cisco CallManager Extension Mobility is automatically installed with
Cisco CallManager. Then you configure Cisco CallManager Extension Mobility in
CallManager Administration. On the System Parameters page, you can define how the
feature will work in your system. For example, you can specify duration limits on phones
and enable an automatic logout time for all users.

The Cisco CallManager Extension Mobility feature works on phones within a single
Cisco CallManager cluster only.

Cisco CallManager Extension Mobility supports a maximum number of operations
(logins and logouts) of 2000 per hour.

ipexpert

Users access Cisco CallManager Extension Mobility by pressing the Services button on Cisco IP Phones and then entering login information in the form of a Cisco CallManager UserID and a Personal Identification Number (PIN). If a user has more than one device profile, a prompt displays on the phone asking the user to choose a device profile for use with Cisco CallManager Extension Mobility.

When a user logs in, the Cisco CallManager Extension Mobility application receives the XML-over-HTTP request for user authentication and verifies the information against the Cisco IP Telephony Directory.

On authentication, the phone automatically reconfigures with the individual user device profile information.

Users log out by pressing the Services button and choosing logout. If users do not log out themselves, the system will automatically log them out if you configured the Service Parameters to do so. Or, the next user of the phone can log out the previous user. After logout, Cisco CallManager sends the original user profile to the phone and restarts the phone.

Device Profiles

A device profile defines the attributes of a particular device. A device profile includes information such as the phone template (the only required field), user locale, and subscribed services.

However, the device profile is not associated with a physical phone; a device profile can be viewed as a template for a physical phone. It has all the properties of a device except those which are explicitly tied to a device, like MAC address or directory URL, for example.

When a device profile has been loaded onto a device, that device adopts the attributes of that device profile.

User Device Profile

As system administrator, you configure a user device profile for each individual user. Using the Cisco CallManager User Options web page, a user can access this profile and make changes, such as adding a service, for example.

After you assign the user device profile to a user, the phone picks up the attributes of that device profile when the user logs in.

You can add, modify or delete a user device profile in the Cisco CallManager administration pages.

ipexpert

Autogenerated Device Profile

The autogenerated device profile is a special device profile that gets generated when you configure a phone for Cisco CallManager Extension Mobility and choose "Use Current Settings" from the Phone Configuration window. The autogenerated device profile then associates with a specific phone to be the logout device profile.

Configuration

Start the Extension Mobility Service from Call Manager Serviceability.

Server: 10.2.200.21
Status: Ready

| Update | Set Default |

Service Name	Activation Stat
NT Service	
☑ Cisco CallManager	Activated
☑ Cisco Tftp	Activated
☐ Cisco Messaging Interface	Deactivated
☑ Cisco IP Voice Media Streaming App	Activated
☑ Cisco CTIManager	Activated
☑ Cisco Telephony Call Dispatcher	Activated
☑ Cisco MOH Audio Translator	Activated
☑ Cisco RIS Data Collector	Activated
☑ Cisco Database Layer Monitor	Activated
☐ Cisco CDR Insert	Deactivated
☐ Cisco Extended Functions	Deactivated
Tomcat Web Service	
☑ Cisco Extension Mobility	Deactivated
☐ Cisco IP Manager Assistant	Deactivated
☐ Cisco WebDialer	Deactivated

ipexpert

Ensure that the Cisco Tomcat service is started.
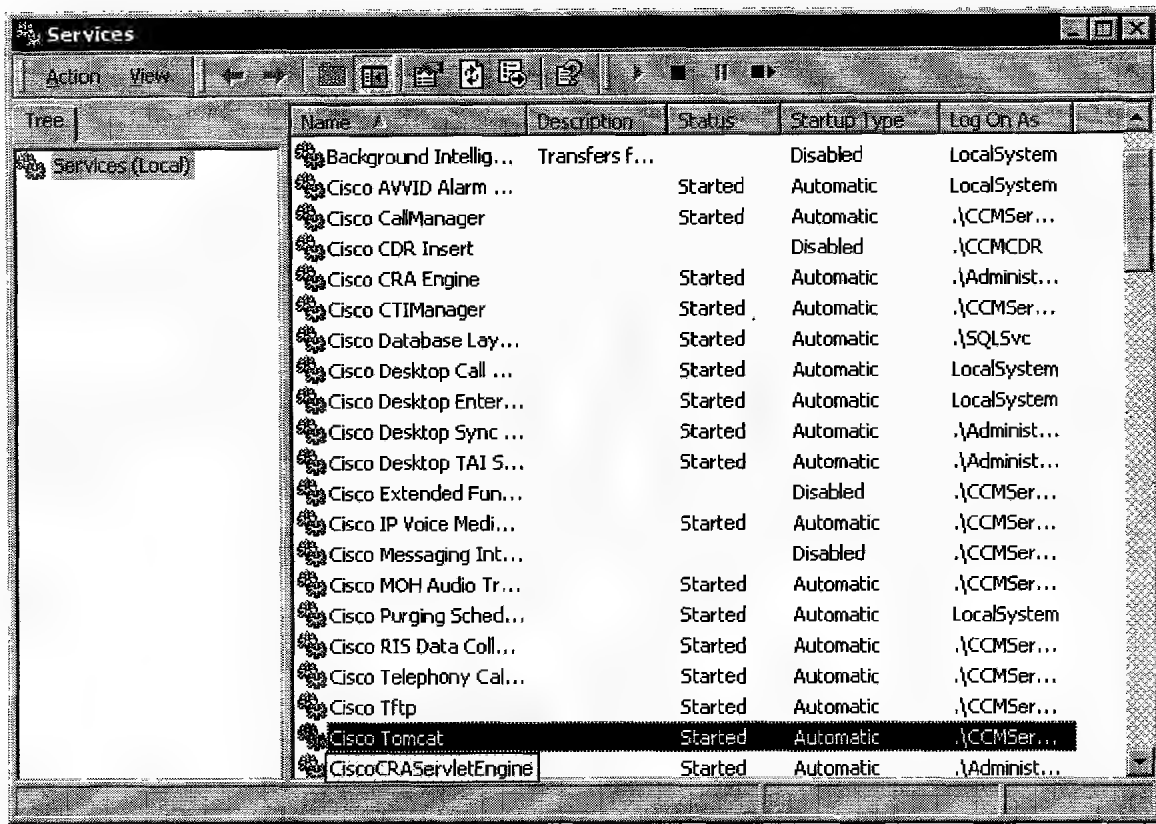
Configure Extension Mobility Service Parameters:

- Define a maximum login time.
- Define the multi-login behavior, that is, whether you allow the user to log in to more than one device at a time.
- Enable the Cisco CallManager Extension Mobility debug traces.

You must restart the Cisco Tomcat service after changing these Service Parameters.

ipexpert

Current Server : 10.2.200.21

Current Service: Cisco Extension Mobility

Status: Ready

[Update]   [Set to Default]   [Advanced]

All parameters apply to the current server except those in the Clusterwide group(s)

Clusterwide Parameters (Parameters that apply to all servers)

Parameter Name	Parameter Value	Suggested Value
Service Trace File Location*	C:\Program Files\Cisco\Trace\CULS\	C:\Program Files\Cisco\Trace\CULS\
Enforce Maximum Login Time*	False	False
Maximum Login Time (Hours:Minutes)*	8:00	8:00
Multiple Login Behavior*	Multiple Logins Not Allowed	Multiple Logins Not Allowed
Debug Traces On*	False	False
Alphanumeric UserId*	True	True
Remember last user logged in*	False	False

Create the Cisco CallManager Extension Mobility service

Cisco IP Phone Services Configuration

Back t

IP Phone Service: New

Status: Ready

[Insert]

Service Information

Service Name*   Service Description

EM

Service URL*

http://10.2.200.21:emapp/EMAppServlet?device=#DEVICENAME#

Note:
If you are using a language other than English for Service Name and Description text, mak (shown below) is selected. Text displays incorrectly if the wrong characterset is selected. (E in all character sets.)

Character Set   Western European (Latin 1)

ipexpert

Create the Device Profile from **Device > Device Settings > Device Profile and** Also
subscribe the Device Profile to the Extension Mobility Service.

User Device Profile Configuration

Directory Numbers
Base Phone
Line 1 - 1111
Line 2 - Add new DN

User Device Profile: DPUSER1
Status: Ready
Copy   Update   Delete

User Device Profile Information

Device Type	Cisco 7960
User Device Profile Name*	DPUSER1
Description	
User Hold Audio Source	< None >
User Locale	< None >

Phone Button Template Information

Phone Button Template*	Standard 7960 (View button list)
Expansion Module 1	< None > (View button list)
Expansion Module 2	< None > (View button list)

Softkey Template Information

Softkey Template	< None >

Logged Out (Default) Profile Information

Login User ID**	(Select Login User ID)

* indicates required item
** this optional setting is applied when this profile is used as the default (log out) profile

Associate a User Device Profile to a User

Extension Mobility

Find profiles where:

[User Device Profile ▼]   [Profile Name ▼]   [begins with ▼]   [_____]

Select Profiles

Filter Active

1 available device profile(s) listed at last search
0 device profile(s) controlled at last search
0 device profile(s) selected currently

☐ Enable Authentication Proxy Rights

Available Profiles

☑ Check All on Page   ☑ Check All in Search   ○ No Default Profile
                                                 ○ No Primary Extension

Type	Profile Name	Description	Default Profile	Primary Ext	Extension
☑ 📞7960	DPUSER1		◉	○	1111

Update Selected

Configure and subscribe Cisco IP Phones to the feature.

Idle Timer (seconds)   [_____]

Extension Mobility (Device Profile) Information

☑ Enable Extension Mobility Feature

Log Out Profile   [< Use Current Device Settings > ▼]

Log In User ID   < None >

Log In Time   < None >

Log Out Time   < None >

Product Specific Configuration   [i]

Disable Speakerphone   ☐

Cisco CallManager Administration
For Cisco IP Telephony Solutions   CISCO SYSTEMS

[Cisco CallManager 3.3 Administration]

Phone Configuration

Directory Numbers   **Phone: SEP00059A3C7800 (Auto 1000)**
Registration: Unknown

ipexpert

High Availability

SRST

SRST is a feature in IOS software that allows a router at a remote branch to assume basic call processing responsibilities in the event that the IP Phones at a remote site are unable to contact the central Call Manager.

In normal operation, when the WAN is operational, the Branch IP Phones establish a Skinny registration to Call Manager.

When the IP Phone loses connectivity to the Call Manager (the phones have a periodic heartbeat to all Call Managers configured in their Call Manager Group) it tries the SRST router as its last resort.

SRST only provides basic survivability for remote sites in the event of a WAN outage. When the IP phone is in fall back mode the prompt on the phone displays the message "CM Fallback Service Operating" to inform users fallback mode is active.

SRST has some restrictions:

- ATA/VG248 cannot register with SRST gateway
- Extension Mobility does not work in SRST mode
- SRST does not have the concept of partitions and Calling Search Spaces. Class of Restriction (CoR) can be configured but it does not have the same flexibility.
- Each Line only supports one call (normally in Call Manager each Line supports two calls). Transfering and conferencing are still supported in SRST.
- All transfers are blind transfers.
- MWI may be out of sync
- All forwarding in SRST is lost
- All call routing decisions are made on the SRST gateway through dial-peers.
- MGCP endpoints do not function in SRST mode however MGCP endpoints can be configured to become H323 endpoints when SRST mode is operating due to a WAN failure.

SRST configuration

The **ip source-address** parameter should match the IP Address of the interface your IP Phones use as their default gateway or the IP Address configured in Call Manager as the SRST Reference.

The max-ephones and max-dn parameters specifies the maximum number of IP Phones/Lines allowed to register with the SRST router- they are configured based on the number of SRST client licenses that has been purchased.

```
call-manager-fallback
 ip source-address 10.2.201.1 port 2000
 max-ephones 24
 max-dn 48
```

SRST needs to be enabled on a per-Device Pool basis.

Device Pool: New (Copy of HQ)
Status: Ready
[Insert]

Device Pool Settings

Device Pool Name*	BR1
Cisco CallManager Group*	Default
Date/Time Group*	CMLocal
Region*	BR1
Softkey Template*	Standard User
SRST Reference*	Disable
Calling Search Space for Auto-registration	— Not Selected — Disable
Media Resource Group List	Use Default Gateway
Network Hold MOH Audio Source	< None >
User Hold MOH Audio Source	< None >
Network Locale	< None >
User Locale	< None >

* indicates required item

If the Source Address of the SRST router is NOT the default gateway, then an SRST Reference needs to be created and assigned to the Device Pool.

System   Route Plan   Service   Feature   Device   User   Application   Help

Server
Cisco CallManager
Cisco CallManager Group
Date/Time Group
Device Defaults
Region
Device Pool
AAR Group
Enterprise Parameters
Location
SRST

ence Configuration

Add New SRST Reference
Back to Find/List SRST References

Insert   Cancel

SRST Reference Name*   BR1

IP Address*   10.10.10.10

Port*   2000

Once SRST has been assigned to the Device Pool, reset the Devices and check that the SRST router appears in the list of Call Managers in the Phone's network configuration settings..

To verify phones are registered to the SRST router use the **sh ephone registered** command.

MGCP Fallback

As well as IP Phones, MGCP Gateways can survive in the event of the WAN failing.

Remember, with MGCP Gateways the D-Channel is backhauled to the Call Manager- in the event of the Call Manager becoming unavailable the entire T1 PRI (23 Bearer Channels as well as the D-Channel) is lost.

In the event of a WAN outage, there is a method to allow the MGCP gateway to transition into H323 gateway- this is known as MGCP Fallback.

ipexpert
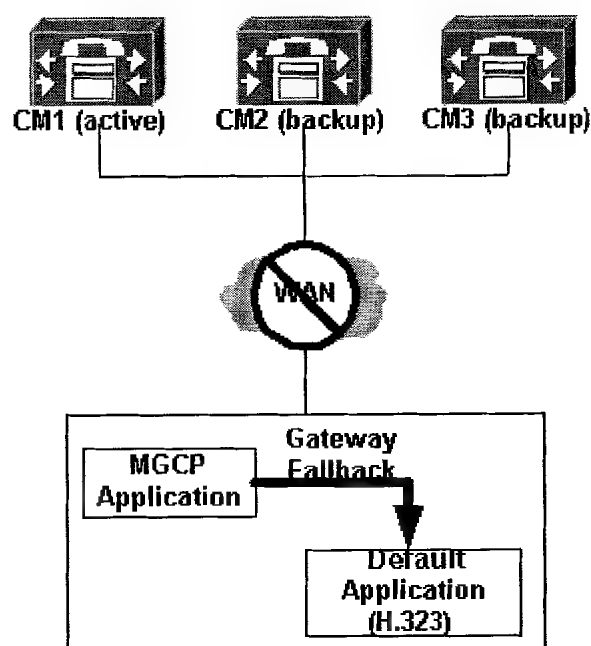
For the router to fallback to the default application (H323), configure this command in global configuration mode:

```
P2-BRI-RTR(config)#call application alternate default
```

If the MGCP application is not available, the default application takes over.

Enable Call Manager Fallback.

```
P2-BRI-RTR(config)#ccm-manager fallback-mgcp
```

Finally configure H323 Dial-Peers for Call routing. (see H323 dial-peer section in CME)

The **show ccm-manager fallback-mgcp** command output shown here is taken before MGCP fallback happens.

```
mgcp-gateway# show ccm-manager fallback-mgcp
Current active Call Manager:    192.168.1.2
MGCP Fallback mode:         Enabled/OFF
Last MGCP Fallback start time:  None
Last MGCP Fallback end time:    None
```

When the connection to the Cisco CallManager is lost, and MGCP Fallback kicks in, the output is as follows:

```
mgcp-gateway# show ccm-manager fallback-mgcp
Current active Call Manager:    None
MGCP Fallback mode:         Enabled/ON
```

ipexpert

```
Last MGCP Fallback start time:  05:58:48 UTC Oct 6 2004
Last MGCP Fallback end time:    05:56:30 UTC Oct 6 2004
```

This console message helps in verifying the MGCP fallback operation.

```
Sep 23 16:35:34.707: %CALL_CONTROL-6-APP_NOT_FOUND: Application
mgcpapp in dial-peer 1 not found.
Handing callid 98 to the alternate app default
```

Class of Restriction (COR)

COR is used to implement Class of Restriction on phones registered to an IOS gateway (either CCME or SRST).

Before considering COR it is worth noting that a phone registered to CCME or SRST (ephone) has an associated pots voice port and an associated dial-peer (enter *"show dial-peer voice summary"* to view the dial-peers/pots ports).

A call place to the PSTN from an ephone has two legs to the call like any other call from an IOS gateway- an incoming and outgoing leg.

The COR feature provides the ability to deny certain call attempts based on the incoming and outgoing CORs provisioned on the dial–peers. COR is used to specify which incoming dial–peer can use which outgoing dial–peer to make a call. Each dial–peer can be provisioned with an incoming and an outgoing COR list. If the COR applied on an *incoming* dial–peer (for incoming calls) is a super set or equal to the COR applied to the *outgoing* dial–peer (for outgoing calls), the call goes through. *Incoming* and *outgoing* are terms used with respect to the "voice ports".

Coniguration is done using the steps below- we shall use the same terminology as Call Manager uses to implement Calling Restrictiion, namely Calling Search Spaces (CSS) and Partitions.

First configure **dial–peer cor custom** and assign a meaningful name that specifies the way CORs apply to dial–peers- this is in effect defining the list of partitions.

```
Dial-peer cor custom
name pt-911
name pt-local
name pt-ld
name pt-international
```

Create the actual lists of the restrictions that apply to the dial–peer- this is the equivalent of CSS the difference between COR and Call Manager CSS/Partitions is that we apply

ipexpert

CSS to the incoming AND outgoing leg of the call whereas in CCM CSS is applied to the incoming call leg only.

```
Dial-peer cor list css-911
Member pt-911

Dial-peer cor list css-local
Member pt-local

Dial-peer cor list css-ld
Member pt-ld

Dial-peer cor list css-international
Member pt-international

Dial-peer cor list css-restricted-phones
Member pt-911
Member pt-local

Dial-peer cor list css-unrestricted-phones
Member pt-911
Member pt-local
Member pt-ld
Member pt-international
```

Apply COR list (or CSS) to the outgoing dial-peer.

```
Dial-peer voice 911 pots
Destination-pattern 911
Port 0/0/0:0
Corlist outgoing css-911
Port 1/1/0

Dial-peer voice 7 pots
Destination-pattern 9[2-9]......
Port 0/0/0:0
Corlist outgoing css-local

Dial-peer voice 11 pots
Destination-pattern 91[2-9]..[2-9].....
Port 0/0/0:0
Corlist outgoing css-ld

Dial-peer voice 110 pots
Destination-pattern 011T
Port 0/0/0:0
```

```
Corlist outgoing css-international
```

Note: If no outgoing COR list is applied to an outgoing dial-peer, that particular dial-peer has no restrictions and is invisible by all incoming dial-peers and hence all phones registered to CCME and SRST.

The next step is to apply COR to the incoming dial-peer.

In SRST this is done inside *"call-manager-fallback"*.

```
call-manager-fallback
...
cor incoming restricted-phones 1 2001
cor incoming unrestricted-phones 2 2003
...
```

In CCME this is done on the *"ephone-dn"*.

```
Ephone-dn 1
Number 3001
Cor incoming restricted-phones
Ephone-dn 2
Number 3002
Cor incoming unrestricted-phones
```

If there is no incoming COR list applied for a particular ephone then that phone has visibility to all outgoing dial-peers since the incoming dial–peer, by default,has the highest COR priority when no COR is applied. Therefore, if you apply no COR for an incoming call leg to a dial–peer, then this dial–peer can make calls out of any other dial–peer, irrespective of the COR configuration on the outgoing dial–peer.

Automated alternate routing (AAR)

Automated alternate routing (AAR) provides a mechanism to reroute calls through the PSTN or other network by using an alternate number. Cisco CallManager automatically reroutes calls through the PSTN or other networks when Cisco CallManager blocks a call due to insufficient location bandwidth. With automated alternate routing, the caller does not need to hang up and redial the called party.

When a call is made from the device of one location to the device of another location, location bandwidth gets deducted from the maximum available bandwidth that is available for the call at either location. If not enough location bandwidth for the call exists at either location, instead of blocking the call, Cisco CallManager uses the table of AAR groups and the external number of the terminating directory number to supply the alternate number that is used to reroute the call through the PSTN or other network. The

Cisco IP Phone displays the message "Network congestion, rerouting" by default. Cisco CallManager automatically attempts to reroute the call by using the alternate number. If the reroute is successful, the caller connects to the called party.

AAR supports the following call scenarios for insufficient bandwidth:

- Call originates from a line or directory number (DN) of an IP phone within one location and terminates to a line or DN of another IP phone within another location. This scenario includes calls that terminate at the shared line with terminating IP phone devices that are resident in multiple locations and calls that terminate at the Cisco voice-mail port.
- Incoming call through a gateway device within one location terminates to a line or DN of an IP phone within another location. This scenario includes calls that terminate at the shared line with terminating IP phone devices that are resident in multiple locations and calls that terminate at the Cisco voice-mail port.

Cisco CallManager automatically attempts to reroute calls, due to insufficient bandwidth, through the PSTN or other network only when the AAREnable enterprise parameter (moved to CCM Service Parameters in CCM3.3(4) is set to true. Cisco CallManager uses the device-based AAR calling search space, which is assigned to Cisco IP Phone station devices and gateway devices, when it attempts to route the call to the gateway device that connects to the PSTN or other network. Cisco CallManager uses the external phone number mask and the directory number of the line or DN and the Cisco voice-mail port to derive the alternate number that is used to reroute the call.

The AAR group appears as an entry in the line/DN table, in the Cisco voice-mail port table, and in the gateway device table. AAR group comprises a character string with a default value of the null string. The AAR group represents the dialing area where the line/DN, the Cisco voice-mail port, and the gateway are located.

Cisco CallManager uses the AAR group value to index into the AAR dial prefix matrix table, which contains the prefix digits for transforming the alternate number.

**Automated Alternate Routing Example**

In the following scenario, line/DN 1001 in the HQ site AAR group calls line 2001 in the Branch 1 AAR group. If not enough location bandwidth exists, the call attempts to reroute through the PSTN or other network. To route the call from AAR group HQ to AAR group BR1, Cisco CallManager needs to know the access digit(s) to dial out to the PSTN and the full PSTN digit string since sending the digits "2001" will not be recognized by the PSTN- this is retrieved from AAR Prefix Digit and External Number Mask respectively.

ipexpert

Location = HQ
DN=1001
AAR Group = HQ
Ext Number Mask
212221XXXX

WAN

Location = BR1
DN=2001
AAR Group = BR1
Ext Number Mask
– 617521XXXX

PSTN

DN '1001' dials DN '2001' → Locations CAC causes CCM to return 'Network Congestion' → CCM checks whether AAR is enabled. → The External Number Mask of the Called Party is prepended to the dialed digits

↓

Call is routed out of PSTN ← A Route Pattern is matched- the partion must be visible by the AAR CSS of the Calling Device ← Digit String has been transformed from '2001' to 916175212001 ← The Dial Prefix from AAR Group is added to the Called Number- usually '91'

ipexpert

Unity

Call Manager Integration

Run the voicemail port wizard from the Call Manager Administration web page click on
Feature-Voice Mail-Cisco Voice Mail Port Wizard.
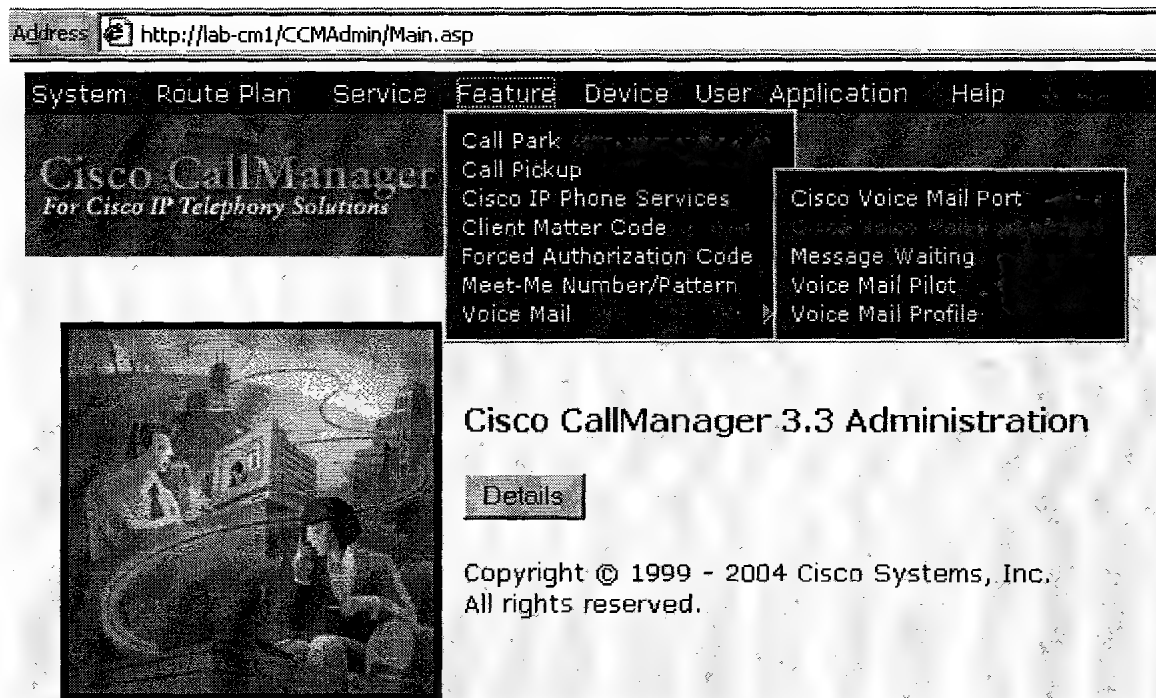
Leave the name of the port-prefix as the default.

Cisco Voice Mail Port Wizard

Cisco Voice Mail Server

There are no Cisco Voice Mail Servers configured in Cisco CallManager. To create the first
Cisco Voice Mail Server, enter a name below and click Next.

Add ports to a new Cisco Voice Mail Server using this name: CiscoUM1

Back   Next   Cancel

ipexpert

Select the number of ports you wish to configure- this is based on how many are licensed.

Cisco Voice Mail Port Wizard

Cisco Voice Mail Ports

CiscoUM1 currently has 0 ports configured.

How many ports do you want to add? [4]

Back   Next   Cancel

Configure Device Pool, Calling Search Space and Location settings for voicemail ports. If the Unity Server is physically located in the HQ site, these settings should be the same as the HQ phones.

Cisco Voice Mail Port Wizard

Cisco Voice Mail Device Information

Enter the device information for ports 1 through 4 of CiscoUM1. A Device Pool selection is required. The Wizard applies these settings to all new ports.

Device Information

Description	Voicemail
Device Pool*	Default
Calling Search Space	< None >
AAR Calling Search Space	< None >
Location	< None >

* indicates required item

Back   Next   Cancel

On the next page enter the DN of the Pilot Number and configure Partition and CSS- use the same as the phones you have configured on your system.

ipexpert

Cisco Voice Mail Port Wizard

Cisco Voice Mail Pilot Number

Enter the directory number settings for the new Cisco Voice Mail Server (CiscoUM1). The Pilot number is the number people call to access the Cisco Voice Mail Server. A pilot number is required. If a Partition is selected, you must select a Calling Search Space that includes the selected Partition.

Pilot Number*	1600	(each new port receives the next available directory number)
Partition	< None >	
Calling Search Space	< None >	
Display	Voicemail	
AAR Group	< None >	
External Number Mask		

* indicates required item

[Back] [Next] [Cancel]

Note- if AAR is required for Unity then the External Number Mask, AAR Groups and AAR Calling Search Space will need to be configured on the two previous pages.

On the next page you can optionally configure an operator- Call Manager will attempt to transfer the call to this extension if the voicemail server is busy.

Cisco Voice Mail Port Wizard

Cisco Voice Mail Operator Number

The Operator number is the number to which the last port is forwarded. A caller is directed to this number if all ports on the Cisco Voice Mail Server are busy. Use of the Operator number is optional. Supplying an attendant's number here gives the caller another chance to reach the party they were calling, instead of getting a busy signal.

Operator Number (optional) [ ]

[Back] [Next] [Cancel]

ipexpert

Ready to Add Cisco Voice Mail Ports

The information shown below will be applied to the Cisco Voice Mail Ports being created. If this information
is correct, click Finish to add the new ports. If the information shown is not correct, click the Back button
to edit the information, or Cancel to quit without adding any ports.

Cisco Voice Mail Device Information (apply to all ports)

Number of Ports to Add	4 (adding ports 1 – 4)
Cisco Voice Mail Server Name	CiscoUM1
Description	Voicemail
Device Pool	Default
Calling Search Space	< None >
AAR Calling Search Space	< None >
Location	< None >

Directory Number Information

Pilot Directory Number	1600
New Directory Numbers	1600 – 1603
Operator Directory Number	
Partition	< None >
Calling Search Space	< None >
Display	Voicemail

Cisco Voice Mail Port Wizard - Microsoft Internet Explorer

Update in Progress

Please wait while the Cisco Voice Mail Ports are added. During this
time, please do not use your browser. The page will update
automatically when processing is complete.

[Back] [Finish] [Cancel]
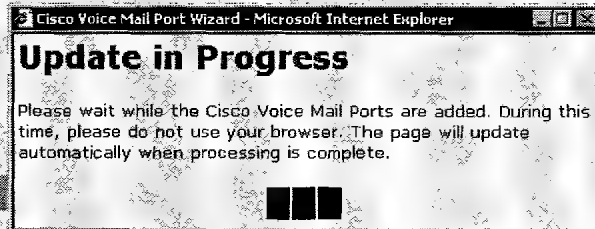
When you have completed these steps, check the information before clicking on the
Finish tab. The wizard takes a few seconds to configure the voicemail ports.

From Feature-Voice Mail- Voice Mail Pilot add the Voicemail Pilot.

Voice Mail Pilot Configuration

Back to Find/List Voice Mail

Voice Mail Pilot Number : New

Status: Ready

[Insert]

Voice Mail Pilot Number	1600
Description	
Calling Search Space	< None >

☑ Make this the default Voice Mail Pilot

* indicates required item

Microsoft Internet Explorer

⚠ By enabling this Voice Mail Pilot to be the default pilot, the
previously assigned default pilot will no longer be the default.

[OK]
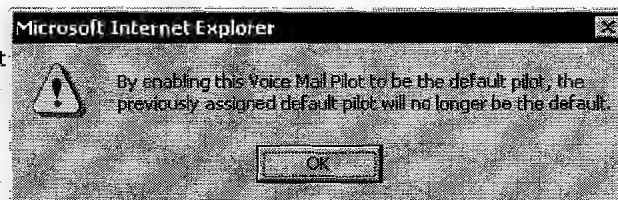
Configure the Pilot DN and ensure that the CSS can see the phone partitions.

From Feature-Voice Mail-Voice Mail Profile add the profile- by making this the default profile each LINE in the system does NOT need to have a profile specifically configured to use voicemail.

Voice Mail Profile Configuration

Voice Mail Profile: New
Status: Ready

Insert

Voice Mail Profile Name*   unity

Description   unity

Voice Mail Pilot **   < Use Default >

Voice Mail Box Mask

☑ Make this the default Voice Mail Profile for the system

* indicates required item
** The Voice Mail Pilot is com [...] g Search Space Name
(<Voice Mail Pilot Number>/

Microsoft Internet Explorer

⚠ By enabling this Voice Mail Profile to be the default profile, the previously assigned default profile will no longer be the default.

OK
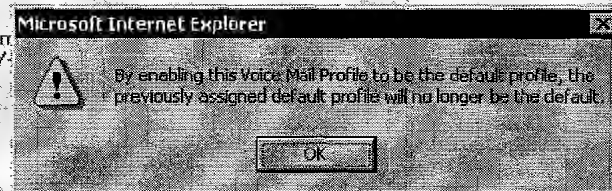
Configure Message Waiting Indicator from **Feature-Voice Mail-Message Waiting.** Enter the DN that will be used to turn on and off the MWI light.

Message Waiting Configuration

Message Waiting Number : New
Status: Ready

Insert

Message Waiting Number*   1999

Description

Message Waiting Indicator   ◉ On ○ Off

Partition   < None >

Calling Search Space   < None >

* indicates required item

ipexpert

Message Waiting Configuration

Message Waiting Number : New (Copy of 1999)

Status: Ready

Insert

Message Waiting Number*	1998
Description	
Message Waiting Indicator	○ On ⦿ Off
Partition	< None >
Calling Search Space	< None >

* indicates required item

For all LINES in the system, you will have to configure Call Forward No Answer and Call Forward Busy to VoiceMail. Notice that Voice Mail Profile is not required since we configured the Profile we created as the default.

ipexpert

Update **Delete**   **Reset Devices**

Directory Number

Directory Number*   1000

Partition   < None >

Directory Number Settings

Voice Mail Profile   < None >   (Choose <None> to use default)

Calling Search Space   < None >

AAR Group   < None >

User Hold Audio Source   < None >

Network Hold Audio Source < None >

Call Waiting   Default

Auto Answer   Auto Answer Off

Call Forward and Pickup Settings

	Voice Mail	Destination	Calling Search Space
Forward All	☐		< None >
Forward Busy	☑		< None >
Forward No Answer	☑		< None >

Call Pickup Group < None >

At this stage Call Manager configuration for voicemail is now complete. The Unity Server now needs to be configured to communicate with Call Manager.

Launch UTIM via the Desktop or from the Windows Start menu, click Programs > Cisco Unity > Tools Depot. UTIM appears.

Launch The Telephone Integration Manager from Switch Integration.

ipexpert
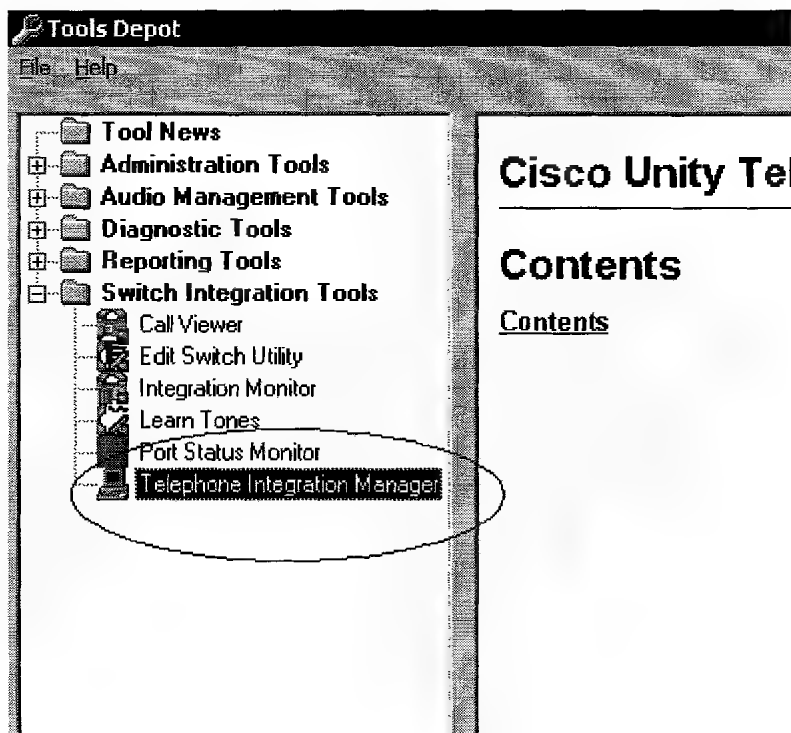
Delete any existing Integrations and if prompted to reboot, you must reboot the Unity server. Otherwise click 'Create Integration'.

ipexpert
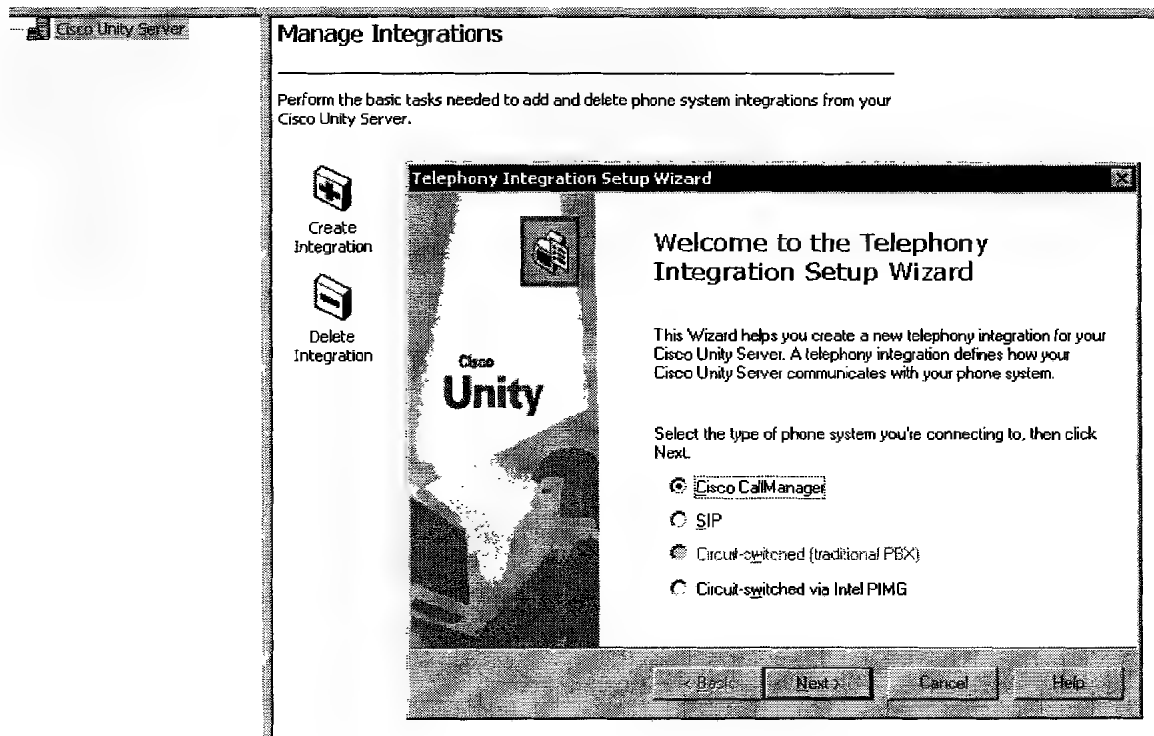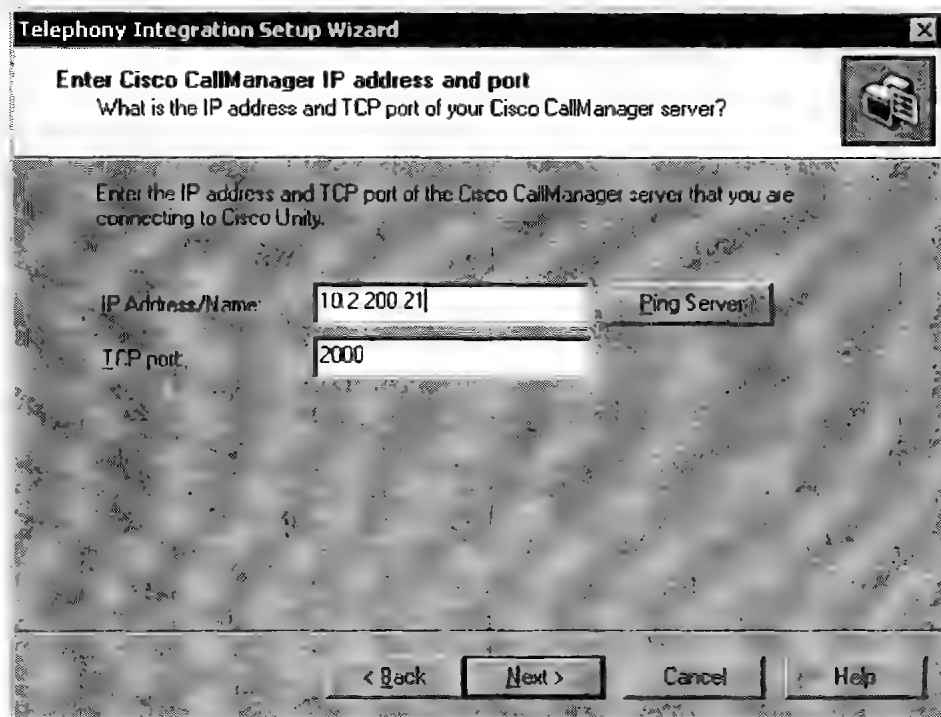
Choose the Call Manager option and the Integration a descriptive name such as Call
Manager. On the Enter Cisco CallManager IP Address and Port page, enter the following
settings, then click Next.

Table 11 Settings for the Enter Cisco CallManager IP Address and Port Page	
Field	Setting
IP Address/Name	The IP Address of the Cisco CallManager server that you are connecting to Cisco Unity; if you are connecting to a Cisco CallManager cluster, we recommend entering the IP address of the subscriber Call Manager.
TCP Port	The TCP port of the Cisco CallManager server that you are connecting to Cisco Unity- leave as default.

You can click Ping Server to confirm that the IP address is correct.

On the Enter Secondary Server Settings page, in the IP Address/Name field, enter the IP
address and port of the publisher Cisco CallManager server. If there is only one
Cisco CallManager server in the cluster, leave this page blank.

ipexpert
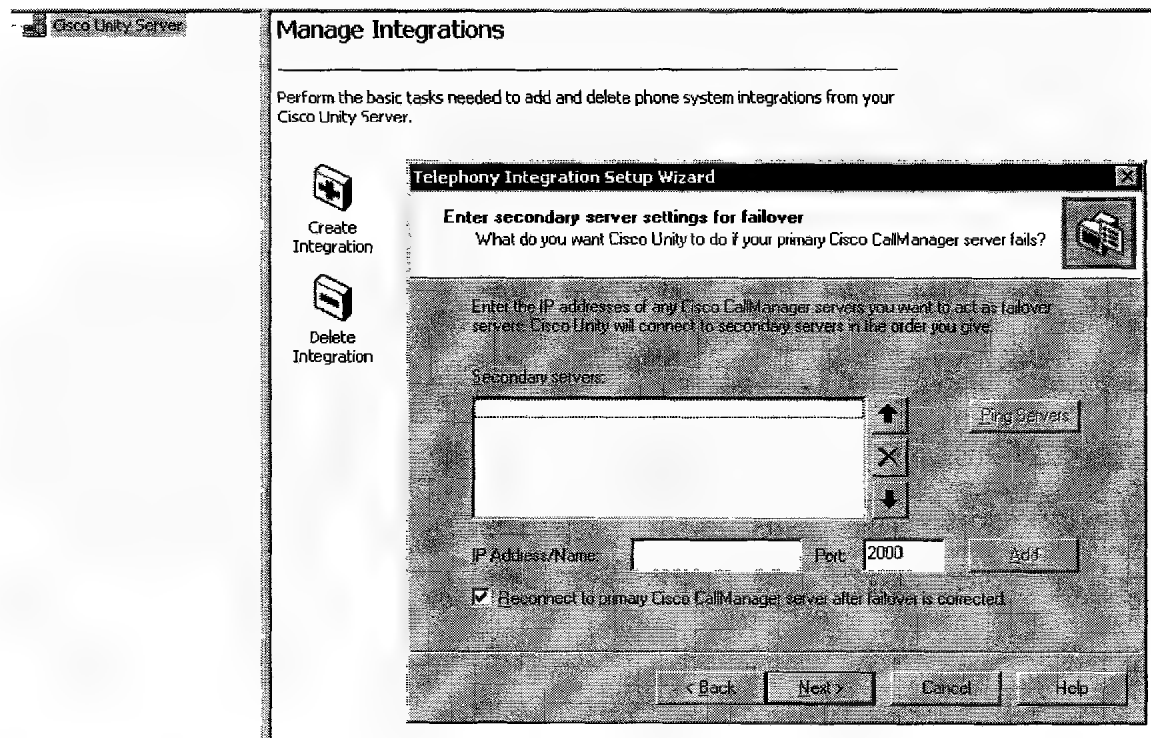
You can click Ping Servers to confirm that the IP addresses are correct.

If you want Cisco Unity to automatically reconnect to the primary Cisco CallManager server after failover has been corrected, check the Reconnect to Primary Cisco CallManager Server check box.

On the Enter Cisco CallManager MWI Extensions page, enter the following settings, then click Next.
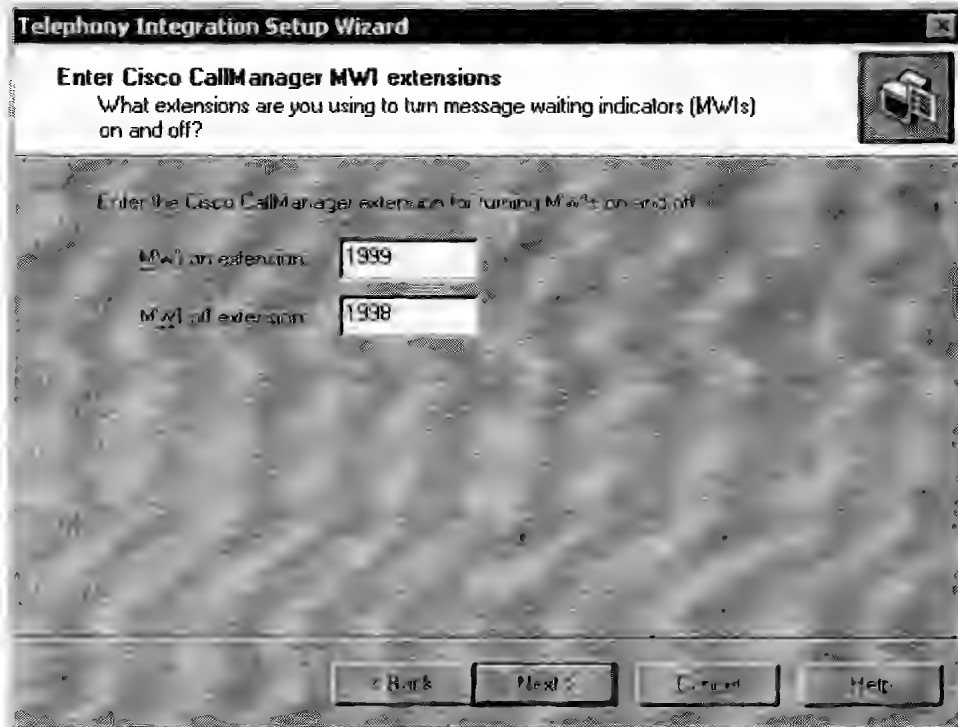
Table 12 Settings for the Enter CallManager MWI Extensions Page	
Field	Setting
MWI On Extension	The extension you specified in Cisco CallManager Administration for turning MWIs on
MWI Off Extension	The extension you specified in Cisco CallManager Administration for turning MWIs off

ipexpert

Manage Integrations

Perform the basic tasks needed to add and delete phone system integrations from your
Cisco Unity Server.

On the Set Number of Voice Messaging Ports page, enter the following settings, then
click Next.

Table 13 Settings for the Set Number of Voice Messaging Ports Page	
Field	Setting
Number of Ports	The number of voice messaging ports connecting Cisco Unity to the Cisco CallManager server; if Cisco Unity is connected to a single Cisco CallManager server, this number cannot be more than the number of ports set up on Cisco CallManager; if Cisco Unity is connected to multiple clusters of Cisco CallManager, this number cannot be more than the number of ports set up on the Cisco CallManager cluster, and the total number of ports on all clusters connected to Cisco Unity cannot be more than the number of ports enabled by the Cisco Unity license.
CallManager Device Name Prefix	The prefix Cisco CallManager adds to the device name for voice messaging ports; this prefix must match the prefix used by Cisco CallManager.

ipexpert

Manage Integrations

Perform the basic tasks needed to add and delete phone system integrations from your Cisco Unity Server.
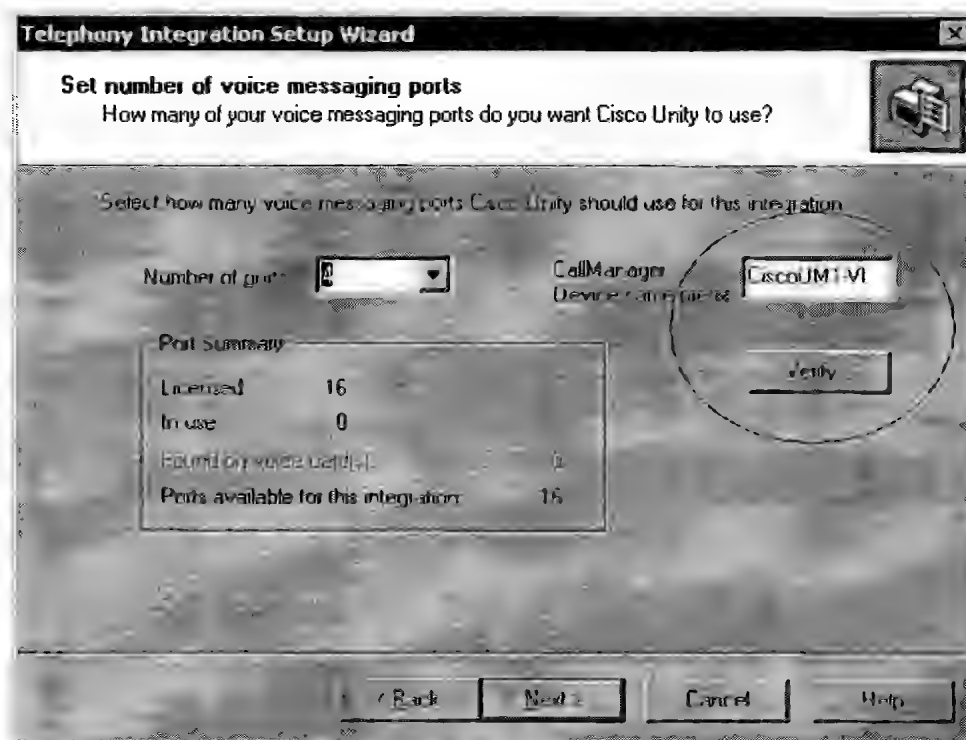
You can click Verify to confirm that the CallManager device name prefix is correct- the name is resolved via NETBIOS.

The next page prompt you to enter a Trunk Access Code- you do not need to configure anything here.

On the Completing page, verify the settings you entered, then click Finish.

At the prompt to restart the Cisco Unity services, click Yes. The Cisco Unity services restart.

Alternatively, you can restart the Cisco Unity services in UTIM on the Tools menu by clicking *Restart Cisco Unity*. Do not use the taskbar icon to restart the Cisco Unity for UTIM changes because the taskbar icon does not restart all of the Cisco Unity services.

When the Unity services have restarted (or Unity has been rebooted), you must configure the voicemail ports from the Telephone Integration page from UTIM.

ipexpert
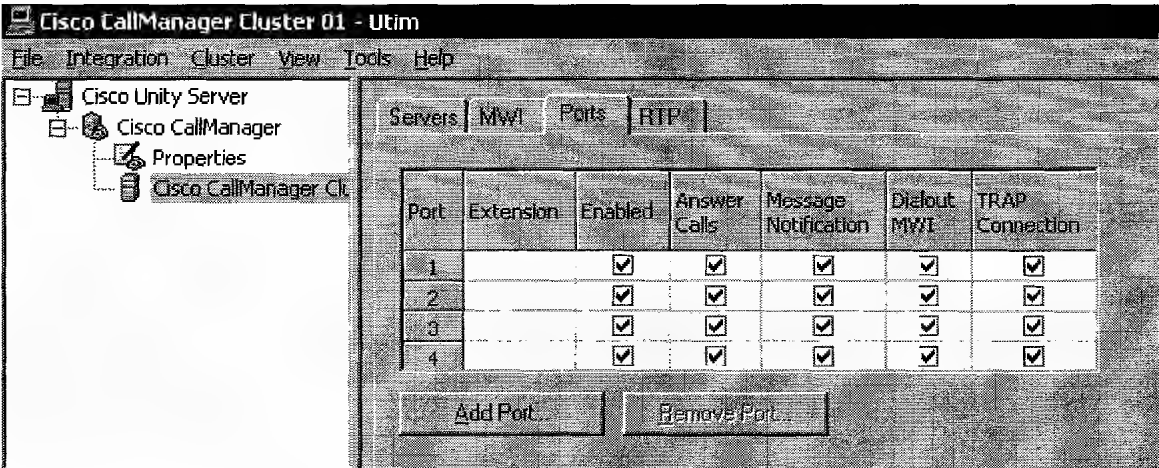
The settings for the voice messaging ports are explained in Table 14.

If the Call Manager has a dedicated port for voicemail then the corresponding Unity port should be dedicated to MWI- this port should have Dialout MWI and Message Notification enabled.
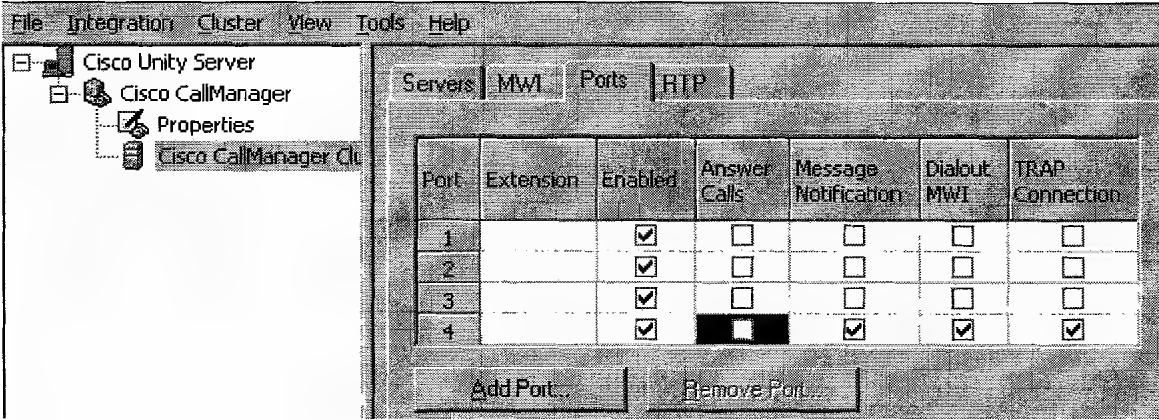
In programming Cisco CallManager, do not send calls to voice messaging ports in Cisco Unity that cannot answer calls (voice messaging ports that are not set to Answer Calls). For example, if a voice messaging port is set only to Dialout MWI, do not send calls to it.

Table 14 Settings for the Voice Messaging Ports	
Field	Considerations
Extension	Enter the extension for the port as assigned on the phone system.
Enabled	Check this check box to enable the port. The port is enabled during normal operation. Uncheck this check box to disable the port. When the port is disabled, calls to the port get a ringing tone but are not

ipexpert

	answered. Typically, the port is disabled only by the installer during testing.
Answer Calls	Check this check box to designate the port for answering calls. These calls can be incoming calls from unidentified callers or from subscribers. As a general guideline, set Answer Calls on approximately 75 percent of the ports.
Message Notification	Check this check box to designate the port for notifying subscribers of messages. Assign Message Notification to the least busy ports, which typically are those with the highest port numbers for the phone system. As a general guideline, set Message Notification, Dialout MWI, and TRAP Connection on approximately 25 percent of the ports.
Dialout MWI (not used by serial or SMDI integrations)	Check this check box to designate the port for turning MWIs on and off. Assign Dialout MWI to the least busy ports, which typically are those with the highest port numbers for the phone system. As a general guideline, set Message Notification, Dialout MWI, and TRAP Connection on approximately 25 percent of the ports.
AMIS Delivery (available with the AMIS licensed feature only)	Check this check box to designate the port for making outbound AMIS calls to deliver voice messages from Cisco Unity subscribers to users on another voice messaging system. Cisco Unity supports the Audio Messaging Interchange Specification (AMIS) protocol, which provides an analog mechanism for transferring voice messages between different voice messaging systems. This setting affects outbound AMIS calls only. All ports are used for incoming AMIS calls. Because the transmission of outgoing AMIS messages may tie up voice ports for long periods of time, you may want to adjust the schedule on the Network > AMIS > Schedule page so that outgoing AMIS calls are placed during closed hours or at times when Cisco Unity is not processing many calls.
TRAP Connection	Check this check box so that subscribers can use the phone as a recording and playback device in Cisco Unity web applications and e-mail clients. Assign TRAP Connection to the least busy ports, which typically are those with the highest port numbers for the phone system. As a general guideline, set Message Notification, Dialout MWI, and TRAP Connection on approximately 25 percent of the ports.

ipexpert

Call Manager Express Integration

Unity Ports will have a Skinny registration to the CME in the same way as Unity ports register to the Call Manager. **Note** that calls to voicemail from CME do NOT require PSTN connectivity.

It is very important to complete the CME IOS configuration before configuring the Unity server to communicate with CME. Otherwise the Unity ports will register in no particular order.

On the CME increase the maximum number of phones and DN's. The ephone-dn's need to be created with the voicemail port DN information. The ephone-dn's are then assigned to ephone's – do NOT use the auto-assign capability.

```
telephony-service

max-ephone xxx
max-dn xxx
voicemail 3600                      // Speed dial for 'Messages' button to call
Unity

!

ephone-dn 1 dual-line              // DN already created on the system
 number 3001
 call-forward noan 3600 timeout 10
!

ephone-dn 2 dual-line
 number 3002
 call-forward noan 3600 timeout 10
!


ephone-dn 11
 number 3600
 preference 1
 no huntstop
!
ephone-dn 12
 number 3600
 preference 2
 no huntstop
!

ephone-dn 13
 number 3600
 preference 3
```

ipexpert

```
no-huntstop
!
ephone-dn 14
 number A01                      // MWI only
!
ephone-dn 15
 number 3999 secondary 3998      // configure MWI on a one-off ephone-dn
that is not
 mwi on-off                      // assigned to any ephones
!
ephone 11
 vm-device-id CiscoUM2-VI1
 button 1:11
!
ephone 12
 vm-device-id CiscoUM2-VI2
 button 1:12
!
ephone 13
 vm-device-id CiscoUM2-VI3
 button 1:13
!
ephone 14
 vm-device-id CiscoUM2-VI4
 button 1:14
```

CME can be integrated into Unity- from UTIM-Telephone Integration add the CME as a
New cluster.
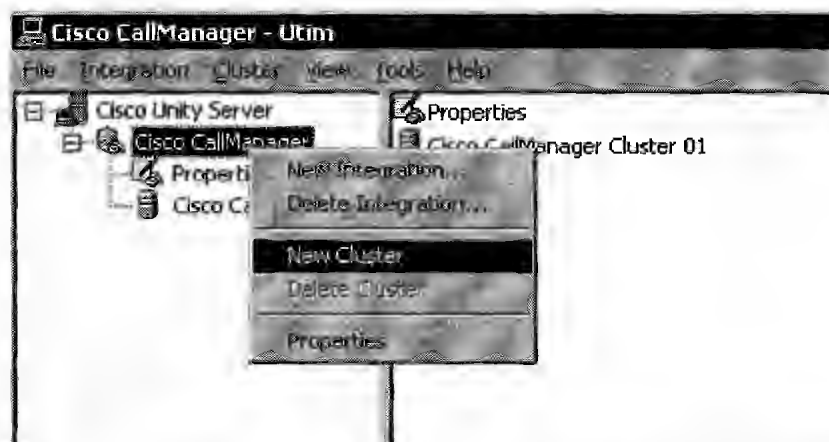
Configure the server change the Display namem IP Address and Cisco Call Manager
Prefix.

♣ ipexpert
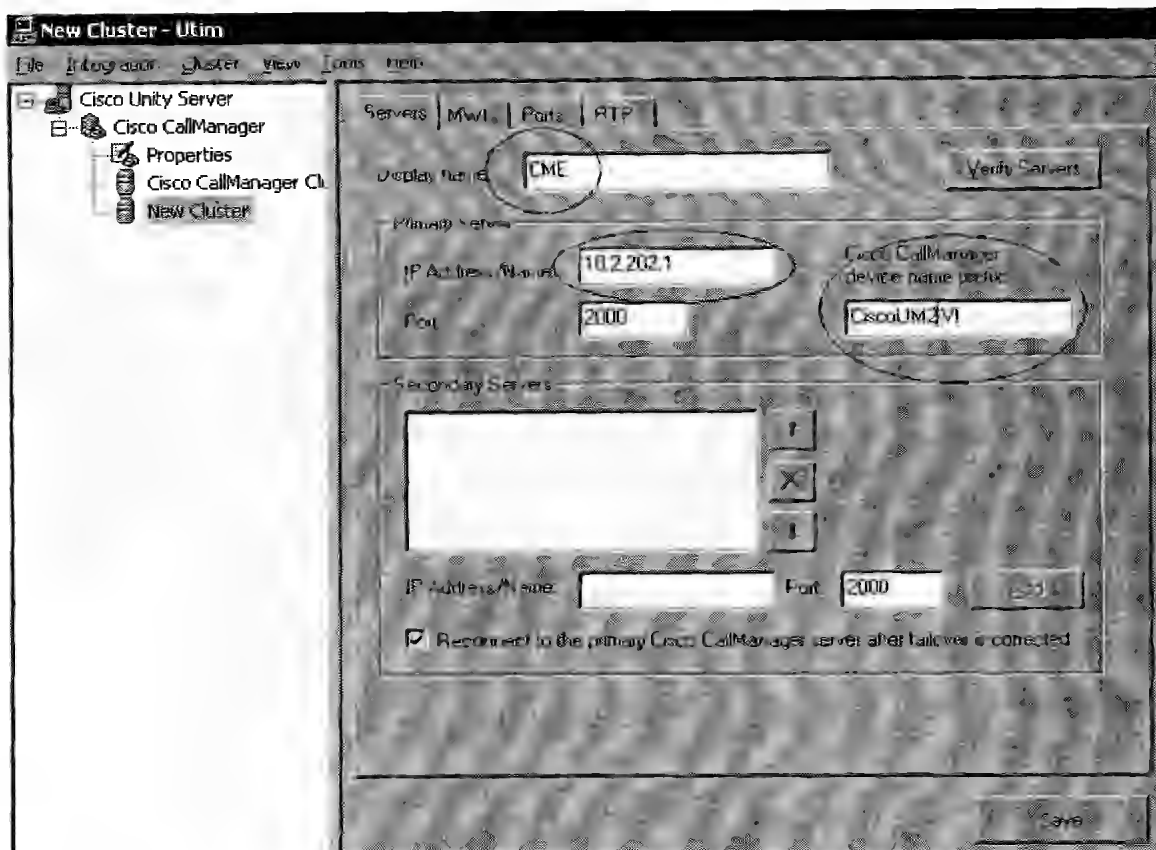
Configure MWI DN's.
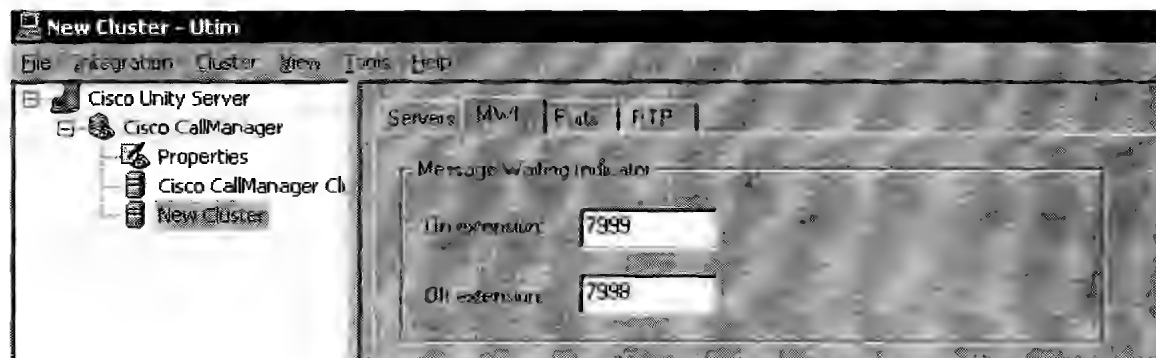
Add the required number of Voicemail Ports.
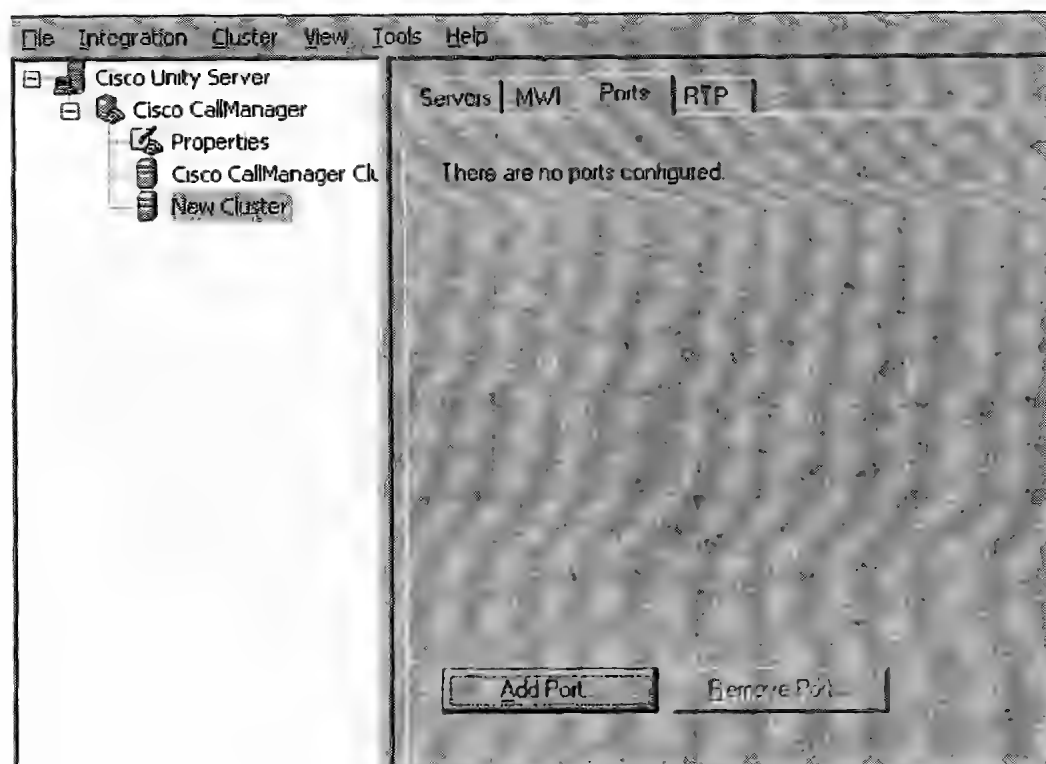
Again, in this example the fourth port is dedicated for MWI.

TRAP is **disabled** on all CME ports since the Call Manager Integration is being used for Recording Prompts using Media Master. We don't recommend enabling the TRAP on two clusters at the same time.

ipexpert
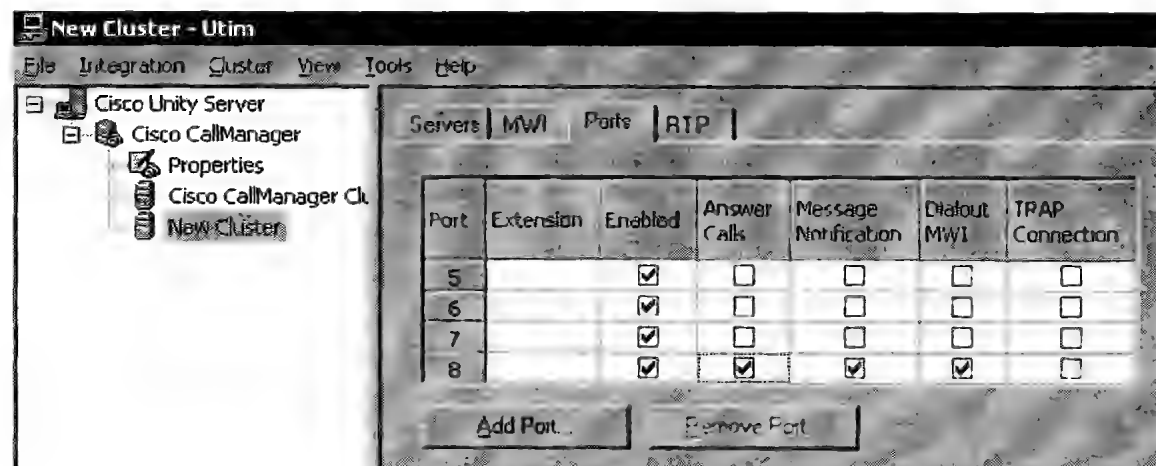
Unity Administration

Unity is configured using the administration web page- this is launched by right-clicking on the Unity icon on the right hand side of the taskbar.

During the Unity setup an administrator account is created. The 'Example Administrator' account serves as a default owner, message recipient, and member of the following Cisco Unity entities:

- Unaddressed Messages distribution list (by default, the Example Administrator is the only member of this distribution list)
- All Subscribers distribution list
- Operator call handler
- Opening Greeting call handler
- Goodbye call handler
- Example Interview call handler
- Default Directory handler
- Default Administrator Class of Service (by default the Example Administrator is the only account with this class of service)

The Example Administrator subscriber account cannot be deleted from the Cisco Unity Administrator. In fact, the account includes the instructions "Do Not Delete" as part of the subscriber name. However, the account can be deleted if necessary, by using SQL and Exchange tools. We recommend you do not configure or delete this account.

Before configuring the Unity server, some of the most important areas of the System Administration (SA) interface are discussed.

ipexpert

Call handlers

The high level call handler properties visible in the SA are discussed briefly below.

Profile

This page shows the basic top level information about a call handler.

The "**Name**" field, of course, is what shows up in the administration interface and is how you search for a handler by name. However this is also it's unique alias in the CallHandler table in the UnityDB SQL database. For this reason the names of all call handlers on a local Unity box must be unique.

The "**Created**" field is the time and date the handler was created – it's a read only property.

If you are listed as the "**Owner**" or are a member of the public distribution list that is listed as the owner of a call handler, you are allowed to change the greetings for that call handler from over the phone.

The "**Active Schedule**" field indicates what times this call handler considers "standard" (business hours) and what times are considered "closed" (after business hours). The

ipexpert

schedule comes into play when deciding which transfer rule and/or which greeting rule to trigger when callers reach the call handler.

The "**Extension**" field is a 3 to 30 digit extension that can be assigned to the handler and is optional.

The "**Language**" field indicates what language the system prompts will be played in to callers reaching this handler.
The "**Switch**" field indicates which phone switch the call handler is associated with in the case that Unity is configured for dual switch support. This value defaults to the first switch (switch "0") defined in the system.

ipexpert

Call Transfer

Handler: Goodbye*

Call Transfer

Transfer Rule applies to: Standard

Standard

Status:
- Enabled
- Disabled

Transfer incoming calls?
- No (send directly to this handler's greeting)
- Yes, ring message recipient's extension   Example Administrator (99999)
- Yes, ring a subscriber at this extension: 9,52611

Transfer type:
- Release to switch
- Supervise transfer

Rings to wait for 2

- If the call is busy
  - Always hold
  - No holding
  - Ask caller

Gather caller information:
- Announce
- Introduce ("call for name")
- Confirm (call can be accepted or refused)
- Ask caller's name

Under "**Status**" the enabled and disabled radio buttons should be reasonably obvious.
However notice in the screen shot above the buttons are disabled and "Enabled" is set.
This is because the selected **transfer rule** is "Standard" which can never be disabled.

ipexpert

For call handlers there are three transfer rules: "Standard", "Off Hours" and "Alternate". Both off hours and the alternate rules can be enabled/disabled as desired however at least one transfer rule must always be active to tell Unity what to do with the call should it enter the transfer conversation for this call handler. The Standard rule, then, is treated as the "backstop" transfer rule and is always enabled.

Note that on the subscriber page in the SA the transfers don't show a drop down list to select one of the three. This is because subscribers are limited to one transfer rule that's either on or off, they do not have a selection of three like application call handlers have. This is the only thing you can do with call handlers that you can't do with subscribers.

The "**Transfer Incoming Calls?**" section lets you decide if Unity will attempt to ring a phone, which number to dial or to skip the transfer attempt entirely and proceed onto the greeting rules. Note that you can stick any number you want in the transfer string, including long distance or international numbers, provided the "Transfers" restriction table associated with your Class of Service allows it. This is an important concept and is probably one of the most commonly misunderstood parts of the Unity administration design. The restriction tables are enforce ONLY at the time the number is changed and the restriction tables of the person MAKING THE CHANGE are what Unity uses to test against. Once a number is in a notification delivery dialout, transfer or fax delivery number field, Unity will use it. It is not checked again at dialout time or any other time.

The **Transfer type** field tells Unity to either dial the number and hang up (release) or stay on the line to see if the called number answers or not (supervised). Supervised transfers are useful in that they offer some nice features like call screening and call holding, however they also tie up voice ports longer. If the transfer type is set to release, the remainder of the options on this page are disabled since they don't apply.

The **rings to wait** for supervised transfers indicates how long Unity will wait before deciding a phone is not answered and will pull the call back. This value must be at least two but it's advisable to have more rings than that, of course. If you have your phone system set to forward to voice mail on a Ring No Answer condition you'll need to make sure Unity is set to ring fewer times than the phone system is set to forward on or you can potentially get Unity talking to itself. You'll also want to remember not to set the phones to forward on busy when using supervised transfers since, again, you can end up forwarding the phone right back to Unity in this scenario.

The "**if the call is busy**" option allows Unity to hang onto the call and play a series of hold music prompts (recorded classical music). After each hold music prompt is played, roughly 30 seconds a shot, Unity will check the line again to see if the phone is still busy. If not, the call goes through, if so Unity will ask the user if they would like to continue holding. There's no way to turn off the option where Unity prompts the user to stay on the line. This is designed to make sure someone doesn't tie up a voice line for overly long. It should be noted that you can't use Unity's call holding feature if your phones are set to forward on busy. Again, for Unity to know the phone is busy we have to get "busy" back from the switch and if the phone is set to forward somewhere we may not get that.

ipexpert

The **ather Caller information** section is made up of 4 options:

- **Announce**. If this is checked Unity will play a short beep tone when the subscriber answers their phone. This is to warn them that it's an external caller coming through the auto attendant.

- **Introduce** . If this is checked Unity will play the voice name of the subscriber the call is for ("call for <voice name>"). This is used in situations where you have more than one subscriber sharing the same phone extension.

- **Confirm**. If this is checked, the subscriber is asked if they want to take the call or send it to voice mail before the call is released to their extension. This is normally used in conjunction with the Ask Callers Name option so you know who's calling and can decide if you're up to talking to them or not. If the call is rejected, Unity smoothly lies to the caller and tells them you're busy or away from your phone.

- **Ask caller's name**. With this checked, Unity will ask the caller to speak their name before ringing the subscriber's phone. This recorded name is played to the subscriber before the call is released to their extension. Normally this is used in conjunction with Confirm so the subscriber can accept or reject the call.

ipexpert
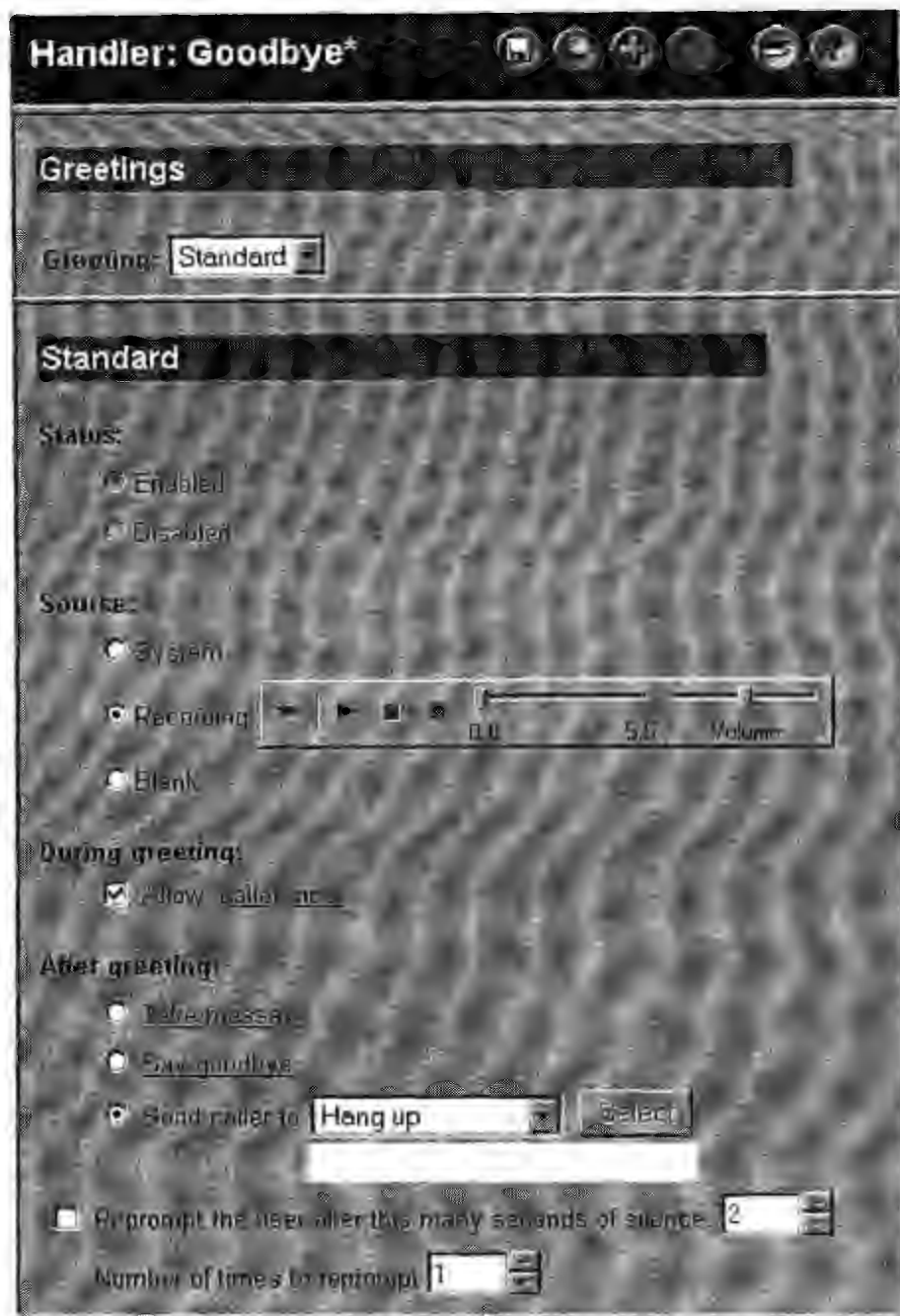
Greetings

After a transfer attempt fails Unity proceeds to the greeting rules. A caller can also be routed directly to the greeting rules in some cases and skip the transfer attempt altogether.

There are six greetings for each call handler in the system, although by default only 5 show up in the SA. The usual list of greetings includes Alternate, Standard, Off Hours, Internal and Busy. The Error greeting is the sixth and is hidden by default- you can expose it in the SA by using the Advanced Settings Tool if you want to see it. You can

also get at it in the BulkEdit utility which offers some options for changing its behavior across groups of subscribers and/or call handlers.

Under "**Status**" the enabled and disabled radio buttons should be reasonably obvious. Notice again that the buttons are disabled and the "Enabled" option is set. Similar to the transfer rule behavior discussed above, this is because the selected greeting rule is "Standard" which can never be disabled. One greeting must always be active and serve as the "backstop" and that's the standard greeting here. Error greetings cannot be disabled either but that's because they serve a special purpose and are not included in the normal hierarchy of greeting rules precedence the other 5 greetings are in. We'll cover the order precedence of the greetings and the function of the error greeting in the call flow section later.

The **source** section indicates what Unity should play to the caller when this greeting rule is invoked. The System option means Unity will construct a prompt using the voice name of the subscriber or call handler (if present) or the extension number if it's not there or, failing both of those, the voice name or extension of the message recipient for the call handler. The Recording option is just what it sounds like, a custom recorded greeting that is played to callers. Blank means just that, no greeting is played and the system skips right to the after greeting action. This is useful for various call flow scenarios where you're using call handlers to route calls around the system.

The **Allow caller input** option is a short hand way of turning off all user input keys while this greeting is active. This option affects only the current greeting so you can, say, have a standard greeting that allows user input the closed greeting can have it turned off. Remember all greetings share the same set of user input keys, there are not separate sets of user input mappings. Turning this option off also restricts users from dialing other extension numbers while listening to the greeting.

The **After Greeting Action** determines what Unity will do with the call after the greeting defined in the Source section completes. Normally this is set to "take message" by default however you have the full compliment of routing options here and you can do anything from simply hanging up to sending the call to a call handler of your choosing to going to the subscriber sign in conversation.

The **Reprompt** option at the bottom is useful if you are expecting an input from a caller and they don't enter anything. By default this value is "0", meaning the greeting will be played only one time and then the after greeting action is executed. You can wait a set number of seconds and then replay the greeting again, giving callers another chance to enter a selection provided in the greeting. You can set it to reprompt many times but once or twice is normally as many as you want. If someone can't figure out what to do after three times through the greeting, it's probably time to send them to a human operator for assistance.

Caller Input

Handler: Goodbye*

Caller Input

☑ Allow callers to dial an extension during greeting

Will sespire to call for additional digits 1500

Key: 1

☐ Lock this key to the action (do not wait for an additional keypress)

Action

○ Ignore key
○ Skip greeting
○ Take message
○ Say goodbye
● Send caller to Hang up ▾ Select

Caller input map

Key	Locked	Action
1	No	Send caller to Hang up
2	No	Ignore key
3	No	Ignore key
4	No	Ignore key
5	No	Ignore key
6	No	Ignore key
7	No	Ignore key
8	No	Ignore key
9	No	Ignore key
*	Yes	Send caller to Sign-in
0	Yes	Send caller to Attempt transfer for Operator
#	Yes	Send caller to Attempt transfer for Opening Greeting

You can define actions that Unity will take when user's enter digits 0-9, * or # while listening to a greeting for this call handler or subscriber. The same set of key action mappings in this user input page are active for all greetings for the call handler.

If user input is allowed during a greeting (see the greetings page above) then the greeting will play through until a key is pressed by the caller. At this point (with one exception noted below) the greeting will stop playing and Unity will wait for the interdigit time out period – this is the "milliseconds to wait for additional digits" field at the top of the form. If no further digits are entered then the action that key is associated with is taken. If the action is "ignore" then Unity considers this an error and will send the call to the Error greeting which by default says "I'm sorry I did not hear that entry" and then sends the caller to the opening greeting call handler created by setup (this can be changed). If, instead, the user enters more digits Unity will continue collecting digits until the user stops for the timeout period or presses # to terminate the input process. Unity will then look that string of digits up in the database to see if any extension number for a call handler, interview handler, subscriber, or name lookup handler matches. If a match is found the call is sent off to that object. If no match is found then again, Unity considers this an error and sends the call to the Error greeting.

If a key is **locked**, this means if that's the first digit the user enters to interrupt the greeting, the action the key is associated with will take place immediately without waiting for the inter digit time out for more digits to be entered. If the key's action is set to "locked" AND "ignore" however, the key is thrown away and the greeting is not interrupted at all.

The "**Allow callers to dial an extension during the greeting**" is simply short hand for locking all the keys. As such when a user enters a digit it's acted on immediately and there's never any period where Unity is waiting to see if you'll enter more digits. This is different than unchecking the "allow user input" box on the greeting page. If you do that, it's the same as locking all the keys AND setting them to ignore. No input is allowed at all and the greeting will never interrupt.

Messages

The messages page is pretty straight forward. The primary input here is designating which subscriber or public distribution list should get messages if the call handler has an after greeting or a one key option set to take a message. Even if no option in the handler is configured to let callers leave a message, you still have to have a valid subscriber or distribution list designated here. The first thing Unity does when it loads a call handler is go fetch the recipient. If they don't exist (i.e. you deleted the subscriber you had set as the recipient) then it'll send the call to the ever-popular "failsafe" greeting and the caller will be sent to the opening greeting call handler.

The maximum message length does exactly what it says: you can limit the number of seconds a caller can record for. Note that this does not affect subscribers leaving messages for other subscribers. This value only affects outside callers leaving messages for subscribers. You can dictate how long a message any given subscriber can leave in their Class of Service on the "messages" page. By default all subscribers can leave 300 second (5 minutes) messages for other subscribers. If you would like to extend this or, more likely, trim it back, you can do that in the class of service settings.

By default Unity will not warn callers when they are nearing the end of their record session. However you'll find three settings in the Advanced Settings Tool that start with the string "Record Termination Warning" that you can turn on such that Unity will play a beep or a WAV file you dictate to callers when they approach the end of their recording leash.

The after message action section dictates what Unity will do with the caller after they have completed leaving their message. By default this is set to go to the "say goodbye" call handler.

You can also decide if users can rerecord or append to their message with the "Callers can edit message" check box and decide if they can opt to mark the message urgent or not.

Call Handler Flow

A call handler flows through 4 separate "stages" in its life cycle. Transfer rules (contact rules in the SQL database) are executed first then, if necessary, the greeting rules (messaging rules in the database) are evaluated followed by the after greeting action followed, if necessary, by the after message action.
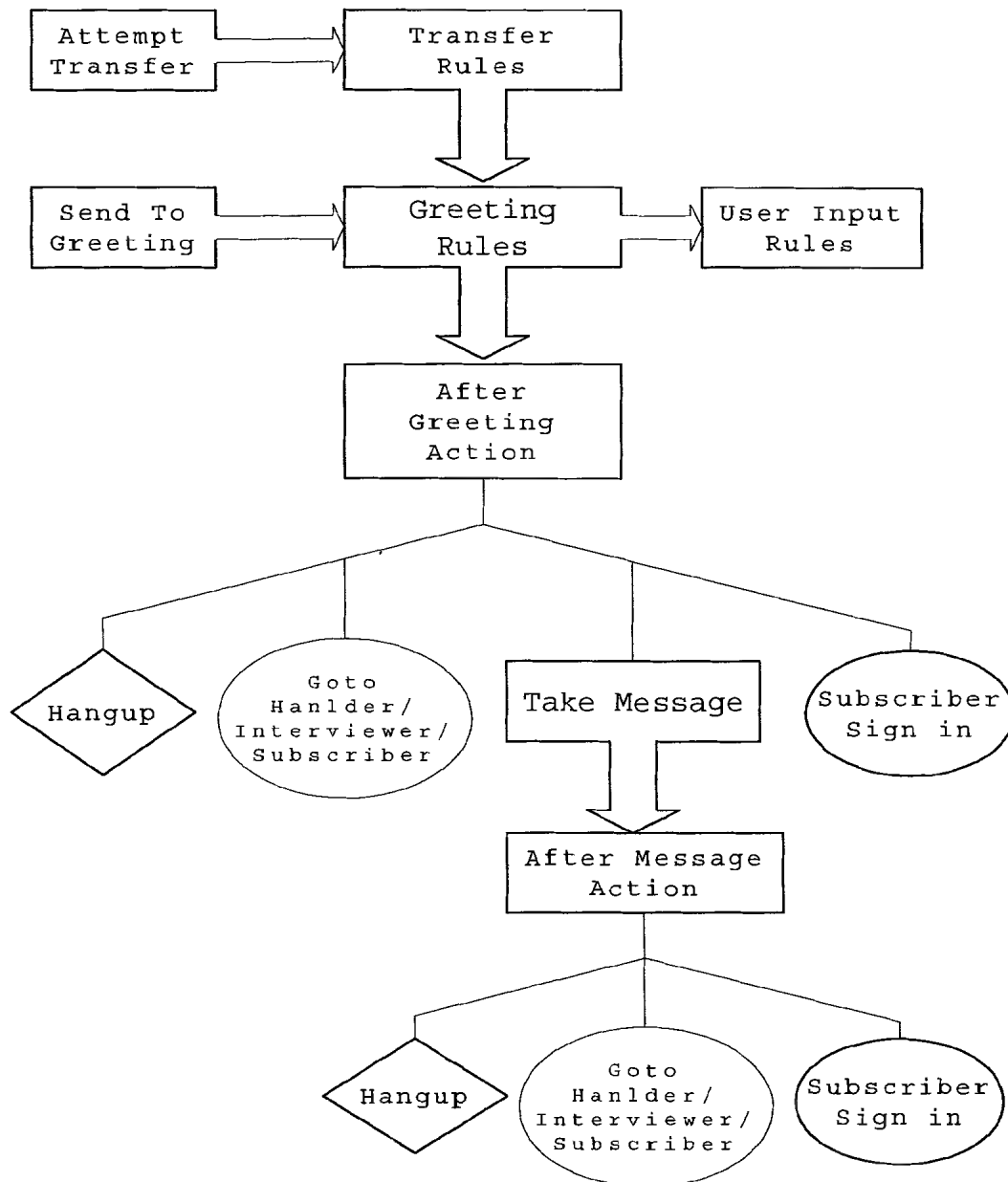
The first thing to notice is that there are exactly two entry points into a call handler. You can jump in at the top and start with the transfer rules or you can jump in right at the greeting rules. The idea here is that many times you want to send a caller directly to the

ipexpert

greeting for a subscriber or a call handler without ringing their phone and sometimes you want to ring the phone. The default when you choose to send a call to either a call handler or a subscriber is to go directly to the greetings and skip the transfer rules. This option is selected in the "conversation" drop down list when you choose which handler or subscriber you want to send the call to as shown below.
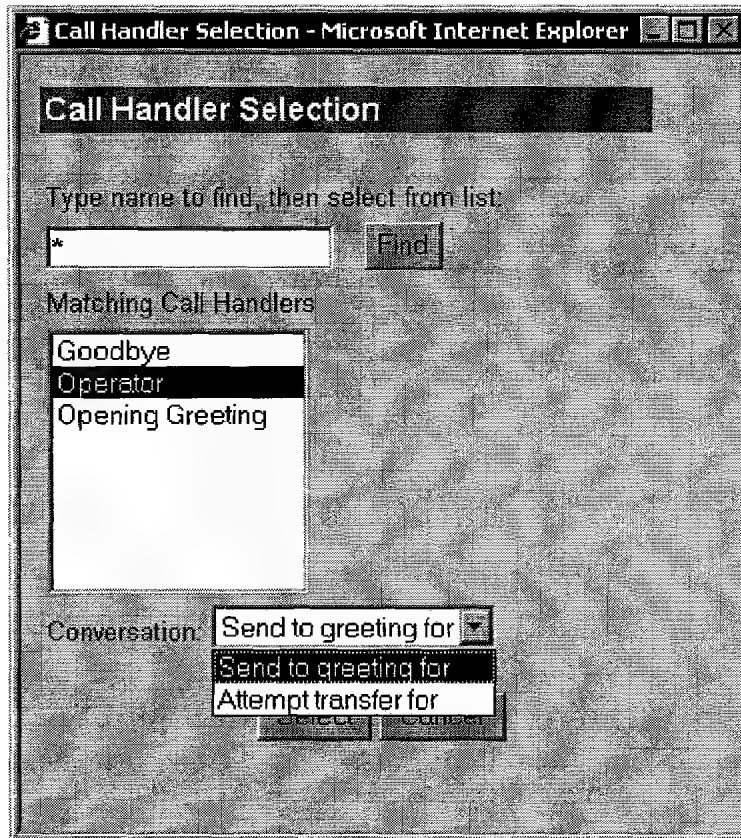
If you leave the default of "**send to greeting for**" it will skip the transfer rules. If you select "**Attempt transfer for**" it will start at the top of the flow with the transfer rules.

Transfer Rules

At the top of the chart is the Transfer entry point. In the SA this is characterized with the "Attempt transfer for" selection. Remember that even when sending a call to a subscriber you still go to a call handler, it's just the primary call handler associated with that subscriber record.

If the call handler is an application handler (i.e. a "normal" call handler as opposed to a "primary" call handler associated with a subscriber) then there are three rules that can be active here. The order of precedence is simple in this case. If the alternate transfer rule is enabled it will be the one evoked no matter what. It over rides the other rules and they will never be called until the alternate rule is disabled. After that if the schedule the call handler is associated with indicates it's "after hours" then the off hours transfer rule will be triggered. In all other cases the standard contact rule will be the one used. Remember

ipexpert

that you can't disable the standard greeting so we can always count on it being there for our use.

Remember, however, that if the call handler is a primary handler tied to a subscriber, the alternate transfer rule is hard coded active and cannot be disabled. For subscribers transfer are very basic indeed: they are either on or off.

There's one scenario that will cause the transfer rules to be skipped that throws folks in the field off now and again. When a call forwards from an extension into Unity, by default Unity will search for the original forwarding extension among all call handlers and subscribers. If it's found the call is sent directly to the greetings for that call handler, no attempt is made to go to the transfer rules even if they're active. This is done such that Unity doesn't get caught in a "transfer loop" where a call forwards into Unity and we forward the phone to the extension which, of course, then forwards back to us and so on. This will quickly chew through all your available ports and cause all kinds of problems.

Greeting Rules

The greeting rules have a much more complex order of precedence. The five greetings used for handling incoming calls are processed in order from the top down. The first enabled rule in this list that matches the call criteria (if necessary) is used to handle the call.

- **Alternate**. At the top of the heap, of course, is the alternate greeting. Again, if it's active all other greetings are ignored and this greeting will always play no matter where the call came from or what schedule the call handler is associated with.
- **Busy.** If the call forwards into Unity from a busy extension and, of course, the phone switch integration passes this information along accurately, and the busy greeting is enabled then it will be the one that handles the call.
- **Internal.** If the calling number is reported and corresponds to the extension (either primary or alternate) of a subscriber homed on the local Unity server it's considered an internal call. If the internal greeting is active then it will be used to handle the call.
- **Off Hours**. If the schedule the call handler indicates it's now "off hours" and this greeting is enabled then the off hours greeting handles the call.
- **Standard**. If all other rules are disabled or fail to match the call data, the standard rule is invoked. Remember that you can never disable the standard greeting (or shouldn't be able to anyway) and Unity can count on this rule always being enabled.

Yes, there is the **Error greeting** but it's not included in the flow of precedence here. The Error greeting is invoked only when the user enters an invalid selection or dials an extension number that doesn't exist, it's never used to handling incoming calls directly.

ipexpert

After Greeting Action

As the name would imply, this is the action Unity takes after the greeting is played. Each greeting has it's own action field, of course, so you can do different things depending on which greeting is active for a given call. By default this is set to "take message" since most of the time that's what you want to do. You can, however, do what you want with it like sending the call to another handler, hanging up, even going to the subscriber sign in conversation if you like. This becomes especially important when using a call handler as a "router" with a blank greeting which is handy for several scenarios.

After Message Action

After taking a message the default action is to go to the "say goodbye" call handler and hang up on the user politely. You can pick other actions, however the list is a little smaller here since you aren't allowed to select "take a message" as the after message action – that be pretty annoying for callers.

Subscribers

Subscribers and call handlers are almost identical with respect to their call handling characteristics. Subscribers are really two separate objects that work together. There's a mail user object and it's corresponding "primary call handler". This is just a call handler that's assigned to a subscriber and doesn't appear in the call handler search dialogs. The one difference between the primary call handler of the subscriber and 'normal' call handlers is that subscribers have only one transfer rule instead of the full three that regular call handlers do.

Two fields that are very useful, Alternate Extension and Alternate MWI, are discussed below.

Alternate Extensions

In addition to the "primary" extension that you specify for subscribers, you can assign subscribers up to nine alternate extensions. (The primary extension is the one that you assign to each subscriber when you create his or her subscriber account; it is listed on the Subscribers > Subscribers > Profile page).

This is an easy way to configure a shared mailbox- when other phones (phones that do not have the primary extension configured) are used as alternate extensions, and are set to forward to Cisco Unity, callers can listen to the subscriber greeting, and leave messages for the subscriber just as they would when dialing the primary extension for the subscriber.

Alternate extensions cannot exceed 30 characters in length. By default, each administrator-defined alternate extension must be at least 3 characters in length, while subscriber-defined alternate extensions must be at least 10 characters.

You can use the Advanced Settings tool in Tools Depot to specify a minimum extension length for the extensions entered in the Cisco Unity Administrator and the Cisco Unity Assistant. Refer to the Advanced Settings Tool Help for details on using the settings. Respectively, the settings are Administration—Set the Minimum Length for Locations and Administration—Set the Minimum Length for Subscriber-Defined Alternate Extensions.

You can control whether subscribers can use the Cisco Unity Assistant to view the alternate extensions that you specify in the Cisco Unity Administrator. To do so, see the Subscribers > Class of Service > Profile page. The Subscriber-Defined Alternate Extension table displays the alternate extensions that the subscriber adds.

Neither the Cisco Unity Administrator nor the Cisco Unity Assistant will accept an extension that is already assigned to another subscriber (either as a primary or alternate extension), or to a public distribution list, call handler, directory handler, or interview handler. Cisco Unity verifies that each alternate extension is unique—up to the dialing domain level, if applicable—before allowing either an administrator or a subscriber to create it.

All alternate extensions utilize the same transfer settings as the primary extension.

Alternate MWIs

You can set up Cisco Unity to activate alternate MWIs when you want a new message for a subscriber to activate the MWIs at up to 10 extensions. For example, a message left at extension 1001 can activate the MWIs on extensions 1001 and 1002.

Configuring Alternate Ext/MWI

From the SA interface for the Subscriber, the Alternate Extensions can be configured.

To configure alternate MWI use the Messages option.

ipexpert

Interview Handlers

An interview handler is a specialized handler that's designed to interrogate a user for specific information so they don't forget to provide, for instance, their product serial number, return phone number or whatever else you need callers to provide. An interviewer is considerably less complex than a call handler or subscriber since there's no user input options, call transfer options or the like.

Directory Handlers

A Directory Handler is a mechanism by which callers can find subscribers in the directory by spelling their name either starting with the last name or the first name.

Routing Rules

Every call that comes into Unity goes through the call routing rules no matter what. Unity gets information about a call coming in from Call Manager which can include the calling number, the number it forwarded from, the dialed number etc… Unity then starts at the top of the list of routing rules and looks for the first rule that matches the information it got from the switch. If that rule "succeeds" the routing rules are done and the call is now in the hands of the Unity conversation as it passes around in the collection of call handlers, subscribers, interviewer and name lookup handlers in the database. If not, it'll proceed to the next rule in the list until it finds a rule that succeeds. A rule will ALWAYS succeed here since there is a special rule at the bottom of the table that is hard coded to catch all calls and send them to the opening greeting call handler created by the Unity setup which cannot be deleted and should always be there. You can, of course, add your own rules to this list by going to the SA's "routing rules" page and adding new rules for forwarded or direct calls into the list. You cannot, however, delete or move that hard coded "send to opening greeting" rule in either list. It is there as a backstop ensuring Unity can always do something with an inbound call.

Bulk Import Wizard

Subscribers can be added manually from the SA interface or by using the bulk import wizard accessible from **Start-Programs-Unity**.

The example here uses the Bulk Import wizard.

You can import users from the Active Directory or from a CSV file- CSV file is quicker in this instance.

ipexpert
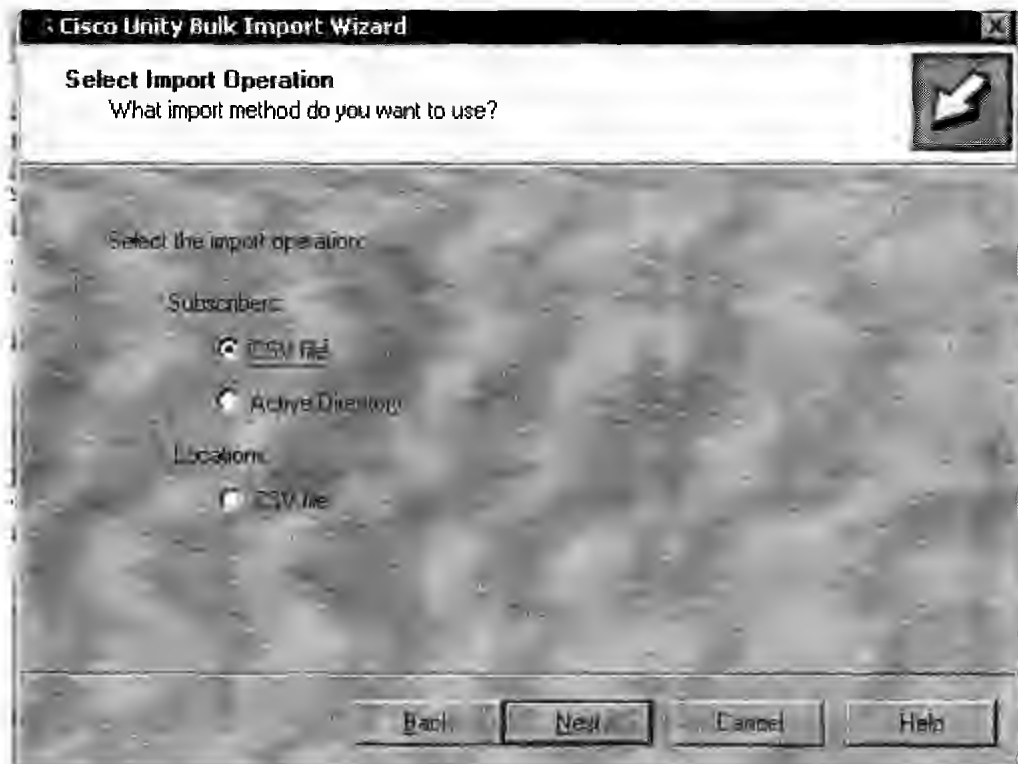
Leave the location of where the log files are stored to the default locations.

The LAB Blueprint only supports Voice-mail only so we will create Voice-Mail only subscribers.

ipexpert

Since the Exchange and Windows accounts do not exist we will create them at this stage as well.
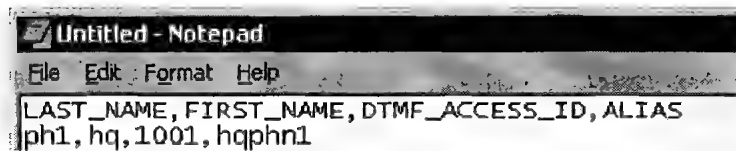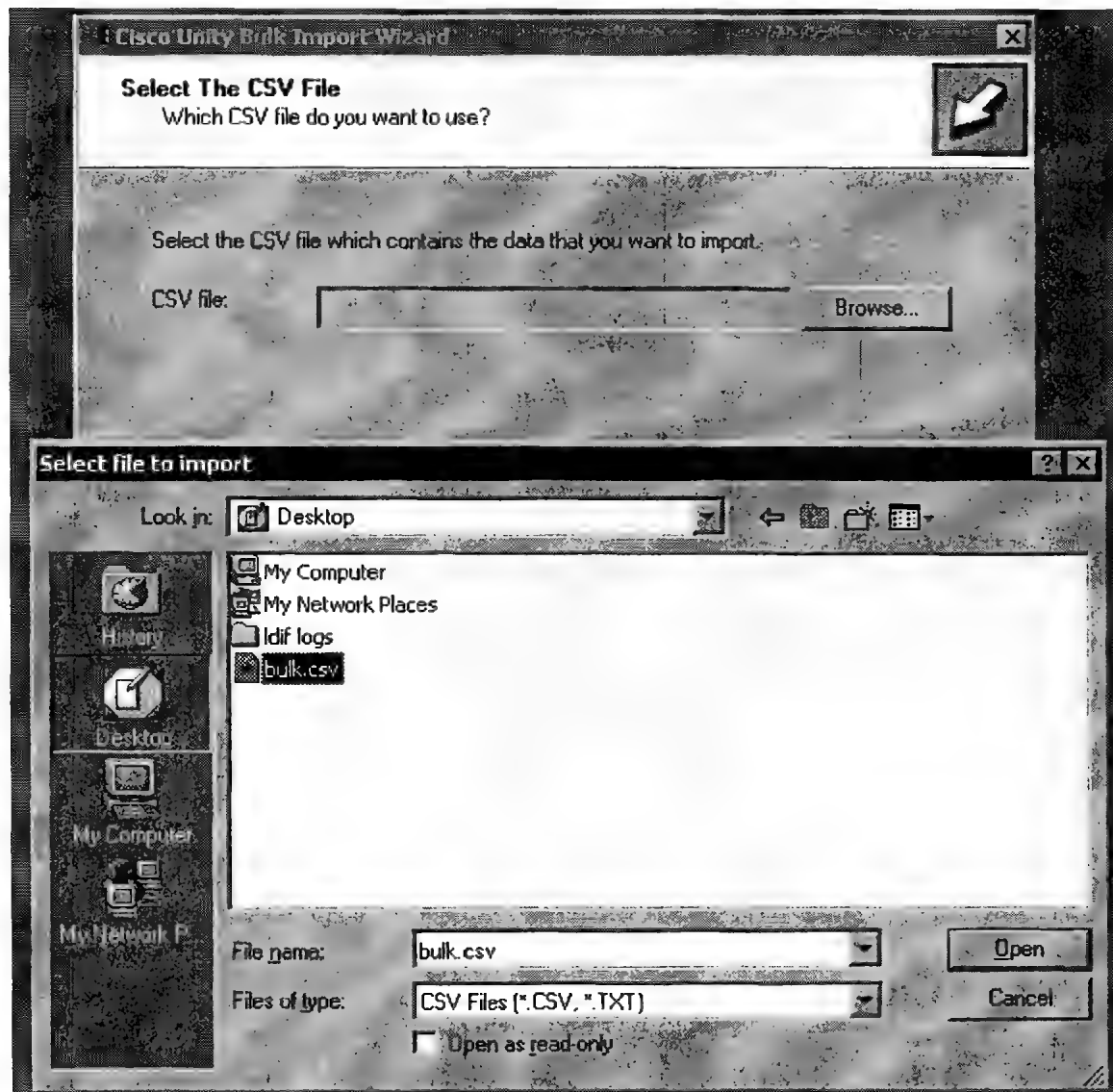
ipexpert
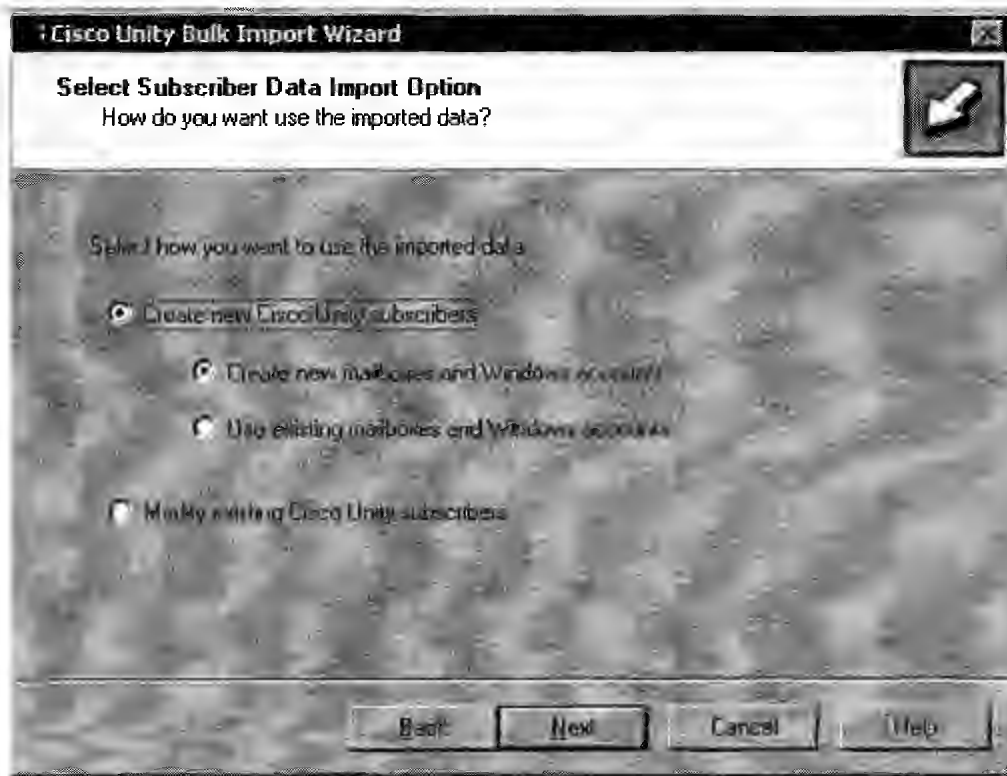
Select Default Subscriber Template.
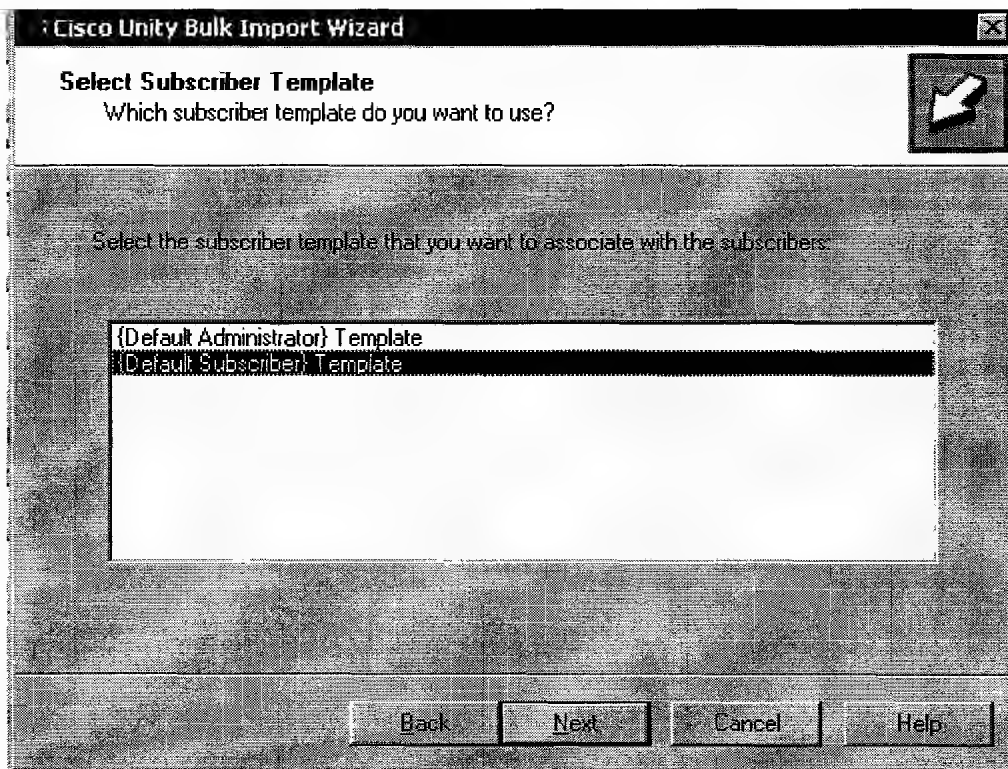
Select the Domain and Container (leave as default).

ipexpert
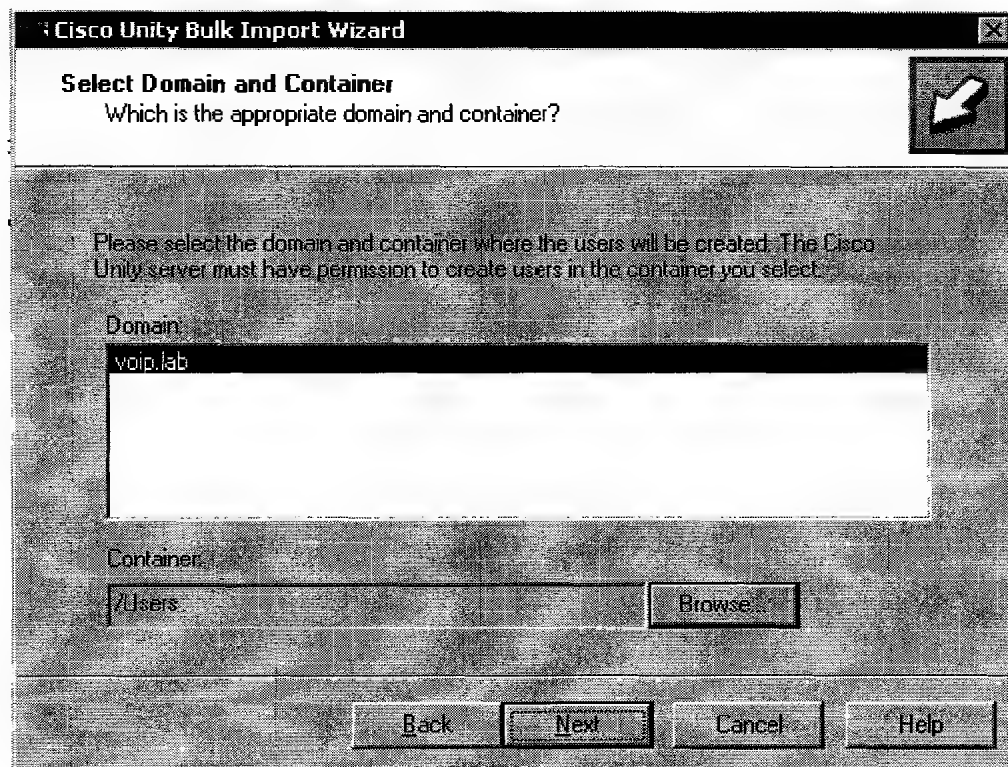
Create the CSV file- note that the suffix must end with .csv and NOT .csv.txt. Therefore when saving the files save as 'All Files'. The first line must be syntactically correct with the four mandatory fields.


```
Untitled - Notepad
File   Edit   Format   Help
LAST_NAME,FIRST_NAME,DTMF_ACCESS_ID,ALIAS
ph1,hq,1001,hqphn1
```

Find the CSV file you have created

Once you have located the CSV file you will be prompted to add the subscribers- all that remains to be done is to verify that there were no errors and you are done!

ipexpert

Example Call Handler: Auto-Attendant

An example of creating a Auto-Attendant Call Handler is shown below. The Call Handler is given a DN of 1570 will play a greeting to prompt the caller to press an entry. The Caller Input will route the call such that if the user presses

'1': the caller is prompted to sign-in
'2': the caller is redirected to extension 1001
'3': the caller is sent to the voicemail of extension 1001
All other entries: Re-route back to the Auto-Attendant greeting

Create the Call Handler and to save time base it on the Opening Greeting call handler.
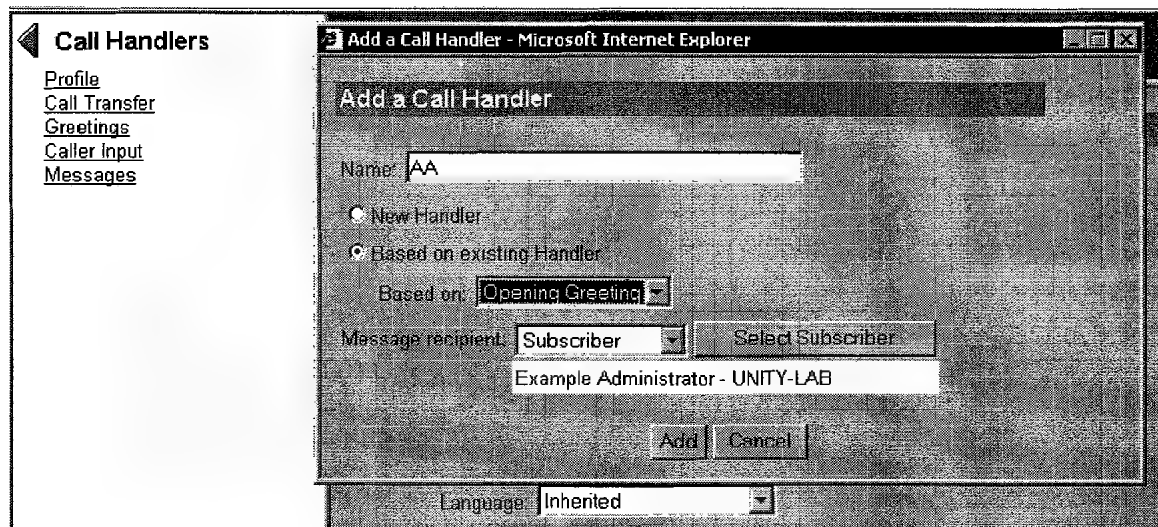
Change the Active Schedule so the 'Closed' greeting is not used out of business hours. Also assign the appropriate DN to the Call Handler.

ipexpert

Call Handlers

Profile
Call Transfer
Greetings
Caller Input
Messages

Handler: AA*

Profile

Name: AA
Created: 5/28/2005 9:33:44 AM
Owner: Example Administrator - UNITY-LAB
Owner Type: Subscriber
Recorded voice:
Active schedule: All Hours - All Days
Extension (optional): 1570
Language: Inherited

From the '**Greetings**' page go to options and specify the Unity Server and Extension Number of the phone which will be used with Media Master to record the Call Handler Greeting (Welcome to PODX, press '1' to sign in, '2' for HQ phone 1, '3' for voicemail of HQ Phone 1).

Call Handlers

Profile
Call Transfer
Greetings
Caller Input
Messages

Handler: AA

Greetings

Greeting: Standard

Standard

Status:
Disabled
Enabled - No end date and time

Source:
System
Recording
Blank

During greeting:
All call

After greeting:
Take message
Send caller to

Options...

Select Call Handler

ipexpert

On the same page specify that the caller is allowed to enter digits during the greeting. After 5 seconds of silence Unity will play the prompt again (twice) before ending the call.
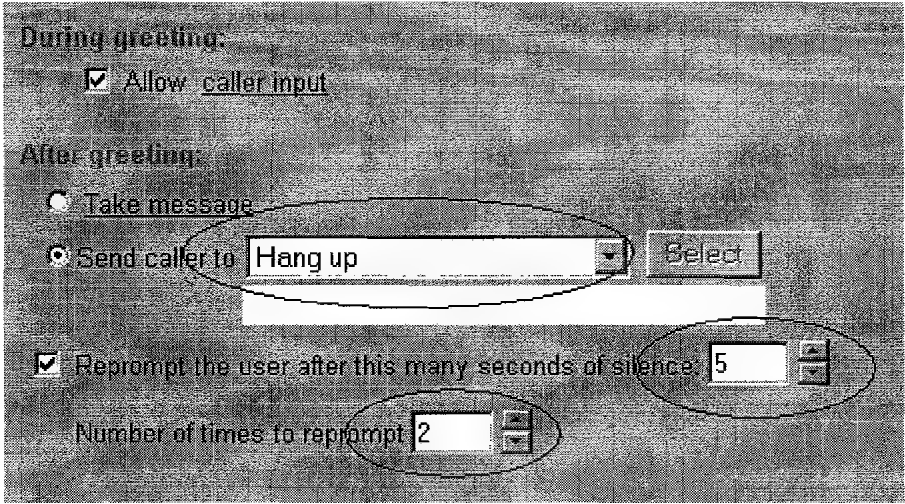
From the '**Caller Input**' specify the actions required on relevant key presses. By locking keys Unity proceed to the desired action without waiting for the inter-digit timeout. All unused keys should be set to 'Ignore'- this will invoke the Error Greeting.

Key: 1

☑ Lock this key to the action (don't wait for an additional keypress)

Action:

○ Ignore key

○ Skip greeting

○ Take message

○ Say goodbye

◉ Send caller to [Sign-in ▾] [Select]

Caller input map

Key	Locked	Action
1	Yes	Send caller to Sign-in
2	Yes	Send caller to Attempt transfer for hq ph1
3	Yes	Send caller to Send to greeting for hq ph1
4	No	Ignore key
5	No	Ignore key
6	No	Ignore key
7	No	Ignore key
8	No	Ignore key
9	No	Ignore key
*	Yes	Ignore key
0	Yes	Ignore key
#	Yes	Ignore key

ipexpert

Go to the Call Handler Greeting and check if the Error Greeting is allowed to be configured.
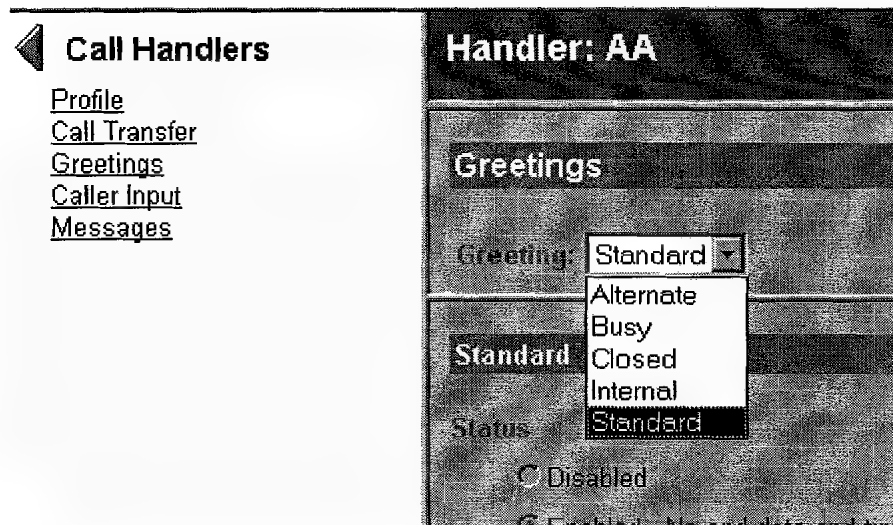
In this case the Error Greeting cannot be configured- use the Advanced Settings tool from Administrative Tool under Unity Tools to expose the Error Greeting. Note- the Unity server does NOT need to be restarted to expose the Error Greeting.

Close down the current browser and launch the SA Admin Interface again. Check the Call Handler Greeting to see if the Error Greeting is now exposed.

ipexpert
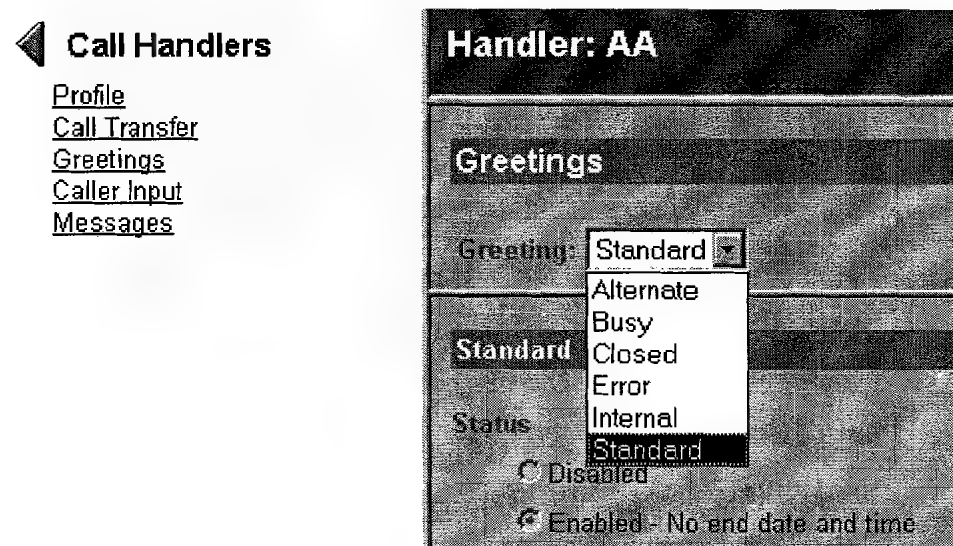
Configure the Error Greeting- play a blank greeting and send to the Greeting of the Auto-Attendant.

One last vital step- configure the subscriber's **Call Transfer** options to permit dialing the extension.

Multi-Tenancy with Unity

When the Call Manager has an overlapping dial plan there is a need to create Unity subscribers which do NOT match the DN of the subscriber line in Call Manager since Unity has no concept of partitions and calling search spaces.

Take for example a Call Manager that is shared between two clients- customer A and customer B. In this install of Call Manager there is an overlapping dial plan.

Call Manager is configured with a phone with extension 2001 in the customer A partition and a phone with extension=2001 in the customer B partition.

Unity is configured with two subscriber accounts: customer A partition phone with DN=2001 has a corresponding Unity Subscriber account with DN=2001. Customer B partition phone with DN=2001 has a corresponding Unity subscriber account with **DN=22001**.

This configuration is fine for Customer A but the scenario above poses two problems for customer B- how does Unity know to play the subscriber greeting of '22001' when a call is redirected to Unity in a Call Forward No Answer from '2001'? And how does Unity turn MWI on/off for 2001 when it thinks the DN of the relevant phone is '22001'?

The first of these questions is solved by creating an additional VoiceMail Profile in Call Manager. The Voicemail is masked to prefix a leading '2'- when sending calls to Unity

the Call Manager prefixes the forwarding number (or calling number on direct calls to Unity) with a '2' so '2001' is transformed to '22001'.

Voice Mail Profile Configuration ₿

Voice Mail Profile: New (Copy of unity)
Status: Ready

[Insert]

Voice Mail Profile Name*   [customerB]

Description   [unity]

Voice Mail Pilot **   [< Use Default > ▼]

Voice Mail Box Mask   [2xxxx]

☐ Make this the default Voice Mail Profile for the system
* indicates required item

This profile needs to be assigned to the relevant Line.

[Update] [Delete] [Reset Devices]

Directory Number

Directory Number*   [2001]

Partition   [< None > ▼]

Directory Number Settings

Voice Mail Profile   [< None > ▼] (Choose <No

Calling Search Space   [< None >]
                          [customerB]
AAR Group   [Default]
                          [NoVoiceMail]
User Hold Audio Source   [unity]

Network Hold Audio Source [< None > ▼]

Call Waiting   [Default ▼]

The problem of MWI is solved using Translation Patterns- in the customer B partition we will transform '22001' to '2001'. A Translation Pattern with DN=22001 is created with **'Called Transform Mask'** is set to **'xxxx'** – Call Manager looks only at 4 digits right justified.

Translation Pattern: New

Status: Ready

[Insert]

Pattern Definition

Translation Pattern	22001
Partition	< None >
Description	
Numbering Plan*	North American Numbering Plan
Route Filter	< None >
Calling Search Space	< None >
Route Option	⦿ Route this pattern ⃝ Block this patt

☑ Provide Outside Dial Tone   ☑ Urgent Priorit

Calling Party Transformations

☐ Use Calling Party's External Phone Number Mask

Calling Party Transform Mask	
Prefix Digits (Outgoing Calls)	
Calling Party Presentation	Default

Called Party Transformations

Discard Digits	< None >
Called Party Transform Mask	xxxx
Prefix Digits (Outgoing Calls)	

In order to use transformation masks with MWI a CCM Service Parameter need to be edited. The **'Multiple Tenant MWI modes'** needs to be set to **'True'** in order for MWI to be able to work with Translation Patterns.

Once this has been changed don't forget to restart the Call Manager service from Control Centre.

ipexpert

Clusterwide Parameters (Feature - General)

Parameter Name	Parameter Value	Suggested Value
Barge Enabled Flag*	False	False
Suppress MOH to Conference Bridge Flag*	True	True
Call Park Display Timer (sec)*	10	10
Call Park Reversion Timer (sec)*	60	60
Call Waiting Enable Flag*	True	True
Call Waiting Timer (sec)*	180	180
Message Waiting Lamp Policy*	Primary Line - Light and Prompt	Primary Line - Light and Prompt
Multiple Tenant MWI Modes*	False / False / True	False
Voice-Mail Maximum Hop Count*	12	12

Troubleshooting

Call Viewer

You'll find the Call Viewer in the Switch Integration Tools section of the Tools Depot.

Call Viewer

File   View

Call #	Time	Origin	Reason	Trunk ID	Port ID	Dialed Number	Calling Number	Forwarding Station
3	16:41:32	Duration = 52 sec						
3	16:40:40	Internal	Fwd(Busy)	0	2	3001	3001	3001
2	16:40:36	Duration = 20 sec						
2	16:40:16	Internal	Fwd(Unconditional)	0	3	3781	3001	3781
1	16:40:07	Duration = 105 sec						
1	16:38:22	Internal	Direct	0	8	1007	3001	

Close

Note that the call viewer only shows incoming call information. Outdials for notification, MWI or TRAP sessions will not show up in the call viewer.

ipexpert

A quick run down on what data shows up in the columns:

- **Call #.** This column is simply a counter of the number of calls that have come in since you opened the call viewer. When you start Call Viewer the first call to come in will be call #1, the next will be 2 etc… This has nothing to do with the call information from the switch at all, it's just there to help you with troubleshooting, in particular if you dump it out to a file for later review. Notice that when a call terminates another row is added with the same call number value and an indication of how long the call lasted.
- **Time.** This is the time the call started or ended depending on which row you're looking at.
- **Origin.** This can be internal or external. For Call Manager this value will ALWAYS be "internal" no matter what.
- **Reason.** This can be either direct or one of three forwarding reasons: Busy, RNA (Ring No Answer) or Unconditional.
- **Trunk ID.** The switch trunk the call came in on.
- **Port ID.** The Unity port that the call came in on.
- **Dialed Number.** The original number the caller dialed when coming into the system.
- **Calling Number.** The calling number, if provided.
- **Forwarding Station.** The number of the station that forwarded to the Unity ports. Note that if a call forwards from one Unity port to the next until a free line is found, the forwarding number reported will be the original forwarding station, not the last redirecting number. The last redirecting number is not exposed anywhere in Unity.

Status Monitor

The status monitor tool can be found in the Tools Depot under the Switch Integration Tools section. Do not confuse this tool with the status monitor web site that is the companion to the SA as they are not the same thing at all. The status monitor tool shows a lot of detailed information about what's happening on calls on each port that can be very useful for determining where calls are going in the system and why. Below is a screen shot that shows what the monitor looks like when a call comes into the opening greeting and the user dials "5551001" to reach a subscriber:

ipexpert
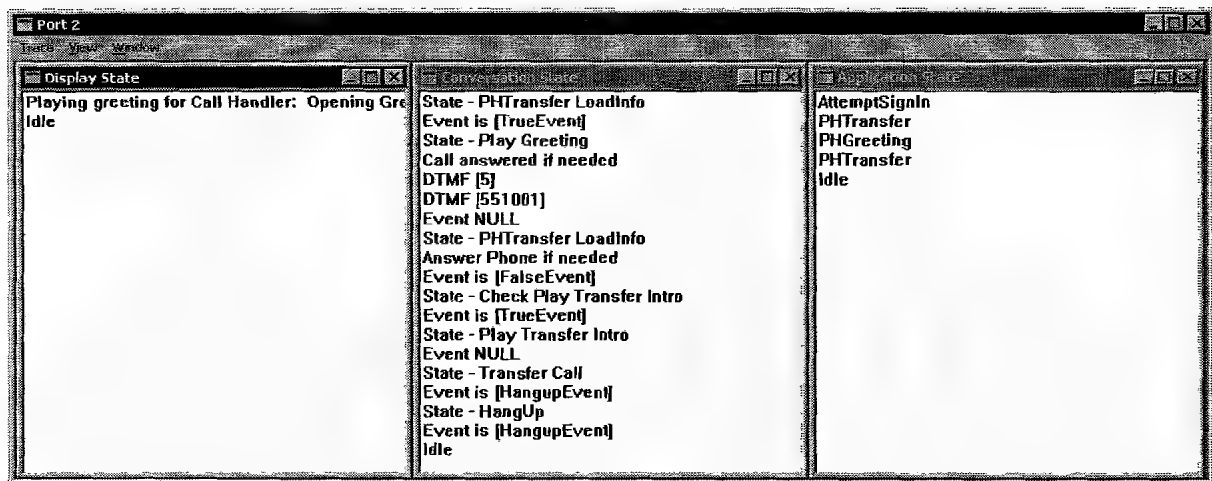
This shows just a single port being monitored, you can actually view all ports on the system at once if you like however the screen gets pretty cluttered. It's much easier to monitor a single port and make your test calls to that line if you can. There are three panes in the window that all show different information:

- **Display State**: This shows very high level information and is, in fact, the text that shows up in the web based status monitor. Not a lot of detail here but it helps you keep the context of what's going on in the other windows straight as you navigate around the system.

- **Conversation State**. This shows a lot more detail, the most interesting thing in this pane is the DTMF events that show each and every key press made. Not that for this test I dialed "5551001" all as one string during the opening greeting. However in the conversation state pane is shows the first 5 by itself followed by the "551001" remainder on the next line. The reason for this is the first 5 pressed interrupted the greeting and is its own event. The other digits were part of the "gather digits" event which will gather as many digits as the user enters up to 30 and then do a lookup in the database. It looks a little odd at first glace but it's supposed to look that way.

- **Application State**. This shows which conversations are being spawned. In this case the "attempt sign in" conversation is spawned on the direct inbound call by the routing rule. The PHTransfer and PHGreeting conversations are spawned when the call is sent to the opening greeting. You'll notice the default routing rules send the calls to the "attempt transfer for" entry point for the opening greeting call handler however the transfer rule is disabled so the PHTransfer conversation exits right out and spawns the PHGreeting conversation. The final PHTransfer conversation is the release transfer on the target subscriber being executed (extension 5551001 in this case).

ipexpert

IPCC Express

IPCC Express or CRA/CRS (terminology is inter-changeable so don't be confused!) is co-resident on the Publisher Call Manager. The main components to successfully configure the IPCC Express server are as follows:

- Call Manager configuration for CRA
- Setting up the Directory
- Setting up the JTAPI Subsystem
- Setting up the ICD Subsystem
- Create Applications and Scripting

Call Manager Setup

Add the CTI Route Points. Give the Route Points easy to remember names such as RPAA and RPICD- in this case the two Route Points will be used for the Auto-Attendant and ICD scripts.

Add the CTI Ports with Call Waiting disabled. Optionally display name can be configured.

Add the necessary Users to the Directory.

UserID	CTI App Required	Device Association	ICD Ext required
crsadmin	N	None	N
jtapi	Y	CTI Route Points and CTI Ports	N
rmuser	Y	Agent Devices	N
agent1	Y	Agent1 Device	Y
agent2	Y	Agent2 Device	Y

The crsadmin user is added to merely assign administrator priviledges to this user. The JTAPI and RMUSER users will be used to configure the JTAPI and ICD subsystems respectively whilst the agent users will be used to login via the Call Manager ICD service.

The crsadmin user being added is shown below.

All other users that are added will need the 'Enable CTI Application Use' checkbox ticked as shown with the JTAPI user below.

ipexpert

Remember to be EXTREMELY careful to associate the correct devices to the correct users.

When associating the relevant devices to the Agent users, remember to check the ICD Extension checkbox.

If the option for ICD Extension is not visible then return to this step when the RM-CM Subsystem is running. You may need to start the IIS and WWW Windows service and possibly toggle the IAQ flag for the default profile in DCDirectory (unlikely).

Before moving onto the configuration of the CRA engine, it is a good time to add the Call Manager ICD Service. The URL is as follows:

http://<CCM-IP-ADDRESS>:6293/ipphone/jsp/sciphonexml/IPAgentInitial.jsp

Address http://10.2.200.21/CCMAdmin/phoneservicesconfig.asp?Status=ic&Service={185071A6-DCB9-4658-8BE2-786B22546925}

System   Route Plan   Service   Feature   Device   User   Application   Help

Cisco CallManager Administration
For Cisco IP Telephony Solutions

Cisco Systems

Cisco IP Phone Services Configuration

Add a New IP Phone Service
Back to Find/List IP Phone Services
Dependency Records

IP Phone Service: ICD

Status: Insert completed

[Update]   [Delete]   [Update Subscriptions]

Service Information

Service Name*	Service Description
ICD	

Service URL*

http://10.2.200.21:6293/ipphone/jsp/sciphonexml/IPAgentInitial.jsp

Service Parameter Information

Parameters

[New]

[Edit]

[Delete]

Any device that will be used by an ICD Agent needs to subscribe to the ICD Service. This normally includes 79XX phones but could also include softphones and Device Profiles that are used by the Extension mobility service.

Note: You must have changed the Services URL to include the ip address of Call Manager to be able to see the ICD Service displayed on the XML Browser of the phone.

ipexpert

Cisco CallManager Administration
For Cisco IP Telephony Solutions

CISCO SYSTEMS

Phone Configuration

Cisco CallManager 3.3 Administration - Subscribe Cisco IP Phone Services for SEP00059A3C7800 - Micro...

Subscribe Cisco IP Phone Services for SEP00059A3C7800

Subscribed Services
<Subscribe a New Service>

Service Subscription: New

Status: Ready

Continue

Select a Service*

ICD

— Not Selected —
ICD

* indicates required item

Note:
If you are using a language other than English for Service Name text, make sure the correct character set (shown below) is selected. Text displays incorrectly if the wrong characterset is selected. (English

Applet RSAspProxyApplet started   Internet

Setting up the Directory

The Call Manager configuration defined in the previous section should take no longer than 15-20 minutes. The CTI Route Points and CTI Ports will not show as 'registered' until the JTAPI subsystem has been configured.

CRA is configured through the Application Administrator web page than can be brought up from the CRA Administrator program from Program Files. The first time you logon to Application Administrator, you will need to use the inbuilt username and password (Administrator / ciscocisco). Note the upper case 'A' in Administrator.

CRA stores all the configuration in the directory- you can either use the inbuilt LDAP Directory (DCDirectory) or a third party directory. In this instance we are setting up access to the DC Directory.

ipexpert

Once logged in, you will be prompted to enter the ip address and password of the Directory user. The only two fields that will need changing are Directory Host Name and Directory Password.

ipexpert

The IP telephony directory contains a subdirectory that stores applications and Cisco scripts. This subdirectory is called the *repository*. For efficient management of resources, the IP telephony directory server stores each type of configuration as a profile.
The CRA system uses two kinds of profiles:

- Configuration profile—Stores all the configuration for a specific CRA server, such as groups, triggers, and subsystems. A configuration profile can be used by only one CRA server at a time.
- Repository profile—Stores information common to multiple CRA servers, such as scripts and application configuration. A repository profile can be shared by multiple CRA servers.

Create a repository profile (call it anything you like) and ensure the 'default repository' option is selected to ensure that the configuration and repository are stored in the same profile.

The next page will prompt you to select a user from the directory to which you want to assign administrator privileges. Note that we logged in using the inbuilt Administrator account the first time we logged into AppAdmin- in this example admin rights are being assigned to the user 'crsadmin'.

ipexpert

User Maintenance

Customer Response Applications Administration
For Cisco IP Telephony Solutions

Cisco Systems

Please add or remove the Administrators or Supervisors from the following list:

CRA Administrator / Supervisor*

crsadmin(Administrator)

CMUsers

Group Administrator

* indicates required item

[< Back] [Finish]

ipexpert

Wait a few moments before you see the following page- it is very important to close this web browser before continuing.

Directory Setup

Configuration Setup - Step 6 of 6

User Configuration done.

Media setup done.

ICD setup done.

Nuance ASR setup done.

Nuance TTS setup done.

Workflow setup done.

Configuration info is saved. The changes take effect when the engine is started next time.

Please close your web browser now!
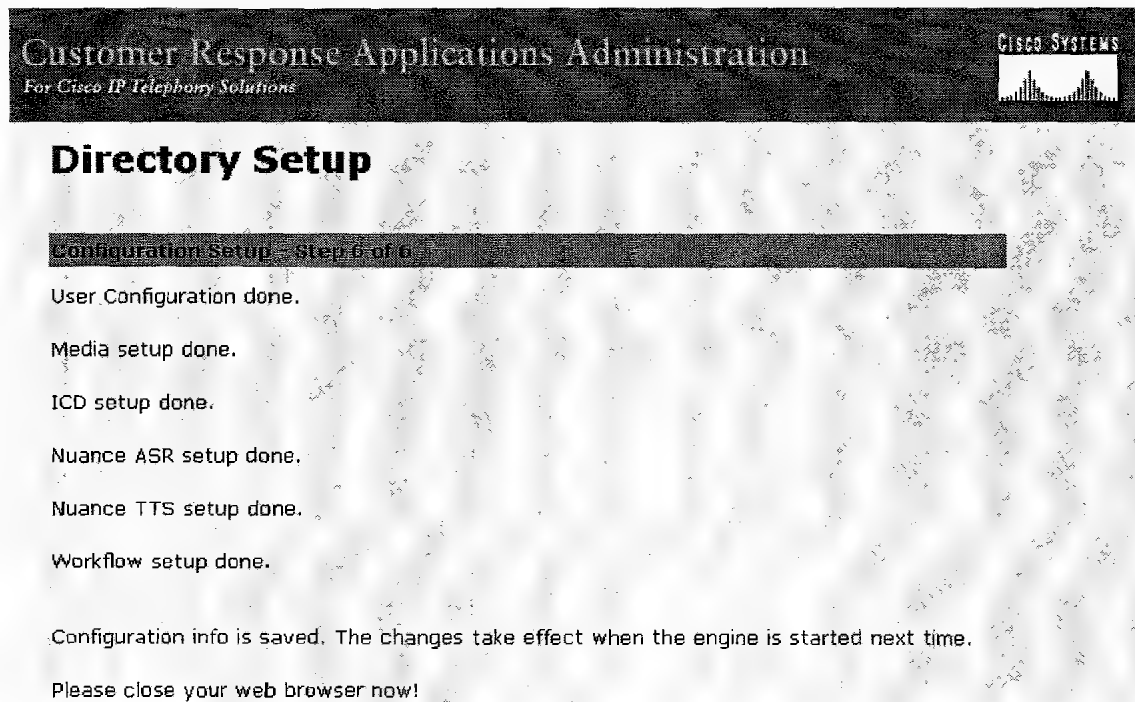
Re-open the AppAdmin web browser and log in using the 'crsuser' account.

Provision the JTAPI Subsystem

The Java Telephony Application Programming Interface (JTAPI) subsystem is the subsystem of the CRA Engine that sends and receives call-related messages from the Cisco CallManager CTI Manager. To enable your CRA server to handle IP telephony requests, you will need to provision the JTAPI subsystem.

To provision the JTAPI subsystem, perform the following tasks:

- Configure a **JTAPI Provider**. You must specify the server on which the Cisco Media Convergence server (Cisco MCS) is running Cisco CallManager CTI Manager, and provide the user ID and password when you configured the JTAPI user in Cisco CallManager.
- Provision **JTAPI call control groups**. JTAPI call control groups pool together a series of CTI ports, which the system then uses to serve calls as they arrive at the CRA server.
- Provision a **JTAPI trigger**.JTAPI triggers invoke application scripts in response to incoming contacts. This can be done when we create the application later on.

ipexpert

To configure the JTAPI Provider go to Application **Administrator-subsystems-JTAPI** enter the ip address of the server running CTI Manager. Also enter the name/password of the JTAPI user you created when configuring Call Manager.
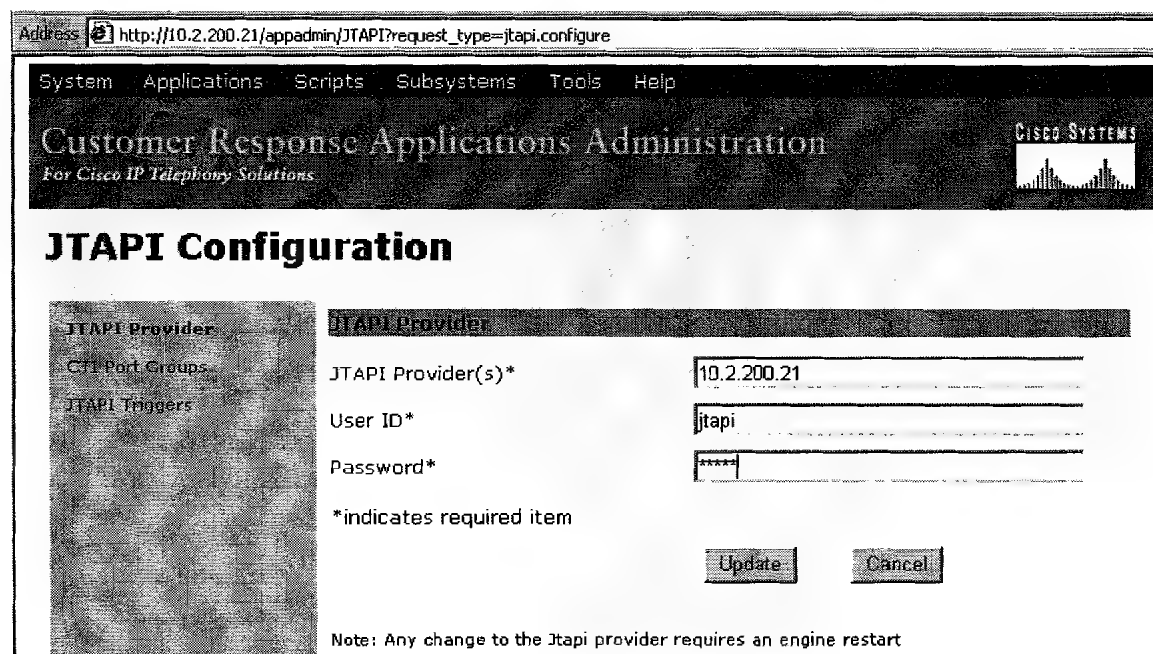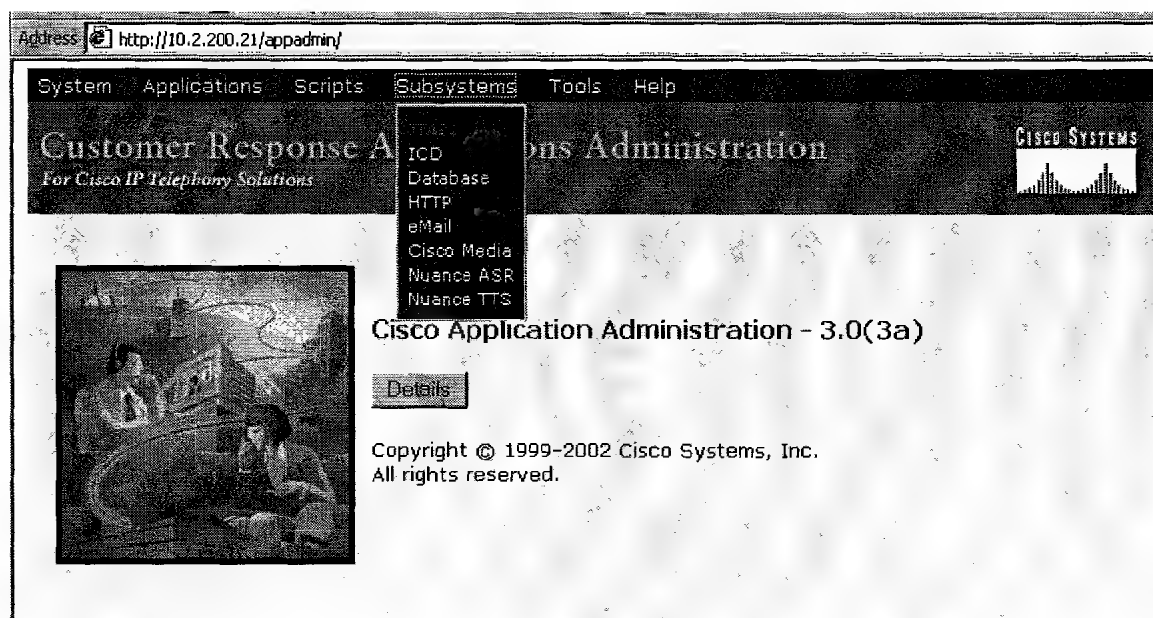
After the JTAPI Provider has been configured you will be prompted to restart the CRA Engine. At this stage the JTAPI Subsystem will not be running- the CTI Port Groups need to be configured first.

The CRA system uses JTAPI call control groups to pool together a series of CTI ports, which the system uses to serve calls as they arrive at the CRA server. You can create

multiple JTAPI call control groups in order to share and limit the resources to be used by specific applications. In this example one CTI Port Group is configured (all 4 CTI Ports are in the same group). Return to the Engine and check that the JTAPI Subsystem is '**In Service**'.

Engine

Engine Status

System	Status
Engine	Running
Subsystems	**Status**
JTAPI Subsystem	IN_SERVICE
Database Subsystem	OUT_OF_SERVICE
Nuance ASR Subsystem	OUT_OF_SERVICE
CMT Subsystem	IN_SERVICE
HTTP Subsystem	IN_SERVICE
Application Subsystem	IN_SERVICE
Voice Browser Subsystem	IN_SERVICE
Enterprise Server Data Subsystem	IN_SERVICE
eMail Subsystem	OUT_OF_SERVICE
RM-CM Subsystem	OUT_OF_SERVICE
Core Reporting Subsystem	IN_SERVICE
Nuance TTS Subsystem	OUT_OF_SERVICE

The Cisco Media subsystem is a subsystem of the CRA Engine. The Cisco Media subsystem manages the CMT (Cisco Media Termination) media resource, which collects Dual Tone Multi-Frequency (DTMF) data from callers.

ipexpert

The Cisco Media subsystem uses *dialog groups* to organize and share resources among applications. A dialog group is a pool of *dialog channels* in which each channel is used to perform *dialog interactions* with a caller, during which the caller responds to automated prompts by pressing buttons on a touch-tone phone.

Configure Cisco Media from Subsystem-Media. In this example only a single Cisco Media Group is configured- the maximum amount of channels available for the group, based on your licensing agreement.

Cisco Media Terminal Dialog Group Configuration

Group ID* 0

Description

Number Of Licensed IVR Ports : 10

Maximum Number Of Channels* 4

*indicates required item

Add Cancel

Provision the ICD Subsystem

Once the Call Manager has been configured for CRA, the Directory has been setup and the JTAPI Subsystem has been configured and is 'IN-SERVICE' you can now configure the ICD Subsystem.

The Resource Manager (RM) of the Cisco IP ICD system is a component of the ICD subsystem. It uses a Cisco CallManager JTAPI (Java Telephony Application Programming Interface) user (called a JTAPI provider) for monitoring agent phones, controlling agent states, and routing and queuing calls.

From Subsystems-ICD configure the ip address of the server running CTI Manager (usually the Publisher Call Manager). Also enter username/password of the RMUSER created in the first section.

ICD Configuration

After adding the RMUSER you will be prompted to restart the Engine. When the Engine has been restarted check the RM-CM Subsystem has started successfully.

Engine

Engine Status

System	Status
Engine	Running

Subsystems	Status
JTAPI Subsystem	IN_SERVICE
Database Subsystem	OUT_OF_SERVICE
Nuance ASR Subsystem	OUT_OF_SERVICE
CMT Subsystem	IN_SERVICE
HTTP Subsystem	IN_SERVICE
Application Subsystem	IN_SERVICE
Voice Browser Subsystem	IN_SERVICE
Enterprise Server Data Subsystem	INITIALIZING
eMail Subsystem	OUT_OF_SERVICE
RM-CM Subsystem	IN_SERVICE
Core Reporting Subsystem	IN_SERVICE
Nuance TTS Subsystem	OUT_OF_SERVICE

In the Bootcamp labs you are asked to create two applications- auto-attendant and ICD. Create from **Applications-Configure Applications**.

Use the default scripts to ensure to verify successful configuration before embarking in custom scripting.

The default Auto-Attendant script is 'aa.aef' and like all other scripts are stored in the C-Program Files-wfavvid directory. Notice max sessions is set to '2'- this is just a sensible split since there are 4 CTI Ports and so it is logical to set each application to have a maximum of 2 calls.

Cisco Script Application

Back to Application List

Triggers can be added after application is created

Name *	AA
Description	
ID*	0
Maximum Number of Sessions*	2
Enabled*	⊙ Yes ○ No
Script*	aa.aef [Edit]
welcomePrompt*	AAWelcome.wav [Edit]
MaxRetry*	3
operExtn*	0
Default Script	- System Default - [Edit]

*indicates required item

[Add] [Cancel]

Once the Application has been configured the JTAPI Trigger must be configured from the hyperlink on the left hand side of the page. Choose the appropriate CTI Route Point and select the correct Call Control and Cisco Media Group (in this case we only configured one of each). Max sessions is 2 for the same reasons as in the previous step.

ipexpert

Cisco Script Application

Back to Applicat

Add new trigger   Name   AA

JTAPI Trigger Configuration

CTI Route Point
Directory Number*   1/10(RPAA)

Language*   - System Default -   Edit

Application Name   AA

Maximum Number Of
sessions*   2

Idle Timeout (in ms)*   5000

Enabled*   ● Yes ○ No

Call Control Group*   JTAPI Group #0(0)

Primary Dialog Group*   Cisco Media Group #0(0)

Secondary Dialog Group   - None -

*indicates required item

Add   Cancel

ipexpert

Create the ICD Application and trigger using the same method. The default ICD script is 'icd.aef'. At this stage don't worry too much about the CSQ field- this will be explained in more detail in the next section.

Cisco Script Application

Triggers can be added after application is created

Name *	ICD
Description	
ID*	1
Maximum Number of Sessions*	2
Enabled*	⦿ Yes ○ No
Script*	icd.aef ▾ Edit
CSQ*	0
DelayWhileQueued*	30
WelcomePrompt*	ICDWelcome.wav ▾ Edit 🔊
QueuePrompt*	ICDQueue.wav ▾ Edit 🔊
Default Script	- System Default - ▾ Edit

*indicates required item

Add   Cancel

At this stage it is worth making a test call to both Triggers- in both cases you should be able to hear the appropriate recorded message. Call from HQ and BR1. If the call works for HQ but NOT for BR1 then this is a sure sign that the transcoder in the HQ Device Pool may not be working.

Creating Custom Scripts

Cisco ICD uses Contact Service Queues (CSQs) as the entities that route calls to your resources (agents). Each CSQ controls incoming Cisco IP ICD calls and determines where an incoming call is placed in the queue and to which agent the call is sent.

Each CSQ selects resources from an associated resource pool (or just the actual resources) that you define. When an agent becomes available to take a call, the system chooses a queued call from one of the CSQs whose resource pool includes the agent, and routes that call to that agent.

To provision any version of Cisco IP ICD, you will need to perform the following tasks:

- Configure users in Cisco CallManager with ICD Extension (this may have been done earlier).
- Provision the RM JTAPI provider (this has been done earlier).
- Provision Resource Groups OR Skills. *Resource groups* are collections of agents that your CSQ uses to handle incoming Cisco IP ICD calls. *Skills* are customer-definable labels assigned to agents. The two IP ICD Enhanced packages can route incoming calls to agents who have the necessary skill or sets of skill to handle the call.
- Provision Resources. Agents that answer calls are also called *resources*. Resources can either be assigned to Resource Groups or Skills directly.Provision CSQs. After you assign an agent to a resource group, or assign skills to an agent, you need to configure the agent for the CSQ to which the agent will be assigned.

In the example given Skills based routing is used and not Resource Groups.

From **Subsystems-ICD** click on the 'Skills' and 'Add a new skill' hyperlink.
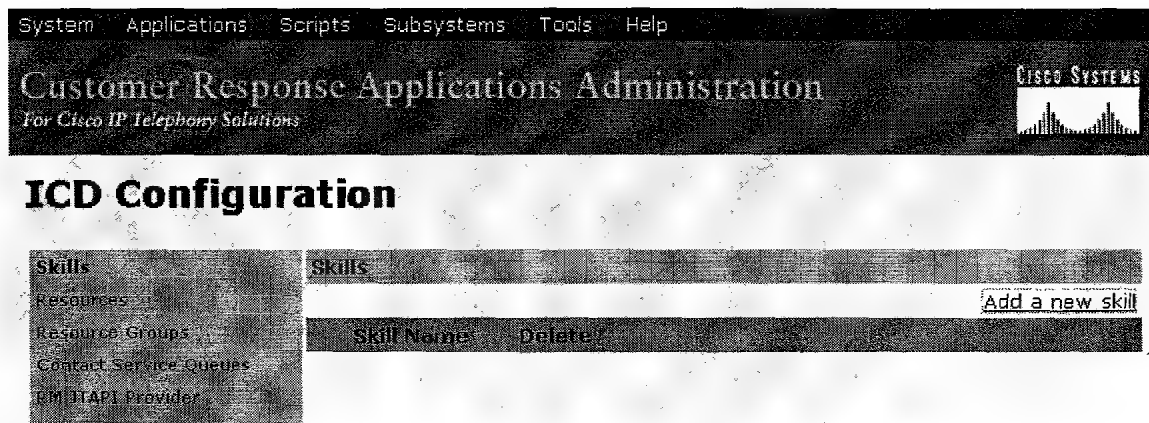
In this example we will have two CSQ- sales and support.

ipexpert

Repeat the procedure to add the support skill.

ICD Configuration

Skills	Skills	
Resources		Add a new skill
Resource Groups	**Skill Name ∇ △**	**Delete**
Contact Service Queues	🔾 sales	🗑
RM JTAPI Provider	🔾 support	🗑

Assign resources to skills. Click on the **'Resources'** option and you should see all users that are assigned Devices with ICD Extensions.

ICD Configuration

Skills	Resources		
Resources	**Resource Name ∇ △**	**Resource Group ∇ △**	**ICD Extension ∇ △**
Resource Groups	🔾 agent1		1000
Contact Service Queues	🔾 agent2		1002
RM JTAPI Provider			

In this instance we are assigning the user 'agent1' to the sales skill and user 'agent2' to the support skill.

ICD Configuration

Skills	Resource Configuration
Resources	Open Printable Report of this Resource configuration
Resource Groups	Resource Name agent1
Contact Service Queues	Resource ID agent1
RM JTAPI Provider	ICD Extension 1000

Resource Group   -Not Selected-   ▼

Automatic Available*   ⦿ Enabled ○ Disabled

Assigned Skills   Unassigned Skills

sales(5)	◀	support
	▶	

Competence Level 5 ▼ (1 – Beginner, 10 – Expert)

* indicates required item

| Update | Cancel |

ICD Configuration

Resource Configuration

Open Printable Report of this Resource configuration

Resource Name   agent2

Resource ID   agent2

ICD Extension   1002

Resource Group   -Not Selected-

Automatic Available*   ⦿ Enabled ○ Disabled

Assigned Skills   Unassigned Skills

support(5)   sales

Competence Level [5 ▼] (1 – Beginner, 10 – Expert)

* indicates required item

[Update] [Cancel]

In this example we will create two CSQ- sales and support. The sales skill will be assigned to the sales CSQ and support skill will be assigned to the support CSQ.

From Contact Service Queue click the '**Add a new Contact Service Queue**'.

ICD Configuration

Contact Service Queues

Add a new Contact Service Queue

Name	Contact Queuing Criteria	Resource Pool Selection Model	Resource Pool	Delete

ipexpert

Create the CSQ with an appropriate name such as sales or salescsq. Note that we are
routing to lines based on Resource Skills and not Resource Groups.

ICD Configuration

Skills	Contact Service Queue Configuration
Resources	Contact Service Queue Name* — sales
Resource Groups	Contact Queuing Criteria — FIFO
Contact Service Queues	Automatic Work* — ○ Enabled ⊙ Disabled
RM JTAPI Provider	Resource Pool Selection Model* — Resource Skills
	Service Level* — 5
	Service Level Percentage* — 70

* indicates required item

[Next]   [Cancel]

ipexpert

Assign the appropriate skill to the CSQ. After clicking on the **'Show Resources'** tab the resources assigned to the skill will display.

ICD Configuration

Skills	**Contact Service Queue Configuration**
Resources	Contact Service Queue Name: sales
Resource Groups	Resource Selection Criteria* : Longest Available
Contact Service Queues	Assigned Skills / Unassigned Skills
RM JTAPI Provider	sales(5) / support

Minimum Competence Level [5] (1 - Beginner, 10 - Expert)

[Show Resources]

agent1

* indicates required item

[Update] [Cancel]

Create the support CSQ and assign the support skill in the same way.

ICD Configuration

Skills	**Contact Service Queues**				
Resources				Add a new Contact Service Queue	
Resource Groups	**Name**	**Contact Resource Queuing Pool Criteria**	**Resource Pool Selection Model**	**Delete**	
Contact Service Queues					
RM JTAPI Provider					
	sales	FIFO	Longest Available	sales(5)	🗑
	support	FIFO	Longest Available	support(5)	🗑

At this stage you are ready to develop your custom script using the CRA Editor.

ipexpert

CRA Editor

The Cisco CRA Editor is a visual programming environment for creating telephony and multimedia application scripts. You can use the CRA Editor on any computer that has access to the CRA server.

The CRA Editor simplifies script development by providing blocks of contact-processing . logic in easy-to-use Java-based steps. Each step has its own unique capabilities, from simple increment to generating and playing out prompts, obtaining user input, queuing calls, or performing complex database operations.

Although the steps are written in Java, you do not need to understand Java programming to build a CRA script. You can assemble a script by dragging step icons from a palette on the left pane of the workspace to the design area on the right pane of the workspace.

The CRA Editor supplies the code required to connect the steps; you provide the variable definitions and other parameters. You can validate and debug the completed script directly in the CRA Editor.

There are 3 sections of the CRA Editor:

- Pallette Pane- this contains all the steps available for developing scripts.
- Design Pane- this is where the sequence of the steps within the script is defined.
- Variable Pane- this is where the variables are stored. Variables store data while a script executes.

ipexpert

```
Cisco Customer Response Application Editor - [C:\Program Files\WfAvvid\icd.aef]
  File  Edit  Tools  Debug  Window  Settings  Help
```

```
⊞ General                    Start
⊞ Session                    Accept (contact: --Triggering Contact--)
⊞ Contact                    Play Prompt (contact: --Triggering Contact--, prompt: WelcomePrompt)
⊞ Call Contact               ⊞ Select Resource (contact: --Triggering Contact--, CSQ: CSQ)
⊞ eMail Contact              End
⊞ Http Contact
⊞ Media
⊞ User
⊞ Prompt
⊞ Grammar
⊞ Document
⊞ Database
⊞ ICD
⊞ JAVA
```

Name	Type	Value	Attrib
resourceID	String		
CSQ	String		Para...
DelayWhileQueued	Integer	30	Para...
WelcomePrompt	Prompt	P[ICDWelcome....	Para...
QueuePrompt	Prompt	P[ICDQueue.wav]	Para...

A commonly asked question is the Parameter option when defining a variable. You can declare variables as parameters by checking the Parameter check box in the Edit Variables dialog box.

This feature allows you to set the value for a parameter in the CRA Administration web interface. Because the value is initialized at configuration time for the script that uses it, you can change the value without having to edit the script in the CRA Editor. Such a variable is called an *exported* variable.

For example, when you create an application of type "Cisco Script Application", you can choose either a script or a default script. The system then refreshes the web page and provides a list of the parameters with their default or current values. You can modify the values in this list.

The variable types that Cisco CRA 3.0 supports for parameters include number, string, Boolean, document, prompt, and grammars.

ipexpert

Once the script has been configured and validated, it needs to be added to the repository.

From the CRA Administration menu bar, choose **Scripts > Manage Scripts**. Select the script from the wfavvid directory and click '**Upload to Repository**'.
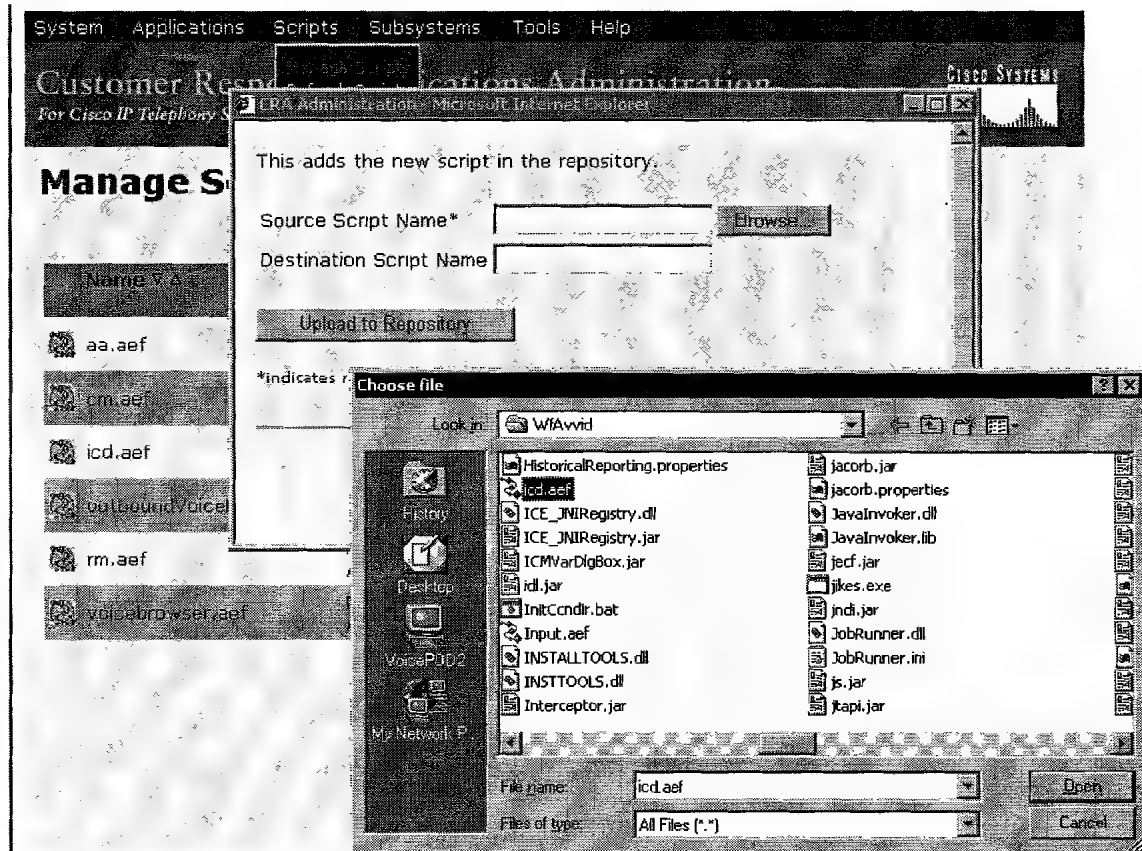
A window appears, informing you that the script was successfully uploaded.

Script uploaded successfully.

FileName –C:\Program
Files\wfavvid\tomcat_appadmin\webapps\appadmin\upload\broadcast.aef
File Size – 24544 bytes

Do you want to refresh the Script?

Return to Script Management

Perform one of the following tasks:

- If the script is already being used by a CRA application, click the **Do You Want to Refresh the Script?** hyperlink, and then click **Yes** when the system prompts you to confirm the operation. When you refresh a script, you copy it from the repository to the CRA server, in order to make it available to the Cisco script application. (If the script does not already exist on the server, you do not need to refresh it.)
- If the script does not already exist on the CRA server, click the **Return to Script Management** hyperlink. The Successful Script Upload window closes.

QoS

Quality of Service needs to be configured at the HQ switch, WAN routers and Branch switches.

QoS is Needed to Minimize Packet Loss, Delay and Delay Variation
Where QoS is Needed

Central Campus

Remote Branch

WAN

QoS - Campus Access	QoS - Campus Distrib	QoS - WAN	QoS - Branch
Speed and Duplex settings	Layer 3 Policing	Low-Latency Queuing	Classification and Trust Boundaries on IP Phone, Access
Classification/Trust on IP Phone and Access switch	Multiple queues on all ports; Priority Queuing for VoIP	Link Fragmentation and Interleave	Layer switch and router
Multiple queues on IP Phone and Access ports	WRED within Data queue for Congestion Management	Bandwidth Provisioning	Multiple queues on IP Phone and all Access ports
		Admission Control	

Branch QoS
General Guidelines

All incoming voice from PSTN classified as DSCP=EF within the dial-peer

PSTN

WAN

All incoming VoIP from WAN should already be tagged as DSCP=EF/AF31 (Video=AF41) at the central site

Use LLQ/LFI on Branch router WAN. Use mod-CLI for L3 -> L2 classification on the Ethernet interface

Branch Ethernet switches with multiple queuing based on CoS on all interfaces

Classify all IP Phone VoIP trafic CoS=5 All Data traffic CoS=0

ipexpert

6500 CatOS

Connecting the IP Phone
Multiple Cables

ports 6/1-24 - data untrusted (Default)

Catalyst 6000

ports 6/25-48 - voice trust dot1p
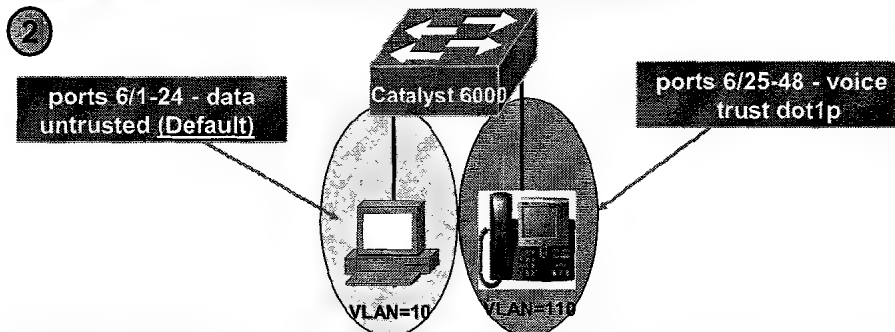
VLAN=10   VLAN=110

```
cat6k-access> (enable) set vlan 10 6/1-24
cat6k-access> (enable) set vlan 110 6/25-48
cat6k-access> (enable) set port auxialaryvlan 6/25-48 dot1p
cat6k-access> (enable) set port host 6/25-48
cat6k-access> (enable) set port qos 6/25-48 trust-ext untrusted
cat6k-access> (enable) set port qos 6/25-48 trust trust-cos
```
14

Port Trust on the Catalyst 6000

set port qos <mod/port> trust-ext _____

Only applies to port trust on the IP Phone PC Ethernet port

Un-related to actual cat6k port trust

set port qos <mod/port> trust ____

Applies to the actual cat6k port trust rules

untrusted (default), trust-cos, trust-ipprec, trust-dscp

10/100 cards require an additional ACL to actually enable port trust:

```
cat6k-access> (enable) set qos enable
cat6k-access> (enable) set port qos 5/1-48 trust trust-cos
cat6k-access> (enable) set port qos 5/1-48 vlan-based
cat6k-access> (enable) set qos acl ip ACL_IP-PHONE dscp 26 tcp
any any eq 2000
cat6k-access> (enable) set qos acl ip ACL_IP-PHONES trust-cos ip
any any
cat6k-access> (enable) commit qos acl all
cat6k-access> (enable) set qos acl map ACL_IP-PHONES 110
```

ipexpert

======================================

Enabling QoS
======================================

set qos enable

======================================

Configuring Transmit Queues
======================================

All VoIP (CoS of 5) traffic will be placed into the egress interface priority queue on 1p2q2t interfaces and queue 2 on 2q2t interfaces as soon as you enable QoS. However, you must perform the additional step of configuring the Catalyst 6500 CoS queue admission rules to ensure that traffic with a CoS of 3 (VoIP control) is placed into the second queue.

Step 1 Place CoS of 3 in queue 2 for 1p2q2t.
Step 2 Place CoS of 3 in queue 2 for 2q2t.

```
set qos map 2q2t tx 2 1 cos 3
set qos map 1p2q2t tx 2 1 cos 3
```

======================================

Modify the CoS-to-DSCP mappings.
======================================

```
set qos cos-dscp-map 0 8 16 26 34 46 48 56
```

======================================

Trust CoS on 10/100 IP Phone ports and make QoS VLAN-based
======================================

```
set port qos <mod/port> vlan-based
set port qos <mod/port> trust-ext untrusted
set port qos <mod/port> trust trust-cos
set qos acl ip ACL_IP-PHONES trust-cos ip any any
commit qos acl ACL_IP-PHONES
set qos acl map ACL_IP-PHONES <Auxiliary VLAN>
```

NOTE: On non-GigabitEthernet linecards that use 2Q2T Transmit Queuing and 1Q4T Receive queuing (such as the WS-X6248-RJ-xx and WS-X6348-RJ-xx linecards), a hardware limitation prevents the proper functioning of port-based trust (which affects trust-cos, trust-ipprec, and trust-dscp). On such linecards, a workaround ACL can be used to achieve trust-functionality for trust-cos, trust-ipprec, and trust-dscp. The trust-cos example is shown above.

===

Set up Policer

===

QoS policing on a network determines whether network traffic is within a specified profile (contract). This may cause out-of-profile traffic to drop or to be marked down to another differentiated services code point (DSCP) value to enforce a contracted service level.

Do not confuse traffic policing with traffic shaping. Both ensure that traffic stays within the profile (contract). You do not buffer out-of-profile packets when you police traffic. Therefore, you do not affect transmission delay. You either drop the traffic or mark it with a lower QoS level (DSCP markdown). In contrast, with traffic shaping, you buffer out-of-profile traffic and smooth the traffic bursts. This affects the delay and delay variation. You can only apply traffic shaping on an outbound interface. You can apply policing on both inbound and outbound interfaces.

The Catalyst 6500/6000 Policy Feature Card (PFC) and PFC2 only support ingress policing. The PFC3 supports both ingress and egress policing.

To set up policing, you define the policers and apply them to ports (port-based QoS) or to VLANs (VLAN-based QoS). Each policer defines a name, type, rate, burst, and actions for in-profile and out-of-profile traffic. Policers on Supervisor Engine II also support excess rate parameters. There are two types of policers: microflow and aggregate.

- Microflow—police traffic for each applied port/VLAN separately on a per-flow basis.
- Aggregate—police traffic across all of the applied ports/VLANs.

Each policer can be applied to several ports or VLANs. The flow is defined using these parameters:

- source IP address
- destination IP address
- Layer 4 protocol (such as User Datagram Protocol [UDP])
- source port number
- destination port number

The policer can do one of two things to an out-of-profile packet:

- drop the packet (the drop parameter in the configuration)
- mark the packet to a lower DSCP (the policed-dscp parameter in the configuration)

To mark down the packet, you must modify the policed DSCP map. The policed DSCP is set by default to remark the packet to the same DSCP. (No mark down occurs.)

In the following example we mark down control traffic to from DSCP 26 to DSCP 10.

```
set qos policed-con-map 26:10
set qos policer aggregate remark-sccp rate 64 burst 32 policed-dscp
```

==

Server Classification and Policing

==

For Server classification either trust dscp or manually mark control traffic originating from the Call Manager to DSCP 26. Traffic types are SCCP, H245, H225/RAS, MGCP. In the example we are applying the the policing SCCP traffic- the exceed action is to remark to DSCP 10.

```
set port qos <mod/port> port-based
set qos acl ip ACL_SERVER dscp 26 tcp aggregate remark-sccp any range 2000 2002 any
set qos acl ip ACL_SERVER dscp 26 tcp any any  range 11000 11999
set qos acl ip ACL_SERVER dscp 26 tcp any any  eq 1720
set qos acl ip ACL_SERVER dscp 26 udp any eq 2427 any
set qos acl ip ACL_SERVER dscp 26 tcp any eq 2428 any
commit qos acl ACL_SERVER
set qos acl map ACL_SERVER <mod/port>
```

==

Trust DSCP for traffic from the WAN router

==

```
cat6k-distrib> (enable) set port qos <mod/port> port-based
cat6k-distrib> (enable) set port qos <mod/port> trust trust-dscp
cat6k-distrib> (enable) set qos acl ip ACL_TRUST-WAN trust-dscp ip any any
cat6k-distrib> (enable) commit qos acl ACL_TRUST-WAN
cat6k-distrib> (enable) set qos acl map ACL_TRUST-WAN <mod/port>
```

3550

For the Catalyst 3550, QoS requires the following changes to the access switch configuration:

1. Enable QoS globally.

```
3550G-Access(config)#mls qos
```

2. Modify the default CoS-to-DSCP mapping table.

ipexpert

The default CoS-to-DSCP mapping is as follows:

```
3550G-Access#show mls qos maps
Cos-dscp map:
cos: 0 1 2 3 4 5 6 7
--------------------------------
dscp: 0 8 16 24 32 40 48 56
```

Change the default mapping table so that CoS 3 = AF31, CoS 4 = AF41, and CoS 5 = EF. Remember to use the decimal equivalents.

```
3550G-Access(config)#mls qos map cos-dscp 0 8 16 26 34 46 48 56
```

3. Turn on priority queuing and move CoS 5 traffic to the priority queue

Specify the interface range.

```
3550G-Access(config)#interface range f0/1 - 3
Step 2 Specify the priority queue.
3550G-Access(config-if-range)#priority-queue out
Step 3 Move the CoS 5 traffic to queue 4, which is the priority queue for the Catalyst
3500 family.
3550G-Access(config-if-range)#wrr-queue cos-map 4 5
```

4. Enable QoS features when classification is required.

```
interface range FastE 0/1 - 3
mls qos trust cos
switchport priority extend cos 0
```

5. Enable QoS features for the uplink to distribution.

```
mls qos map cos-dscp 0 8 16 26 34 46 48 56
```

```
interface FastEthernet0/24
switchport trunk encapsulation dot1q
switchport mode trunk
duplex full
mls qos trust cos
priority-queue out
wrr-queue cos-map 4 5
```

WAN QOS: ATM to Frame relay Interworking

QoS in the WAN
General Guidelines

* **Properly Provision the WAN Bandwidth**
* **Use cRTP where possible**
* **Call Admission Control is a requirement where VoIP calls can over-subscribe the provisioned BW**
* **Use LLQ anytime VoIP over the WAN is involved**
* **Use LFI techniques for all links below 768Kbps**
* **Traffic Shaping is a requirement for Frame-Relay/ATM environments**
* **TX-Ring sizes may require modifications**

33

LLQ Logic Tree
Queuing

Layer 3 Queuing Subsystem   Layer 2 Queuing Subsystem

Low Latency Queuing   Link Fragmentation & Interleave

PQ Voice   Police

Interleave   TX Ring

Class = X

Packets In   Class = Y   CBWFQ   Fragment   Packets Out

WFQ   Default

34

ipexpert
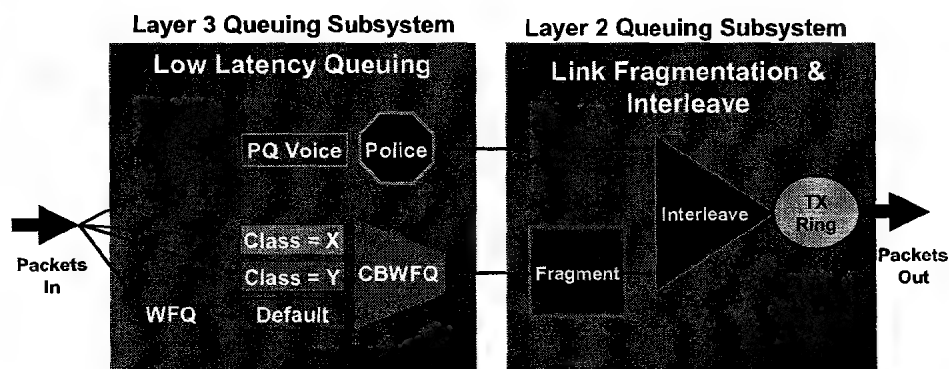
Traffic Shaping—Why?
Misc. VoIP QoS Tools

Result:
Buffering which will Cause Delay
and Eventually Dropped Packets

Remote Sites

128 kbps
256 kbps
512 kbps
768 kbps
Frame Relay-ATM
T1
T1
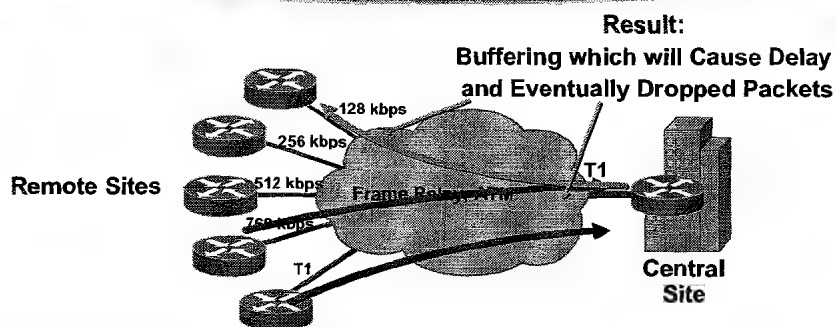
Central
Site

1. Central to Remote Site Speed Mismatch
2. To Avoid Remote to Central Site Over-Subscription
3. To Prohibit Bursting above Committed Rate
   What Are You Guaranteed above You Committed Rate?

Link Speeds

In the context of WAN links there are two groupings (based on the Qos SRND Aug 2002) of link speeds.

- Slow: Links equal to or slower than 768Kbps.
- Fast: Links faster than 768Kbps.

It is important to remember this cut-off since LFI is recommended for slower speed links.

=================================

Create Policies and LLQ for number of calls

=================================

Create class maps which rely on Switch classification working correctly. These class-maps can be used for multiple policy-maps.

```
class-map match-all VOICE-CONTROL
  match ip dscp af31
class-map match-all VOICE
  match ip dscp ef
```

Create policy-maps- beware that if you specify the amount of bandwidth to reserve as a percentage in the priority queue, then you must also specify the amount of bandwidth reserved for signaling in the CFWFQ must also be specified as a percentage.

ipexpert

```
policy-map LLQ
 class VOICE
  priority xx (or priority percent xx)
 class VOICE-CONTROL
  bandwidth xx (or bandwidth percent xx)
class class-default
 fair-queue
```

High Speed ATM Configuration

Use the Class-maps and Policy-maps mentioned above- LFI is not required for links faster than 768Kbps. Bind the MQC policy to the PVC using the "service-policy" command.

==================================

Apply LLQ to PVC
==================================

```
interface ATM0/IMA0.101 point-to-point
 description BRANCH 1
 ip pim dense-mode
 bandwidth 1544
 pvc br1pvc 1/1
  vbr-nrt 1544 1544
  broadcast
  service-policy output LLQ
 encapsulation aal5snap
```

Bandwidth/Max-Reserved-Bandwidth

You will notice a "bandwidth" statement in the ATM interface. This is used when the router is calculating the amount of reservable bandwidth for the MQC policy. By default only 75% of the bandwidth is reservable (configurable through the "max-reserved-bandwidth" command).

Available bandwidth = (interface_bandwidth * max-reserved-bandwidth/100)

The reason you would need to specify the bandwidth value is when the provisioned rate of the interface does not match the interface bandwidth command. For example, suppose you have a 1Mbps circuit you are leasing that is dropped off as FastEthernet. Although the interface bandwidth is 100Mbps, it would not make sense to calculate a QoS policy on 100Mbps, as the upstream provider is policing at 1Mbps. Therefore the "bandwidth" value should be adjusted to 1Mbps.

ipexpert

High Speed Frame-Relay Configuration

For the High Speed Frame-Relay, enable Frame Relay Traffic shaping- the parameters are defined in the map-class command. **CIR** should be set to 95% of the link speed, **MINCIR** should be set to CIR, **BC** should be set to CIR/100 and **BE** should be set to 0.

Define Frame Relay Traffic Shaping Parameters

```
map-class frame-relay FRTS-1544
frame-relay cir 1466800
frame-relay bc 14668
frame-relay be 0
frame-relay mincir 1466800
```

Apply map class to DLCI and enable Frame Relay Traffic shaping

Enable traffic shaping on the main interface and bind the map-class to the DLCI.

```
interface Serial0/3/0

frame-relay traffic-shaping

interface Serial0/3/0.101 point-to-point

bandwidth 1544
frame-relay interface-dlci 101
class FRTS-1544
```

Apply LLQ to Map Class

Apply the MQC policy to the map-class- a common mistake is to bind it to the Serial interface.

```
map-class frame-relay FRTS-1544
frame-relay cir 1466800
frame relay bc 14668
frame relay be 0
frame-relay mincir 1466800
service-policy output LLQ
```

ipexpert

Slow Speed ATM Configuration

MLP LFI

Link Fragmentation and Interleaving tools—With slow-speed WAN circuits, large data packets take an excessively long time to be placed onto the wire. This delay, called *serialization delay*, can easily cause a VoIP packet to exceed its delay and/or jitter threshold. There are two main tools to mitigate serialization delay on slow (768 kbps) links: Multilink PPP Link Fragmentation and Interleaving (MLP LFI) and Frame Relay Fragmentation (FRF.12). For ATM-to-Frame Relay interworking FRF.12 is not supported and MLP LFI is recommended.

Serialization delays are variable because they depend not only on the line rate of the link speed, but also on the size of the packet being serialized. Variable (network) delay also is known as jitter. Because the end-to-end one-way jitter target has been set as 30 ms, the typical per-hop serialization delay target is 10 ms (which allows for up to three intermediate hops per direction of VoIP traffic flow). This 10 ms per-hop target leads to the recommendation that a link fragmentation and interleaving (LFI) tool (either MLP LFI or FRF.12) be enabled on links with speeds at or below 768 kbps (this is because the serialization delay of a maximum-size Ethernet packet—1500 bytes—takes more than 10 ms to serialize at 768 kbps and below). Naturally, LFI tools need to be enabled on both ends of the link.

TX-Ring

Transmit ring (Tx-Ring) tuning—The Tx-Ring is a final interface First-In-First-Out (FIFO) queue that holds frames to be immediately transmitted by the physical interface. The Tx-Ring ensures that a frame is always available when the interface is ready to transmit traffic, so that link utilization is driven to 100 % of capacity. The size of the Tx-Ring is dependant on the hardware, software, Layer 2 media, and queueing algorithm configured on the interface. The Tx-Ring may have to be tuned on certain platforms/interfaces to prevent unnecessary delay/jitter introduced by this final FIFO queue.

For MLP LFI it is recommended to tune the ATM PVC Tx-ring to 3.

======================= ===========

Configuring MLP LFI

==

MLPoATM functionality is enabled through the use of virtual-access interfaces. Virtual-access interfaces are built on demand from virtual-template interfaces and inherit their configuration properties from the virtual templates they are built from. Thus, the IP address, **service-policy** statement, and LFI parameters all are configured on the virtual template. In addition we shall enable MLP, MLP fragmentation and Interleaving.

```
interface ATM0/IMA0.101 point-to-point
no ip address

interface Virtual-Template101
 bandwidth 256
 ip address 10.205.1.1 255.255.255.0
 service-policy output LLQ
 ppp multilink
 ppp multilink fragment delay 10      //This is not always 10ms depending on the speed.
 ppp multilink interleave
```

The next step is to bind the PVC to the Virtual Template.

```
interface ATM0/IMA0.101 point-to-point
 description BRANCH 2
 ip pim dense-mode
 pvc br1pvc-1/1
  vbr-nrt 256 256
  broadcast
  tx-ring-limit 3
 encapsulation aal5snap
 protocol ppp Virtual-Template101
```

Slow Speed Frame Relay Configuration

The same principles as already mentioned in the slow speed ATM configuration are also applied for slow speed Frame Relay. A Virtual-Template is created and the DLCI is bound to the Virtual-Template. All settings such as ip address, ip pim, bandwidth and service policy are moved to the Virtual-Template in order that the Virtual-Access interfaces which bind to the Template are correctly configured.

============== ================

Remove existing interface config and create Virtual Template

============== ================

```
interface Serial0/3/0
 frame-relay traffic-shaping
interface Serial0/3/0.101 point-to-point
 no ip address
 no frame-relay interface-dlci 101     //The dlci is only temporarily being removed.
```

ipexpert

```
=================================
```
Create Virtual Template
```
=================================
```

```
interface Virtual-Template101
 bandwidth 256
 ip address 10.205.1.2 255.255.255.0
 ip pim sparse-dense-mode
 service-policy output pm256k
 ppp multilink
 ppp multilink fragment delay 10
 ppp multilink interleave
```

```
=================================
```
Apply mapping of DLCI to Virtual interface
```
=================================
```

Add the DLCI back in except this time bind to the Virtual Template. Remember to bind to the map-class which defines the FR traffic shaping parameters.

```
interface Serial0/3/0.101 point-to-point
 bandwidth 256
 frame-relay interface-dlci 101 ppp Virtual-Template101
 class FRTS-256kbps
```

```
=================================
```
Verification
```
=================================
```

"show policy-map interface xxx" will display statistics for the LLQ. In the example below we can see that the Virtual-Access shows RTP, Signaling and "other" packets being matched.

```
P4-HQ-RTR#sh policy-map interface
 Virtual-Template1

 Service-policy output: br2

  Service policy content is displayed for cloned interfaces only such as vaccess and sessions.
Virtual-Access4

 Service-policy output: br2

   Class-map: voice (match-all)
    4670 packets, 227460 bytes
    5 minute offered rate 0 bps, drop rate 0 bps
    Match: dscp ef
    Queueing
     Output Queue: Conversation 41
      Bandwidth 33 (%)
```

♣ ipexpert

```
        Bandwidth 42 (kbps) Max Threshold 64 (packets)
        (pkts matched/bytes matched) 0/0
        (depth/total drops/no-buffer drops) 0/0/0

    Class-map: vc (match-all)
      4670 packets, 227460 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: dscp af31
      Queueing
        Output Queue: Conversation 42
        Bandwidth 2 (%)
        Bandwidth 2 (kbps) Max Threshold 64 (packets)
        (pkts matched/bytes matched) 4670/227460
        (depth/total drops/no-buffer drops) 0/0/0

    Class-map: class-default (match-any)
      20915 packets, 3865454 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
      Queueing
        Flow Based Fair Queueing
        Maximum Number of Hashed Queues 32
        (total queued/total drops/no-buffer drops) 0/0/0
```

ipexpert

ATA

To configure the ATA use the web page- the URL is http://<ATA-IP>/dev

To check the IP Address of the ATA
- Hold down the ATA button to get into main menu
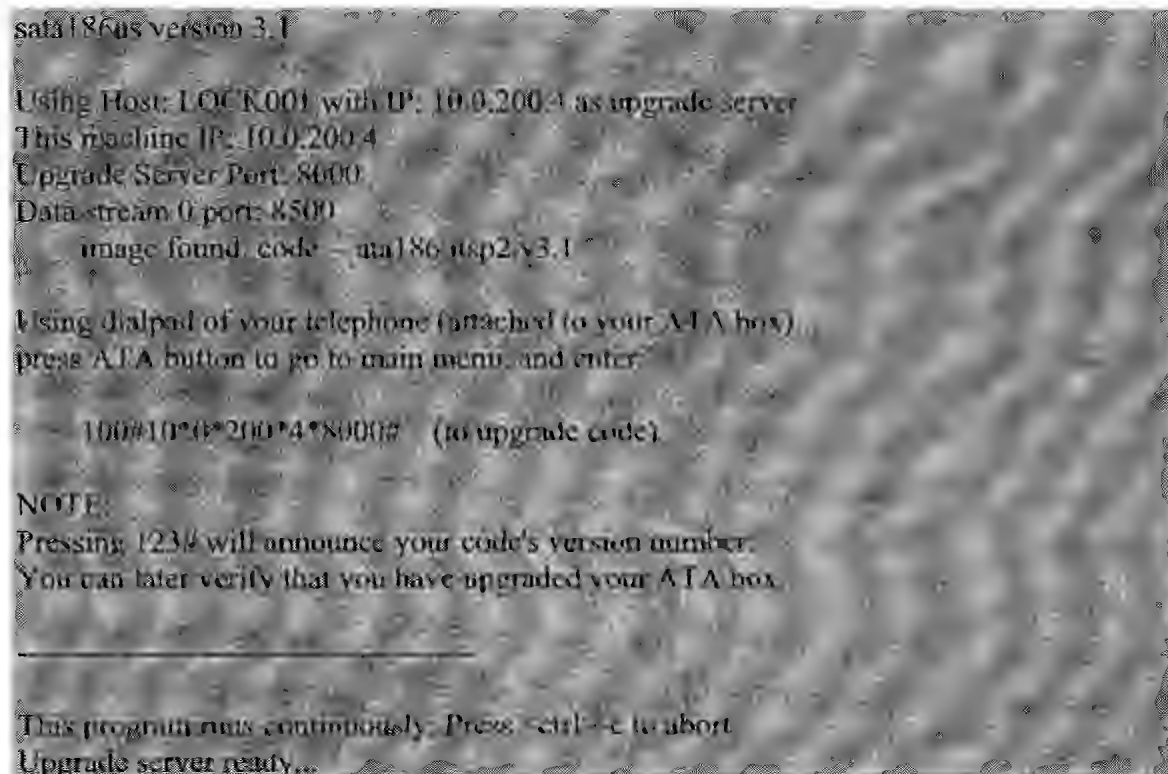- Press 21#

Upgrading to SCCP firmware

The sata186us.exe tool can be used to perform a cross-protocol upgrade to Skinny.

Step (1): Go to the directory where the SCCP firmware load is stored (suffix is .zup)

Step (2): Running the tool

C:\ ata_03_01_01_sccp_040610_1> sata186us -any -d1 ATA030101SCCP040610A.zup

```
sata186us version 3.1

Using Host: LOCK001 with IP: 10.0.200.4 as upgrade server
This machine IP: 10.0.200.4
Upgrade Server Port: 8000
Data stream 0 port: 8500
    image found, code - ata186 usp2 v3.1

Using dialpad of your telephone (attached to your ATA box)
press ATA button to go to main menu, and enter:

    100#10*0*200*4*8000#    (to upgrade code)

NOTE:
Pressing 123# will announce your code's version number.
You can later verify that you have upgraded your ATA box
_____

This program runs continuously. Press <ctrl>-c to abort
Upgrade server ready...
```

ipexpert

Step (3): Instruct ATA to retrieve firmware

- Hold ATA button to go to main menu
- On the dialpad of the telephone enter: 100#10*1*200*21*8000# where 10.2.200.21 is ip address of the server/PC you ran the tool and 8000 is the port number.2
- Refresh ATA Web Page

SCCP Configuration

Most of the settings the ATA uses are defined in Call Manager (e.g. Device Pool/Regio defines codec). There are a few exceptions to this rule such as enabling Fax Passthru and Disabling the second Phone Port (when unused)

SIDx specifies whether to enable the **Phone 1** and/or **Phone 2** ports on the Cisco ATA to register with Cisco Call Manager. (EPIDx is not for SCCP.) SIDx can be one of the following values:

- 0—Disables port; port does not attempt to register with Cisco CallManager
- . or <mac_address>—Uses the default Skinny ID, which is the Cisco ATA MAC address (MAC) for the **Phone** 1 port and MAC[1-5]+01 for the **Phone 2** port. The port attempts to register with Cisco CallManager.
- For example, if the MAC address of the Cisco ATA is 0001.2D01.073D, then SID0 is 0001.2D01.073D and SID1 is 012D.0107.3D01.
- Other values are reserved.

Fax Passthru is discussed in the Fax section.

Upgrading to H323 firmware

The same method used to upgrade to SCCP can be used or when performing a cross-protocol upgrade from SCCP changing Device Defaults in Call Manager would achieve the same thing.

From **System-Device Defaults** change the default ATA-186 firmware with the H323 load name (strip the suffix '.zup') and reload the ATA.

ipexpert
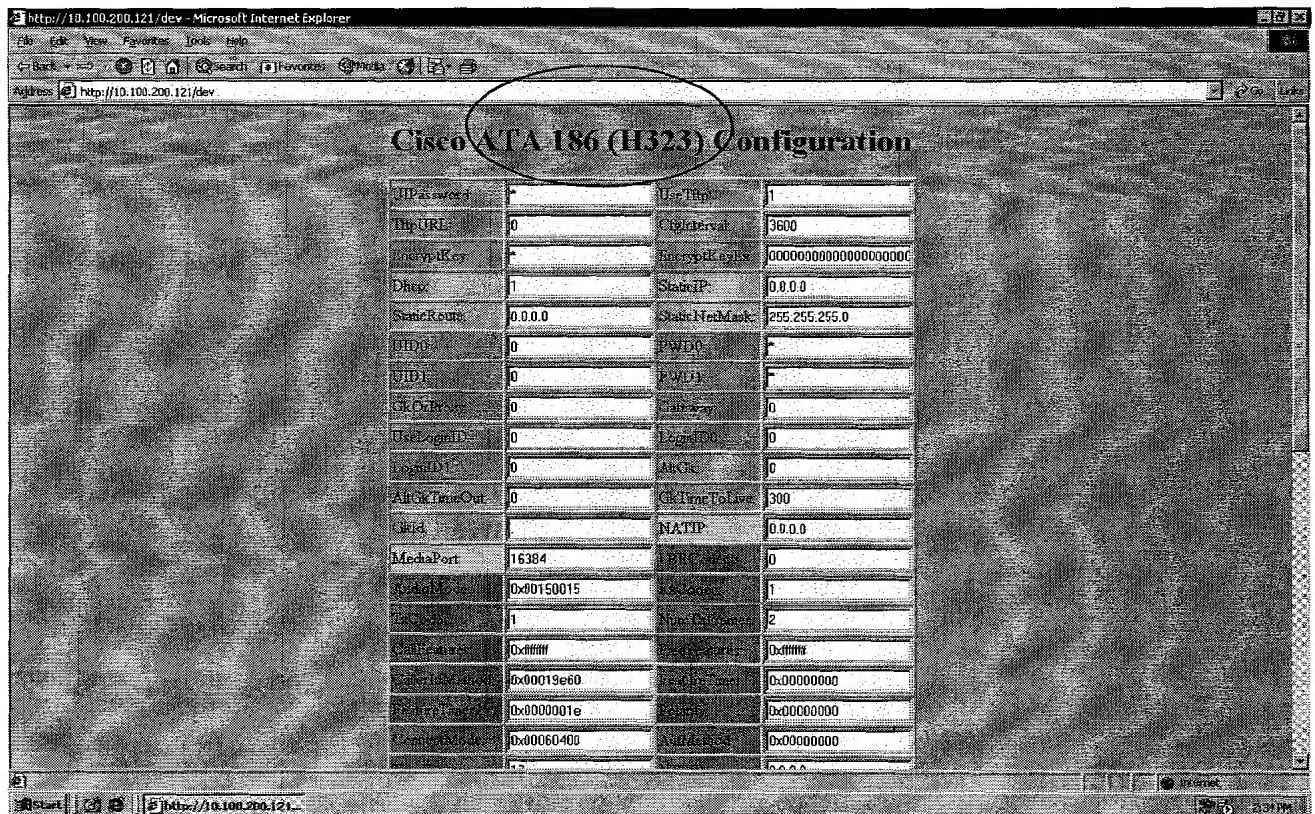
Verify firmware at the top of the ATA screen.

H323 Configuration

The ATA will be registering to the Gatekeeper as a Terminal. To achieve this, the following ATA Parameters are required.

    GKorProxy: <Gatekeeper IP Address>
    GkId   <Zone Name>
    UID0   E.164 phone number for the **Phone 1** port.

Codecs being used can be defined by setting the following ATA parameters.

RXCodec and TXCodec- Use this parameter to specify receiving-audio codec preference. The following values are valid:

- 0—G.723 (can be selected only if LBRCodec is set to 0) •   1—G.711A-law
- 2—G.711µ-law
- 3—G.729A (can be selected only if LBRCodec is set to 3)

If G711 or G729 is required then RX/TXcodec = 2 and LBRCodec=3

Fax

Most Cisco voice gateways currently support two methods to transmit fax traffic across the IP network:
- Cisco Fax Relay — In fax relay mode, the gateways terminate the T.30 fax signaling.
- Fax Pass-Through — In fax pass-through mode, the gateways do not distinguish a fax call from a voice call.

Cisco Fax Relay mode is the preferred method to transmit fax traffic. However, if a specific gateway does not support Cisco fax relay, it supports fax pass-through.

ATA Fax Passthru

ATA only supports Fax Passthru and not Fax Relay.

To enable Fax Passthru configure the following parameters:
- **AudioMode**: Audio mode bit '1' should be set to 1 to force G711. The Audiomode parameter should be '0x00160016'
- **ConnectMode** should be set to '0x00000400'

WS-6608 Fax Settings

The 6608 gateway supports both fax passthru and fax relay.

ipexpert

MGCP Fax Settings

Fax relay is on by default.

To configure Fax Passthru configure as follows:

```
no ccm-manager fax protocol
mgcp modem passthrough voip mode nse
```

H323 Fax

Fax relay is on by default, to enable Fax Passthru change the settings in the dial-peer.

```
dial-peer voice 10 voip
destination-pattern 3333
modem passthrough nse codec g711ulaw
session target ipv4:1.1.1.1
incoming called-number 2222
fax rate disable
no vad
```

ipexpert

VG248 Fax

```
------------------------------------------------------------
| Cisco VG248 (VGC10d8002407) |
----- ------------------------------------------------------
| Advanced settings |
|----------------------------------------------------------|
| Allow last good configuration (enabled) |
| SRST policy (disabled) |
| SRST provider () |
| Call preservation (enabled: no timeout) |
| Media receive timeout (disabled) |
| Busy out off hook ports (disabled) |
| DTMF tone dur ---------------------- 100ms) |
| Echo cancelli| Passthrough signalling |e: use DSP) |
| Passthrough s|----------------------|) |
| Hook flash ti| legacy | default>) |
| Hook flash re| IOS mode | |
| Fax relay max ---------------------- 14400 bps) |
| Fax relay playout delay (default: 300) |
----------------------------------------------------
----------------------------------------------------
------------------------------------------------------------
| Cisco VG248 (VGC10d8002407) |
----- ------------------------------------------------------
| Advanced settings |
|----------------------------------------------------------|
| Allow last good configuration (enabled) |
| SRST policy (disabled) |
| SRST provider () |
| Call preservation (enabled: no timeout) |
| Media receive timeout (disabled) |
| Busy out off hook ports (disabled) |
| DTMF tone duration (default: 100ms) |
| Echo cancelling policy (alternate: use DSP) |
| Passthrough signalling (IOS mode) |
| Hook flash timer (<country default>) |
| Hook flash reject period (none) |
| Fax relay maximum speed (default: 14400 bps) |
| Fax relay playout delay (default: 300) |
----------------------------------------------------
----------------------------------------------------
```

ipexpert